

**RESOURCE MATERIAL
SERIES No. 79**

UNAFEI

Fuchu, Tokyo, Japan

December 2009

Masaki Sasaki
Director

United Nations
Asia and Far East Institute
for the Prevention of Crime and
the Treatment of Offenders
(UNAFEI)

1-26 Harumi-cho, Fuchu, Tokyo 183-0057, Japan
<http://www.unafei.or.jp>
unafei@moj.go.jp

CONTENTS

INTRODUCTORY NOTE..... vii

PART ONE

WORK PRODUCT OF THE 140TH INTERNATIONAL TRAINING COURSE

“The Criminal Justice Response to Cybercrime”

Visiting Experts’ Papers

- An Introduction to Cybercrime
by *Dr. Marco Gerke (Germany)*..... 3
- Managing Large Amounts of Electronic Evidence
by *Mr. Joel Michael Schwarz and Co-Authors (USA)*..... 32
- Rethinking the Storage of Computer Evidence
by *Mr. Joel Michael Schwarz and Co-Authors (USA)*..... 42
- The Current Situation and Countermeasures to Cybercrime and Cyber-Terror
in the Republic of Korea
by *Mr. Junsik Jang (Republic of Korea)* 46
- Best Practices in Cybercrime Investigation in the Republic of Korea
by *Mr. Junsik Jang (Republic of Korea)* 57

Participants’ Papers

- The Criminal Justice Response to Cybercrime
by *Mr. Elcio Ricardo de Carvalho (Brazil)*..... 64
- Current Situation and Issues of Illegal and Harmful Activities in the Field of
Information and Communication Technology in Pakistan
by *Mr. Syed Abbas Ahsan (Pakistan)* 70
- Country Report on Cybercrime: The Philippines
by *Mr. Gilbert Caasi Sosa (Philippines)*..... 80
- The Criminal Justice Response to Cybercrime: Thailand
by *Mr. Santipatn Prommajul (Thailand)*..... 87

Reports of the Course

- Issues and Measures Concerning the Legal Framework to Combat Cybercrime
by *Group 1*..... 98
- Challenges and Best Practices in Cybercrime Investigation
by *Group 2*..... 107

PART TWO

WORK PRODUCT OF THE ELEVENTH INTERNATIONAL TRAINING COURSE ON THE CRIMINAL JUSTICE RESPONSE TO CORRUPTION

Visiting Experts' Papers

- The United Nations Convention against Corruption: Its Relevance and Challenges in Its Implementation
by *Giovanni Gallo (UNODC)* 115
- National Anti-Corruption Strategy: the Role of Government Ministries
by *Tony Kwok Man-wai (Hong Kong)* 133
- Investigation of Corruption Cases
by *Tony Kwok Man-wai (Hong Kong)* 140

Participants' Papers

- The Criminal Justice Response to Corruption – Bangladesh Perspective –
by *Ms. Jahanara Pervin (Bangladesh)* 146
- Effective Legal and Practical Measures in Combating Corruption
by *Mr. Tshering Namysel (Bhutan)* 153
- The Criminal Justice Response to Corruption (In the Context of Nepal)
by *Mr. Rajan Prasad Bhattarai (Nepal)* 160
- The Criminal Justice Response to Corruption
by *Mr. Shreelal Poudel (Nepal)* 165

PART THREE

WORK PRODUCT OF THE 141ST INTERNATIONAL SENIOR SEMINAR

“The Improvement of the Treatment of Offenders through the Enhancement of Community-Based Alternatives to Incarceration”

Visiting Experts' Papers

- Community-Based Alternatives to Incarceration in Thailand: Current Trends and Future Prospects
by *Kittipong Kittayarak (Thailand)* 173
- Community-Based Alternatives to Incarceration
by *Christine Glenn (United Kingdom)* 190

- Improving the Treatment of Offenders through the Enhancement of Community-Based Alternatives to Incarceration: The Philippine Experience
by *Ismael Juanga Herradura (Philippines)* 199
- Community-Based Alternatives in Sentencing
by *Bala Reddy (Singapore)* 220

Participants' Papers

- The Improvement of the Treatment of Offenders through the Enhancement of Community-Based Alternatives to Incarceration
by *Boitumelo Makunga (Botswana)* 235
- The Criminal Justice Response to Crime Prevention - Guyana
by *Fay Ingrid Clarke (Guyana)* 256
- Enhancing Crime Prevention through Community-Based Alternatives to Incarceration
by *Leo S. Carrillo (Philippines)* 265
- Overcrowded Prisons and Present Practices and Experiences in Relation to Community-Based Alternatives to Incarceration
by *Jagath Abeysirigunawardana (Sri Lanka)* 279
- Measures against Overcrowding in Uruguay's Jails, Prisons and Reform Centres
by *José Enrique Colman (Uruguay)* 287

Reports of the Seminar

- The Use of Community-Based Alternatives at the Pre-Trial and Trial Stages to Reduce Overcrowding in Prisons
by *Group 1* 306
- Effective Measures to Improve the Treatment of Offenders through the Enhancement of Community-Based Alternatives to Incarceration at the Post-Sentencing Stage
by *Group 2* 312

APPENDIX 321

INTRODUCTORY NOTE

It is with pride that the United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) offers to the international community the Resource Material Series No. 79.

This volume contains the work produced in the 140th International Training Course, which was conducted from 1 September to 10 October 2008; the work produced in Eleventh International Training Course on the Criminal Justice Response to Corruption, which was held from 16 October to 14 November 2008; and the work product of the 141st International Senior Seminar, which was held from 13 January to 13 February 2009. The main theme of the 140th Course was “The Criminal Justice Response to Cybercrime”, while the main theme of the 141st Senior Seminar was “The Improvement of the Treatment of Offenders through the Enhancement of Community-Based Alternatives to Incarceration”.

UNAFEI, as a regional institute of the United Nations Crime Prevention and Criminal Justice Programme Network, decided that the focus of the 140th Course would be on the subject of cybercrime in order to provide an opportunity for criminal justice personnel with responsibility for the investigation, prosecution and adjudication of cybercrime to consider the various issues for the purpose of clarifying challenges and discovering solutions suitable for their own countries.

The detrimental effects of corruption on society are many and varied. In particular, corruption by public officials seriously undermines their integrity and neutrality in performing their official duties, leading to public distrust of the government and its institutions and potentially resulting in their eventual collapse. Corruption is a problem that needs constant challenge and attention; for this reason UNAFEI holds an annual international course specifically focused on corruption control. In recognition of the harm corruption can cause, especially in developing countries, and the fact that it can transcend national borders, the General Assembly of the United Nations adopted the UN Convention against Corruption in 2003. The Convention came into force in December 2005 and requires States Parties to implement a number of measures to tackle corruption in a comprehensive way, including measures directed at prevention, criminalization, international co-operation, and asset recovery. It is hoped that all countries, including our participants' countries, will become party to this Convention and fully implement it, thereby taking a step closer to freeing the world from the grip of corruption.

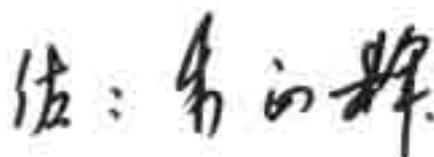
Regarding the 141st Seminar, the detention of offenders is one of the most basic measures used by criminal justice systems to secure proper legal procedures in the investigation and trial of criminal offences, and in maintaining justice and security in the community during the execution of a sentence. However, blanket detention of all offenders is inappropriate, for a number of reasons: in consideration of the humanitarian principle of avoiding restricting prisoners' rights more than is necessary; to avoid the problem of prison overcrowding; and to enhance correctional and community treatment to meet offenders' individual requirements. The United Nations has attempted to address this issue with various measures, including The United Nations Standard Minimum Rules for Non-Custodial Measures (the Tokyo Rules), “The Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-First Century”, and “The Bangkok Declaration: Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice” which have, in various different ways, guided Member States in the better treatment of offenders and the prevention of crime. However, despite the introduction of these measures and policies, the continuous increase of the prison population and subsequent overcrowding is still one of the most pressing problems in criminal justice in many countries. In view of the ongoing need for the formulation and implementation of effective community-based alternatives to incarceration, and the importance of such measures as stressed by the various UN instruments, UNAFEI, as a regional institute of the UN Crime Prevention and Criminal Justice Network, decided to hold this Seminar.

In this issue, in regard to the 140th Course and 141st Senior Seminar, papers contributed by visiting experts, selected individual presentation papers from among the participants, and the Reports of the Course and Seminar are published. In regard to the Eleventh Corruption Course, papers contributed by visiting experts and selected individual presentation papers from among the participants are published. I regret that not all the papers submitted by the Course and Seminar participants could be published.

I would like to pay tribute to the contributions of the Government of Japan, particularly the Ministry of Justice, the Japan International Cooperation Agency, and the Asia Crime Prevention Foundation for providing indispensable and unwavering support to UNAFEI's international training programmes.

Finally I would like to express my heartfelt gratitude to all who so unselfishly assisted in the publication of this series; in particular, the editor of Resource Material Series No. 79, Ms. Grace Lord.

December 2009

A handwritten signature in black ink, consisting of the Chinese characters '佐: 昌 的 祥' (Sasaki Masaki).

Masaki Sasaki
Director, UNAFEI

PART ONE
RESOURCE MATERIAL SERIES
No. 79

Work Product of the 140th International Training Course
“The Criminal Justice Response to Cybercrime”

UNAFEI

VISITING EXPERTS' PAPERS

AN INTRODUCTION TO CYBERCRIME

Marco Gercke*



I. THE IMPORTANCE OF THE ABILITY TO FIGHT CYBERCRIME

A. Development towards an Information Society

The development of the Internet and its continuing growth has a significant impact on the development of societies worldwide.¹ Developing countries as well as developed countries have started to turn into information societies.² The process is in general characterized by an emerging use of information technology to access and share information.³ It offers various opportunities that range from access to information to the ability to communicate with any user who has access to the Internet.⁴ These advantages led to an ongoing process of integrating information technology into the everyday life of people worldwide.⁵ More than a billion people are already using the Internet.⁶ Not only individuals but also businesses benefit from the emerging use of the Internet. They can offer goods and services in a global environment with very little financial investment.⁷

B. Importance of the Ability to Fight Cybercrime

The ability to effectively fight against cybercrime is an essential requirement to support the initiation and continuation of this process.⁸ Without creating the legal framework that enables law enforcement agencies to identify offenders and prosecute them, it is almost impossible to stop such cybercrime attacks. Despite the importance of technical protection measures⁹ in the prevention of cybercrime it is important to highlight, that especially in those cases, where such technology is not available, failed, or was circumvented the existence of a proper legal framework is of great importance for recreating and maintaining cyber-security.

* Professor, University of Cologne, Germany. This article is an excerpt from a publication that the author drafted for the Council of Europe. The author would like to thank the Council of Europe for the permission to use the publication as a contribution to this publication.

¹ Related to the development of the Internet, see: *Yang, Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, Page 52 – 56.

² For more information on the information society see: *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

³ World Summit on the Information Society, Document WSIS-03/GENEVA/DOC/5-E, December 2003, available at: <http://www.itu.int/wsis/docs/geneva/official/poa.html>

⁴ See for example: Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions, Challenges for the European Information Society beyond 2005, page 3 – available at: http://ec.europa.eu/information_society/eeurope/i2010/docs/communications/new_chall_en_adopted.pdf.

⁵ See *Goodman*, “The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism” in *Sofaer/Goodman*, “The Transnational Dimension of Cyber Crime and Terrorism”, 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf. Regarding the threat of attacks against computer systems integrated in cars, see: BBC News, Cars safe from computer viruses, 11.05.2005, available at: <http://news.bbc.co.uk/1/hi/technology/4536307.stm>.

⁶ According to the ITU, there were 1.14 billion Internet users by the start of 2007, available at: <http://www.itu.int/ITU-D/icteye.default.asp>.

⁷ See for example: Impact of the IT Revolution on the Economy and Finance, Report from G7 Finance Ministers to the Heads of State and Government, 2000 – available at: <http://www.mof.go.jp/english/if/if020.pdf>.

⁸ Regarding the importance of the availability of a legal framework to effectively fight Cybercrime see *Gercke*, The slow wake of a global approach against Cybercrime, CRI 2006, page 140 et seqq.

⁹ See for example US GAO, Technology Assessment, Cybersecurity for Critical Infrastructure Protection, GAO Document GAO-04-321, page 44 et seqq. – available at: <http://www.gao.gov/new.items/d04321.pdf>.

The importance of the ability to ensure that a legal framework for cybercrime investigation and prosecution exists is not limited to direct measures to identify and prosecute offenders. Creating and efficiently using such a legal framework can enhance the trust of individual users as well as businesses in the security of information technology. If users are losing trust in information technology this can negatively influence the development of e-commerce in the affected countries.¹⁰ The existence of a sufficient legal framework for the fight against cybercrime can therefore be considered one essential requirement for e-commerce.¹¹

C. Worldwide Phenomenon

The decreasing prices of communication services is one of the reasons why the above mentioned development towards an information society is not limited to the highly developed countries. Developing countries are actively participating in this process.¹² Since 2005 the number of Internet users in developing countries has surpassed the number of users in developed countries.¹³ Efforts to enhance cyber-security in those countries where important communication infrastructure (such as servers of search engines or e-mail providers) is located are an important step towards cyber-security.¹⁴ But without the protection of the growing number of users, cyber-security cannot be achieved. The user, from an offender's point of view, is often the weakest point, and needs to be included in the strategy. Phenomena like botnets,¹⁵ which are based on successful mass scale attacks against users, clearly show the importance of the ability to effectively fight against cybercrime in order to protect the users in those countries where Internet users are most numerous.

D. National Interaction and International Co-operation

The fight against cybercrime is proceeding with unique challenges.¹⁶ Two aspects that are of great importance for the success of cybercrime-related investigations are the interaction of the different organizations/institutions on the national level and international co-operation on the global level.

1. Requirements at the National Level

The investigation of cybercrime on a national level can in general only be carried out if the victim, the organizations involved in the fight against cybercrime and the businesses whose services were used are working together closely.

- A first important step is the report of an offence by the victim. Very often the victims of cybercrime do not report offences to the law enforcement agencies.¹⁷ There are two main reasons for this phenomenon. The first reason is the fact that a number of cybercrime scams are based on the principle of multiple offences with a rather small profit each instead of single offences with a high profit. If the damage caused by a single cybercrime is below a certain amount the victims will – after evaluating the time and energy required to report and offence and provide the necessary evidence

¹⁰ *Ratnasingham*, The importance of trust in electronic communication, *Internet Research*, 1998, Vol. 8, Issue 4, page 313 et. Seqq; *Meech/Marsh*, Social Factors in E-Commerce Personalization – available at: <http://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-43664.pdf>; *Shim/Van Slyke/Jiang/Johnson*, Does Trust reduce concerns for information privacy in e-commerce? – available at: <http://sais.aisnet.org/2004/.%5CShim,%20VanSlyke,%20Jiang%20&%20Johnson.pdf>.

¹¹ Regarding the importance of the availability of a legal framework to effectively fight Cybercrime see *Gercke*, The slow wake of a global approach against Cybercrime, *CRi* 2006, page 140 et seqq.

¹² UK Parliamentary Office of Science and Technology, Postnote, March 2006, No. 261, *ICT in Developing Countries*; *Nulens*, *Digital Divide in Developing Countries: An Information Society in Africa*, 2002; *Roy*, *Globalisation, ICT and Developing Nations: Challenges in the Information Age*, 2005.

¹³ See “Development Gateway’s Special Report, *Information Society – Next Steps?*”, 2005, available at: <http://topics.developmentgateway.org/special/informationssociety>.

¹⁴ Regarding the impact of the Council of Europe Convention on Cybercrime on the protection of infrastructure see *Gercke*, *National, Regional and International Legal Approaches in the Fight Against Cybercrime*, *CRi* 2008, page 9.

¹⁵ Botnets is a term for a group of compromised computers running programmes that are under external control. For more details, see *Wilson*, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, 2007, page 4 – available at: <http://www.fas.org/sgp/crs/terror/RL32114.pdf>.

¹⁶ See below, section II.

¹⁷ US GAO, *Cybercrime – Public and Private Enterties face challenges in addressing cyber threats*, GAO document: GAO-07-705 – available at: <http://www.gao.gov/new.items/d07705.pdf>; *Computer Crime & Abuse Report (India) 2001-02*, Page 8 – available at: <http://www.asianlaws.org/report0102.pdf>; *Gross*, *Investigator: Report Cybercrime*, *Info World* 2006 – available at: http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/06/08/24/HNreportcybercrime_1.html.

with the chance that the offender is identified – decide not to report the offence. But it is not only private users who very often do not report offences. In 2007 the FBI called for business in the US to more intensively report cybercrime.¹⁸ The effect of the underreporting of cybercrime was also addressed by the US Attorney General Ashcroft in 2001. He expressed the opinion that without such reports offenders will go unpunished.¹⁹ In addition, he pointed out that the fear of bad publicity²⁰ is one of the main reasons why businesses do not report successful cybercrime attacks.²¹

- The second requirement is the ability of the law enforcement agencies to carry out the investigation after an incident was reported by the victim. If they do not have access to the necessary technology, did not receive the required special training or cannot base their work on a legal framework that enables them to carry out the necessary investigations they will very likely not be able to identify the offender.²²
- In addition, efficient interaction between law enforcement agencies and the judiciary is necessary.²³ One example of the need for co-operation is the court order. In a number of countries certain investigations require a court order.²⁴ An inefficient interaction between law enforcement and the courts can delay investigations and as a consequence decrease the chances to identify and prosecute the offender.
- Finally cybercrime investigations do very often require access to certain data that is not under control of the law enforcement agencies but in the possession of private businesses such as Internet Service Providers (ISP).²⁵ Without the assistance of Internet Service Providers investigations can be very time consuming. A legal framework and related procedures that enable efficient co-operation between law enforcement agencies and Internet Service Providers can significantly increase the abilities of the law enforcement agencies to carry out investigations.²⁶

2. Requirements at the International Level

Cybercrime is a truly international phenomenon.²⁷ Due to the structure of the network an offender

¹⁸ “The US Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform the authorities, so that they can be better informed about criminal activities on the internet. “It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack,” explained Mark Mershon, acting head of the FBI’s New York office.” See Heise News, 27.10.2007, - available at: <http://www.heise-security.co.uk/news/80152>.

¹⁹ See Remarks Of Attorney General John Ashcroft at the First Annual Computer Privacy, Policy & Security Institute, 2001 – available at: <http://www.justice.gov/criminal/cybercrime/AGCPPSI.htm>.

²⁰ Bases on the Computer Crime & Abuse Report (India) 2001-02 60% of the victims did not report incidents due to fear of bad publicity. See Computer Crime & Abuse Report (India) 2001-02, Page 8 – available at: <http://www.asianlaws.org/report0102.pdf>.

²¹ Not only bad publicity, but also fear of the consequences of freedom of information legislation that could give competitors access to that information.

²² Regarding training activities in the OAS and the APEC see for example: Cybercrime Convention Committee document T-CY (2006) 6 – available at: [http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/\(T-CY%20_2006_%2006%20-%20e%20-%20US%20Activities%20to%20improve%20cybercrime%201_205\)_en.pdf](http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/(T-CY%20_2006_%2006%20-%20e%20-%20US%20Activities%20to%20improve%20cybercrime%201_205)_en.pdf); Regarding the importance of the enforcement see Broadhurst, Development in the global legal enforcement of cyber-crime, *Policing: An International Journal of Police Strategies and Management* 29, page 408-433.

²³ See: Communication from the Commission to the European Parliament, The Council and the Committee of the Regions, Towards a general policy on the fight against cyber crime, COM (2007) 267 – available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>; *De Hert/Fuster/Koops*, Fighting Cybercrime in the two Europes. The added value of the EU Framework Decision and the Council of Europe Convention, *Revue Internationale De Droit Penal*, 2006, Vol 77, page 503 et. Seqq.

²⁴ Regarding the requirement of court orders for certain investigations see the Explanatory Report to the Convention on Cybercrime, Nr. 174.

²⁵ See: *Callanan/Gercke*, Study on the Cooperation between service providers and law enforcement against cybercrime, 2008

²⁶ See in this context: Guidelines for the cooperation between law enforcement and internet service providers against cybercrime – available at: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf; Regarding the guidelines see: *Kirk*, Council of Europe, ISPs Draft Anti-Cybercrime Guide, *PC World*, 01.04.2008, available at: http://www.pcworld.com/businesscenter/article/144011/council_of_europe_isps_draft_anticybercrime_guide.html; *Gercke*, The Council of Europe Guidelines on the Cooperation of ISP and LEA, *CRI* 2008, issue 4.

²⁷ Regarding the international dimension of Cybercrime see: *Gercke*, “The Slow Wake of A Global Approach Against Cybercrime”, *CRI* 2006, 142.

can act from any place in the world and attack victims worldwide. The ability of national law enforcement agencies to investigate those crimes that have an international dimension is limited due to the principle of national sovereignty that restricts the authorization to carry out investigation in foreign territories.²⁸ International investigations therefore require co-operation of the law enforcement agencies based on the legal frameworks for international co-operation.²⁹ The related formal requirements and time needed to collaborate with foreign law enforcement agencies often hinders international investigations.³⁰

E. Co-operation between Law Enforcement Agencies and Private Businesses

An effective fight against cybercrime depends not only on the availability of a sufficient legislation – the relationship between the law enforcement agencies and private businesses (such as Internet Service Provider) is considered another essential element.³¹ As a result the Council of Europe decided in 2007 to develop a set of guidelines to improve the co-operation between law enforcement agencies and Internet Service Providers.³² The guidelines were based on a study that analyses the existing structure of co-operation.³³ During the 2008 Council of Europe Octopus Interface Conference³⁴ the guidelines were adopted.³⁵ During the meeting of the Cybercrime Committee (T-CY) the committee highlighted the importance of the new guidelines within approaches to promote co-operation.³⁶

F. Balancing Freedom of Expression and the Need for Effective Criminal Investigations

The freedom of speech³⁷ and data protection are two issues that are in the focus of the discussion about the protection of Internet users.³⁸ In addition to those measures, the prevention of cybercrime and the ability of law enforcement agencies to identify offenders and hinder them from committing further offences enhances cyber-security and thereby increases the security of the user. But in this context it is important

²⁸ National Sovereignty is a fundamental principle in International Law. See *Roth*, “State Sovereignty, International Legality, and Moral Disagreement”, 2005, page 1, available at: <http://www.law.uga.edu/intl/roth.pdf>.

²⁹ Regarding the need for international co-operation in the fight against Cybercrime, see: *Putnam/Elliott*, “International Responses to Cyber Crime”, in *Sofaer/Goodman*, “Transnational Dimension of Cyber Crime and Terrorism”, 2001, page 35 et seqq., available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, “Cyber Crime and Security – The Transnational Dimension” in *Sofaer/Goodman*, “The Transnational Dimension of Cyber Crime and Terrorism”, 2001, page 1 et seqq., available at: http://media.hoover.org/documents/0817999825_1.pdf

³⁰ See *Gercke*, “The Slow Wake of A Global Approach Against Cybercrime”, CRI 2006, 142. For examples, see *Sofaer/Goodman*, “Cyber Crime and Security – The Transnational Dimension”, in *Sofaer/Goodman*, “The Transnational Dimension of Cyber Crime and Terrorism”, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf;

³¹ See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No.3.

³² For more details see: *Gercke*, The Council of Europe Guidelines for the Cooperation between LEAs and ISP against Cybercrime, Cri 2008, issue 4.

³³ *Callanan/Gercke*, Study on the Cooperation between service providers and law enforcement against cybercrime - Toward common best-of-breed guidelines?, 2008.

³⁴ The programme of the conference is available at: [http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Interface2008/567%20IF08-m-programme3b%20Provisional%20%20\(26%20march%202008\).PDF](http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Interface2008/567%20IF08-m-programme3b%20Provisional%20%20(26%20march%202008).PDF). The conclusions of the conference is available at: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Interface2008/567_IF08-d-concl1c.pdf.

³⁵ Guidelines for the co-operation between law enforcement and internet service providers against cybercrime - available at: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf.

³⁶ The Cybercrime Convention Committee (T-CY), 3rd Consultations of the Parties to the Convention on Cybercrime (ETS No. 185), Meeting Report, 2008, No. 42 - available at: [http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/T-CY_2008\(04\)-Final_en.pdf](http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/T-CY_2008(04)-Final_en.pdf).

³⁷ Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; Regarding the importance of the principle with regard to electronic surveillance see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol 15, No. 2, 2002, page 530 et seqq; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 et. seq. – available at: <http://www.law.ucla.edu/volokh/harass/religion.pdf>; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007 – available at: <http://www.fas.org/sgp/crs/misc/95-815.pdf>.

³⁸ Regarding the fundamental rights of the users that need to be protected see for example: World Summit of the Information Society, Declaration of Principles, 2003 - http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

to highlight that some of the measures designed to increase the ability of law enforcement agencies to investigate cybercrime that are currently discussed (such as data retention obligations) raise concerns that the measures do interfere with the fundamental rights of the users.³⁹ Balancing the necessity of effective instruments for cybercrime-related investigations and the protection of fundamental rights of the user is therefore an important aspect that needs to be taken into consideration while implementing legal frameworks as well as their application within the investigation.

II. THE CHALLENGE IN FIGHTING CYBERCRIME

The Internet is still one of the fastest growing areas of technical infrastructure development.⁴⁰ Within this development, it has grown at an enormous rate since the introduction of the World Wide Web's graphical user interface in the 1990. The process of the introduction of Internet Communication Services into everyday life turns out to be so extensive that it appears to be adequate to speak about a trend towards an Information Society. For society, this development goes along with great opportunities. As examples from Eastern Europe show, the unfiltered access to information can support democracy as the flow of information is taken out of the control of state authorities. The improvement is not limited to these general developments. Law enforcement agencies benefit from the increasing power of computer systems as well. They are today able to automatically carry out investigations that were not possible in the past. An example is the automatic search for evidence on a suspect's computer. Modern forensic systems are able to carry out a hash-values-based search for child pornography pictures as well as for keywords in text documents.

But the integration of information technology is accompanied by serious threats as well. In a society where nearly all services depend on the availability of information technology, attacks against this infrastructure have great risks.⁴¹ In addition, offenders can make use of information technology to protect their criminal activities against a discovery by law enforcement agencies. If the offenders for example encrypt child pornography images stored on their computer the automatic search functions of forensic tools will not be able to identify them. The following chapter gives an overview of some of the most important challenges that law enforcement agencies face while investigating and prosecuting cybercrime cases.

A. Dependence of Society on Information Technology

The modern societies are already heavily dependent on the availability of information technology, such as Internet phone calls or e-mail communication,⁴² and the integration of the communication technology is still continuing.⁴³ This development attracts threats of attack against critical infrastructures such as electricity supply and communication infrastructure.⁴⁴ Even short interruptions of these services have the potential to cause huge financial damage to e-commerce dependant businesses.

From a cyber-security perspective this development is risky as the existing technical infrastructure shows a number of weak points, such as the monoculture of operating systems.⁴⁵ The monoculture offers a

³⁹ Regarding the concerns see for example: Memorandum of Laws Concerning the Legality of Data Retention with regard to the rights guaranteed by the European Convention on Human Rights, 2003 – available at: http://www.privacyinternational.org/countries/uk/surveillance/pi_data_retention_memo.pdf.

⁴⁰ Related to the development of the Internet see: *Yang, Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, Page 52 – 56; According to “Internet World Stats” about one billion people were using the Internet by 2006 (the statistics are available at: <http://www.internetworldstats.com/stats.htm> - March 2006).

⁴¹ Related to Cyberterrorism see: *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, Page 221 – 249.

⁴² It was currently reported that the US Department of Defence to shut down their e-mail system after a hacking attack. See: <http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996>.

⁴³ See *Goodman*, The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism - in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 69 – available at: http://media.hoover.org/documents/0817999825_69.pdf.

⁴⁴ Regarding the impact of attacks see: *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 3 – available at: http://media.hoover.org/documents/0817999825_1.pdf.

⁴⁵ An analysis by “Red Sheriff” in 2002 stated that more than 90% of the users worldwide use Microsoft's operating systems (source: www.tecchannel.de - 20.09.2002).

number of advantages to offenders as they can design their attack to be most effective by concentrating only on one target system. The successful attacks carried out by computer viruses and worms do clearly prove the danger of those attacks for countries that depend on the availability of the information infrastructure.⁴⁶

The dependence of society on information technology on the one hand side and the threats of attacks against this infrastructure should influence the development of strategies to prevent attacks. These could contain the development and promotion of technical means of protection as well as ensuring sufficient laws that enable the law enforcement agencies to effectively fight against cybercrime.

B. Number of Users

Currently more than one billion people worldwide use the Internet⁴⁷ and it is likely that this number will increase continuously in the coming years. Due to the international dimension of the network the number of possible offenders is significant. Even if only one percent of the users made use of information technology to commit criminal offences the total number of offenders would be more 10 million. The number of users and Internet websites is related to the question how to identify web pages with illegal content within billions of web pages available in the Internet. This is only one example that shows how difficult it is for investigating authorities to fight cybercrime.

C. Availability of Devices

The requirements with regard to the tools that are necessary to commit computer crimes are rather low. In order to commit a cybercrime three elements are in general necessary:

- Hardware
- Software
- Internet Access

Rather cheap computer hardware is available in most countries in the world and its power is increasing continuously.⁴⁸ Even without access to the latest generation of computer hardware offenders are able to commit serious crimes. As a matter of fact the criminals are not limited to latest versions of high priced computers but can make use of used computer technology that is less expensive.

In addition to the hardware committing an offence does in many cases require special software tools. Such tools are not only available for sale but are also offered for free download.⁴⁹ One of the examples of such tools is software that automatically scans for open ports.⁵⁰ Due to the use of mirroring techniques and peer-to-peer exchange it is nearly impossible to prevent the availability of such devices by technical means.⁵¹

⁴⁶ A demonstration for the threat of even short interruptions of Internet and computer services was the harm caused by the computer worm "Sasser". In 2004, the computer worm affected computers running vulnerable versions of Microsoft's operation System Windows. As a result of the spreading of the worm a number of offices had to stop their services. Among them the U.S. airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm; and the electronic mapping services of the British Coastguard was disabled for a few hours. See Heise News, 04.01.2005 – available at: <http://www.heise.de/newsticker/meldung/54746>; BBC News, Sasser net worm affects millions, 04.05.2004 – available at: <http://news.bbc.co.uk/1/hi/technology/3682537.stm>.

⁴⁷ According to "Internet World Stats" more than 1.15 billion people were using the Internet by 2007 (the statistics are available at: <http://www.internetworldstats.com/stats.htm>).

⁴⁸ Based on the observation by Gordon Moore the power of computers per unit cost doubles every 24 months (Moore's Law). For more information see *Moore*, Cramming more components onto integrated circuits, *Electronics*, Volume 38, Number 8, 1965 – available at: ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf; *Stokes*, Understanding Moore's Law – available at: <http://arstechnica.com/articles/paedia/cpu/moore.ars/>.

⁴⁹ Websense Security Trends Report 2004, page 11 – available at: http://www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security - Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3 – available at: <http://www.globalsecurity.org/security/library/report/gao/d03837.pdf>. *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

⁵⁰ *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 et seq. – available at: <http://www.212cafe.com/download/e-book/A.pdf>.

⁵¹ In order to prevent availability of such tools some countries criminalize the production and offer of such tools. An example of such a provision can be found in Art. 6 Convention on Cybercrime.

Finally, committing cybercrime requires access to the Internet. It is very likely that within the given opportunities the offender will focus on ways to access the Internet that do not allow the law enforcement agencies to identify him or her or at least make their investigations more difficult. Examples for such means of anonymous access are public Internet terminals and open (wireless) networks.⁵²

D. Availability of Information

As pointed out above the Internet contains millions of webpages.⁵³ One of the key elements for the success of the Internet is the possibility to find relevant information from a wide range of available sources. In this context the success of the Internet is not only influenced by the possibility to publish information but also by the existence of powerful search engines that enable the users to search millions of webpages within seconds. "Googlehacking" or "Googledorks" describe the abuse of search engines to filter through large amounts of search results for information related to computer security issues – e.g. with the intention to search for insecure password protection systems.⁵⁴ Apart from that, offenders can use the information made available by services like satellite picture providers to prepare an attack.⁵⁵ A training manual that was found during investigations against members of a terrorist group highlighted how useful the Internet can be to gather information about possible targets.⁵⁶ It was recently discovered that military units that attacked British troops in Afghanistan used satellite pictures taken from Google Earth to plan their attacks.⁵⁷

E. International Dimension

Very often data transfer processes affect more than one country.⁵⁸ This is a result of the design of the network as well as the Internet protocol that ensures that successful transmissions can be made, even if direct lines are temporarily blocked.⁵⁹ In addition, a large number of Internet services (like for example hosting services) are offered by companies that are based abroad.⁶⁰

In those cases where the offender is not based in the same country where the victim is located the

⁵² With regard to the advantages of wireless networks for the development of an IT infrastructure in developing countries see: *The Wireless Internet Opportunity for Developing Countries, 2003* – available at: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

⁵³ The Internet Systems Consortium identified nearly 490. Million Domains (not to be mixed with webpages) – See: *Internet Domain Survey, July 2007* – available at: <http://www.isc.org/index.pl?ops/ds/reports/2007-07/>; *The Internet monitoring company Netcraft reported in August 2007 that nearly 130 Million websites* – available at: http://news.netcraft.com/archives/2007/08/06/august_2007_web_server_survey.html.

⁵⁴ For more information see: *Long/Skoudis/van Eijkelenborg, Google Hacking for Penetration Testers, 2005; Dornfest/Bausch/Calishain, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.*

⁵⁵ An example is the "Terrorist Handbook" – a pdf-document that contains detailed information on how to build explosives, rockets and other weapons.

⁵⁶ "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of all information required about the enemy". The reports about the sources of the quotation varies: The British High Commissioner Paul Boateng mentions in a speech in 2007 that the quote was "contained in the Al Qaeda training manual that was recovered from a safe house in Manchester" (see: Boateng, *The role of the media in multicultural and multifaitth societies, 2007* – available at: <http://www.britishhighcommission.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1125560437610&a=KArticle&aid=1171452755624>). The US Department of Defence reported that the quote was taken from an Al Qaeda Training Manual recovered in Afghanistan (see: http://www.defenselink.mil/webmasters/policy/rumsfeld_memo_to_DOD_webmasters.html). Regarding the availability of sensitive information on websites see: *Knezo, "Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information, 2006, page 24* – available at: <http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-8704:1>.

⁵⁷ See <http://www.telegraph.co.uk>, news from 13 January 2007.

⁵⁸ Regarding the extent of transnational attacks in the most damaging cyber attacks see: *Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7* – available at: http://media.hoover.org/documents/0817999825_1.pdf.

⁵⁹ The first defined and still most important communication protocols are: TCP (Transmission Control Protocol) and the IP (Internet Protocol). For further information see: *Tanebaum, Computer Networks; Comer, Internetworking with TCP/IP – Principles, Protocols and Architecture.*

⁶⁰ See *Huebner/Bem/Bem, Computer Forensics – Past, Present And Future, No.6* – available at: http://www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf; Regarding the possibilities of network storage services see: *Clark, Storage Virtualisation Technologies for Simplifying Data Storage and Management.*

investigation requires the co-operation of law enforcement agencies in all affected countries.⁶¹ Transnational investigations without the consent of the competent authorities in the countries involved are difficult with regard to the principle of national sovereignty. This principle does in general not allow one country to carry out investigations within the territory of another country without a permission of the local authorities.⁶² Therefore the investigations need to be carried out with the support of the authorities of all countries involved. With regard to the fact that in most cases there is only a very short time gap available, in which successful investigations can take place, the application of the classic mutual legal assistance regimes turns out to add to difficulties in Cybercrime investigations as mutual legal assistance in general requires time consuming formal procedures. There are different legislative approach to speed up the investigation. One example is the G8 24/7 Network another one the provisions related to international co-operation in the Council of Europe Convention on Cybercrime.

F. Independence of Place of Action and the Presence at the Crime Site

Committing a cybercrime does in general not require the presence of the perpetrator at the place where the victim is based. This independence of place of action and the location of the victim can add difficulties in regard to cybercrime investigations. Offenders can try to avoid criminal proceedings by acting from countries with weak cybercrime legislation.⁶³ An effective fight against cybercrime does therefore require the prevention of “safe haven” that would enable the offenders to hide their activities.⁶⁴ An example of difficulties resulting from safe havens was the “Love Bug” computer worm that was first discovered in 2000.⁶⁵ The computer worm infected millions of computer systems worldwide.⁶⁶ Intensive investigations led to a suspect in the Philippines. Due to the fact that the development and spreading of malicious software was at that time not sufficiently criminalized in the Philippines, the local investigation was seriously hindered.⁶⁷

G. Resources

One of the main challenges for law enforcement agencies is the fact that a number of organized crime groups have access to a significant number of computer systems that they can use to carry out automated attacks.⁶⁸ An example of the use of a large number of computer systems to carry out an attack was the successful computer attack against government websites in Estonia.⁶⁹ Analysis of the attacks point out, that

⁶¹ Regarding the need for international co-operation in the fight against Cybercrime see: Putnam/Elliott, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 et seqq. – available at: http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et seqq. – available at: http://media.hoover.org/documents/0817999825_1.pdf

⁶² National sovereignty is a fundamental principle in International Law. See Roth, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1 – available at: <http://www.law.uga.edu/intl/roth.pdf>.

⁶³ An example are offences related to phishing. Although most sites are stored in the US (32%), China (13%), Russia (7%) and the Republic of Korea (6%) are following. Apart from the US none of them has yet signed and ratified Cybercrime specific international agreements that would enable and oblige them to effectively participate in international investigations.

⁶⁴ The issue was addressed by a number of international organizations. The UN General Assembly Resolution 55/63 points out: “States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies”. The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: “There must be no safe havens for those who abuse information technologies”.

⁶⁵ For more information see <http://en.wikipedia.org/wiki/ILOVEYOU>; regarding the effect of the worm on Critical Infrastructure Protection see: Brock, “ILOVEYOU” Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000 – available at: <http://www.gao.gov/archive/2000/ai00181t.pdf>.

⁶⁶ BBC News, Police closes in on Love Bug culprit, 06.05.2000 – available at: <http://news.bbc.co.uk/1/hi/sci/tech/738537.stm>. Regarding the technology used: <http://radsoft.net/news/roundups/luv/20000504,00.html>.

⁶⁷ See for example: CNN, Love Bug virus rains spectre of cyberterrorism, 08.05.2000, <http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html>; *Chawki*, A Critical Look at the Regulation of Cybercrime, <http://www.crime-research.org/articles/Critical/2>; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension - in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10 – available at: http://media.hoover.org/documents/0817999825_1.pdf;

⁶⁸ See “Emerging Cybersecurity Issues Threaten Federal Information Systems”, GAO, 2005 – available at: <http://www.gao.gov/new.items/d05231.pdf>.

⁶⁹ Regarding the attacks see: Lewis, Cyber Attacks Explained, 2007 – available at: http://www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf; A cyber-riot, The Economist, 10.05.2007 – available at: http://www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598; Digital Fears Emerge After Data Siege in Estonia, The New York Times, 29.05.2007 – available at: <http://www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print>.

those attacks could have been committed by thousands of computers that were part of a so called "botnet".⁷⁰ Botnets is a term characterizing a group of compromised computers running programmes that are under control of someone.⁷¹ In general the computer that became part of the botnet were previously infected with malicious software that installed a tools that enables the perpetrator to take over the control. Those botnets can for example be used to carry out a denial of service attack⁷² or operate file-sharing server.⁷³

H. Means of Anonymous Communication

The Internet offers various possibilities for an offender to hide his identity. Using public Internet terminals⁷⁴ or an anonymous remailer⁷⁵ are just two possibilities to make an identification of an offender difficult or even impossible. Another well-known way to hide identity is to use fake e-mail addresses.⁷⁶ Many e-mail services can be used without the need to go through a formal registration process where the entered data are checked. If law enforcement agencies are trying to identify an offender that is using such e-mail address they are at least not able to solely base their investigation on the subscriber information.

III. THE PHENOMENON OF CYBERCRIME AND THE LEGAL RESPONSE

The following chapter will provide an overview about some of the most serious phenomena of cybercrime and the legal response provided by the Convention on Cybercrime. Currently the Council of Europe Convention on Cybercrime⁷⁷ is, apart from the UN Resolution 55/63,⁷⁸ the only complex international legislative framework in the fight against Cybercrime. Forty five countries signed⁷⁹ and 23 countries ratified⁸⁰ the Convention on Cybercrime, as of July 2008. With regard to the fact that it was initiated by the Council of Europe, it is important to point out that the Convention is not limited to the Members of the Council of Europe.⁸¹ The Convention on Cybercrime was from the beginning of its drafting designed as an international Convention. Apart from the involvement of the non-members Canada, South-Africa, Japan and the United States, who participated as observers, further non-member states have recently been

⁷⁰ See: *Toth*, Estonia under cyber attack, http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

⁷¹ See: *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3 – available at: <http://www.cert.org/archive/pdf/Botnets.pdf>;

⁷² Regarding the use of botnets in the attacks against computer systems in Estonia see: See: *Toth*, Estonia under cyber attack, http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

⁷³ If the offender uses such botnets it is difficult to trace back and identify them as the first traces do only lead to the member of the botnets.

⁷⁴ Regarding legislative approaches to require an identification prior to the use of public terminals see Art. 7 of the Italian Decree-Law No. 144.

⁷⁵ See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999.

⁷⁶ Regarding the possibilities of tracing an offender by using the e-mail header see: Al-Zarouni, Tracing E-mail Headers, 2004 – available at: <http://scissec.scis.ecu.edu.au/publications/forensics04/Al-Zarouni.pdf>.

⁷⁷ Convention on Cybercrime, European Treaty Series - No. 18. The full text of the Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: www.coe.int.

⁷⁸ A/RES/55/63. The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf (April 2006)

⁷⁹ Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

⁸⁰ Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Norway, Romania, Slovakia, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine, United States.

⁸¹ *Article 37 – Accession to the Convention*

(1) *After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.*

(2) *In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.*

invited to accede to the Convention.⁸² The Convention contains regulations that, due to the singular status of the Convention, reflect international standards. The importance of the Convention and its relevance as a potential global model law, setting standards for cybercrime legislation cannot be measured solely by the number of signatures or ratifications. A significant number of countries have already made use of the Convention to update their national criminal law in accordance with international standards without formally acceding to the Convention. Examples are Argentina,⁸³ Pakistan,⁸⁴ Philippines,⁸⁵ Egypt,⁸⁶ Botswana⁸⁷ and Nigeria,⁸⁸ who have already drafted parts of their legislation in accordance with the Convention.

A. Illegal Access (“Hacking”)

1. Phenomenon

Ever since computer networks were developed, their ability to remotely access data on another computer systems has been abused for criminal purposes. The term “hacking” is used to describe the act of unlawfully accessing to a computer system.⁸⁹ Due to the fact that many famous computer systems, such as the those of NASA, the Pentagon, Google and the Estonian and German Government, were successfully attacked, hacking has become one of the most well known computer offences.⁹⁰ It is one of the oldest computer offences.⁹¹ The first acts of illegal access to a computer system were discovered shortly after the introduction of network technology.⁹² But in addition to its long history, the offence has a great relevance in recent times. Entering a computer system without right is very often the first act of combined acts such as phishing⁹³ and identity theft.⁹⁴ The fact, that researches recorded more than 250 million hacking incidents worldwide during the month of August 2007 underlines the relevance of the offence.⁹⁵

Within the scope of recognized offences, the perpetrators’ motivations have been wide-ranging.⁹⁶ They

⁸² Costa Rica, Mexico and the Philippines.

⁸³ Draft Code of Criminal Procedure, written by the Advisory Committee on the Reform of Criminal Procedural Legislation, set up by Decree No. 115 of the National Executive Power of 13 February 2007 (Boletín Oficial of 16 February 2007).

⁸⁴ Draft Electronic Crime Act 2006

⁸⁵ Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefor and for other Purposes, House Bill No. 3777.

⁸⁶ Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

⁸⁷ Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.

⁸⁸ Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.

⁸⁹ In the early years of IT development, the term “hacking” was used to describe the attempt to get more out of a system (software or hardware) than it was designed for. Within this context, the term “hacking” was often used to describe a constructive activity.

⁹⁰ For an overview of victims of hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotriente*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et sq.; Regarding the impact see *Biegel*, Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 et. seq.

⁹¹ See *Levy*, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005 – available at: <http://www.aic.gov.au/publications/htcb/htcb005.pdf>; *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, 2001, page 61.

⁹² With regard to the fact that most criminal law systems did not have such offences the acts could in most countries not be prosecuted until the criminal law was amended.

⁹³ The term “phishing” describes attempts to fraudulently acquire sensitive information (such as passwords) by masquerading as a trustworthy person or business (e.g. financial institution) in a seemingly official electronic communication. See the information offered by anti-phishing working group – available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing – available at: <http://www.informatics.indiana.edu/markus/papers/aci.pdf>; *Gercke*, CR 2005, 606; The term “phishing” describes an act that is carried out to make the victim disclose personal/secret information. The term “phishing” originally described the use of emails to “phish” for passwords and financial data from a sea of Internet users. The use of “ph” linked to popular hacker naming conventions. See *Gercke*, CR, 2005, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks – available at: <http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf>. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

⁹⁴ The term identity theft describes the criminal act of fraudulently obtaining and using another person’s identity. For more information see: *Gercke*, Internet-related Identity Theft, 2007 – available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf;

⁹⁵ The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported in the month of August 2007. Source: www.hackerwatch.org.

⁹⁶ They are ranging from the simple proof that technical protection measures can be circumvented, to the intention of obtaining data stored on the victimized computer.

range from political activism to purely fraudulent intentions. For the perpetrator, access to stored data via a network offers the advantage that security measures at the physical location of the “target” computer, that guard the system against physical access, do not need to be circumvented. In addition, perpetrators do not even have to be present at the crime scene.

2. Legal Response

Taking into account the above mentioned relevance of the offence it might surprise that not all countries criminalize illegal access to a computer system. One example for a country that did for a long time not criminalize illegal access to a computer system is Germany. Until 2007, such acts were intentionally not covered by the German Penal Code.⁹⁷ A prosecution was therefore only possible if the offender committed further acts such as the alteration of data.

Analysing the various national approaches to criminalizing illegal access shows a great degree of inconsistency. Some countries, such as Romania, criminalize the mere illegal access to a computer system,⁹⁸ while others limit the criminalization by requiring a circumvention of security measures, or harmful intentions, or where data was obtained, modified or damaged during the act.⁹⁹ Others do not criminalize mere access, but only subsequent offences.¹⁰⁰

The Convention on Cybercrime includes a provision on illegal access that protects the integrity of the computer systems by criminalizing unauthorized access to a computer system. The subject of protection is the integrity of computer systems.¹⁰¹

(i) *Article 2 – Illegal access*

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

The provision does not criminalize a specific method of gaining access to a computer system. To ensure that not every development of new technology requires an amendment of the legislation the provision was drafted by used terms that are neutral with regard to the technology used. The provision requires that the offender acts intentionally¹⁰² and “without right”.¹⁰³

Within the implementation of the provision the member states have various possibilities to restrict the application of the provision. They can, for example, require that security measures are circumvented or that the offender acted with a special intent to obtain computer data.

⁹⁷ See Gercke, Comparing the Convention and the current legislation in Germany, MMR 2004, 729.

⁹⁸ See for example: Art. 42 Romanian Law No. 161/2003. A country profile that lists the Cybercrime related provisions in the Romanian legislation is available on the Council of Europe website.

⁹⁹ Opponents to the criminalization of mere illegal access refer to situations where no dangers were created by mere intrusion, or where the acts of “hacking” led to the detection of loopholes and weaknesses in the security of targeted computer systems. This approach can not only be found in national legislation but was also recommended by the Council of Europe Recommendation N° (89) 9.

¹⁰⁰ An example for this is the German Criminal Code, which criminalized only the act of obtaining data (Section 202a). The provision has recently been changed. The excerpt below was in power until 2007.

Section 202a - Data Espionage

(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.

(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

¹⁰¹ Explanatory Report, No. 22.

¹⁰² Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

¹⁰³ The element “without right” is a common component in the substantive criminal law provisions of the Convention on Cybercrime.

B. Illegal Interception

1. Phenomenon

During transmission processes in a communication network data transfer processes can be intercepted. One example for such interception is the recording of communication in a wireless network. If for example an offender succeeds in intercepting the communication between a computer system and a wireless access point he can intercept all non-encrypted communication such as e-mails sent or received or websites opened. While taking into account the increasing popularity of wireless access and the wireless interconnection of communication devices (e.g. linking mobile communication devices via Bluetooth) it is important to keep an eye on the related vulnerability of the technology with regard to illegal interception.¹⁰⁴

2. Legal Response

The Convention on Cybercrime includes a provision that protects the integrity of non-public transmission by criminalizing their unauthorized interception.¹⁰⁵ By criminalizing the illegal interception the Convention aims to equate the protection of electronic transfers with the protection of voice phone conversations against illegal tapping.¹⁰⁶

(i) *Article 3 – Illegal interception*

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

The provision criminalizes the interception of non-public transmissions. It is neither applicable with regard to public transmissions nor with regard to acts of obtaining information transferred by non-technical means.¹⁰⁷ Based on the definition provided in the Explanatory Report to the Convention on Cybercrime a transmission is “non-public” if the nature of the transmission process is confidential.¹⁰⁸ It is therefore necessary to analyse the status of transmission processes. In general, individual communication (such as sending out an e-mail or downloading information from a website) can be considered non-public. Similar to the provision mentioned above, the acts must be committed intentionally and without right.

C. Data Interference

1. Phenomenon

With regard to the fact that today more and more information is stored in a digital format, the manipulation or destruction of such information can result in great damages. Unlike corporal objects, where the ability to destroy the object in general requires physical access, computer data can in some cases be destroyed without physical access to the storage devices. One example is the use of malicious software such as computer viruses. Computer viruses are software tools that are - without permission - installed on the victim’s computer in order to carry out operations such as the deletion of data.¹⁰⁹ Like illegal access, data interference can be considered a traditional computer crime. The first computer viruses appeared in

¹⁰⁴ Kang, “Wireless Network Security – Yet another hurdle in fighting Cybercrime” in Cybercrime & Security, IIA-2, page 6 et seqq.

¹⁰⁵ Like Art. 2, Art. 3 enables the signatory states to adjust the extent of the criminalization within the implementation process by requiring additional elements like “dishonest intent” or the relation to a computer system that is connected to another computer system.

¹⁰⁶ Explanatory Report No. 60.

¹⁰⁷ Within this context only interceptions made by technical means are covered by the provision - Article 3 does not cover acts of “social engineering”.

¹⁰⁸ Explanatory Report, No. 54.

¹⁰⁹ See Spafford, “The Internet Worm Program: An Analysis”, page 3; Cohen, “Computer Viruses - Theory and Experiments” – available at: <http://all.net/books/virus/index.html>. Cohen, “Computer Viruses”; Adleman, “An Abstract Theory of Computer Viruses”. Regarding the economic impact of computer viruses, see Cashell/Jackson/Jickling/Webel, “The Economic Impact of Cyber-Attacks”, page 12; Symantec “Internet Security Threat Report”, Trends for July-December 2006 – available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

the 1970s.¹¹⁰ Since then, not only the number of computer viruses but also the damage they cause has risen significantly.¹¹¹ The emerging use of networks enable the viruses to spread much quicker than in those times, where the exchange of disks was the main way of distribution. One example is the “Love Bug” computer worm that was developed by a suspect in the Philippines in 2000¹¹² and infected millions of computers worldwide.¹¹³ The increasing speed of distribution influenced the damage caused by virus attacks. In 2000 the financial loss caused by malicious software was estimated to an amount of up to 17 billion US\$.¹¹⁴

2. Legal Response

In Article 4, the Convention on Cybercrime includes a provision that protects the integrity of data against unauthorized interference.¹¹⁵ The aim of the provision is to fill the existing gap in some national penal laws and to provide computer data and computer programmes with a protection similar to those enjoyed by corporeal objects against the intentional infliction of damage.¹¹⁶

(i) *Article 4 – Data interference*

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

(2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

The provision not only criminalizes the damage and deletion of computer data, e.g. by computer virus.¹¹⁷ In addition to traditional manipulations the drafters of the Convention decided to include acts that can lead to similar damages. One example is the alteration of computer data. If a computer virus randomly changes the content of a document the damage can be comparable to a deletion of the file. Similar to the provisions mentioned above, the acts must be committed intentionally and without right.

D. System Interference

1. Phenomenon

Information technology has become an important element of business communication and operation. As pointed out previously,¹¹⁸ the integration of computer technology in the everyday life reached a level that the information societies are depending on the availability of those services. The interruption of important

¹¹⁰ One of the first computer virus was called (c)Brain and was created by Basit and Amjad Farooq Alvi. For further details, see: http://en.wikipedia.org/wiki/Computer_virus.

¹¹¹ *White/Kephart/Chess*, Computer Viruses: A Global Perspective – available at: <http://www.research.ibm.com/antivirus/SciPapers/White/VB95/vb95.distrib.html>.

¹¹² For more information, see <http://en.wikipedia.org/wiki/ILOVEYOU>; regarding the effect of the worm on Critical Information Infrastructure Protection, see: *Brock*, “ILOVEYOU” Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000, available at: <http://www.gao.gov/archive/2000/ai00181t.pdf>.

¹¹³ BBC News, “Police close in on Love Bug culprit”, 06.05.2000, available at: <http://news.bbc.co.uk/1/hi/sci/tech/738537.stm>. Regarding the technology used, see: <http://radsoft.net/news/roundups/luv/20000504,00.html>.

¹¹⁴ *Cashell/Jackson/Jickling/Webel*, “The Economic Impact of Cyber-Attacks”, page 12 – available at: http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf. The fact that the number of people using the Internet has increased since then, but that the estimated losses have decreased, shows that the number of users of networks is only one aspect that influences development.

¹¹⁵ Article 4 offers the possibility of restricting criminalization by limiting it to cases where the actions result in serious harm.

¹¹⁶ Explanatory Report, No. 60.

¹¹⁷ A computer virus is software that is able to replicate itself and infect a computer, without the permission of the user to harm the computer system. See *Spafford*, “The Internet Worm Program: An Analysis”, page 3; *Cohen*, “Computer Viruses - Theory and Experiments” – available at: <http://all.net/books/virus/index.html>. *Cohen*, “Computer Viruses”; *Adleman*, “An Abstract Theory of Computer Viruses”. Regarding the economic impact of computer viruses, see *Cashell/Jackson/Jickling/Webel*, “The Economic Impact of Cyber-Attacks”, page 12; Symantec “Internet Security Threat Report”, Trends for July-December 2006 – available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

¹¹⁸ See above: Chapter 1.

services can have a negative impact on the development of the society.¹¹⁹ If, for example, servers that are responsible for providing communication services are not available, the users have to switch to alternative means of communication. The existence of alternative means of communication is very likely an essential part of a Cyber-Security strategy of most global businesses but due to the cost of keeping redundant systems available it is not likely that they are available to the majority of Internet users.¹²⁰

Affecting the availability of services can take place in various ways. The impact of the damage to the undersea cable in 2008, which was very likely caused by anchoring ships, led to a dramatic decrease of the transmission speed in the Asian Pacific region and shows the potential of accidents.¹²¹ But in addition to accidental interruption there are various ways in which offenders can influence the availability of Internet services. One possibility is the physical termination of critical infrastructure – e.g. the physical damage of an Internet server. A way to hinder a computer system from operating without being present at the physical location of the server is the installation of a computer virus that deletes important files on the computer system.¹²² But a successful attack with a computer virus requires the circumvention of protection measures. With regard to fact that depending on the configuration of the protection system can have unique difficulties, a third possibility of interfering with the functioning of a computer system has become very popular in recent times. A number of famous web pages¹²³ became victims of so-called “Denial-of-Service (DOS) attacks”.¹²⁴ Within such attacks the offenders are targeting a computer system with more requests than the computer system can handle.¹²⁵ Even powerful systems can be affected by these attacks.

¹¹⁹ This is especially relevant with regard to the trust of the users. If due to frequent unavailability of critical services the users lose the trust in the reliability of the provider this can seriously influence its operations. Regarding the importance of trust in e-commerce see: *Ratnasingham*, The importance of trust in electronic communication, Internet Research, 1998, Vol. 8, Issue 4, page 313 et. seq; *Meech/Marsh*, Social Factors in E-Commerce Personalization – available at: <http://it-iti.nrc-cnrc.gc.ca/it-publications-iti/docs/NRC-43664.pdf>; *Shim/Van Slyke/Jiang/Johnson*, Does Trust reduce concerns for information privacy in e-commerce? – available at: <http://sais.aisnet.org/2004/.%5CShim,%20VanSlyke,%20Jiang%20&%20Johnson.pdf>.

¹²⁰ As a consequence, the fact that a business provides a redundant system for communication does not necessarily mean that the ability to communicate with its customers is not affected if the main communication system fails as the users might not have the ability to switch means of communication.

¹²¹ Regarding the underwater cable damage see for example: US Department of Homeland Security, Daily Open Source Infrastructure Report, 4 February 2008 – available at: http://www.globalsecurity.org/security/library/news/2008/02/dhs_daily_report_2008-02-04.pdf; Hamblen, A third underwater cable is cut in Middle East, Computerworld, 1 February 2008 – available at: <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9060658>; New cable cut compounds net woes, BBC News, 4 February 2008 – available at: <http://news.bbc.co.uk/2/hi/technology/7222536.stm>.

¹²² A computer virus is software that is able to replicate itself and infect a computer, without the permission of the user to harm the computer system. See *Spafford*, “The Internet Worm Program: An Analysis”, page 3; *Cohen*, “Computer Viruses - Theory and Experiments” – available at: <http://all.net/books/virus/index.html>. *Cohen*, “Computer Viruses”; *Adleman*, “An Abstract Theory of Computer Viruses”. Regarding the economic impact of computer viruses, see *Cashell/Jackson/Jickling/Webel*, “The Economic Impact of Cyber-Attacks”, page 12; Symantec “Internet Security Threat Report”, Trends for July-December 2006 – available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

¹²³ *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 et. seq; *Lemos*, Web attacks: FBI launches probe, ZDNet News, 09.02.2000 – available at: http://news.zdnet.com/2100-9595_22-501926.html;

¹²⁴ In 2004 the web-services of the German Airline Lufthansa was affected by such a DOS-attack. As a result the use of the online booking-service was not or only with delay available for the period of 2 hours.

¹²⁵ A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, “Understanding Denial-of-Service Attacks”, available at: <http://www.us-cert.gov/cas/tips/ST04-015.html>; *Paxson*, “An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks”, available at: <http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html>; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, “Analysis of a Denial of Service Attack on TCP”; *Houle/Weaver*, “Trends in Denial of Service Attack Technology”, 2001, available at: http://www.cert.org/archive/pdf/DoS_trends.pdf. In 2000 a number of well known US e-commerce businesses were targeted by denial of service attacks. A full list of the attacks business is provided by *Yurcik*, “Information Warfare Survivability: Is the Best Defense a Good Offence?”, page 4, available at: <http://www.projects.ncassr.org/hackback/ethics00.pdf>. For more information see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 et. seq; *Lemos*, Web attacks: FBI launches probe, ZDNet News, 09.02.2000 – available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20 – available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, “Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and

2. Legal Response

In order to protect the interest of operators and users to have appropriate access to telecommunication technology the Convention on Cybercrime includes in Article 5 a provision that criminalizes the intentional hindering of the lawful use of computer systems.

(i) *Article 5 – System interference*

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

The provision does not criminalize specific acts that lead to system interference but covers any activity that interferes with the proper functioning of the computer system.¹²⁶ This covers physical termination of a server as well as computer viruses or a DoS attack. The fact that the provision limits the criminalization to serious attacks enables the signatory states to the Convention to limit the criminalization to attacks against important services or attacks that caused significant damage.¹²⁷ The act must be committed intentionally and without right.

E. **Misuse of Devices**

1. Phenomenon

A serious issue concerning cybercrime is the availability of software and hardware tools designed to commit crimes. Most of these devices are available on a large scale, the majority distributed for free. They are easy to operate and can therefore even be run by users without any specific technical knowledge. Such software can be used for the interception of wireless communication or the identification of open wireless networks (“Wardriving¹²⁸”), the decryption of encrypted files or to run Denial of Service (DOS)¹²⁹ attacks. With regard to the fact, that the commission of these offences often requires the possession of tools, there is a strong incentive to acquire them for criminal purposes, which could lead to the creation of a kind of black market for their production and distribution. Apart from the proliferation of “hacking devices”, the exchange of passwords that enable the unauthorized user to access a computer system is taking place on a large scale.

2. Legal Response

Facing this development, the drafters of the Convention decided to establish an independent offence criminalizing specific illegal acts regarding certain devices or access to data that can be misused for the purposes of committing offences against the confidentiality, integrity and availability of computer systems or data.¹³⁰

(i) *Article 6 – Misuse of Devices*

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

Implications for the Department of Homeland Security”, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3 – available at: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

¹²⁶ Explanatory Report, No. 66.

¹²⁷ Although the connotation of “serious” does limit the applicability, it is likely that even serious delays of operations resulting from attacks against a computer system can be covered by the provision.

¹²⁸ Wardriving is a term used to characterize the search for wireless networks (WLAN / Wi-Fi) by moving vehicles. As long as the search for wireless networks does not go along with the misuse of the networks the legality of this action is in most countries not clearly defined. Regarding the situation in Germany see Baer, Wardriver, MMR 2005, 434.

¹²⁹ A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, “Understanding Denial-of-Service Attacks”, available at: <http://www.us-cert.gov/cas/tips/ST04-015.html>; Paxson, “An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks”, available at: <http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html>;

¹³⁰ Due to the controversial discussion on the need for criminalization of the possession of the devices, the Convention is – in addition to Paragraph 1 b) Sentence 2 - offering the option of a complex reservation in Article 6 Paragraph 3. If a Party makes use of this reservation it can exclude the criminalization for the possession of tools and a number of illegal actions under Paragraph 1) a) – e.g. the production of such devices.

(a) the production, sale, procurement for use, import, distribution or otherwise making available of:

- (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
- (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

(b) the possession of an item referred to in paragraphs a) i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

(2) This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system.

(3) Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

The threat of these devices makes it difficult to focus the criminalization on the use of these tools to commit crimes only. Most of the national criminal law systems do, in addition to the “attempt of an offence”, have some provision criminalizing acts of preparation of crimes. In general this criminalization – which goes along with an extensive forward displacement of criminal liability – is limited to the most serious crimes. Especially in EU legislation, there are tendencies to extend the criminalization to preparatory acts to less grave offences.¹³¹

The connection factor of criminalization as established by Paragraph 1 (a) are on the one hand devices¹³² designed to commit cybercrimes and on the other hand passwords that enable access to a computer system. With regard to these items, the Convention criminalizes a wide range of actions. In addition to production, it sanctions the sale, procurement for use, import, distribution or otherwise making available of the devices and passwords. A similar approach (but limited to devices designed to circumvent technical measures) can be found in EU legislation regarding the harmonization of copyrights.¹³³

F. Computer-Related Forgery

1. Phenomenon

Due to the shift from classic tangible documents to electronic documents the forgery of computer-related data is playing an increasing role. The offence has especially become very popular with regard to “phishing”

¹³¹ An example is the EU Framework Decision ABl. EG Nr. L 149, 2.6.2001.

¹³² With its definition of “distributing” in the Explanatory Report (‘Distribution’ refers to the active act of forwarding data to others – Explanatory Report No. 72) the drafters of the Convention indicate a restriction of devices to software. Although the Explanatory Report is not certain in this matter it is likely that not only software devices are covered by the provision but hardware tools as well.

¹³³ Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society:

Article 6 – Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

- (a) are promoted, advertised or marketed for the purpose of circumvention of, or
- (b) have only a limited commercially significant purpose or use other than to circumvent, or
- (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

attacks.¹³⁴ The term “phishing” is used to describe a type of crime that is characterized by attempts to fraudulently acquire sensitive information, such as passwords, by masquerading as a trustworthy person or business (e.g. financial institution) in an apparently official electronic communication.¹³⁵ Most of these phishing attempts are operated via e-mail. The person receiving such e-mail is for example ordered to verify his online bank account (“Click here to verify your account”) and by entering his or her account number and password on a webpage that was set up by the offenders, the offenders get access to the data.

2. Legal Response

The criminalization of the forgery of tangible items has a long legal tradition in most countries.¹³⁶ The Convention aims to create a parallel offence to the forgery of tangible documents in order to fill gaps in criminal law related to traditional forgery, which require visual readability of statements or declarations embodied in a document and therefore do not apply to electronically stored data.¹³⁷

(i) *Article 7 – Computer-Related forgery*

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

The target of a computer-related forgery is only data – not depending on whether they are directly readable and intelligible. To draw the line on the forgery of tangible documents Article 7 requires – at least with regard to the mental element - that the data is the equivalent of a public or private document. This includes the need for legal relevance. The forgery of data that cannot be used for legal purposes is therefore not covered by the provision.

¹³⁴ See for example: *Austria*, Forgery in Cyberspace: The Spoofer could be on you, University of Pittsburgh School of Law, Journal of Technology Law and Policy, Vol. IV, 2004 – available at: <http://tlp.law.pitt.edu/articles/Vol5-Austria.pdf>.

¹³⁵ Regarding the phenomenon of phishing, see. *Dhamija/Tygar/Hearst*, “Why Phishing Works”, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; “Report on Phishing”, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006, available at: http://www.usdoj.gov/opa/report_on_phishing.pdf

¹³⁶ See for example 18 U.S.C. § 495:

Whoever falsely makes, alters, forges, or counterfeits any deed, power of attorney, order, certificate, receipt, contract, or other writing, for the purpose of obtaining or receiving, or of enabling any other person, either directly or indirectly, to obtain or receive from the United States or any officers or agents thereof, any sum of money; or Whoever utters or publishes as true any such false, forged, altered, or counterfeited writing, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited; or

Whoever transmits to, or presents at any office or officer of the United States, any such writing in support of, or in relation to, any account or claim, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited – Shall be fined under this title or imprisoned not more than ten years, or both.

A similar approach can be found in Sec. 267 German Penal Code:

Section 267 Falsification of Documents

(1) Whoever, for the purpose of deception in legal relations, produces a counterfeit document, falsifies a genuine document or uses a counterfeit or a falsified document, shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

(3) In especially serious cases the punishment shall be imprisonment from six months to ten years. An especially serious cases exists, as a rule, if the perpetrator:

1. acts professionally or as a member of a gang which has combined for the continued commission of fraud or falsification of documents;

2. causes an asset loss of great magnitude;

3. substantially endangers the security of legal relations through a large number of counterfeit or falsified documents; or

4. abuses his powers or his position as a public official.

(4) Whoever commits the falsification of documents professionally as a member of a gang which has combined for the continued commission of crimes under Sections 263 to 264 or 267 to 269, shall be punished with imprisonment from one year to ten years, in less serious cases with imprisonment from six months to five years.

¹³⁷ Explanatory Report, No. 81.

G. Computer-Related Fraud

1. Phenomenon

Fraud remains one of the most popular crimes in cyberspace. Especially the success of online shopping and Internet auctions increased the opportunities of offenders. The most popular crimes are credit card fraud and auction fraud.¹³⁸ Apart from that, the development of assets administered in computer systems (electronic funds, deposit money, e-gold) has become the target of manipulations. To avoid these criminal acts, especially with regard to Internet auctions, a number of confidence-building measures have been taken on the technical side.¹³⁹ But the missing personal contact between the seller and customer limits the possibilities of self-protection.

As fraud is a common problem outside the Internet as well, most national laws contain provisions criminalizing such offences. The application of those provisions to Internet-related cases can be difficult if the traditional national criminal law provisions relate to a falsity of a person.¹⁴⁰ In many cases of fraud committed on the Internet the offender is manipulating a computer system. If the traditional provisions that criminalize fraud do not apply to computer-systems an update of the national law is necessary.

2. Legal Response

The Convention is aiming to criminalize any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property by providing an Article regarding computer-related fraud.¹⁴¹

(i) Article 8 – Computer-Related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

- a. any input, alteration, deletion or suppression of computer data;*
- b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.*

Article 8 combines the most relevant acts with regard to computer-related fraud (input, alteration, deletion and suppression) with the general act “interference with the functioning of a computer system” in order to open the provision for further developments.¹⁴²

In most national criminal law systems the fraud must lead to an economic loss. In addition to a general intent with regard to the elements of crime (especially the manipulation) Art. 8 therefore requires a special fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another. As an example of acts excluded from criminal liability because of a missing special intent the Explanatory Report mentions commercial practices with respect to market competition that may cause an economic detriment to a person and a benefit to another, but are not carried out with fraudulent or dishonest intent.¹⁴³

¹³⁸ “Law Enforcement Efforts to combat Internet Auction Fraud”, Federal Trade Commission, 2000, page 1, available at: <http://www.ftc.gov/bcp/reports/int-auction.pdf>; *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 7 – available at: <http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf>.

¹³⁹ An example for this is the service offered by PAYPAL: PAYPAL is an internet business that enables the user to transfer money, avoiding traditional paper methods such as money orders. It also performs payment processing for auction sites.

¹⁴⁰ An example of this is Section 263 of the German Penal Code that requires the falsity of a person (mistake). The provision does therefore not cover the majority of computer-related fraud cases:

Section 263 Fraud

(1) Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another, by provoking or affirming a mistake by pretending that false facts exist or by distorting or suppressing true facts, shall be punished with imprisonment for not more than five years or a fine.

¹⁴¹ Explanatory Report, No. 86.

¹⁴² As a result not only data related offences but also hardware manipulations are covered by the provision.

¹⁴³ The drafters of the Convention point out that these acts are not meant to be included in the offence established by Article 8. Explanatory Report, No. 90.

H. Child Pornography

1. Phenomenon

During the last years the Internet has become the primary instrument for trading child pornography.¹⁴⁴ There are two main reasons for this development:

- The Internet offers unique possibilities with regard to the dissemination of content. By making a file available in a file-sharing system it can be downloaded by millions of users worldwide. This increases the number of potential consumers compared to traditional ways of distribution.
- A second reason for the success of web pages with pornographic material is the fact that users are considering themselves to be less “visible” while gaining access to the material online compared to accessing a regular shop. This is an advantage for investigation as most users do not even know about the traces they leave while surfing in the Internet.¹⁴⁵

2. Legal Response

In order to improve the protection of children against sexual exploitation by modernizing criminal law provisions, the Convention provides an Article dealing with child pornography.

(i) Article 9 – Offences related to child pornography

(1) *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:*

- a) producing child pornography for the purpose of its distribution through a computer system;*
- b) offering or making available child pornography through a computer system;*
- c) distributing or transmitting child pornography through a computer system;*
- d) procuring child pornography through a computer system for oneself or for another person;*
- e) possessing child pornography in a computer system or on a computer-data storage medium.*

(2) *For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:*

- a) a minor engaged in sexually explicit conduct;*
- b) a person appearing to be a minor engaged in sexually explicit conduct;*
- c) realistic images representing a minor engaged in sexually explicit conduct.*

(3) *For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.*

(4) *Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.*

It is important to point out two controversial discussed elements of the offence established by Article 9: The criminalization of the possession of child pornography and the integration of fictional images.

Within its approach to improve the protection of minors against sexual exploitation the Council of Europe introduced a new Convention in 2007.¹⁴⁶ On the first day the Convention was opened for signature 23 states signed the Convention.¹⁴⁷ One of the key aims of the Convention is the harmonization of criminal

¹⁴⁴ Krone, A Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279.

¹⁴⁵ Regarding the possibilities to trace back offenders of computer-related crimes see: Lipson, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

¹⁴⁶ Council of Europe - Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

¹⁴⁷ Austria, Belgium, Bulgaria, Croatia, Cyprus, Finland, France, Germany, Greece, Ireland, Lithuania, Moldova, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovenia, Sweden, the Former Yugoslav Republic of Macedonia, and Turkey. Denmark, Iceland, Italy, Ukraine and the United Kingdom followed (July 2008).

law provisions that aim to protect children from sexual exploitation.¹⁴⁸ To achieve this aim the Convention contains a set of criminal law provisions. Apart from the criminalization of the sexual abuse of children (Art. 18) the Convention contains provisions dealing with the exchange of child pornography (Art. 20) and the solicitation of children for sexual purposes (Art. 23).

(ii) Article 20 – Offences concerning child pornography

(1) Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalized:

- a) producing child pornography;*
- b) offering or making available child pornography;*
- c) distributing or transmitting child pornography;*
- d) procuring child pornography for oneself or for another person;*
- e) possessing child pornography;*
- f) knowingly obtaining access, through information and communication technologies, to child pornography.*

(2) For the purpose of the present article, the term “child pornography” shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes.

(3) Each Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material: – consisting exclusively of simulated representations or realistic images of a non-existent child; – involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use.

(4) Each Party may reserve the right not to apply, in whole or in part, paragraph 1.f.

(iii) Article 23 – Solicitation of children for sexual purposes

Each Party shall take the necessary legislative or other measures to criminalize the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a, or Article 20, paragraph 1.a, against him or her, where this proposal has been followed by material acts leading to such a meeting.

Art. 20 of the Convention on the protection of children is to a large degree comparable to Art. 9 of the Convention on Cybercrime. The first main difference is the fact that the Convention on Cybercrime focuses on the criminalization of acts related to information and communication services (“producing child pornography for the purpose of its distribution through a computer system”) while the Convention on the Protection of Children follows a broader approach (“producing child pornography”) and even covers acts that are not related to computer networks. In addition Art. 20 (1) f) of the Convention on the Protection of Children criminalizes the act of obtaining access to child pornography.¹⁴⁹ The Convention on Cybercrime does not contain such a provision.

Art. 23 Convention on the protection of children criminalizes the solicitation of children for sexual purposes by means of information and communication technology. The Convention on Cybercrime does not contain such a provision.

I. Copyright Crimes

1. Phenomenon

The switch from analogue to a digital distribution of music and videos led to new forms of copyright

¹⁴⁸ For more details see Gercke, ZUM 2008, 550ff.

¹⁴⁹ The provision is especially relevant in those cases where the offender is accessing information in a computer network without downloading it. In those cases the access to the information is – depending on the configuration of the computer system and the services used - not in accordance with a possession of the information.

violations. Millions of copyright protected songs and movies are exchanged in file-sharing systems every day.¹⁵⁰ Some movies even appeared in file-sharing systems before their world premiere in cinema.¹⁵¹

The entertainment industry responded by implementing technical measures (DRM) to prevent reproduction,¹⁵² but until now these measures have always been circumvented shortly after their introduction. A number of software tools are available that enable the user to copy music CD's and movie DVD's that are protected by DRM-systems. In addition, the Internet offers the possibility to distribute the copies worldwide. As a result, the infringements of intellectual property rights are among the most commonly committed offences on the Internet.

2. Legal Response

The Convention contains a provision that aims to harmonize the various approaches to criminalize copyright violations in the national laws of the signatory states.

Article 10 – Offences related to infringements of copyright and related rights

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

(2) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

(3) A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

One of the main differences between Art. 10 Convention on Cybercrime and most national approaches is the fact that Art. 10 does not explicitly name those acts that are supposed to be criminalized, but refers to a number of international agreements – such as the WIPO Copyright treaty. This led to criticism from those countries that are not members of WIPO.¹⁵³

The criminalization¹⁵⁴ of copyright crimes established by Art. 10 Convention on Cybercrime is limited to serious cases and therefore excludes minor violations of copyrights.¹⁵⁵ In addition the Convention does only cover

¹⁵⁰ The latest analysis regarding file-sharing activities in Germany identify up to 7.3 million users who download music files from the Internet. Up to 80% of these downloads are related to file-sharing systems. Source: GfK, Brennerstudie 2005.

¹⁵¹ An example is the movie “Star Wars – Episode 3”, that appeared in file-sharing systems hours before the official premiere. See: <http://www.heise.de/newsticker/meldung/59762> that is taking regard to a MPAA press release.

¹⁵² The technology that is used is called Digital Rights Management – DRM. The term Digital rights management (DRM) is used to describe several technologies used to enforce pre-defined policies controlling access to software, music, movies, or other digital data. One of the key functions is the copy protection that aims to control or restrict the use and access to digital media content on electronic devices with such technologies installed.

¹⁵³ In this context it is important to highlight that the signature of the Convention does not oblige the states to become members of the WIPO. It is sufficient to implement criminalization for those violations mentioned in Art. 10 Convention on Cybercrime.

¹⁵⁴ Paragraph 3 enables the parties to make a reservation and not criminalize copyright violations as long as they provide that other effective remedies are available and the reservation does not derogate from the parties' international obligations.

¹⁵⁵ The Convention is designed to set minimum standards for Internet-related offences. Therefore parties can go beyond the threshold of “commercial scale” in the criminalization of copyright violations.

acts that are committed by the means of a computer system. Copyright violations that do not involve information technology are not covered by the provision. Another major limitation of the criminalization is granted by the requirement of a violation on a commercial scale. A similar restriction is contained in the TRIPS Agreement, which requires criminal sanctions only in the case of “piracy on a commercial scale”. As most of the copyright violations in file-sharing systems are not committed on a commercial scale they are not covered by Article 10.

IV. PROCEDURAL INSTRUMENTS CONTAINED IN THE CONVENTION ON CYBERCRIME

As pointed out previously, cybercrime investigations involve a number of unique challenges, such as the high speed of data exchange processes. To be able to react to the challenges, law enforcement agencies need procedural instruments that enable them to take those measures that are necessary to identify the offender and collect the evidence required for criminal proceedings.¹⁵⁶ With regard to the special challenges related to cybercrime investigation the traditional investigation instruments, such as search and seizure, will not be sufficient to carry out successful investigations. The Convention on Cybercrime therefore contains a set of special instruments.

A. Expedited Preservation of Data

1. The Situation

The identification of a cybercrime offender very often requires the analysis of traffic data.¹⁵⁷ In particular, the IP address used by the offender while committing the offence is an important information that can help to trace him or her back. One of the main challenges for investigation is the fact that traffic data that are relevant for the identification are often deleted automatically within a rather short period of time.¹⁵⁸ Some countries have strict laws that prohibit the storage of certain traffic data after the end of a process. One example for such restriction is Art. 6 EU Directive on Privacy and Electronic Communication.¹⁵⁹

2. The Related Procedural Instrument

Art. 16 Convention on Cybercrime enables the law enforcement agencies to order the preservation of traffic as well as content data (“quick freeze”).

Article 16 – Expedited preservation of stored computer data

(1) Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

(2) Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified

¹⁵⁶ Regarding user-based approaches in the fight against Cybercrime see: *Goerling*, The Myth Of User Education, 2006 - www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See as well the comment made by *Jean-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: “More broadly, we have to educate users. They must all understand what they can and can’t do on the Internet and be warned of the potential dangers. As use of the Internet grows, we’ll naturally have to step up our efforts in this respect.”

¹⁵⁷ “Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required”, See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 155.; Regarding the identification of suspects by IP-based investigations see: *Gercke*, Preservation of User Data, DUD 2002, 577 et. seq.

¹⁵⁸ The reason for this automated deletion process is the fact that after the end of a process (e.g. sending out an e-mail, accessing the Internet or downloading a movie) those traffic data that have been generated during the process and that ensure that the process could be carried out are not anymore needed and the storage of the data would increase the cost of operating the service. The cost issue was especially raised within the discussion about data retention legislation in the EU. See for example: E-communications service providers remain seriously concerned with the agreement reached by EU Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005 – available at: <http://www.ispai.ie/EUROISPADR.pdf>; See as well: ABA International Guide to Combating Cybercrime, page 59.

¹⁵⁹ Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/1_20120020731en00370047.pdf.

stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

(4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

This instrument should enable the law enforcement agencies to react immediately after becoming aware of an offence and avoid the risk of a deletion as a result of long lasting procedures.¹⁶⁰ After receiving such order the providers are obliged to preserve those data that were processed during the operation of the service.¹⁶¹ Art. 16 does not include an obligation of an Internet Service Provider to transfer the relevant data to the authorities. The transfer obligation is regulated in Art. 17 and 18 Convention on Cybercrime.

In this context it is important to highlight that Art. 16 does not contain a data retention obligation. A data retention obligation forces the provider of Internet services to save all traffic data for a certain period of time.¹⁶² This would enable the authorized agencies to gain access to data that is necessary to identify an offender even month after the perpetration.¹⁶³ A data retention obligation was recently adopted by the EU Parliament¹⁶⁴ and is currently discussed in the US.¹⁶⁵

B. Production Order

1. The Situation

As mentioned above Art. 16 does only oblige the provider to save those data that were processed by the provider and not deleted at the time the provider receives the order.¹⁶⁶ The provision does not oblige the provider to transfer the relevant data to the authorities.

2. The Related Procedural Instrument

The transfer obligation is regulated in Art. 18 Convention on Cybercrime.

Article 18 – Production order

(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its

¹⁶⁰ However, it is recommended that States consider the establishment of powers and procedures to actually order the recipient of the order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases. Explanatory Report to the Convention on Cybercrime, No. 160.

¹⁶¹ 'Preservation' requires that data, which already exists in a stored form, be protected from anything that would cause its current quality or condition to change or deteriorate. Explanatory Report to the Convention on Cybercrime, No. 159.

¹⁶² Regarding The Data Retention Directive in the EU see *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, *Chicago Journal of International Law*, 2007, Vol. 8, No.1 – available at: [http://eprints.law.duke.edu/archive/00001602/01/8_Chi_J._Int'l_L._233_\(2007\).pdf](http://eprints.law.duke.edu/archive/00001602/01/8_Chi_J._Int'l_L._233_(2007).pdf); *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, *European Law Journal*, 2005, page 365 et. seqq.

¹⁶³ See: Preface 11. of the EU Data Retention Directive: "Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive."

¹⁶⁴ Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

¹⁶⁵ See for example: Draft Bill to amend title 18, United States Code, to protect youth from exploitation by adults using the Internet, and for other purposes - Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act (SAFETY) of 2007 – available at: <http://www.govtrack.us/congress/bill.xpd?bill=h110-837>. Regarding the current situation in the US see: ABA International Guide to Combating Cybercrime, page 59.

¹⁶⁶ 'Preservation' requires that data, which already exists in a stored form, be protected from anything that would cause its current quality or condition to change or deteriorate. Explanatory Report to the Convention on Cybercrime, No. 159.

competent authorities to order:

- a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
- b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

(2) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

(3) For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

- a) the type of communication service used, the technical provisions taken thereto and the period of service;
- b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
- c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Art. 18 of the Convention on Cybercrime is not only applicable after a preservation order is issued: the provision is a general instrument that law enforcement agencies can make use of. If the Internet Service Providers are voluntarily transferring the requested data law enforcement agencies are not limited to seizing hardware but can make use of the less intensive production order.

C. Partial Disclosure of Traffic Data

1. The Situation

As pointed out previously, the Convention strictly divides between the obligation to preserve data on request and the obligation to disclose them to the competent authorities.¹⁶⁷

2. The Related Procedural Instrument

Art. 17 combines the obligation to ensure the preservation of traffic data in cases where a number of service providers were involved with the additional obligation to disclose the necessary information in order to enable the LEAs to identify the path through.

Article 17 – Expedited preservation and partial disclosure of traffic data

(1) Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

- a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
- b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

(2) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Without such partial disclosure law enforcement agencies would in some cases not be able to trace back the offender and preserve more relevant data when more than one provider was involved in a data exchange process.¹⁶⁸

¹⁶⁷ Gercke, The Convention on Cybercrime, MMR 2004, 802.

¹⁶⁸ "Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination." See Explanatory Report to the Convention on Cybercrime, No. 167.

D. Submission of Subscriber Information

1. The Situation

The main aim of most cybercrime investigations is the identification of the suspects involved in committing the offences. Therefore the individualization of the suspect is a major aim of the procedural instruments. Such identification can be achieved with the help of subscriber information. The use of many Internet services, such as the access to the Internet or the rental of server storage require registration. The subscriber information submitted during the registration process can enable the individualization process.

2. The Related Procedural Instrument

In addition to the obligation to submit computer data, Art. 18 CoC enables law enforcement agencies to order the submission of subscriber information.

Article 18 – Production order

(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

- a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and*
- b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.*

(2) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

(3) For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

- a) the type of communication service used, the technical provisions taken thereto and the period of service;*
- b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;*
- c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.*

This investigation instrument is of great importance in IP-based investigations. If the law enforcement agencies are able to identify an IP-address that was used by the offender while carrying out the offence they will need to identify the person¹⁶⁹ who used the IP-address at the time of the offence. Based on Art. 18 Subsection 1 b) Convention on Cybercrime a provider is obliged to submit those subscriber information listed in Art. 18 Subsection 3 Convention on Cybercrime.

E. Search

1. The Situation

Search and seizure is one of the most important instruments in cybercrime investigation.¹⁷⁰ Search and seizure of tangible objects is a traditional investigation instrument in most criminal procedural codes.¹⁷¹ The reason why the drafters of the Convention on Cybercrime nevertheless included a provision dealing with search and seizure is the fact that national laws often do not cover data-related search and seizure

¹⁶⁹ An IP-address does not necessarily immediately identify the offender. If law enforcement agencies know the IP-address an offender used to commit an offence this information only enables them to identify the connection used to log on to the Internet. If a group of people had access to this connection (e.g. in an Internet café) further investigations are necessary to identify the offender.

¹⁷⁰ A detailed overview about the elements of search procedures is provided by the ABA International Guide to Combating Cybercrime, 123 et. seqq. For more information on Computer-related Search and Seizure see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 et seqq.; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 et seqq.

¹⁷¹ See Explanatory Report to the Convention on Cybercrime, No. 184.

procedures.¹⁷² Based on such provision the investigators would be able to seize an entire server but not seize only the relevant data by copying them.¹⁷³

2. The Related Procedural Instrument

(i) Article 19 – Search and seizure of stored computer data

(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

- a. a computer system or part of it and computer data stored therein; and*
- b. a computer-data storage medium in which computer data may be stored in its territory.*

(2) Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

[...]

Art. 19 sub-paragraph 1 of the Convention on Cybercrime aims to establish an instrument that enables investigators to search computer systems as efficiently as they are able to perform traditional search procedures.¹⁷⁴ Art. 19 sub-paragraph 2 of the Convention on Cybercrime addresses a growing problem within cybercrime related investigations. During the search for information at the physical location of a computer system investigators frequently realize that the suspect did not store the relevant information (e.g. child pornography) on local hard drive but on an external server which he can access via Internet.¹⁷⁵ Using Internet servers to store data is becoming more and more popular.¹⁷⁶ To ensure that investigations can be carried out efficiently it is important to maintain a certain flexibility of investigations. If the investigators discover that the relevant information is stored in another computer system they should be able to extend the search to this system.¹⁷⁷

F. Seizure

1. The Situation

The examination of computer systems and especially internal and external storage devices is an

¹⁷² “However, in a number of jurisdictions stored computer data *per se* will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data.” Explanatory Report to the Convention on Cybercrime, No. 184.

¹⁷³ This can cause difficulties in those cases where the relevant information are stored on a server with the data of hundreds of other users that would not be available anymore when law enforcement agencies seize the server.

¹⁷⁴ “However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record.” Explanatory Report to the Convention on Cybercrime, No. 187.

¹⁷⁵ The importance of being able to extend the search to connected computer systems was already addressed by the Council of Europe Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology that was adopted by the Committee of Ministers on 11.09.1995 at the 543rd meeting of the Ministers Deputies. The text of the Recommendation is available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf

¹⁷⁶ One of the advantages of storing the information on Internet servers is the fact that the information can be accessed from any place with Internet connection.

¹⁷⁷ In this context it is important to keep in mind the principle of national sovereignty. If the information is stored on a computer system outside the territory an extension of the search order could violate this principle. The drafters of the Convention on Cybercrime therefore pointed out: “Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be ‘in its territory’” - Explanatory Report to the Convention on Cybercrime, No. 193. With regard to this issue see as well: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12 – available at: <http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf>.

important aspect of computer forensics.¹⁷⁸ In general an investigation of the storage devices requires physical access to the hardware.¹⁷⁹

2. The Related Procedural Instrument

(i) *Article 19 – Search and seizure of stored computer data*

[...]

(3) *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:*

- a) seize or similarly secure a computer system or part of it or a computer-data storage medium;*
- b) make and retain a copy of those computer data;*
- c) maintain the integrity of the relevant stored computer data;*
- d) render inaccessible or remove those computer data in the accessed computer system.*

(4) *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.*

Art. 19 sub-paragraph 3, Convention on Cybercrime enables the law enforcement agencies to seize computer hardware.¹⁸⁰ In addition to the tradition of seizure of the hardware, the Convention on Cybercrime enables the law enforcement agencies to copy the relevant data instead of seizing the hardware.¹⁸¹ If the law enforcement agencies decide not to seize the hardware but only to copy the relevant data there are a number of side-measures provided by Art. 19 Convention on Cybercrime to maintain the integrity of the copied data and remove the original data.¹⁸²

Very often the investigators will not be able to identify the exact location of relevant data without the help of the system administrator that is responsible for the server infrastructure.¹⁸³ But even if they are able to identify the hard drive protection measures might stop them from searching for the relevant data.

¹⁷⁸ *Hannan*, To Revisit: What is Forensic Computing, 2004 – available at: <http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf>; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4 – available at: http://www.acpr.gov.au/pdf/ACPR_CC3.pdf;

¹⁷⁹ Regarding the advantages of remote forensic tools compared with traditional search and seizure procedures see *Gercke*, Secret Online Search, CR 2008, page 245 et. seqq. But there are also disadvantages related to remote investigations. Apart from the fact that direct access enables the law enforcement agencies to examine the physical condition of storage media physical access to a computer system it is the only way to ensure that the files on the suspects computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6 – available at: <http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf>.

¹⁸⁰ For guidelines how to carry out the seizure of computer equipment see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory – available at: <http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm>; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice – available at: <http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf>.

¹⁸¹ Regarding the classification of the act of copying the data see: *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 et seqq.

¹⁸² “Since the measures relate to stored intangible data, additional measures are required by competent authorities to secure the data; that is, ‘maintain the integrity of the data’, or maintain the ‘chain of custody’ of the data, meaning that the data which is copied or removed be retained in the State in which they were found at the time of the seizure and remain unchanged during the time of criminal proceedings. The term refers to taking control over or the taking away of data.” Explanatory Report to the Convention on Cybercrime, No. 197.

¹⁸³ “It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognizes that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted.” Explanatory Report to the Convention on Cybercrime, No. 200.

The drafters of the Convention therefore included an obligation of system administrator and other people, who have knowledge about the location of stored information to assist the law enforcement agencies.

G. Collection of Traffic Data

1. The Situation

Traffic data play an important role in cybercrime investigation.¹⁸⁴ Having access to content data enables the law enforcement agencies to analyse the nature of messages of files exchanged and help to trace the offender. By monitoring the traffic data generated during the use of Internet services, law enforcement agencies are able to identify the IP-address of the server and can then try to determine the physical location of the offender.

2. The Related Procedural Instrument

With Art. 20 the Convention on Cybercrime provides the legal basis for the real time collection of traffic data.

(i) Article 20 – Real-time collection of traffic data

(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

- a) collect or record through the application of technical means on the territory of that Party, and*
- b) compel a service provider, within its existing technical capability:*

- i) to collect or record through the application of technical means on the territory of that Party; or*
- ii) to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.*

(2) Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

(4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

The provision is neither drafted with preference to a specific technology nor is it intending to set standards that go along with the need for high financial investments for the industry involved.¹⁸⁵

H. Interception of Content Data

1. The Situation

In some cases the collection of traffic data is not sufficient to collect the evidence that is required to convict the suspect. This is especially relevant in those cases where the law enforcement agencies do already know the communication partners and the services used but have no information about the information exchanged.

¹⁸⁴ “In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication’s route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn’t reveal the content of the communication which is regarded to be more sensitive.” See: Explanatory Report to the Convention on Cybercrime, No. 29. Regarding the importance of traffic data in Cybercrime investigations see as well: ABA International Guide to Combating Cybercrime, page 125; Gercke, Preservation of User Data, DUD 2002, 577 et. seqq.

¹⁸⁵ “The article [Art. 20] does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems.” Explanatory Report to the Convention on Cybercrime, No. 221.

2. The Related Procedural Instrument

Art. 21 enables the law enforcement agencies to record data communication and analyse the content.¹⁸⁶

(i) *Article 21 – Interception of content data*

(1) Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

- a) collect or record through the application of technical means on the territory of that Party, and*
- b) compel a service provider, within its existing technical capability:*

- i) to collect or record through the application of technical means on the territory of that Party, or*
- ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.*

(2) Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

(4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

This includes files downloaded from websites or file-sharing systems, e-mails sent or received by the offender and chat conversations.

¹⁸⁶ One possibility to prevent law enforcement agencies to analyse the content exchanged between two suspects is the use of encryption technology. Regarding the functioning of encryption procedures see: *Singh*; *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, 2006; *D'Agapeyev*, *Codes and Ciphers – A History of Cryptography*, 2006; *An Overview of the History of Cryptology* – available at: <http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf>.

MANAGING LARGE AMOUNTS OF ELECTRONIC EVIDENCE

*Cybercrime Lab**
Computer Crime and Intellectual Property Section
Criminal Division

Ovie L. Carroll, Director, CCIPS Cybercrime Lab
Stephen K. Brannon, Cybercrime Analyst, CCIPS Cybercrime Lab
Thomas Song, Senior Cybercrime Analyst, CCIPS Cybercrime Lab
Joel M. Schwarz, Trial Attorney, CCIPS



I. INTRODUCTION

Investigations usually focus on finding and getting evidence. A computer-related investigation often generates a particularly large amount of evidence. Managing all this data and using it effectively through the lifecycle of an investigation presents special problems. This article explores those problems and describes general strategies and some specific solutions for managing large amounts of electronic evidence.

The Cybercrime Lab in the Computer Crime and Intellectual Property Section regularly provides advice and assistance with the issues in this article. You can contact the Lab at (202) 514-1026 or at www.cybercrime.gov. Also, from within the Criminal Division or US Attorneys' offices, you can access resources on our intranet site, CCIPS Online, by going to DOJ Net and clicking the "CCIPS Online" link.

II. CONCEPTS AND CONCERNS

A. Preliminary Concerns

There is one cardinal rule for electronic evidence: always work on a copy. Original evidence or the single best copy should be duplicated and kept safe. A clean chain of custody record should be maintained for that best copy. Only use working copies of evidence for review and analysis. Always keep the original or best copy safe and disturb it as little as possible.

Working directly with original evidence or your best copy is extremely dangerous. The first reason is that simply interacting with it will likely change it. It is also dangerous because there is a greater risk that data will become corrupted or lost due to hard disk failure. The integrity of electronic evidence is important just as with other types of evidence. But the integrity of electronic evidence is also important because if it is intact, forensic copies should theoretically be exact. With some other types of forensic evidence, testing and analysis use up the evidence itself. But with electronic evidence, any number of exact copies can be made, and the defence is often entitled to receive a copy for review.

If the government can't produce an exact copy of the evidence that it seized or obtained for any reason, it opens a Pandora's Box of questions about what went wrong. Even if someone accidentally modifies evidence, it is still likely admissible. If the modification is clearly documented and explained then the evidence can probably be used. However, the modification may influence the evidence's weight.

Electronic evidence is much easier to manage if a system of organization is already in place before it is collected. As investigations get evidence, they naturally document and preserve original versions. But as copies are made, it is helpful to plan a system of organization and start filing copies of evidence into it. Far too often, investigations let the order in which they get evidence or its sources dictate its organization. Then at the end of the investigation when the evidence needs to be sorted differently to be used, there may not be time to reorganize it.

* The Cybercrime Lab is a group of technologists in the Computer Crime and Intellectual Property Section (CCIPS) of the Department of Justice, in Washington, DC. The lab serves CCIPS attorneys, Computer Hacking and Intellectual Property (CHIP) units in the US Attorneys' offices, and Assistant US Attorneys in general, by providing technical and investigative consultations, assisting with computer forensic analysis, teaching, and conducting technical research in support of DOJ initiatives.

The idea is to think forward to your analysis so it can guide your initial setup. For example, you may be starting an investigation of multiple targets using multiple websites. If you know that most of your questions will be about one target or another, then you would organize evidence by target as you get it. On the other hand, if you know you will need to paint a coherent picture of the activity on each website, you would organize evidence by website. Planning and setting up an organizational system at the beginning of an investigation may determine whether or not electronic evidence is manageable at the end.

Another preliminary concern for electronic evidence is the use of date and time information. Problems with computer date and time settings can be fatal to an investigation. Overlooked date and time issues can ruin an investigation quickly. Targets can be misidentified, evidence can show a target did something he or she did not really do, and evidence from different computers can be inconsistent. They are all too common, but they are still often overlooked. Every computer, server, etc. has an internal clock. The date and time - or at least what the computer believes they are - will be spread through all the evidence the computer produces, especially any logs. The clock setting may be set wrong or it may be set to a different time zone. Investigations need to find and adjust both for inaccuracies of any particular clock and for discrepancies between different clocks.

Fortunately, it is possible to document and compensate for almost any problem with dates and times as long as it's both *identified* and *quantified*. Say you are running an undercover website and logging the activity that takes place on it. You may discover that the computer running the website had an incorrectly set clock and it was set exactly 23 minutes fast for the last year. With both of those pieces of information, the year's worth of log evidence can be salvaged and used by subtracting 23 minutes from every time.

A final idea that should guide everything you do with electronic evidence is: *let the computer do the work*. You may find yourself in a situation where you are tempted to have an army of investigators or paralegals process mountains of evidence manually. This is almost always the wrong answer. It's far better to think of a way for the computer to do brute force searching, sorting, etc.

A human brute-force attack is too slow, but it also introduces the potential for too many errors. Even the most conscientious person can't avoid making mistakes when he or she has to do the same thing 1,000 times. On the other hand, once you give a computer accurate instructions, it can easily execute them a million times without any mistakes. A long list of answers without mistakes is often what you need from electronic evidence.

What are some things an investigation might need to do with electronic evidence? Thinking about this question helps structure our discussion. The first task is to organize and manage it. The next task is to search it. It often feels like trying to find a needle in a haystack. For example, an investigation may need search through millions of lines of logs to find the one record that shows a target did something on a website.

The third and final type of task is analysing and interpreting evidence. This entails looking at all of the evidence, or a large part of it, and synthesizing new information from it. This type of task is anticipated less often but can still provide the most useful information. For example, think again about an investigation of many targets using many websites. It might be necessary to identify the most egregious users to select targets for prosecution. We would need to quantify each target's conduct across all the websites throughout the course of the investigation and then compare the targets.

B. Indexing

Indexing is a technique to search through large bodies of data faster. Indexing goes through the entire body of data and creates a map of what information is where. This map, or index, functions like the index in a book or the card catalogue in a library. Building an index can take a long time. But once it's done, searches can be done much faster. For example, Google and LexisNexis have indexed all their data to enable users to search it quickly. It is hard to imagine how long it would take to search every word on the Internet or every word in the LexisNexis databases if they had not already been indexed. In situations with a large amount of data where multiple searches will be necessary, it's generally best to index once and then use that index to search. In the long run, this is far faster than conducting each search through all the data.

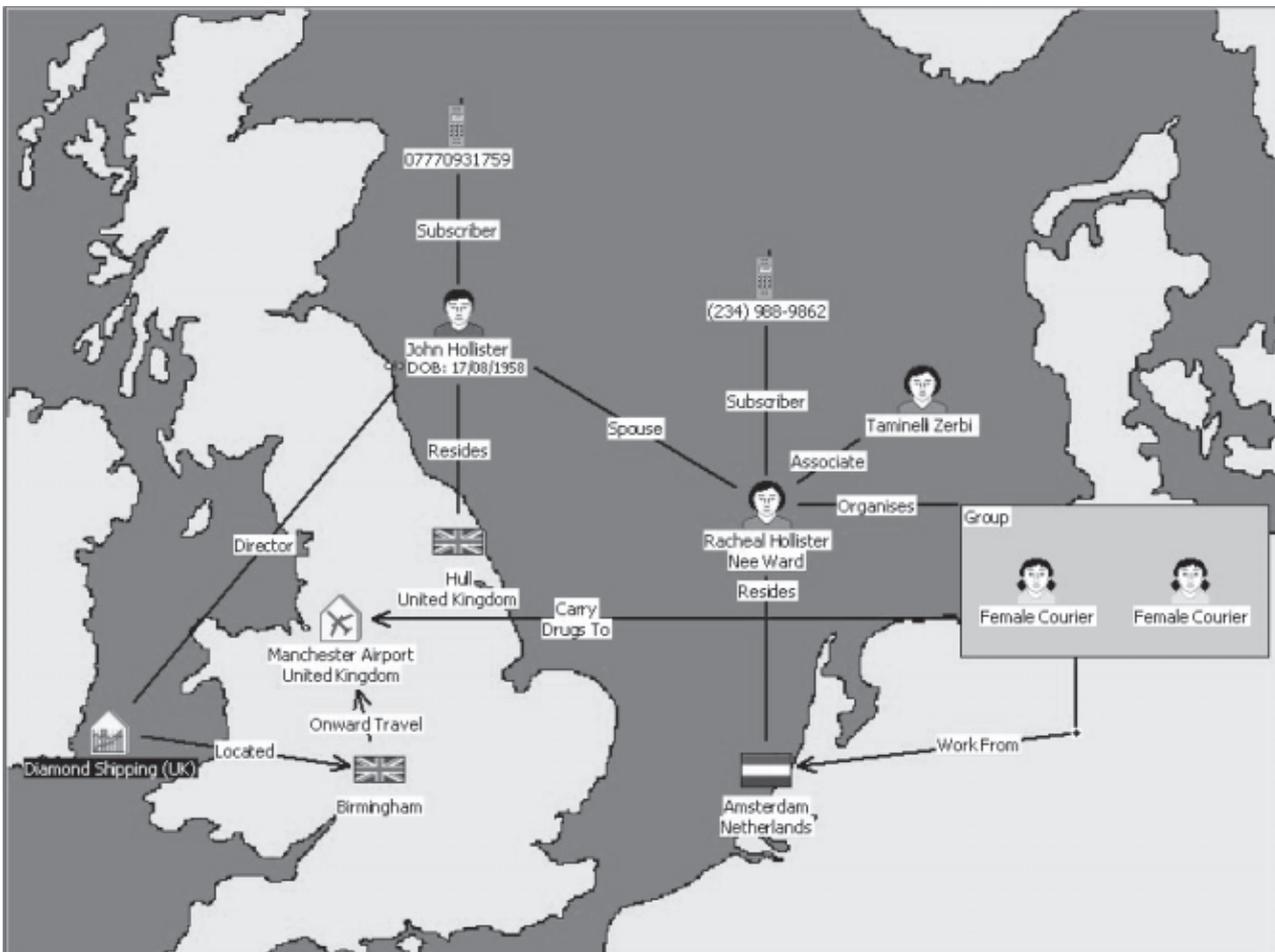
Indexed searching can be done within computer forensics programmes. It can also be done using stand-alone programmes that only index and search data. The computer forensics programme Forensic Toolkit

(FTK) made by AccessData has the capability to index data built in and is widely considered the leader in indexed searching. The other leading computer forensics software is EnCase, made by Guidance Software. Its newest version, version 6, also incorporates indexing capabilities. Indexing can be done in previous versions of EnCase by using a third-party add-on, such as Mercury by MicroForensics. Once data in a forensics programme has been indexed, searches that would have taken minutes or hours are completed almost instantly.

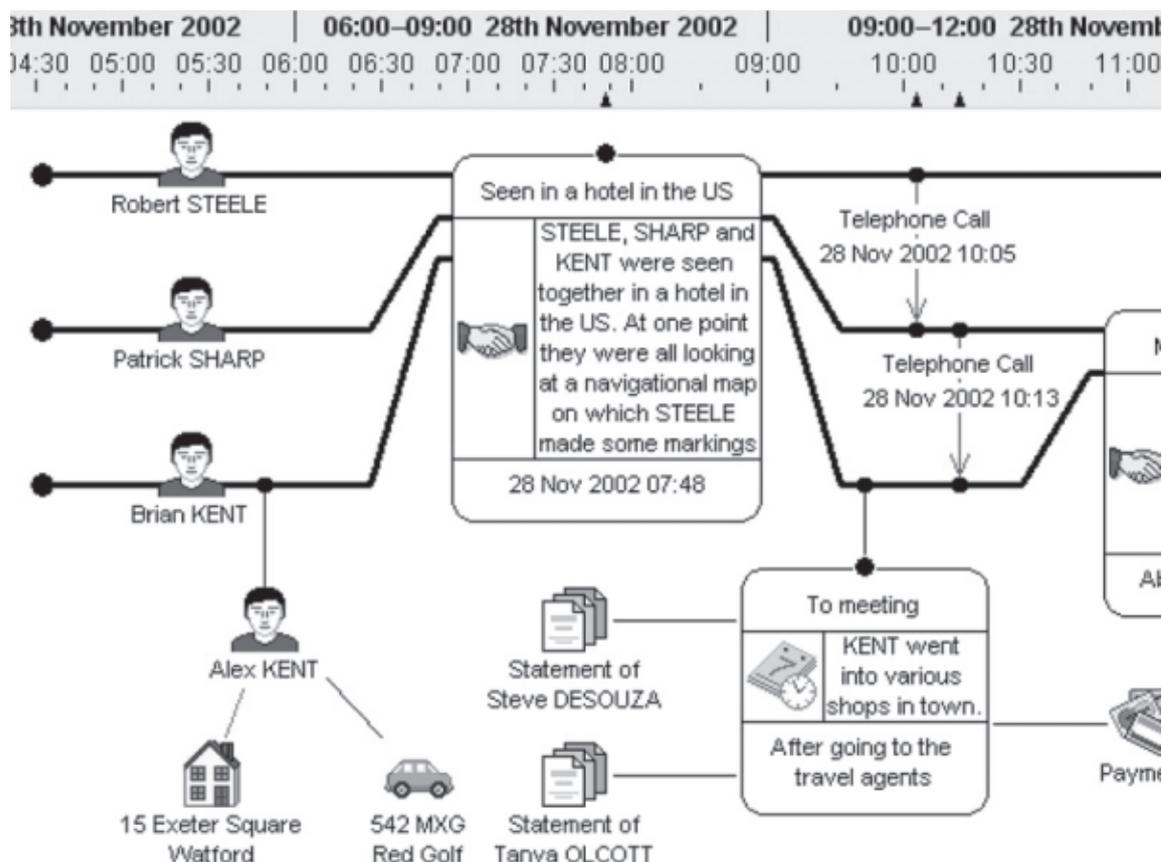
There are also stand-alone programmes that just do indexed searching. DtSearch produces a mature suite of programmes that use the same indexing engine as FTK. The basic programme searches text in multiple formats and highlights results. It also has options to use fuzzy, phonic, wildcard, stemming, and thesaurus search options. These are all search techniques that find results similar to or related to the term you provide. This can find misspelled occurrences of words, so it is especially useful when searching through anything written by a person. For example, a fuzzy search for “apple” would also find “apple”. DtSearch can also display results as web pages that are easy to use. Another programme in the product suite, dtSearch Publish, lets you publish and distribute your evidence in an indexed and quickly searchable package. This product is excellent for giving indexed copies of your evidence to others to review.

C. Visualization

This article discusses many ways to manage, search, and analyse electronic evidence. Sometimes the only way to see important relationships is to visualize large amounts of information. Also, some results are only useful to a prosecutor or jury when they are presented visually. There are programmes available that combine database and visualization features to enable an analyst to find connections and illustrate them. These tools are often used in cases with extensive financial data or phone records. They are also particularly useful to show relationships indicated by email exchanges or network traffic. One of the most popular programmes is Analyst’s Notebook by i2 (http://www.i2.co.uk/Products/Analysts_Notebook/default.asp). It can illustrate relationships as shown in the screen capture below.



The analyst's notebook can also perform and illustrate timeline analysis. An example of this is below.



III. TECHNIQUES AND TOOLS

A. Email

It is important that electronic evidence only be reviewed on a computer that's not connected to the Internet. It is most important when reviewing email evidence. Reviewing email on a computer connected to the Internet risks accidentally sending a read receipt response to addressees on the email. Also, some email uses HTML, the language for making web pages, to control formatting. In fact, Outlook created message in this format by default. Since HTML can have references to images and other files on websites, simply opening it can cause your computer to connect to those websites to retrieve message elements. This can directly or indirectly warn a tech-savvy target that he or she is under investigation.

Reviewing email on a computer connected to the Internet even risks sending an email to a target tipping him or her off. We know of a case where the agent reviewing an email between conspirators accidentally double-clicked the "reply-all" button. Worse yet, the agent was reviewing the email in his own email account on his work computer. So he created and sent an email from his work email address to all the conspirators jeopardizing the investigation. In fact, a computer used to review email should not only be disconnected from the Internet, but it should also be dedicated to offline evidence review. An offline computer may keep track of read receipts that it is unable to send, then if it is later connected to the internet, it will take the opportunity to send them all.

Email provides several sources for valuable information. Some will often be in the body of an email. In addition to content, one can search or sort email by elements of the header, like the sender, recipient, subject, or date sent. It may also be helpful to search or sort by other less obvious attributes like the number of attachments, attachment names, priority, or age.

Once an investigation gets email from one or more sources, the first step is usually to import it all into one email programme. This facilitates organization and management. Sometime an investigator will instead review email one message at a time or import different groups of email into different email programmes. But this makes managing the evidence harder and searching it harder still. When all email is in one programme, one can easily organize it by folders in a structure that makes sense. Then one can conduct searches across all email or just across certain folders.

There are many free and commercial email programmes available. In our lab's experience Mozilla Thunderbird is one of the best free programmes for managing and searching email for all but the largest cases. The programme is free and available at <http://www.mozilla.com/en-US/thunderbird/>. Other programmes that are either free or likely already installed on most computers include Outlook, Outlook Express, and Eudora. The largest cases may need to use specialized forensics programmes like Access Data's Forensic Toolkit and Paraben's E-mail Examiner.

The rest of this section about email will describe the steps to import, manage, and search email. A preliminary step is needed for most email programmes. In order to operate, most programmes need the user to create a profile. This simply involves entering a name, email address, and a few other pieces of information. When a programme first starts, it usually walks the user through the account creation process. Made-up information is fine for this since the computer won't be connected to the Internet anyway.

Email in the most common formats can be imported into Mozilla Thunderbird. One common format is the mbox format. Such files are easily recognizable by the file extensions .mbx or .mbox. In fact, the mbox format is very common, and if a file with email has no file extension, it is likely an mbox file.

Thunderbird uses the mbox format internally, so the simplest way to import emails in that format is to copy the file to the directory where Thunderbird stores its own files. Then the next time the programme starts, the mbox file and all its email appears as a folder under "Local Folders".

On Windows XP, the directory is C:\Documents and Settings\[User Name]\Application Data\Thunderbird\Profiles\xxxxxxx.default\Mail\Local Folders\ (xxxxxxx is 8 random characters).

On Windows Vista, the directory is C:\users\[User Name]\AppData\Roaming\Thunderbird\Profiles\xxxxxxx.default\Mail\Local Folders\ (xxxxxxx is 8 random characters).

Just copy email evidence files to that directory, then open the programme and it's ready to use.

Another common email format is Microsoft's .pst (Personal Folders) format. Thunderbird can't import a .pst file directly, but it can be imported into Microsoft Outlook first and then from Outlook into Thunderbird. Again, it is essential to first create a profile in each programme as described above. Importing a .pst file into Outlook only takes a few steps. The goal for this step is to get email from a .pst file into the Personal Folders in the Outlook profile. These instructions are specifically for Outlook 2003.

1. In Outlook, click the File menu then Data File Management.
2. Click the Add button then click OK.
3. Find and select the .pst file.
4. Optionally, type in a new name in the "Name" box (for example, "warrant response") then click OK.
5. Click Close.

Now the .pst file should appear as a folder on the bottom of the left pane (in our example, "warrant response"). The last thing to do in Outlook is move the mail from the new folder to a folder inside the Personal Folders. To do that:

1. Right-click on Personal Folders and select New Folder.
2. Name the folder (for example, "Bad Guy1") and click OK.
3. Click on the .pst folder at the bottom ("warrant response").
4. Select all the emails by clicking the Edit menu then selecting Select All.

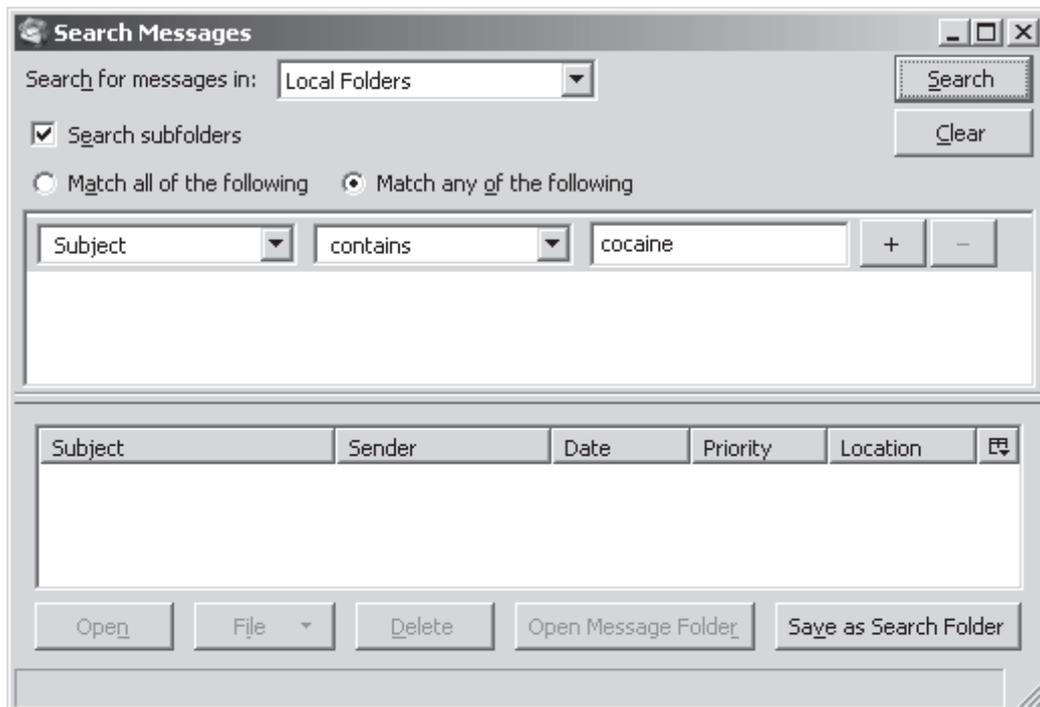
5. Carefully click on any email and drag it into the folder created in the Personal Folders ("Bad Guy1"). This should move all email from the .pst file into the local folder.

Now you can close Outlook and open Thunderbird to import the email from Outlook. These instructions are for Thunderbird 2.0.0.6.

1. In Thunderbird, click the Tools menu then Import.
2. Select Mail then click Next.
3. Select Outlook then click Next.
4. The process imports every folders from Outlook, so it may be helpful to delete empty or unrelated folders.

Bringing all email evidence into one programme has two main advantages. First, you can organize and manage it in a way that works best for your case regardless of how you got it. Second, and even more beneficial, you can search through all email evidence at the same time or search only through sections that make sense.

To open Thunderbird's search interface click Edit, then Find, then Search Messages. The search interface looks like this:



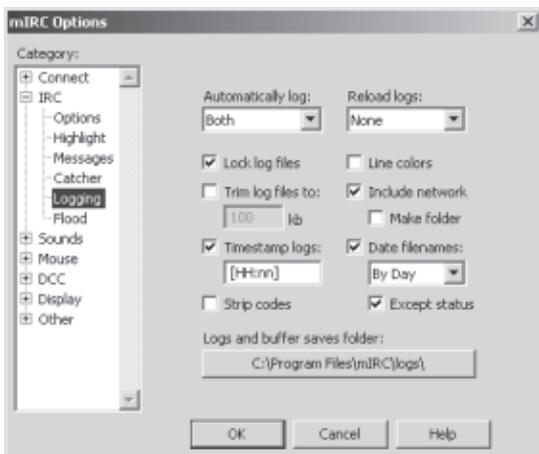
The box at the top selects which folder or folders to search. Select "Local Folders" and leave the "Search Subfolders" box checked to search in all email. The two radio buttons and the middle pane specify search conditions. The radio buttons determine whether *all* the conditions must be met for a result to be included or if it will be included when *any* of the conditions are met. Each search condition specifies where in the email to look, the condition to meet (i.e., contains, doesn't contain, begins with), and the search term. You can easily add or remove any number of conditions by clicking the + or - buttons.

Click the Search button and search results are displayed in a list in the bottom pane. This list can be sorted by any field. A search hit is easy to file into a folder. For example, you can create a folder called "key emails." Then when you select an email in the search results list, you can click the File button on the bottom and select the folder you want to move it to. You can also save a useful search. Click the Save as Search Folder button and it will create a search results folder. The results will be viewable as if they were a folder, but the original email won't be moved.

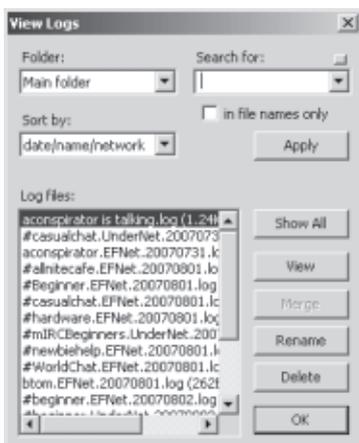
B. Chat Logs

Many computer-related investigations involve records of online chat, or instant messaging. Instant messaging lets two or more people to have a real-time, text-based conversation over the Internet. Each user types messages into a window on his or her computer, and every user who is party to the conversation sees all the typed messages in real time. So for example in a one-on-one chat, two people send text message back and forth. Both people see the conversation scroll by in a window. Or in a chat room, or channel, with several people communicating, each person sees a window representing the room and everything everybody types is visible. Most instant messaging programmes allow users to log their chats and some programmes even log by default. You may get chat logs from a target's computer, from a victim, or you may record them yourself using a co-operator or undercover agent.

The programme mIRC is the most common programme used for IRC chat. IRC is a type of chat popular in many tech-savvy crime circles, such as hacking, ID theft, and high-level copyright infringement. The mIRC programme conveniently has an option to log its communications. The person using the programme only needs to check the right boxes and the programme produces its own logs and organizes them in folders. So even as it creates the logs mIRC can already introduce a level of organization.



The programme also has an interface for viewing and searching its logs. Even if you later reorganize the chat logs into a different folder structure that is easier to manage, this interface can still see them and interact with them in the same way. It looks like this:



Extensive chat log evidence may require powerful techniques like those described in the next section of this article. But for smaller collections of chat logs, this interface allows you to perform basic searching,

sorting, and analysis. The controls at the top search and filter which chat logs are listed. The bottom of the interface lists log files that meet the criteria in the top half. It provides ways to view and manage them. You can open any chat by double-clicking on it. By default it will open in a text editor, like Notepad, where you can again search for specific terms within that chat. It is also possible to merge related logs into a single file. You can select multiple files from the list (or all of them), and then click the Merge button. This combines the selected files into one new file.

Here are several examples of how you can use this interface to search and analyse chat logs. If you want to see who you have logs of conversations with, you can simply sort by name. If you want to see what a particular target has been chatting about, you could search for his or her user name. The resulting list of log files would be the chats in which he or she spoke. Then you could merge these into one file and send it to someone else for further analysis. You can find out who was talking about a particular topic and when they were doing it. You could do this by searching for a term linked to the topic. Sorting the results by name first and date second would show you who was involved in conversations about the topic and when the conversations took place.

C. Logs

Sometimes commercial off-the-shelf programmes are best for managing electronic evidence of the type they are designed to manipulate. Sometimes a programme can even manage its own logs. Often simple solutions like this are best. But some types of evidence have no readily available programme to manage them. Or if a programme is available, it may not do everything needed. This is often the case with raw log evidence. Log evidence is a file generated by a computer that records events, usually sequentially. These files can be logs of system events, such as every time a user logged on. They can also be logs of activities, for example, a file server may log every file transfer. Networking elements like firewalls can also generate logs that record activity on a network. These log files can easily be millions of records long or longer, and normal tools and techniques for managing them quickly become insufficient.

Microsoft Excel can open smaller log files, but it has several limits to its usefulness. First, in versions up to Excel 2003, a worksheet could not have more than 65,536 rows. Many log files have more lines. Excel 2007 can now have up to 1,048,576 rows, so it can at least theoretically open most typical log files. A second limitation is that when Excel opens a file it attempts to load the entire file's data into memory at the same time. For large files this can be impractically slow. Excel's final limitation is that its search and analysis capabilities are far inferior to those of databases.

The Cybercrime Lab has had great success using custom Microsoft Access Databases to manage log evidence. Using Access has several benefits: as part of Microsoft Office, it is already installed on most computers. It is reasonably easy for people with other technical experience to learn and use. Finally, it is powerful enough to handle all but the most voluminous log evidence (we almost never need to move to a more robust database with a bigger capacity). Not everyone is comfortable working with databases. But it is likely you can find someone in your organization with the aptitude for basic database work who can assist your investigation.

The same tools and techniques can be used for any kind of log evidence, but for the sake of clarity we'll discuss one type of log as an example. In our section we manage log evidence for many "warez", or online piracy cases. Targets in these cases often use file servers where each file transfer is logged. Each time a file is transferred, a line is written to a log file with information such as the date and time, the file name, the direction (upload or download), and the user's name. These log files can easily grow to be millions of lines long. Managing them as text files quickly becomes difficult and searching them or making sense of them quickly becomes impossible.

The logs are easy to manage once they are imported into a table in an Access database. The essential step is to split each line of the log into pieces and put each piece into a separate column in the table. So in our transfer log databases, a row in the table represents one line of the log. And every row has a column for each piece of information in it. For example there is a date/time column, a filename column, a direction column, etc. Splitting each log line into its parts is essential: it allows you to use the full power of a database. Depending on the format of a log file, Access may be able to import it and split each line into separate fields at the same time. Otherwise a simple Visual Basic module can parse the log files into pieces and perform any additional logic necessary while it imports them. Here is sample code for importing lines of a log file into a table in Access:

```

Public Function import(path As String)
    Dim rs As Object 'destination table
    Set rs = CurrentDb.OpenRecordset("tablename")

    Dim pcs() As String 'pieces
    Dim inp As String 'line read from input file

    Open path For Input As #1 'open file for input

    'import file
    Do While Not EOF(1) 'check for end of file
        Line Input #1, inp 'read line of data
        If inp <> "" Then
            'split line
            pcs = Split(inp)

            'put in record
            With rs
                .AddNew
                .field1 = pcs(0)
                .field2 = pcs(1)
                .field3 = pcs(2)
                'etc.
            End With
        End If
    Loop

    Close #1 'close file
    rs.Close
End Function

```

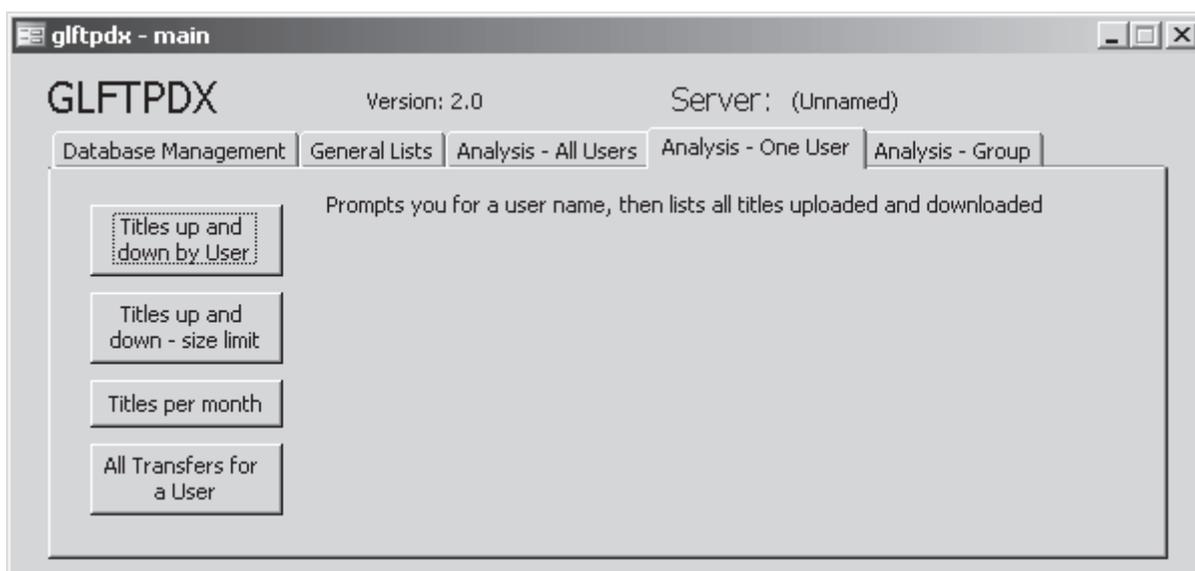
Once the logs are in a table in a database, you can do any searching or sorting by creating queries. A query is a structured way of getting data out of a database to answer a question. Access has a friendly interface to guide you through the process of setting up a query. You can select which fields you want in your answer, which fields you want sorted, and you can add any conditions. Keep in mind that Access can save any query you create and run it again at any time. This way, if you add or change data, you can ask the database the same question again and get the updated answer.

For example, sometimes we want to know who was using a particular file server. We made a query that told the database, “show just the user column, sort it in alphabetical order, and don’t show duplicates”. When we run the query, the database quickly generates a new set of data, like a mini-table, that answers the exact question we described. It gives us an alphabetical list of unique user names. Databases do this efficiently, so it easily runs through millions of records and gives us an answer in a few seconds.

We also often want to know what a particular target has done. We want a list of his transfers. To do this we made a query selecting three columns: file transferred, date, and user. We sorted the query by the date and limited it to one user (a condition for the user column). Again, we had another mini data set to answer our question in a matter of seconds.

Finally, sometimes we need to run a more complex kind of query. For example, we want to know who the most active users are on a server. In other words, who uploaded and downloaded the most. Our answer was a table with these three columns: user, count of his uploads, and count of his downloads. Counting something for each user requires something called a crosstab query. Fortunately, Microsoft knows it’s a little more complicated so they provide a special wizard that walks you through creating one. You don’t even have to understand how it works: you just use the wizard to describe what you want.

In our lab, we had many related cases like this and many people needed to use the evidence. So we programmed a user interface to make the functions described above look like a friendly programme. A screenshot of the programme's main window is below. It uses tabs to group tasks (Database Management) and questions (General Lists, Analysis – All Users, Analysis – One user, etc.). On each tab there is a buttons for each query. If you point the mouse at a button it shows a brief description of what the query does. A database application with a user interface like this certainly isn't necessary for every case. But it may be appropriate when you need to harness the power of a database and make it available to a large number of non-technical users.



IV. CONCLUSION

We hope that the strategies and examples in this article will help prepare you to manage electronic evidence in your cases. The Computer Crime and Intellectual Property Section and the Cybercrime lab is also available to AUSA's for consultation on computer forensic and other technical investigative matters by calling (202) 514-1026. Many other resources are available on our section's public website, www.cybercrime.gov. In addition, anyone in the Criminal Division or US Attorneys' Offices can find additional resources on our new intranet site, CCIPS Online. Just go to DOJ Net and click on the "CCIPS Online" link. We also encourage AUSAs to take advantage of the many courses we present at the National Advocacy Center throughout the year.

RETHINKING THE STORAGE OF COMPUTER EVIDENCE

*Computer Crime and Intellectual Property Section
Criminal Division, US Department of Justice*

*Tyler Newby, Trial Attorney, CCIPS
Joel M. Schwarz, Trial Attorney, CCIPS
Ovie L. Carroll, Director, CCIPS Cybercrime Lab*

I. INTRODUCTION

When a federal criminal investigation involves computer evidence, prosecutors and investigators often rely on the services of investigators who have special training and accreditation in the field of computer forensics. These forensic examiners are typically responsible for the collection, processing and analysis of digital evidence acquired during an investigation. Primary among computer forensic examiners' duties is ensuring that the data seized during an investigation remains unaltered through trial.

The foundation of electronic evidence collection and analysis and the subsequent admissibility and use of that evidence at trial is the creation of a forensic image. Once a forensic image of the original data is created, it is typically copied to a hard disk drive, which is then stored in a locked evidence room. Chain of custody logs are maintained for anyone who accesses the hard drive image.

In complex cases, such as intrusion cases, a prosecutor or case agent may request full forensic analysis of an image to search for evidence to be used at trial. In less complex cases, a case agent or prosecutor may want to conduct a triage review of the image to search for easily identifiable evidence of a crime, such as pirated software and movies, chat logs and e-mails discussing the crimes, digital photographs and the like. In that case, the case agent may want to review a working copy of the forensic image, which requires putting in a request for a working copy image to be made.

In either situation, case agents and prosecutors are likely to confront a long queue when they put in a request for assistance from computer forensic specialists. As electronic storage of data has become increasingly common, the demands placed on a limited pool of computer forensic examiners have increased. For example, in the Federal Bureau of Investigation's *FY2008 Authorization and Budget Request to Congress*, it noted that its Computer Analysis and Response Team's (CART) case backlog increased 58% from 1,258 cases to 1,991 in just a one year period from FY2004 to FY2005 and is likely to increase in the future. As electronic communication devices, home networks and increasingly capacious hard drives become more prevalent, already thinly stretched investigative resources are likely to be in even more demand. Thus, it is not unlikely that a hard drive containing the evidence prosecutors need to prepare and try their cases will sit on a shelf for a period of several months, if not years.

This reality raises the basic question of whether storing an increasing number of hard drives – which like all things mechanical can break – for years on shelves in evidence rooms is the best way to store digital evidence. This article suggests an alternative evidence storage method for forensic images – storing them on secured Redundant Array of Independent (or Inexpensive) Disks (RAID) systems. This alternative may save space in evidence rooms and will better protect sensitive evidence from inadvertent destruction. Furthermore, storing images on a RAID, if done properly, will not affect authentication of the image as a duplicate of the original electronic media at trial.

This storage method most clearly applies to cases in which investigators make an image copy of the electronic media at the scene. Where investigators remove computers containing electronic evidence from the scene, use of RAID storage may also be appropriate, but prosecutors should consider the possibility of defence challenges before wiping the original computer hard drive or returning it to its owner. Of course, if the computer hardware is seized because it is contraband, the fruit of a crime, or an instrumentality it should be retained pending disposition of the case or forfeiture proceeding.

II. THE BASICS OF FORENSIC IMAGING

Forensic imaging is the process used to obtain a bit for bit copy of the data residing on the original electronic media obtained by law enforcement – regardless of whether that media is a single hard disk drive, flash memory card, DVD, compact disc or mobile phone SIM card. The imaging process entails the copying of all of the data present on the original storage media device, including system files, hidden and deleted data from allocated (partitioned), unallocated (un-partitioned), and free space (un-used space on a formatted partition).

Once the imaging procedure is completed, the image of the hard drive contains all logical files, erased files, and unused space which are available to the original hard disk drive. From there, the investigator can examine the image for relevant evidence, without accessing the original seized hard drive at all. This process allows investigators to review a duplicate of the original evidence while preserving that evidence in exactly the form it existed at the time of seizure.

III. EVIDENTIARY ISSUES RAISED BY FORENSIC IMAGING

Prosecutors and investigators must be mindful that the ultimate goal of any investigation is to acquire evidence that will be admissible at trial. The creation of a copy of original electronic evidence raises authentication, best evidence and reliability concerns. How can one be sure the forensic imaging process produced a true copy of the original evidence? Could the forensic image have been altered or corrupted in the time between its creation and offering into evidence at trial?

A. Best Evidence Issues

Federal Rule of Evidence 1002 requires the use of an original writing, recording or photograph to prove the contents of those items, unless provided otherwise by federal statute or the Federal Rules of Evidence. FED. R. EVID. 1002. The exception that proves the rule for forensic images is Rule 1003, which provides that a “duplicate” is admissible to the same extent as an original unless a genuine challenge is made to the authenticity of the original or it would be unfair to admit the duplicate instead of the original. FED. R. EVID. 1003. Rule 1001(4) defines a duplicate as a copy of the original made by, among other things, “mechanical or electronic re-recording . . . or by other equivalent techniques which accurately reproduces the original.” FED. R. EVID. 1004. Thus, the focus must be on whether the image is an accurate and authentic reproduction of the original evidence.

B. Authentication of Forensic Images

Authentication is a predicate to the admissibility of any physical evidence. See FED. R. EVID. 901(a). To satisfy Rule 901, the proponent must produce “evidence sufficient to support a finding that the matter in question is what its proponent claims.” *Id.*; see, e.g., *United States v. Simpson*, 152 F.3d 1241, 1250 (10th Cir. 1998). This requirement is typically easy to satisfy when the evidence is a single document and a co-operating witness, such as a recipient, author or custodian is available to authenticate it.

While the authentication requirements for computer data are no different than for other forms of evidence, authentication can appear more daunting when the data was extracted from a *copy* of the defendant’s media that was made outside the defendant’s presence. Furthermore, due to backlogs in obtaining forensic analysis of seized computer media, it is likely that the copies of the seized media sat in on a shelf in an evidence room for months or years before trial. These factors, combined with the ease (perceived or real) of altering computer data without notice, may tempt a particularly aggressive defence counsel to challenge authenticity of the proffered data.

Courts have generally looked askance at authenticity challenges to electronic evidence that are unsupported by anything other than speculation that the original data was altered by an unseen hand. See, e.g., *United States v. Whitaker*, 127 F.3d 595, 602 (7th Cir. 1997) (affirming admission of computer records where allegation of tampering was “almost wild-eyed speculation . . . [without] evidence to support such a scenario.”); *United States v. Glasser*, 773 F.2d 1553, 1559 (11th Cir. 1985) (“The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records.”) In *Whitaker*, the Seventh Circuit upheld a district court’s admission of print-outs of spreadsheets

from the original computer seized, where the FBI agent involved in the seizure and the printing testified as to their authenticity. *Id.* Despite the permissive standard applied in *Whitaker*, good trial pre-strategy is to foreclose potential authenticity challenges before they are raised.

IV. HASH ALGORITHMS – AN ANSWER TO EVIDENTIARY ISSUES

To blunt potential authentication challenges to data extracted from a forensic image, it is useful to have a procedure to verify that the data on the image is an exact match of the original media. Computer forensic specialists have developed a procedure that guarantees just that. This process uses “hash” algorithms, which verify that the acquired image is the exact copy of the original media. The most commonly used hash algorithms – the Message Digest 5 (MD5) and Secure Hash Algorithm-1 (SHA-1) – take as input a message of arbitrary length and produces as output an n-bit “fingerprint” or “message digest” of the input. The algorithm then produces a digital signature which can be used to identify uniquely a given file, and therefore establish that the image is an authentic copy of the original evidence.

Verification using hash algorithms is highly reliable. The odds of two random files having the same hash are astronomically small – estimated to be approximately a 1 in 10^{38} chance. Moreover, the use of the hashing algorithm is a one way function, which means that it is easy to create a hash from a file but almost impossible to create a file matching a particular hash.

Hash validation, when combined with evidence of a chain of custody between the time the original computer media was seized and the image was created, is strong authenticating evidence that the forensic image is an exact duplicate of the original. Hash algorithms fit the examples listed in Rule 901(b)(4) of “distinctive characteristics” that can be used to authenticate evidence. FED. R. EVID. 901(b)(4). What are hashes if not indicators of “internal patterns, or other distinctive characteristics” of data?

Although published decisions addressing the use of hashing algorithms to authenticate forensic images are few, they are uniform in recognizing hashes as a proper means of establishing authenticity. *See, e.g., Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 655 (D. Kan.2005) (recognizing that hashing “allows a large amount of data to be self-authenticating with a rather small hash mark, efficiently assuring that the original image has not been manipulated.”) In *Williams*, the district court rejected a civil litigant’s purported concerns about producing electronic evidence in its native format by noting that the parties could detect any alteration by comparing hash values. The court found that a hash value is a “‘digital fingerprint’ akin to a tamper-evident seal . . . the file cannot be altered without a change also occurring in the hash mark.” *Id.*; *see also Ohio v. Morris*, 2005 WL 356801, No. 04CA0036, (Ohio App. Feb. 16, 2005) (admitting forensic image even where testimony established that imaging software had validated the MD5 hashes of the original and image matched before forensic examiner erased the original hard drive); *Krause v. State*, 2007 WL 2004940, No. 01-05-01136-CR, (Tex. App. July 12, 2007) (forensic analyst’s methodology was sufficiently reliable for purposes of expert testimony where analyst used forensic software that compared hashes on the image and the original media). Similarly, the Federal Judicial Center has identified MD5 and SHA hashes as commonly used algorithms to establish the authenticity of a forensic image. *See* FEDERAL JUDICIAL CENTER, MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES, FEDERAL JUDICIAL CENTER (2007) at 24, quoted with approval in *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 536-37 (D. Md. 2007)

V. STORING FORENSIC IMAGES – AN ALTERNATIVE TO THE SHELF

As discussed above, provided that proper chain of custody is established between the times the original computer media are seized and forensic images are created, the hash verification process should eliminate any concerns over whether the forensic image was altered prior to trial. However, the practical concern of how and where to store the forensic images remains.

While the prevailing method of storing forensic images is certainly adequate and relatively simple, it has its shortcomings as well. First, as anyone who has dealt with electronic evidence likely knows, hard disk drives fail. A recent study of 100,000 different types of hard disk drives conducted by researchers at Carnegie Mellon University found that the actual reported failure rate of hard disk drives is much higher than stated in manufacturers’ data sheets. Bianca Schroeder and Garth A. Gibson, *Disk Failures in the Real*

World: What Does an MTTF of 1,000,000 Hours Mean to You?, FAST07, 5TH USENIX CONFERENCE ON FILE AND STORAGE TECHNOLOGIES (2007). Although the observed real world failure rates were approximately 2%-4% (with some as high as 13%) are still relatively low, no one wants request a continuance of trial because the hard disk drive on which the forensic image was stored failed. Moreover, frequent handling and transportation of hard disk drives inevitably jostles the sensitive mechanical parts in the drives and can only increase the potential for drive failure.

A more advanced and safer method of maintaining forensic images is to upload or copy the forensic image and hash, to a fault tolerant RAID. A RAID is a category of disk drives that employ two or more drives in combination for fault tolerance and performance. The entire purpose of RAID storage is redundancy – if one disc in the array fails, the data remains secure on one of the other redundant discs. Also, unlike a powered-down hard disk drive, a running RAID system can be configured to conduct routine backups to tape archives, which can be stored off-site. This is a useful data recovery backstop in the event of a disaster, such as a flood or fire at evidence storage location. Indeed, the implementation of secure RAID evidence storage appears to adhere to the National Institute of Justice's Office of Justice Programs recommendation that investigators preserve evidence "in a manner designed to diminish degradation or loss." DEPARTMENT OF JUSTICE OFFICE OF JUSTICE PROGRAMS, NATIONAL INSTITUTE OF JUSTICE, CRIME SCENE INVESTIGATION: A GUIDE FOR LAW ENFORCEMENT (2000).

Moreover, a RAID storage system would save space in crowded evidence storage rooms and simplify the process of locating evidence when it is requested. A RAID system would reduce the necessity of having shelves stacked with numerous individual hard drives, each containing images of media seized from different subjects. Forensic images could be stored in folders corresponding to investigation name and number, subject name, and search location, making it easier to locate desired images when they are requested by prosecutors.

When the time comes to use the image at trial, forensic examiners would copy the image back to a hard drive and verify that the hash is unchanged. Hash validation after the image is transferred onto the RAID will ensure that the image stored on and ultimately recovered from the RAID is no different from the original data that was seized. Because it would rely on the already approved hash validation process, a RAID-based storage system should not undermine the authenticity or reliability of the forensic image that is eventually offered into evidence at trial.

Just like any piece of evidence, care would need to be taken to keep the RAID in a secure setting, such as in a locked, limited access server room with no Internet connections. Logging software could be added to the RAID to keep track of access to the virtual evidence lockers stored on it, and forensic images could be stored in password protected virtual lockers on the RAID. And of course, testing should be performed before a RAID-based evidence storage system is put into use.

Prosecutors interested in these and other computer forensic issues and techniques may register for the Computer Forensics for Prosecutors Course taught by CCIPS at the National Advocacy Center. The Computer Crime and Intellectual Property Section and the Cybercrime lab is also available to AUSA's for consultation on computer forensic and other technical investigative matters by calling (202) 514-1026. Many other resources are available on our section's public website, www.cybercrime.gov. In addition, anyone in the Criminal Division or US Attorneys' Offices can find additional resources on our new intranet site, CCIPS Online. Just go to DOJ Net and click on the "CCIPS Online" link.

THE CURRENT SITUATION AND COUNTERMEASURES TO CYBERCRIME AND CYBER-TERROR IN THE REPUBLIC OF KOREA

*Junsik Jang**



I. INTRODUCTION

The Republic of Korea (hereafter: Korea) is a democratic country with a population of 48.46 million (2007). Korea's stance as a powerhouse in terms of information technology is demonstrated by its vast information communication technologies (ICT) production and exports, development of cutting-edge technology, and also the wide use of Internet and mobile telecommunication devices within the country.

When looking at ICT-related statistics and changes which have occurred in Korean society between 2001 and 2007, the number of broadband Internet subscribers increased from 7.81 million to 14.71 million, while the number of Internet users also increased from 24.38 million to 34.82 million. The number of e-commerce transactions also grew between 2003 and 2006, from 7.2 million transactions to 12.8 million. These figures demonstrate that Korea is one of the most successfully connected places on earth, made possible by the strong driving force of the government.

However, the overwhelming number of cybercrimes and security incidents compared to those of neighbouring countries contrast sharply with the positive aspects of Internet usage in Korea. Some may consider the undesirable phenomena inevitable costs accompanying the acceleration of an information society. In contrast, others may attribute these undesirable phenomena to the lack of social and legal control of online activity in Korea. No one reason can explain the situation. Without waiting to identify the cause, the Korean authorities have made a great effort to tackle cybercrime and other attacks, including the threat of cyber-terror. Here I briefly show the current situation and historic changes in cybercrime with countermeasures to prevent, deter, respond and investigate.

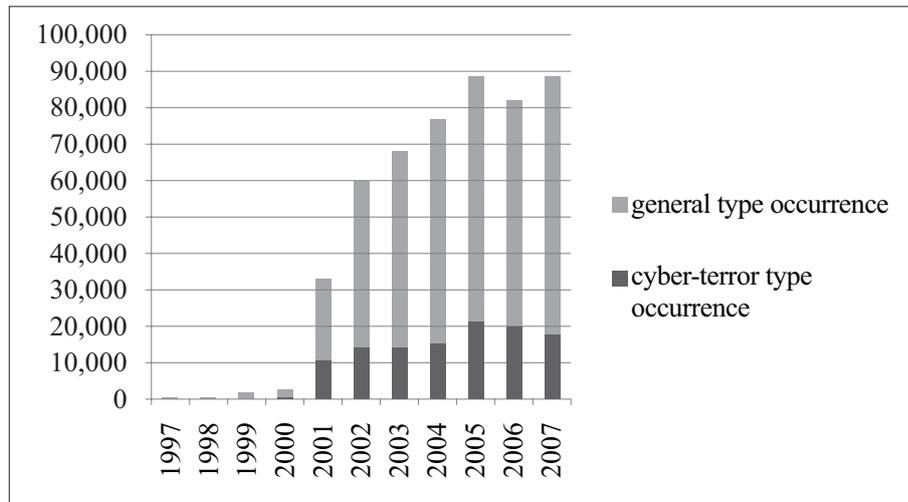
II. THE CURRENT SITUATION OF CYBERCRIME AND CYBER-TERROR IN KOREA

A. Cybercrime Statistics

Korea is one of the most wired countries in the world, but unfortunately statistics show that a variety of cybercrimes also feature in the Korean online environment. Since the Korean National Police Agency (hereafter: KNPA) publicized the first cybercrime statistics in 1997, cybercrime grew at an alarming rate to 2005, as seen in Figure 1. In 2006, we finally saw a decrease in cybercrime for the first time, although this was reversed in 2007.

* Professor/Senior Inspector, Department of Police Science, Korea National Police University, Republic of Korea.

Figure 1: Number of cybercrimes reported to the Korean Police

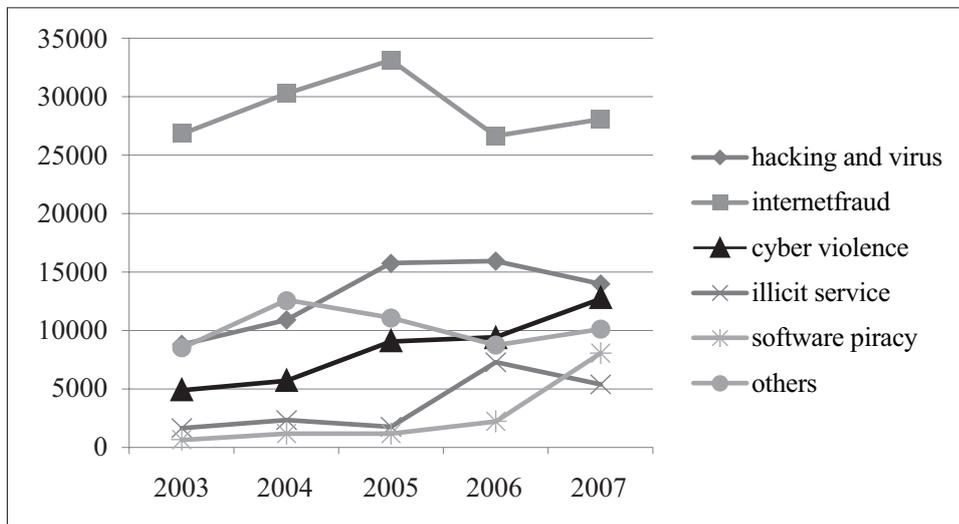


Source : KNPA, March, 2008.

The KNPA has divided cybercrime into two categories;

“Cyber-terror Type Crime” refers to attacks against the information network *per se* such as hacking, mal-ware distribution and Denial-of-Service (DoS) attacks. “General Cybercrime” is crime that uses computers and networks as crime instruments, for example, Internet auction fraud or online child pornography distribution. Each type has several sub-types reflecting the diversity of cybercrime.

Figure 2: Cybercrime occurrence by type



Source : KNPA, March, 2008.

The two most prevalent types of cybercrime are hacking/viruses and Internet fraud. More than half of both types of cases are directly related to online games. Why are there so many cybercrimes? There are a few apparent reasons: digital item trade, anecdotal lack of interest in cyber security, and state-of-the-art Internet infrastructure have all fascinated cyber criminals. Market share of digital items is estimated at more than one billion US dollars in Korea. To improve the situation, legislation prohibiting transactions of virtual money for on-line gambling was activated in 2006.

B. Trends and Issues in Cybercrime

Statistics and cases demonstrate some long-term changes in cybercrime trends. Other changes might occur in a few cases only. These are not exhaustive, but rather representative, examples (cases will be provided separately if appropriate):

- Traditional criminals are hiring tech-savvy cybercriminals internationally. Organized criminal groups have recognized the extent to which they can exploit Internet technology to fulfill their traditional criminal motivations. Their harnessing of technological knowledge makes investigation much harder;
- Mobile Internet devices are replacing Internet cafés as cybercriminals’ preferred method of securing their anonymity;
- Collective opinions form on the Internet, stimulate government and are continued into physical movement;
- Cyber rumours and bullying threaten innocent victims;
- Online banking equipped with Public Key Infrastructure was revealed not to guarantee perfect security of customers;
- Korea is losing its negative reputation as one of the greatest sources of cyber attacks worldwide;
- We need to find a solution to the problem of Chinese hackers who speak Korean and target Koreans;
- Identity theft is at the top of the list of serious cybercrimes in Korea. In recent cases, the personal details of more than 10 million people were stolen;
- Virtual Private Networks for secure communications provide criminals with a cybercrime heaven;
- The majority of criminals are not teenagers.

C. Cyber-terror in Korea

Although the term “cyber-terror” has been in use since the late 1990’s, vagueness of the concept still remains. Distinguishing characteristics of terror are the violent manners and socio-political intentions of the perpetrators. Even though some attacks seemed to be explicit cyber-terror, the two features are not easy to recognize, even for experts in a specific cyber attack. Rather, nowadays, cyber-terror seems to be noted in regard to the information security of governmental and other critical infrastructures.

Table 1: Number of security incidents reported to the National Intelligence Agency

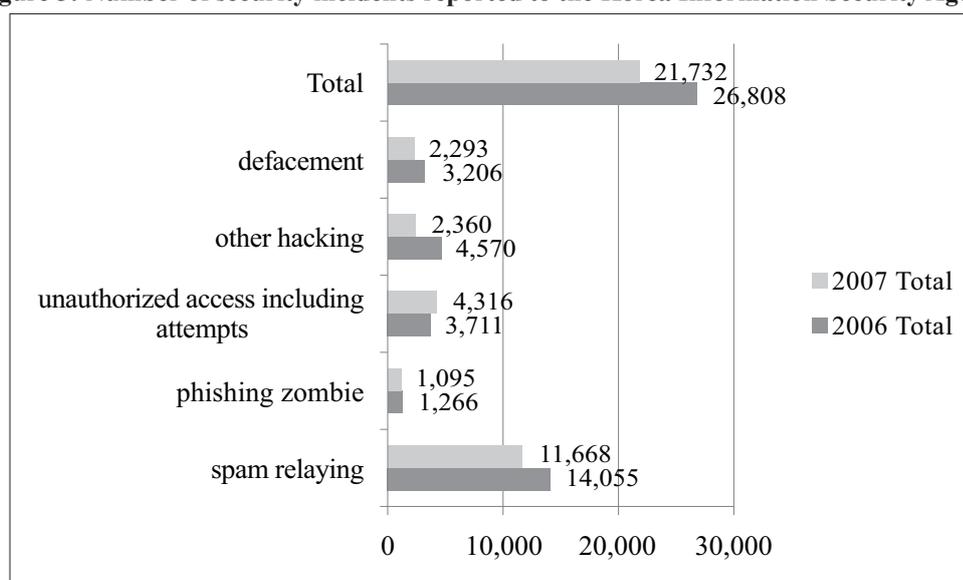
Organization type	Total	Malware Infection	Zombie	Defacement	Impaired or Leaked Data	Others
government	625	498	29	21	55	22
local administrations	3,827	3,583	94	111	24	15
research institutes	198	145	20	8	19	6
education institutes	2,148	1,504	513	91	18	22
affiliated organizations	706	448	85	143	26	4
others	84	16	26	5	34	3
total	7,588	6,194	767	379	176	72

Source: the NIA, April, 2008.

According to the White Paper on National Information Security 2008 by the National Intelligence Agency and Korea Communications Commission, the number of cyber incidents reported in the public domain in 2007 was 7,588 which almost doubled from 4,286 in 2006. The main source of the incidents is infection by Internet worms and viruses.

In contrast, the number of hacking incidents in the private sector which were handled by the Korea Information Security Agency was 21,732. This was a decrease of 18.9% in comparison to 2006.

Figure 3: Number of security incidents reported to the Korea Information Security Agency



Source: the KISA, April, 2008.

Ten important issues concerning cyber security in Korea were selected by the National Intelligence Agency as follows:

- increase in distributed denial-of-service to intimidate for profit;
- promotion of electronic passports containing biometric information;
- incompatibility between Windows Vista and domestic security solutions;
- appointment of the first private information security products accreditation body;
- leakage of personal information from public organizations and huge Internet Service Providers;
- issued certificates for public-key infrastructure exceeded 15 million;
- rapid increase in mobile phone spam;
- User Created Content (UCC) became a new security threat;
- Universal Serial Bus (USB) vulnerability is severe;
- obstinate Voice Phishing.

III. THE LEGAL RESPONSE TO CYBERCRIME AND CYBER-TERROR IN KOREA

A. Overview of the Criminal Justice System of Korea

The Korean legal system combines some elements of European civil law systems, Anglo-American law, and classical Chinese philosophies. Constitutional power is divided into three branches; the administration, the legislature and the judiciary. The constitution provides for an independent judiciary.

The judiciary is composed of the Supreme Court, the High Courts, the District Courts, the Family Court, and the Branch Courts. Since 1988 constitutional challenges go to the Constitutional Court. To become a lawyer in Korea, one must pass the Judicial Examination and complete a two-year training course at the Judicial Research and Training Institute.

The Ministry of Justice belongs to the administration. Prosecutors, who have the authority to investigate criminal cases, belong to the Ministry of Justice. As of March 2008, the total number of prosecutors in Korea, which is growing year by year, is approximately 1,655 and they are assisted by a staff of about 7,524 including investigators, administrative clerks and secretaries. Prosecutors' offices correspond to the counterpart court.

Under the Criminal Procedure Act, the judicial police conduct investigations under the supervision of prosecutors. When most crimes (more than 90%) are recognized, however, the judicial police usually initiate and conduct the investigation. The judicial police consist of general judicial police, dealing with criminal

cases in general and special judicial police, in charge of cases specifically related to railway facilities, forests, fire fighting, the sea, etc. General judicial police belong to the Korean National Police, which has 97,700 full-time employees (sworn-officers and civilian), and about 47,000 auxiliary police, who fulfill their constitutional duty of military service by assisting police. According to the White Paper on the police by the KNPA, the number of crimes reported to the police was 1,719,075 in 2006, including 1,073 murders and 4,838 robberies.

In applying the universality principle to cybercrime, the major international treaty that may become the threshold of domestic laws is the Council of Europe Convention on Cybercrime of 2001. Korea has yet to sign the Convention on Cybercrime, but governmental organizations have begun discussing it.

B. Substantive Cybercrime Laws

Currently, Korea provides for the punishment of cybercrimes in the Criminal Act concerning traditional crimes committed by means of a computer, and in various other laws. The most relevant of these are the Act on the Promotions of Information and Communications Network Utilization and Information Protection, etc. (hereafter: Information and Communications Network Act) and the Information and Communications Infrastructure Protection Act, which are special additions to the Criminal Act.

Besides, the following laws are also relevant: the Framework Act on Electronic Commerce and the Digital Signature Act, concerning e-commerce; the Act on the Punishment of Sexual Crimes and the Protection of the Victims Thereof, concerning cyber-sexual harassment; the Act on the Protection of Juveniles' Sex, etc., concerning child pornography; the Copyright Act or Computer Program Protection Act, concerning on-line copyright infringement; the Act on Promotion of the Game Industry, and the Act on Special Cases Concerning Regulation and Punishment of Speculative Acts, etc., concerning on-line games.

1. Criminal Act (revised in 1995)

The Criminal Act was revised in 1995, accommodating social needs and the regulation of emerging types of crime. Most provisions, except those regarding computer fraud, overlapped with those of the Information and Communications Network Act and the sentences defined in the latter are heavier, so the overlapped provisions are not applicable in most cases. Some features of the Act are:

- Manipulating public electromagnetic records (Art. 227-2, max 10 years) and private electromagnetic records (Art. 232-2, max five years or fine of up to 10 million won);
- Computer fraud (fraud by means of computers): Art. 347-2, max 10 years or fine of up to 20 million won;
- Computer interference with business: Art. 314.2, max 5 years or fine of up to 15 million won;
- Impairment of electromagnetic records: public records (Art. 141.1, max 7 years or fine of up to 10 million won); any other records (Art. 366, max 3 years or fine of up to 7 million won).

2. Information and Communication Network Act (revised in 2008)

- Unauthorized access: Art. 63.1.1 and 48.2, max three years or fine of up to 30 million won;
 - making such attempts is also punishable;
- Transmitting or distributing malicious programmes: Art. 71.9 and 48.2, max five years or fine of up to 50 million won;
 - writing malicious programme *per se* is not punishable;
- Denial-of-service attack (sending a large volume of signals or data for the purpose of hindering the stable operation of a network): Art. 71.10 and 48.3, max five years or fine of up to 50 million won;
- Cyber-pornography (distributing, selling, renting, or openly displaying lascivious codes, letters, sounds, visuals, or films through information and communications network): Art 74.2 and 44.7.1.1, max one year or fine of up to 10 million won;
- Cyber-stalking (repeatedly sending words, sounds, letters, visuals, or films inciting fears and uneasiness to any other person through information and communications network): Art 74.3 and 44.7.1.3, max one year or fine of up to 10 million won;

- Others:
 - cyber-defamation with alleging facts (max three years or of up fine to 20 million won) or openly alleging false facts (max seven years or fine of up to 50 million won);
 - transmission of advertisement information for illegal acts (max one year or fine of up to 10 million won);
 - collecting e-mail addresses without permission by technical means (max one year or fine of up to 10 million won);

C. Procedural Cybercrime Laws

The attitude of the judicial system in the application of law to a new legal issue is to interpret current law or to amend or add new provisions to meet emerging needs. Digital evidence is the most widely used term to depict the new type of evidence consisting of zeros and ones, which signify the greatest challenges concerning criminal procedural law in cybercrime investigations and in court.

Legitimacy of the procedures followed during the collection of digital evidence is the top issue. The most significant method of doing this is a search and seizure operation as defined in the Criminal Procedure Act which is the foundational law for all criminal procedure. There is almost no provision allowing for the statement of digitalized evidence; therefore, the search and seizure issue is basically an interpretation problem. Special procedures, including wiretapping electronic communication to collect specific types of data from specific sources, are defined in a few different laws as outlined below. In court, there are also numerous legal issues.

However, the legal issues concerning digital evidence have been challenged in only a few cases. That is why many investigators are still confused as to how to apply the law in their cases.

1. Search and Seizure

Search and seizure is one of the most important procedures used to acquire evidence. For the search and seizure of electromagnetic records stored in a computer, the cybercrime investigative organizations should first obtain warrants under the legal conditions in force, just like they do in cases of other crimes, unless there exists an exceptional situation, including circumstances in which an emergency arrest is appropriate. Therefore, in response to the Constitution, the suspicion, the scope and the place of the search, as well as the target of the seizure, etc., must be specified by the search and seizure warrant for electromagnetic records.

2. Telecommunication Information

The Telecommunications Business Act (revised in 2006) regulates the procedure of acquiring account and other basic information from the Telecommunications Business Operator. The objects of the request include:

- Names of users;
- Resident registration numbers of users;
- Addresses of users;
- Phone numbers of users;
- IDs (referring to the identification codes of users which are used to identify the rightful users of computer systems or communications networks);
- Dates on which users subscribed or terminated their subscriptions.

The request should be made by way of a written document of a court, a prosecutor or the head of the investigation agency.

3. Transaction Records

Transaction records are defined as “communication confirmation data” in the Protection of Communications Secrets Act (revised in 2008). An investigative authority may ask any operator of the telecommunications business for the perusal or the provision of the communication confirmation data. The records of telecommunications falling under any one of the following items are communication confirmation data:

- The date of telecommunication by subscribers;
- The time that the telecommunication commenced and ended;
- The number of outgoing and incoming calls, etc. and the subscriber’s number of the other party;
- The frequency of use;

- The computer communications or Internet log-records relating to facts of using the telecommunications services by the users of computer communications or the Internet;
- The data on tracing a location of information communications apparatus connecting to the information communications networks;
- The data on tracing the location of connectors capable of confirming the location of information communications apparatus used to connect with the information communications networks.

When an investigative authority officer asks for the provision of the communication confirmation data, he or she must obtain permission from the court, with a document. If urgent grounds exist, he or she shall obtain permission immediately after asking for the provision of the communication confirmation data. Provision of real-time records is executed by the same articles in practice. Asking other parties, including non-public information holders, for the same type of data is executed under search and seizure clauses.

The co-operative obligations of operators of telecommunications businesses for wiretapping and acquiring transaction records and the minimum three-month mandatory period of keeping transaction records are defined in law, but operators are not compelled by any other measure to follow the necessary provisions.

4. Wiretap

Wiretapping telecommunications is strictly confined by the Protection of Communications Secrets Act (revised in 2008). Most importantly, wiretapping can be permitted by a court only for prevention and investigation of serious crimes enumerated in the law. There is no typical cybercrime included in the serious crime types. Therefore, in practice, monitoring, surveillance, or packet capturing for the purposes of cybercrime investigation must be conducted without accessing the content of the communication.

5. Digital Evidence in Court

Electromagnetic records seized by warrant are not made readable until printed. The admissibility of the records thus printed, if submitted as evidence, may be questioned. There is no written regulation on this matter, but the Supreme Court adjudicated on a recent case requiring high level reliability of the programme used, the person who dealt with the evidence, the chain of custody, procedures, etc., to admit authentication and admissibility of digital evidence.

Regarding the identity of the electromagnetic records and the printed document, the person who printed out the electromagnetic records by means of a certain programme should have to testify to the authenticity of the printed document at the trial. In addition, to the extent that the electromagnetic record is deemed identical to the printed document, the latter should be deemed original.

On the other hand, if the document that is made visible and readable by printing the electromagnetic records is used as evidence of a crime, this document may be deemed statement evidence made by extracting a human idea through an electronic method, i.e., hearsay evidence without cross-examination. Therefore, the rule of hearsay evidence under Article 311 of the Criminal Procedure Act and the provisions that follow shall be applied in determining the admissibility of such documents.

IV. THE COUNTERMEASURES TO CYBERCRIME AND CYBER-TERROR IN KOREA

A. Framework for National Cyber Security

The Framework for National Cyber Security has been formulated not by design, rather it has developed by trial and error. A few critical cases, including Slammer Worm hits in 2003 which caused catastrophic interference to country-wide Internet connections, and alleged organizational attacks targeted at major governmental networks found in 2004, served as a crucial momentum to reform past frameworks.

The main focus of the reforms was to integrate distributed resources and capabilities within a single framework and make strict ties between the spots to draw a bigger picture. The current National Cyber Security can be divided into three sub-systems: General Cyber Security responsibility; Critical Infrastructure Protection systems; and Cyber Security Management systems.

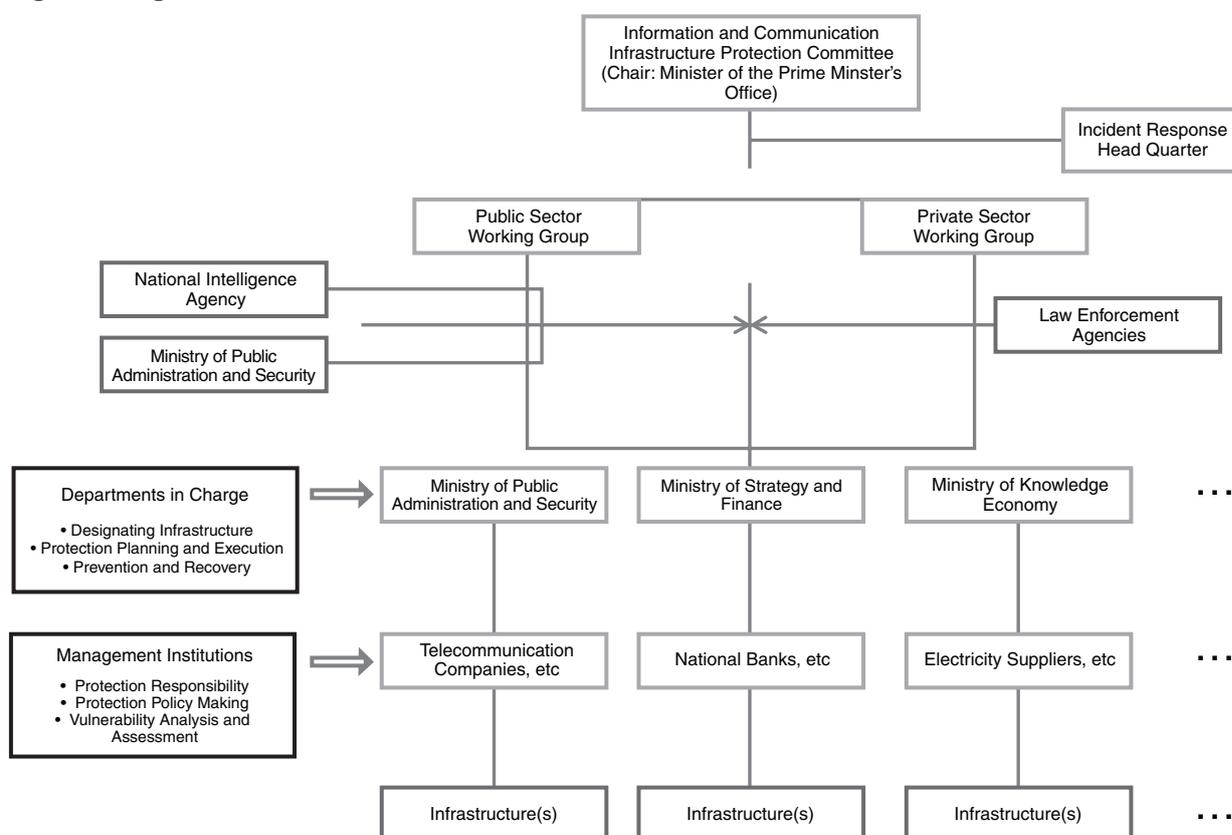
B. General Cyber Security

As an extension of traditional national security management, each governmental organization is responsible for its own assets and affiliated organizations. The National Intelligence Agency Act and the Regulations on Intelligence and Security Affairs Co-ordination (Presidential Decree No. 16211) are legal grounds for this responsibility.

C. Critical Infrastructure Protection

In 2001, Korea enacted the Act on Information and Communications Infrastructure Protection to make a framework to protect highly important networks such as military, communications, finance and so forth. Once designated, a governmental administrative organization that is responsible for the network has to form an effective information security policy followed by vulnerability analysis and assessment. The punishments for an attack and attempt to damage the Critical Infrastructure are more severe than those for similar actions directed towards the other systems and networks.

Figure 4: Organization Chart for Critical Infrastructure Protection



The chairman of the Information and Communication Infrastructure Protection Committee, which directs government organizations which manage infrastructure under its supervision, answers to the minister of the prime minister's office. Once a major incident happens in any critical infrastructure, a temporal incident response headquarters is set up. Law enforcement agencies are responsible for investigation of the incidents.

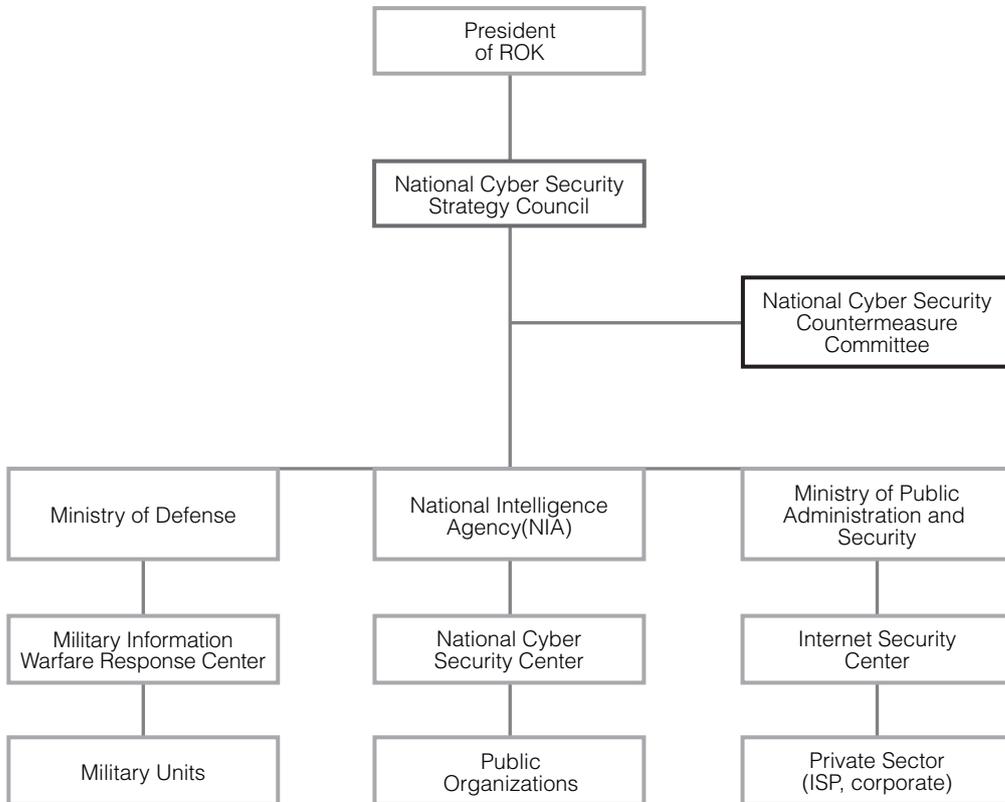
1. Cyber Security Management

A Cyber Security Management system was established to enhance mainly the capability to respond to incidents in three comprehensive parts; public, private and military. Major operations of Cyber Security Management are:

- Integration and implementation of national-level cyber security policies;
- Cyber-security proactive actions;

- Collecting, analyzing and disseminating information on cyber threats;
- Emergency response, investigation, and recovery support during intrusion incidents.

Figure 5: Organization Chart for Cyber Security Management



Among these agencies listed above, investigation is responsibility of law enforcement agencies. Presidential Directive No. 141, the National Cyber Security Management Regulation, is the main legal source. Several important organizations implement the policies directed by each central administrative agency.

(i) National Cyber Security Center

The National Cyber Security Center is the central point of government for identifying, preventing and responding to cyber attacks. The NCSC is responsible for analysing cyber threats and vulnerabilities and disseminating threat warning information.

(ii) Military Information Warfare Response Center

The Military Information Warfare Response Center is responsible for protection of military infrastructure and response against attacks on the network.

(iii) Korea Internet Security Center

The Korea Internet Security Center is one of the divisions of the Korea Information Security Agency (KISA). The mission of the KISC is collecting information and detecting attacks, major network monitoring, disseminating alerts, incident analysis and technical support, mainly for the private sector.

(iv) Other Specialized Organizations

- National Security Research Institute: Researching and developing technologies concerning cryptography, counter-attack, and other security technologies;
- Korea Information Security Agency: Reacting to security threats properly at the national level, and providing integrated and systematic information security services. It includes the Internet Security Center;

- Electronics and Telecommunications Research Institute: Non-profit government-funded research organization that has been at the forefront of excellence on information technologies;
- Financial Security Agency: Being established by entire financial industry to provide proper security service for member corporations and customers.

2. Prosecutor as an Investigative Authority

Not only are public prosecutors responsible for prosecution, but also they have authority to investigate all kinds of crime through investigative units within prosecutor's offices. The public prosecutors' offices of Korea have a hierarchical structure consisting of the Supreme Public Prosecutors' Office (SPO), five High Public Prosecutors' Offices (HPPO), thirteen District Public Prosecutors' Offices (DPO), and forty branch offices of the District Public Prosecutors' Offices. Among them, the SPO and the Seoul District Public Prosecutor's Office have units designated for high-tech crime investigation, including cybercrime. Those units are the High-tech and Financial Crimes Investigation Division in the SPO and the High-tech and Financial Crimes Investigation Department in the Seoul District Public Prosecutor's Office.

(i) *Investigation by Prosecutors*

Most cybercrime investigations are initiated by the police. Prosecutors conduct continuing investigation after the transfer of each case to decide whether or not to file for prosecution. Prosecutors also conduct investigations *ex officio*. The cases initiated by prosecutors are commonly distinguishable from those investigated by police. Prosecutors tend to focus on cases having a bigger social impact. Most of them are not dynamic but static. Theft or leakage of trade secrets is a typical investigation initiated by prosecutors. This creates natural divide in types of crime investigated by the police and prosecutors.

The High-tech and Financial Crimes Investigation Division is also responsible for co-operation concerning Internet crime and is the contact point of the G8 24/7 High-Tech Crime Network in Korea.

(ii) *Digital Forensics for Prosecutors*

Digital forensics is a key element in solving a variety of types of crime today. The effectiveness of digital forensics have been proven in a number of financial, high-tech, corruption cases. To integrate and improve digital forensic capability, a comprehensive digital forensic lab is under construction.

3. The Cyber Terror Response Center and Cyber Policing in Korea

The Korean National Police has devoted its efforts to securing safety in cyberspace with the establishment of the Cyber Terror Response Center in 2000, which was initiated from establishment of the Computer Crime Investigation Squad at the National Police Agency in 1997.

In regard to the outstanding activities gaining renown in the global law enforcement society, the Korean government selected the brand name "*Cyber cop NETAN*", a compound of "Net" and "An", meaning "safety" in Korean, as one of the renovation symbols of cybercrime investigation in 2007.

(i) *Organization and Human Resources*

The Cyber Terror Response Center (CTRC) is the cyber division of the Korean National Police Agency (KNPA), operated within the Agency's Investigation Bureau. The object of the CTRC's investigation includes, but is not limited to, cyber attacks against the Republic of Korea and its people. It is headquartered within the KNPA main building; at present the Center's administrative wing commands and controls all cybercrime investigation teams nationwide, which are installed in each of the investigation functions of the 16 provincial police agencies and 238 local police agencies. The CTRC consists of six teams:

- Administration and Co-operation Team: Plans policies against cybercrime, training and co-ordination of domestic and international co-operation;
- Three Investigative Teams: Conduct major, national-level cybercrime investigations, including cyber-terror type attacks;
- Investigative Planning Team: Receives crime reports, analyses trends of cybercrime and plans a nationwide crackdown operation on special issues;
- Technical Assistance Team: Researches and develops investigative techniques, provides digital forensic services to all law enforcement agencies through the Digital Forensic Center.

As of July 2008, about 900 sworn officers and civilians are exclusively dedicated to cybercrime investigation and support. The majority are police officers working as cybercrime investigators. Among them, 168 officers have been recruited through a special hiring process for ICT specialists possessing adequate academic education and work experience. Most forensic examiners in the Digital Forensic Center are qualified civilian experts.

(ii) *Cybercrime Response Activities*

(a) Strengthen investigation capability with professionalism

The top priority to enhance investigative capability is to encourage specialized personnel to join and train. The CTRC provides initial training, domestic and international continuing education, and on-the-job training.

(b) Satisfying citizens by rapid responses and a strategic approach

A 24/7 complaints procedure which receives and responds to complaints through an exclusive website and a cybercrime call centre linked with the police emergency network are being maintained. The reports are saved in a data warehouse called e-CRM (Customer Relationship Management) and are analysed by dedicated specialists.

(c) Domestic co-operation and crime prevention activity

No fewer than 125 private enterprises and 85 organizations including academia and non-governmental organizations are tied with a single contact point and hotline. Educational activities and an alert system are playing a crucial role in preventing cybercrime and reducing the number of teenage criminals. *Nuricops*, civilian supporters, are not only enhancing mutual understanding, but they are sometimes helpful enough to notify police of unknown but important events on the net.

(d) International co-operation in cybercrime investigation

The CTRC has hosted several international events related to cybercrime and cyber-terrorism, including the Annual Symposium on Cyber Terror. Instructors are frequently dispatched for international training programmes or to deliver specially designed instruction to requesting countries. Through the Interpol network or other channels such as the Cybercrime Technology Information Network System (CTINS), the CTRC maintains a hotline with more than 110 countries. The CTRC has so far contracted a Memorandum of Understanding (MOU) with leading agencies on cybercrime investigation in 15 countries.

BEST PRACTICES IN CYBERCRIME INVESTIGATION IN THE REPUBLIC OF KOREA

*Junsik Jang**

I. INTRODUCTION

The Internet and the rapid deployment of information and communication technologies in recent years have changed historic trends and practices in criminal investigation. This has created a tremendous challenge for law enforcement to develop the capacity to confront transnational crimes and follow evidence trails. Among the obstacles were legal, technical and operational challenges, but these are not the total extent of the difficulties faced; rather, they have been recognized as the main issues to be addressed in order that law enforcement agencies are able to meet the emerging challenges of cybercrime.

When police conduct a cybercrime investigation, they are encouraged to refer to the following several sources of regulations and guidelines:

- **National Law:** Both of the main procedural barriers and weapons are produced by national criminal procedural laws. Without meeting the legal requirement, investigative activities would be considered illicit and the admissibility of evidence acquired will be denied. As previously mentioned, several laws regulate directly collecting cybercrime evidence, including the Criminal Procedural Act, the Protection of Communications Secrets Act and the Telecommunications Business Act.
- **International Law, Standards and Guidelines:** There are such conventional frameworks as Mutual Legal Assistance Treaties and organizations such as Interpol which are useful for international investigative co-operation considering the borderless nature of cybercrime. Even without compulsory regulation, pursuing international legal references is considered desirable.
- **Domestic Guidelines and Manuals:** To provide practitioners with a practical reference for action, the Korean National Police Agency has developed several guidelines and manuals.

Table 1: Cybercrime manuals and guideline

Title	Scope	Contents
Cybercrime Investigation General Manual (classified)	All members of police	<ul style="list-style-type: none"> • Cybercrime definition, category • Preliminary Investigation • Processing Crime Scenes • Tracing, Search and Seizure • Evidence Handling • Interview and Interrogation • Checklists • Cybercrime Laws
Internet Tracing (classified)	Cyber Investigators (mandatory) Other police members (recommended)	<ul style="list-style-type: none"> • Foundation • Internet Protocols and Addressing • Web, e-mail, Other service tracing • Subscriber's Line • Real-time tracking and tools

* Professor/Senior Inspector, Department of Police Science, Korea National Police University, Republic of Korea.

Digital Evidence Analysis (classified)	Cyber Investigators (mandatory) Other police members (recommended)	<ul style="list-style-type: none"> • Foundation and Process • Windows Analysis • Unix System Analysis • Network Analysis • Tools (Encase, ILook, Final Forensics, X-ways)
Cybercrime Investigation Techniques for Its Types (classified)	Cyber Investigators Other police members (recommended)	<ul style="list-style-type: none"> • Hacking and Virus Investigation • Illegal Contents Distribution Investigation • E-commerce Investigation • Complainants Counselling Q&A
Standard Guidelines for Handling Digital Evidence (unclassified)	Public (recommended)	<ul style="list-style-type: none"> • Collecting Evidence • Transferring and Requesting Examination • Evidence Analysis • Writing Reports
Digital Forensics Technical Manual (classified)	Cyber Investigators (mandatory) Forensic Examiners (mandatory)	Standard Procedure for: <ul style="list-style-type: none"> • Collecting Evidence • Disk Recovery • Hacking and Malicious Code Analysis • Web Analysis • E-mail and Instant Messaging • Database • Multimedia • Crypt Analysis • Detecting Steganography • Communication Network Analysis • Mobile Device Analysis Checklists

II. INITIAL INFORMATION GATHERING

Investigation generally begins by gathering initial information from a variety of sources. Investigators have to understand the characteristics and develop the sources. Some victims do not want to reveal the damage they have suffered out of consideration for their reputation and for other reasons, or even do not recognize the damage caused to them. On the other hand, for example massive worm infection, others report the same information repeatedly which may make investigative efforts redundant.

Information gathering to fight cybercrime should be strategic. Through their experience, the Korean National Police Agency developed some criteria to alleviate the complexity of cybercrime which should be taken into consideration when developing info-gathering mechanisms.

- Timeliness
- Scope and Impact
- Technical Level Needed
- Proactive vs. Reactive
- Machine-based vs. Human-based
- Attack by Opportunity vs. Attack by Target.

A. Web-based Complaints Report and Counselling Service

To promote convenient complaint systems and to reduce processing costs associated with conventional reporting methods, the Korean Police adopted a web-based crime report system in 1999. But, soon after,

cybercrime investigators realized that the system could be designed so as to collect more information concerning further investigation and to find additional valuable information by analysing multiple complaints. For this, they decided to set up an independent cybercrime report system. Because a similar idea was applied in business, named Customer Relationship Management (CRM), the newly launched system was called e-CRM when it was established in 2003.

Today, the e-CRM system is the greatest resource of cybercrime information. By simultaneously analysing massive reports, the authorities can ascertain pattern, commonality, and level of threat. If more proactive, intensive, and technical investigation is needed, an investigative team of the CTRC is assigned to investigate the case. Drawing a bigger picture with minute events is becoming more and more important.

B. Intelligence Activities

Undercover operations, decoys, and other intelligence activities are easier on the Internet where anonymity can be secured. Keeping accounts for websites and as many other communities as possible is highly recommended.

Traditional intelligence activities should not be neglected. People tend to trust more someone who they have met in person rather than a total stranger. System managers and other personnel in corporations are potential great informers in important cases. Maintaining contact points and systematic management seems one of the most important tasks in fighting cybercrime. Gathering information from international resources is desirable and is encouraged.

C. Honeypots

A honeypot (or honeynet) is a system or network that has intentional security vulnerabilities to gather information and/or evidence in case of access by attacker(s). If it is not designed well, legal challenges may arise. Therefore, a honeypot is usually built during a case investigation.

III. TRACING AND IDENTIFYING CRIMINALS

People take advantage of the anonymity of the Internet to facilitate their digital life. Abuse of the anonymity of the Internet by criminals is a predictable but inevitable dark side in an information society. The difficulty of tracing and identifying criminals is one of the main hurdles that cyber investigators meet every day. On the other hand, techniques used for tracing criminals can be applied to locating non-cybercriminals as well. The Korean Police has been making efforts to develop tracing techniques and the products are being widely used for every kind of criminal investigation.

Tracing is rarely confined to a single action, but rather a series of tedious operations. It is not odd if an investigator sends dozens of written requests seeking legal permission from prosecutors and courts in an investigation. To minimize the burden, investigation should be planned strategically and tactically. In many cases, critical information can be provided by service providers, including Internet Service Providers (ISP). Needless to say, maintaining intimate relationships is important.

Unfortunately, getting helpful information from service providers is frequently difficult for many reasons. An investigator needs technical or human skills to overcome such difficulty. Experienced investigators in the CTRC who know the possibility and the limitation of each technique are available to answer questions concerning tracing matters.

A. Basic Communication Information given by Service Providers

Legal procedures were explained in the previous paper. It usually takes more than a day to complete the whole process unless there is an emergency situation. That is why time management is important. Otherwise, cybercrime investigation will be a chain of requests for communication information with a risk of the case failing. The list of service providers is available for police officers with the help of their own collaborative colleagues.

Some service providers have implemented a real-time notification scheme via an investigator's mobile phone or closed webpage to provide the information possibly containing the cell location of a mobile phone, log-on and log-off status, IP address, etc.

B. Subscriber’s Network Service

To ultimately discover the location and identification of a target, cyber investigators often have to get a subscriber’s information from the Internet Service Providers (ISPs) because many users access the Internet through a subscriber’s network service. The possibility of getting information from an Internet Service Provider depends on the type of service, and the logging policy. Sometimes investigators find out the physical location they want to know without further information, because the ISPs are not helpful without proper logging. The variety of services makes it difficult. Today, rapid propagation of mobile Internet use is a critical issue. Table 3 shows the past and present subscriber’s networks services.

Table 2: Subscriber’s network services in Korea

Type	Service	Usage	Possibility of Tracing by ISP’s information
Wire SNS	Serial Line Internet Protocol/Point to Point Protocol (SLIP/PPP)	Obsolete Very Low	Very High
	Integrated Services Digital Network (ISDN)	Obsolete Not Available	Very High
	Asymmetric Digital Subscribers Line (ADSL)	Prevalent	Depends on ISPs’ authentication method Very High or Low
	Very high Data rate Digital Subscribers Line (VDSL)	Prevalent	Low
	CABLE	Prevalent	Depends
	Power Line Communication (PLC)	Obsolete Not available	N/A
Wireless SNS	Wireless Local Loop/Broadband Wireless Local Loop (WLL/BWLL)	Not Prevalent	High
	Wireless Local Area Network (WLAN)	Prevalent	Depends on circumstances
Mobile SNS	IS-95ABC/ Broadband Wireless Local Loop (IS-95ABC/EVDO)	Decreasing	Circumstantial
	Wireless Broadband Internet (Wibro)	Increasing	
	High Speed Downlink Packet Access (HSDPA)	Not prevalent	
Satellite SNS		Rarely used	High

C. Internet Cafés

Once the target of a trace action can be identified by an online user account or nickname, there is a possibility to capture the suspect before he or she leaves the Internet café. It is effective when real-time tracking is available. Fortunately, the Korean National Police cover the entire country and a dispatch system using police radio make it possible for the responders, typically patrol officers, to reach any Internet Café within 10 to 15 minutes. The fact that this really works has been proved repeatedly, including a case of apprehension of a bank robber who gambled online in an Internet café after committing the robbery.

Otherwise, investigators may find out other clues through examination of the PC used, witnesses, etc. Cyber investigators sometimes forget the importance and potential of physical traces. Traditional trace evidence such as hair, print and fiber may have to be collected for further investigation. Investigators also have to be cautious that many PCs in Internet cafés are equipped with hardware or software-based hard disk recovery tools requiring more careful treatment.

D. IP Laundry

Criminals want to be shielded behind computers to block tracing back by investigators. Since a computer is identified by an IP address, blocking is often called IP laundry. IP laundry is more common for average criminals and this is a universal problem in law enforcement. There is no perfect criminal haven, but, depending on the technique used for IP laundry, some tracing methods are extremely difficult to adopt and very time-consuming. Basic IP laundry techniques are categorized as follows:

- **IP concealing:** Hides the existence of original systems used by a perpetrator by a detour using an intermediate system through a specific Internet service such as proxy, secure shell, socks, VPN, remote control, and so on;
- **IP forgery:** Changes source IP address in packets to conceal and deceive origin. Address Resolution Protocol (ARP) spoofing is usually implemented to intercept communications, called sniffing, but also can be used to hide origin;
- **Domain Name System (DNS) altering:** Does not conceal or change IP addresses of the source computers. Instead, it often changes the source computers themselves, typically zombies, by the using of the functionality of dynamic DNS.

Techniques to defeat IP laundry vary. Some of them are not intentionally documented in the manual to preserve their operational effectiveness. Proper consultation may be needed from a technical support of the CTRC.

E. Tracing Method for Individual Internet Services

- **E-mail:** Due to prevalent use of header forgery, mail server investigation and proactive e-mail tracking is frequently used.
- **P2P:** The CTRC provide automated well-known network-based P2P tracking software.
- **Website users and operators:** Should be tactical enough, especially when tracking operators.
- **Web based short message service (SMS) sender:** Investigators need a full understanding of the service mechanism. It is normally a tedious procedure.
- **Mobile device holder:** If a mobile device is chosen by a criminal to avoid tracking, locating it usually is extremely vexing work. Some software and hardware are available for this purpose from the CTRC.

IV. PRESERVING AND COLLECTING EVIDENCE

Scene processing has to be completed by experienced and qualified investigators or examiners, but they are not always available. In any case, coping with the standard procedure and technique proposed is important. Recently proposed standard procedure for cybercrime scene processing is defined in the Digital Forensics Technical Manual 2007. This standard is applicable for typical digital evidence collecting situations concerning computer systems and peripherals:

- **Photography and Sketching:** Taking pictures of the front and rear shots of object system, peripherals, monitor and other necessary images;
- **Volatile Information Gathering:** Volatile information needed is enumerated in the manual. The Cyber Terror Response Center provides automated tools in a CD called "*Podomi*" (meaning police helper) which is highly recommended if the investigator is not fully qualified to select alternatives;
- **Shutting Down:** The decision of how to shut a system down should depend on the operating system being used. Roughly, server systems follow a normal shut down process and personal computers are unplugged. The details are defined in other parts of the manual;
- **Acquiring Physical Media:** Seizing whole systems is principally recommended. Exceptionally, storage media such as Hard Disk Drive (HDD) can be seized separately. In any case, system time should be

previously recorded in comparison to Korean Standard Time (KST);

- **Labelling and Packaging:** an adequate label has to be attached to each item, including case number, collector, date and time, location, specification of the item, serial number if possible, etc. HDD and other electro-magnetic media should be packed individually using proper bags or boxes;
- **Documentation:** Chain of custody, process of scene investigation, lists of evidence to give the owner and a Q & A sheet should be documented and preserved.

V. DIGITAL FORENSIC ANALYSIS OF EVIDENCE

It is principle that all digital media be examined and analysed by a qualified forensic examiner, but there are too many items that need forensic investigation and the number is rapidly increasing. Consequently, there is an explicit gap between needs and current status. This tends to produce backlogs and sometimes leads to field investigators abandoning requests for forensic service, which can have unexpected consequences. Cyber investigators are trained to examine digital evidence to some extent. Beyond that, forensic service is requested of high level police agencies.

The Digital Forensic Center in the CTRC is the biggest and the most comprehensive digital forensic laboratory in Korea. Several provincial police agencies have digital forensic labs and the number is increasing. The active service is listed in the Digital Forensics Technical Manual published in 2007. However, considering the rapid change in ICT environment, the scope of service request is not confined within the current service list.

Before the establishment of the DFC in 2004, forensic investigation had been conducted by investigators who had ICT backgrounds or as a form of technical support without strict regulation. The number of electromagnetic media requested for forensic service was only 274 in 2005 and it increased to 2,984 in 2007. However, it is believed that the actual needs much exceeded the number of the received media, because many requests are being refused by service providers due to the lack of resources or abandoned by investigators considering the current situation. Increasing media size is also problematic. The average hard disk drive size received for forensic examination was 68.33 gigabytes and increased to 89.14 gigabytes in 2007. Strengthening forensic capability is one of the most urgent problems that the CTRC and cyber police are confronting. Research on 99 sample cases showed that the average waiting period until returning the item, that is the time used to complete a forensic request, was 3.24 days per item.

Forensic labs are required to gain accreditation from a qualified body. There are many unsettled issues concerning digital forensic lab accreditation. The DFC is preparing to apply to domestic or international accreditation bodies.

VI. INTERNATIONAL CO-OPERATION

Although much international co-operation does not achieve tangible output such as apprehension of domestic suspects, Korean investigators, especially those working at the Cyber Terror Response Center, are very proactive in responding to requests from foreign law enforcement agencies. Needless to say, it is because they know the importance of international co-operation and the fact that they may also need similar help by the requesting country someday.

As a result, most of the international co-operation cases are investigated by the Cyber Terror Response Center. If it seems appropriate considering time and difficulty, a request can be transferred to local police, and more time will be needed to respond. Once a request is delivered to an investigator, he or she opens a new domestic case based on the information in the request. It is possible because the majority of requests include domestic suspect(s), victim(s), or a location where a crime was committed. For this, the request should contain a detailed description of the case and the reason that an investigation is needed in Korea.

The most active channel for international cybercrime investigation is the International Criminal Police Organization (hereafter: Interpol). But there are other channels which have respective strengths and weaknesses.

A. Mutual Legal Assistance Treaty (MLAT)

MLATs are the most powerful legal tool. In practice, however, this is rarely used for police investigation of cybercrime because of the length of time needed to complete the whole process.

B. G8 24/7 High Tech Contact Points

The G8 created in 1997 a new mechanism to expedite contacts between countries to enhance and supplement traditional methods of obtaining assistance in cases involving networked communications and other related technologies. The system is maintained by the Supreme Prosecutor's Office in Korea and is not usually available for the police. Because the majority of cybercrime investigations are conducted by the police, the usability of the mechanism is low.

C. Interpol

Interpol, with 186 member countries, is the most commonly used channel for international cybercrime investigation co-operation in Korea. Hundreds of cases are dealt with annually through the Interpol channel. The National Central Bureau, a single contact point in each member country, possesses a 24/7 network and is staffed by highly trained officers.

However, the effect of co-operation through the Interpol channel seems limited because it is not obligatory, but voluntary, and is conducted without a legal basis which would enable the use of more effective methods, including the exchange of physical evidence. In addition, inadequate knowledge of technical matters on the part of the officers of the National Central Bureau often hinders communication between investigators.

D. Liaison Officer (24/7 Contact Point)

To address international co-operation matters, the Cyber Terror Response Center has designated liaison officers. They also maintain the National Central Reference Point (NCPR), proposed by Interpol, which is designed to counteract the disadvantage of traditional co-operation by the National Central Bureau. Typically, once an initial request is delivered to NCB, ongoing co-operation can be conducted via the NCPR through e-mail and/or telephone.

E. Cybercrime Technology Information Network System

The Cybercrime Technology Information Network System (CTINS), operated by the Japanese police, is a network system connecting law enforcement agencies in the Asia-Pacific region. The CTINS is a good instrument to share technical information concerning cybercrime, but is rarely used for specific case investigations.

F. Human Networking

Sometimes, investigators prefer contacting counterparts directly to exchange more detailed information faster. Once acquainted, this unofficial networking would be more smooth but still powerful. The CTRC encourages its investigators develop its human networks.

PARTICIPANTS' PAPERS

THE CRIMINAL JUSTICE RESPONSE TO CYBERCRIME

*Elcio Ricardo de Carvalho**

I. INTRODUCTION

The objective of this paper is to be a comprehensive discussion of the current situation in Brazil regarding the 140th Course's main theme, "The Criminal Justice Response to Cybercrime", following the guidelines provided by the course advisers.

Whenever mentioned, the Convention on Cybercrime refers to the *Convention on Cybercrime of the Council of Europe (2001) (ETS 185)*.

II. ISSUES AND MEASURES CONCERNING CYBERCRIME INVESTIGATION

A. Initial Information Gathering

The Brazilian Federal Police created an e-mail box to which any Internet user can send notices about cybercrimes. However, the great volume of messages, combined with the generally poor quality of the information itself (for instance, not including enough data to allow the identification of the perpetrator or reporting actions not defined as criminal offences under Brazilian law), has made this communication channel fall short of its intended objective.

Some non-governmental organizations dedicated to combating child pornography take a similar approach, triaging the notices received and complementing it with field work, passing this higher quality information to law enforcement. Although the law enforcement agencies are allowed to be more proactive, in general they lack human resources to do this kind of job. Moreover, Brazilian law limits their actions to some degree. For example, if an agent enters a chat room pretending to be a teenager and a paedophile tries to seduce this persona, he cannot be charged based on this action because Brazilian law considers it an impossible crime, i.e., someone trying to seduce a teenager that does not exist. Or if, in an Internet forum, an undercover agent asks for and receives child pornography material, the sender cannot be charged for the sending. Since it was requested by the agent, it can be argued that the situation was a set-up.

In spite of the difficulties presented, some initiatives to actively patrol cyberspace have been successful, such as the monitoring of peer-to-peer networks, which will be discussed in more detail later in this document.

B. Tracing and Identifying the Criminal

In the process of tracing the origin of a cybercrime and trying to identify the perpetrator, major obstacles arise when it comes to getting access to information maintained by service or access providers, such as connection logs. These obstacles have two different origins, according to the location of the providers:

1. When the Provider is in Brazil

Providers in Brazil are not obligated by law to keep any kind of connection logs. Also, due the lack of proper legislation, most providers deem connection logs and subscriber information to be protected by privacy laws, therefore requiring a court order to disclose this type of information.

The combination of this legal state of affairs with the lack of promptness by the Brazilian judicial system often leads to situations where, when the court order finally reaches those responsible for the information, the short period of time during which the providers decided to keep the logs has already elapsed.

* Federal Criminal Expert First Class, Technical-Scientific Directorate, Federal Police Department of the Ministry of Justice, Brazil.

In many cases, even when the first contacted provider is able to supply the information in a timely manner, the investigation path leads to another provider, restarting the whole legal process to obtain the data. For example, an IP address obtained from a webmail service provider has to be correlated to a physical address by the access provider, and this request will require a different court order.

2. When the Provider is Located outside Brazil

Although many of the major service providers, such as Microsoft and Google, have offices in Brazil, they usually claim that their central offices, located in foreign countries, are the real retainers of the requested information. Hence, to obtain the required logs, the investigator has to go through processes as established by Mutual Legal Assistance Treaties or petition a foreign court by means of a Letter Rogatory. According to practical experience, both alternatives take longer than is acceptable in investigations dealing with ephemeral information.

A major step to overcome such obstacles was taken in July 2008, when Google's Brazilian office signed an agreement with the Public Attorney's Office in São Paulo, assuming the responsibility for, among others, accepting court orders from Brazilian judges regarding information owned by Google's central office. This commitment should make smoother investigations involving Google's two most popular services in Brazil, namely GMail, a webmail service, and Orkut, a social network.

Microsoft, another big player in the Brazilian Internet market with services such as MSN Messenger and Hotmail, has a tradition of accepting and forwarding to their central office the court orders they receive, even though, not having signed any formal document and not being bound on this subject by Brazilian laws, they reserve to themselves the right to decide what requests will be complied with.

C. Preserving and Collecting Evidence

1. Expedited Preservation of Stored Computer Data

Currently, there are no specific laws in Brazil regulating expedited preservation of stored computed data as defined by Article 16 of the Convention on Cybercrime.

The Brazilian Internet Management Committee ("*Comitê Gestor da Internet no Brasil*" in Portuguese), an entity composed of government, private sector and academic community representatives, has issued a recommendation to Internet Access Providers to store access and connection logs for at least three years. This recommendation does not have the force of law and there are no penalties for providers that do not comply with it.

Also, the Brazilian Association of Internet Service Providers, ABRANET, has created a self-regulation code that stipulates six months as the minimum period of time the service providers should maintain the access logs. As a recommendation from the Brazilian Internet Management Committee, this directive does not have the force of law.

As a consequence, the Brazilian law enforcement agencies have no means by which to enforce or require the preservation of stored computed data. They have to rely on the individual policies of each service or access provider.

2. Expedited Preservation and Partial Disclosure of Traffic Data

The expedited preservation and partial disclosure of traffic data, as defined by Article 17 of the Convention on Cybercrime, suffers in Brazil from the same legal deficiency described in the previous section of this paper. As a matter of fact, for the purpose of preservation and disclosure, the current legal situation makes no distinction whatsoever between traffic data and generic stored computed data. Usually a court order is necessary to obtain this type of information.

3. Production Order

There are no provisions in Brazilian law allowing a law enforcement agency to issue an administrative order requiring a person or a service provider to submit computer data or subscriber information, in the form described by the Article 18 of the Convention on Cybercrime. Moreover, some interpretations of the current privacy laws consider this kind of information to be protected, requiring a court order before it can be disclosed to the investigator.

Consequently, when it is necessary to obtain such data, the investigator has to go to court and use the same legal tools designed to get hold of traditional, non-cybercrime related, privacy-protected information.

4. Search and Seizure of Stored Computer Data

The empowerment to search and seize stored computer data, as stated by Article 19 of the Convention on Cybercrime, is, to some extent, incorporated into the Brazilian legal system.

While the current laws do not differentiate between stored computer data and data contained on non-digital media, an investigator can obtain a court order to access a computer system, a storage medium and the data stored therein, as required by paragraph 1.

However, and precisely because of the absence of differentiation mentioned above, court orders to access computer systems usually refer to the physical locations where the computer systems are installed. Consequently, if during a search it is found that the data sought is stored on another computer, located on a different site but accessible from the initial system, it is necessary to obtain another court order for this new computer system. There are no provisions for expeditiously extending the search to the remote system, as required by paragraph 2.

The seizure of computer data, as described by paragraph 3, is in effect a consequence of the court-ordered search and is usually authorized by the same warrant. Nevertheless, the power referred to in subparagraph (c) is not taken into account by Brazilian law due the lack of definition of stored computed data and its integrity. Also, the command to render inaccessible or remove computer data, as described in subparagraph (d), is usually contained in a proper court order directed to the owner of the computer system wherein the data is resident. There are no explicit provisions for the authority conducting the search to execute those actions.

More importantly, paragraph 4, “(...) to order any person (...) to provide, as is reasonable, the necessary information”, may directly conflict with a constitutional principle in Brazil and many other countries: the privilege against self-incrimination (*Nemo tenetur se detegere*). Although it would be a very useful power for investigation, and in some cases the only way to get access to vital information, it can be foreseen that in Brazil deep cultural and legal changes would be required to comply with paragraph 4, especially taking into account the conditions and safeguards detailed in Article 15.

5. Real-Time Collection of Traffic Data

The real-time collection of traffic data, as defined by Article 20 of the Convention on Cybercrime, does not exist in the Brazilian legal system. Furthermore, the most common interpretation of the law considers traffic data to be protected by privacy laws. For all purposes, it is as hard to obtain as the content data itself.

Also, the text of paragraph 1 (b), “compel a service provider, *within its existing technical capability*” leads to some practical issues, discussed in depth in the next section.

6. Interception of Content Data

The interception of content data is probably the most sensitive issue in cybercrime investigation. Not only must its implementation always be weighed against the seriousness of the offence and the right to privacy, but, as the technology evolves and the information and communication technologies become more widespread, the interception of content data tends to become the only possible method to obtain vital information to support the investigation, prosecution and adjudication of cybercrimes.

In Brazil, the laws created to administer the interception of telecommunications’ content seem to have taken into account only classical telephonic communications. Nevertheless, communication via computer systems is mentioned in the law, but the legislature did not bear in mind the fundamental differences between the interception of voice and the interception of computer data.

(i) *Complexity*

The interception of computer data in a network like the Internet is several orders of magnitude more complex than the interception of regular phone lines. The communication between two given points can take

multiple different routes and involve any number of network providers around the globe, each one of them capable of intercepting an unencrypted communication.

(ii) The Nature of the Data

While phone communications are usually in the form of audible sounds, the computer data intercepted on a network necessarily require additional processing and possibly the help of third parties to extract the information from the raw data. In fact, the interception itself typically is only a minor part of the problem.

For example, when dealing with encrypted Voice over IP (VoIP) traffic it may be necessary to obtain cryptographic keys from the VoIP service provider in order to extract the audible information from the intercepted data stream. Or the rendering of some kind of content, such as multimedia applications, may be dependent on the knowledge of proprietary algorithms developed by private companies.

(iii) The Roles of the Providers

In a conventional landline, the provider of the service (voice communication) is usually also the provider of the infrastructure (a pair of copper wires). The same does not apply to Internet communications, where the target of an investigation can utilize any number of combinations of services (e-mail, VoIP, Instant Messaging, etc.) and infrastructure providers (Wi-fi, ADSL, etc.), making it harder to determine who should be responsible for implementing the interception.

Also, with the increasing complexity of the services, the infrastructure providers may not be able to properly intercept and deliver the desired data to law enforcement agencies. Furthermore, laws and regulations usually do not clarify how much of the additional processing required by the raw content data is to be performed by the provider and how much is the responsibility of the law enforcement agency.

Contrary to what happens currently in Brazil, legislation dealing with interception of content data should not be adapted from older laws drafted with classical telephone interception in mind. Not only must the peculiarities of the computer communications be taken into account, but the legislation must enforce some sort of technical standard to cope with those peculiarities.

Without such technical standards, a country may end up in a scenario where the service and infrastructure providers, even when complying with a generic interception law, are delivering the required data in a format unsuited or incompatible with the needs and resources available to the law enforcement agencies. Here, the text of Article 20 of the Convention on Cybercrime, paragraph 1 (b), (“compel a service provider, *within its existing technical capability*”), may serve as a justification for the providers who, for economical or commercial reasons, do not want to invest the resources necessary to adapt their networks to comply with a de facto standard. Good examples of technical standards for lawful interceptions are the ones defined by the European Telecommunications Standards Institute (ETSI).

A clear definition of the roles, standards and interfaces between law enforcement agencies and service/infrastructure providers is also crucial on the subject of the admissibility of evidence gathered through content interception. Unlike other types of evidence, digital evidence in general and traffic content data in particular is not suited to *post hoc* validation. If not collected properly at the outset, this kind of evidence can be easily dismissed in court.

For instance, the content of an intercepted telephone conversation can usually be validated by comparing the recorded audio with the actual voices of the speakers. When it comes to intercepted digital data, there is no speaker's voice to be compared with the recorded bits and bytes.

D. Digital Forensic Analysis of Evidence

The Brazilian Federal Police has approximately 150 computer forensics experts with at least a bachelor's degree in Computer Science or Computer Engineering, distributed among all 27 Brazilian states. Besides specific training in computer forensics, they are police officers and undergo the same police training that all the members of the Brazilian Federal Police do.

Currently the bulk of their workload is on the analysis of digital evidence not directly related to

cybercrime, such as computers seized during investigations of financial crimes. But the Brazilian Federal Police is in the process of creating specialized units to concentrate only on cybercrimes.

III. COMPETENCE TO INVESTIGATE, PROSECUTE AND ADJUDICATE OFFENCES DEFINED IN THE CONVENTION ON CYBERCRIME

The Brazilian Federative Republic was inspired by the North American model, comprising a Union and its component States. The judicial system follows this guideline, and with some simplification, it can be said that the Brazilian judicial system is organized on two levels: Federal Justices and State Justices.

The Federal Justices and each instance of the State Justices are basically structured around the same components: the courts; the public attorney's office and the judicial police. On the Federal level the only judicial police force is the Brazilian Federal Police.

The competence of each level of the judiciary in the criminal area is defined by the Constitution. In short, the Federal Justices have competence in issues that involve the interests of the Union, serious human rights violations and the financial system.

Offences included in international treaties that are perpetrated through international borders, such as the ones defined in the Convention on Cybercrime, involve the Union and therefore are investigated by the Brazilian Federal Police. Also, jurisprudence has established that the publishing of child pornography over the Internet falls under the competence of the Federal Justices.

However, it is being accepted that, when the offence does not involve the crossing of national borders, for instance, the transmission of child pornography between two e-mail addresses hosted by providers inside the Brazilian territory, the offence falls under the competence of the State Justices.

IV. CONCRETE CASES

The majority of the cybercrime occurrences investigated by the Brazilian Federal Police falls under one of two categories: bank fraud and publishing of child pornography.

A. Bank Fraud

More a routine task than an isolated case, operations against bank fraud are carried out by the Brazilian Federal Police at a rate of five or six each year. In each one of them, a minimum of fifteen people are detained, most of them recidivists that are allowed back on the streets shortly after their arrest thanks to the lack of proper legislation to define and punish their crimes.

The Brazilian Internet banking system is one of the most advanced in the world. During the hyperinflation years in the 80's and 90's, the banks were forced to research new technologies and increase their efficiency to survive the ferocious market. This natural selection led to an environment where nearly every bank customer with Internet access has little to no physical contact with their bank. Almost every operation can be completed on the Internet utilizing all the security features available on the server side.

But the natural selection works both ways. The criminals evolved as fast as the technology, developing progressively more creative schemes to circumvent the security features developed by the financial institutions. The key, they promptly learned, is to attack the weaker link: the bank's client. By compromising the user's computer by means of malicious software, known as Trojan horses, spread through false e-mails, they can bypass virtually every protection the banks put in place to protect their clients. Once they get the account and passwords information, a wide network of accomplices is used to withdraw the money and make tracing difficult.

The Brazilian Federal Police and the Brazilian Bank Association maintain groups dedicated to registering, analysing, reverse engineering and tracing back to their origins all the password stealing malware they find. After five years of work, as of May 2008, almost 100,000 specimens of malicious software have been identified. The current average is 67 new Trojan horses a day, 11,000 of them in the first five months of 2008.

Nearly all the malicious software is hosted on compromised computers or on rented machines outside Brazil. Half of the specimens are hosted in Russia. All of them send the information they steal from bank clients to email addresses outside Brazil, especially to Google's GMail service.

As already discussed in this paper, the obstacles to investigating cybercrime under the current Brazilian legal framework forced investigators to concentrate on old fashioned, non-digital police methods. With the data provided by the affected banks regarding suspicious money transfers and withdrawals, the suspects are put under surveillance and the structure of the criminal organization can be identified, leading to the arrests.

B. Child Pornography

In order to be more proactive in investigating child pornography publishing cases, the Brazilian Federal Police developed a tool to monitor the peer-to-peer networks eDonkey and Kad.

The tool is based on the open-source client named eMule. When fed with a list of known child pornography media files, it monitors the networks and logs the IP addresses, the country and the user ID of the users sharing each file. A hundred targets within Brazil were prioritized based on the number of illicit shared files. Three hundred foreign targets' information was sent through Interpol to nine countries.

In April 2008 the investigation, named Operation Carousel, went to the streets. A hundred search warrants were executed and, given that Brazilian law punishes the publishing, but not the possession of child pornography files, all teams had a computer forensic expert to try to catch the criminal in the act. Unfortunately, due the long time it took for the providers to identify the addresses of the targets from their IP addresses, most of them were no longer sharing the known child pornography media files. Their computers were seized and are currently being analysed by Brazilian Federal Police computer forensic experts in search of other paedophile material.

In September 2008 a second round of search warrants, in an action named Operation Carousel II, was executed. Simultaneously, law enforcement agencies in Israel, the Czech Republic, Japan, Senegal and Portugal conducted searches based on the information handed by the Brazilian Federal Police through Interpol.

V. CONCLUSION

Although some simplifications had to be made to comply with the theme and format limitations, this paper tried to be a faithful portrait of the current practical and legal obstacles to cybercrime investigations in Brazil.

In addition, it attempted to shed some light on a few details concerning the regulation and implementation of one of the most powerful and controversial tools available to the cybercrime investigator, the Interception of Content Data, hoping that instead of mere technicalities they are looked upon as important topics in the discussion of the adoption of a common framework for combating cybercrime.

CURRENT SITUATION AND ISSUES OF ILLEGAL AND HARMFUL ACTIVITIES IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGY IN PAKISTAN

*Syed Abbas Ahsan**

I. INTRODUCTION

Information infrastructure is increasingly under attack by cyber criminals. The number, cost and sophistication of attacks are increasing at alarming rates. Such attacks threaten the growing reliance of commerce, governments and the public upon the information infrastructure to conduct business and process information. Most of the attacks are transnational by design, with victims throughout the world. Measures thus far adopted by the private and public sectors have not provided an adequate level of security. The reasons for lack of success in the field include the lack of timely sharing of information, slow and un-coordinated investigations, inadequacy of legal/investigative infrastructure governing cybercrime, jurisdictional assertions of multiple states, and lack of international co-operation.

Cybercrimes generally fall into two categories; first where the computer itself or the computer networks are the intended victims e.g. network intrusion, spoofing and spamming; secondly the use of computers to commit more traditional crimes e.g. identity theft and computer fraud, etc. Such activities have a significant negative impact and tend to discourage the use of computers that offer the chance for advancement in knowledge, convenience, commerce and intellectual interaction. This paper focuses on these very issues with reference to Pakistan. An effort has been made to ascertain the extent of problem and the legal and practical steps taken by the government to combat this growing menace. Bottlenecks and obstacles in the process and infrastructure already in place have also been identified.

II. PERSPECTIVE ON CYBERSPACE USE AND ABUSE IN PAKISTAN

It is very difficult to gauge the actual number of people using information and communication technology in Pakistan. The figures available from various sources, only on the number of Internet users in Pakistan, vary from 3 million to 17.5 million online users. However, all the major commercial institutions are making use of information and communication technology and use cyberspace to conduct their businesses, including all commercial banks. Most of the universities in Pakistan and many educational institutions in the major cities have online access and provide students access to computers and the Internet. The reason for establishing a legal framework to regulate electronic transactions and crimes was the dramatic rise in the number of Internet users in the country (almost 9,000%) from 2000 to 2008.

The legal apparatus to regulate electronic transactions and combat cybercrime was established through the Electronic Transactions Ordinance, 2002 and the Prevention of Electronic Crimes Ordinance, 2007. The laws established a regulatory mechanism for the conduct of electronic transactions and provided penal sanctions for the violation of the legal parameters established under these laws. The Prevention of Electronic Crimes Ordinance also provides the infrastructure for the investigation, prosecution and adjudication of cybercrimes along with the procedures for the same. On the abuse of cyberspace, the cybercrime figures may be quite misleading. In all, only 98 complaints have been received in the National Response Center for cybercrimes during the last year, since the promulgation of the Prevention of Electronic Crimes Ordinance. Of these complaints, only 21 cases have been registered and all of the cases are still under investigation. The majority of the complaints received were from corporate bodies and public institutions, mostly relating to fraud and unauthorized access. Almost all the cases required trans-border investigations and co-operation

* Superintendent of Police, Islamabad Capital Territory Police, Pakistan.

140TH INTERNATIONAL TRAINING COURSE
PARTICIPANTS' PAPERS

from international organizations, which is the main reason for delayed prosecution.

Internet Statistics Asia						
ASIA	Population (2008 Est.)	Internet Users, (Year 2000)	Internet Users, Latest Data	Penetration (% Population)	(%) Users in Asia	Use Growth (2000-2008)
Afghanistan	32,738,376	1,000	580,000	1.8 %	0.1 %	57,900.0 %
Armenia	2,968,586	30,000	172,800	5.8 %	0.0 %	476.0 %
Azerbaijan	8,177,717	12,000	1,035,600	12.7 %	0.2 %	8,530.0 %
Bangladesh	153,546,901	100,000	500,000	0.3 %	0.1 %	400.0 %
Bhutan	682,321	500	40,000	5.9 %	0.0 %	7,900.0 %
Brunei Darussalem	381,371	30,000	176,029	46.2 %	0.0 %	486.8 %
Cambodia	14,241,640	6,000	70,000	0.5 %	0.0 %	1,066.7 %
China *	1,330,044,605	22,500,000	253,000,000	19.0 %	43.7 %	1,024.4 %
East Timor	1,108,777	-	1,200	0.1 %	0.0 %	0.0 %
Georgia	4,630,841	20,000	360,000	7.8 %	0.1 %	1,700.0 %
Hong Kong *	7,018,636	2,283,000	4,878,713	69.5 %	0.8 %	113.7 %
India	1,147,995,898	5,000,000	60,000,000	5.2 %	10.4 %	1,100.0 %
Indonesia	237,512,355	2,000,000	25,000,000	10.5 %	4.3 %	1,150.0 %
Japan	127,288,419	47,080,000	94,000,000	73.8 %	16.2 %	99.7 %
Kazakhstan	15,340,533	70,000	1,400,000	9.1 %	0.2 %	1,900.0 %
Korea, North	23,479,089	--	--	--	--	0.0 %
Korea, South	49,232,844	19,040,000	34,820,000	70.7 %	6.0 %	82.9 %
Kyrgyzstan	5,356,869	51,600	750,000	14.0 %	0.1 %	1,353.5 %
Laos	6,677,534	6,000	100,000	1.5 %	0.0 %	1,566.7 %
Macao *	460,823	60,000	238,000	51.6 %	0.0 %	296.7 %
Malaysia	25,274,133	3,700,000	14,904,000	59.0 %	2.6 %	302.8 %
Maldives	379,174	6,000	33,000	8.7 %	0.0 %	450.0 %
Mongolia	2,996,081	30,000	320,000	10.7 %	0.1 %	966.7 %
Myanmar	47,758,181	1,000	40,000	0.1 %	0.0 %	3,900.0 %
Nepal	29,519,114	50,000	337,100	1.1 %	0.1 %	574.2 %
Pakistan	167,762,040	133,900	17,500,000	10.4 %	3.0 %	12,969.5 %
Philippines	92,681,453	2,000,000	14,000,000	15.1 %	2.4 %	600.0 %
Singapore	4,608,167	1,200,000	2,700,000	58.6 %	0.5 %	125.0 %
Sri Lanka	21,128,773	121,500	771,700	3.7 %	0.1 %	535.1 %
Taiwan	22,920,946	6,260,000	15,400,000	67.2 %	2.7 %	146.0 %
Tajikistan	7,211,884	2,000	19,500	0.3 %	0.0 %	875.0 %
Thailand	65,493,298	2,300,000	13,416,000	20.5 %	2.3 %	483.3 %
Turkmenistan	5,179,571	2,000	70,000	1.4 %	0.0 %	3,400.0 %
Vietnam	86,116,559	200,000	20,159,615	23.4 %	3.5 %	9,979.8 %
TOTAL ASIA	3,776,181,969	114,304,000	578,538,257	15.3 %	100.0 %	406.1 %

III. LEGAL FRAMEWORK

The laws related to information and communication technology follow the separation of the e-commerce and cybercrime model. There are separate laws governing both the aspects of the information and communication technology, nonetheless, the laws supplement each other in the regulation of all electronic transactions. The laws relating to electronic transactions provide the legal basis for evidence and give recognition to electronic documents and electronic communications. The laws governing electronic and cybercrime in Pakistan cover both crimes that are traditional in nature, i.e. theft, fraud, forgery, mischief and terrorism in which computers or any other electronic device is used to commit these crimes, as well as misuse of computers that is criminal in nature, or what we call content-related crimes, e.g. damage and access to electronic devices and data with criminal intent.

A. Penal Sanctions for Cybercrime in Pakistan

The first law promulgated in Pakistan regulating all electronic transactions is the Electronic Transactions Ordinance, 2002. The Electronic Transactions Ordinance provides a comprehensive legal infrastructure to facilitate and give legal sanctity to electronic documents as well as protection to e-commerce locally and globally. This law also penalized the misuse of electronic communication and charts the boundaries for certification of service providers. The more recent law, the Prevention of Electronic Crimes Ordinance,

2007, relates to cybercrime and has been framed specifically to criminalize the misuse of electronic media. Furthermore, the Prevention of Electronic Crimes Ordinance creates the structure required for the investigation and adjudication of cybercrimes.

1. Electronic Transaction Ordinance 2002

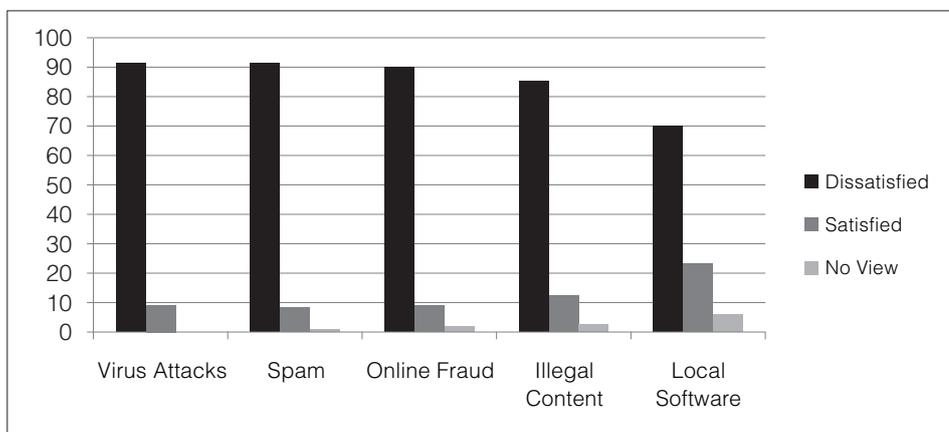
The Electronic Transactions Ordinance was promulgated in 2002, primarily to provide for the legal recognition and facilitation of documents, records, information, communications and transactions in electronic form. The law gives legal recognition to documents, information and records and allows their admissibility in a court of law without the requirement of a witness. The maintenance of documents in physical terms is also satisfied under this law if the document or record is accessible and retrievable. Moreover, the Ordinance delineates the rules on compliance and retention of documents in electronic form. The law also establishes the parameters for electronic communications and thus creates rules for associating documents with the recipient as well as the sender. Rules are also designed for legal acknowledgement, time and date of sending, along with establishing the place of sending and dispatch of electronic communication.

The Electronic Transactions Ordinance also formulates the principles that are required for any document, record, or communication and information to be deemed legally secure, thus setting up a digital signature regime whereby electronic signatures and electronic applications provide the legal security required for any electronic transaction. The Ordinance also establishes the criteria for the authenticity and integrity of advanced digital signatures provided by the certification service providers. The certification service providers extend certifications to websites and digital signatures.

The law does not criminalize most of the offences as supported by different international forums; however, the law does provide legal cover for the evidentiary value of all electronic transactions by amending Pakistan’s evidence laws. The law recognizes the authenticity of all electronic transactions and brought these at par with other documentary transactions. Moreover, the Electronic Transactions Ordinance provides the foundation for the subsequent penal law, the Prevention of Electronic Crimes Ordinance, 2007. As an interim measure to prevent the misuse of now legally acceptable documents and to restrict the misuse of incentives granted in the law, certain offences are penalized. The penal sections of the law relate to false information from the subscriber to the certification service provider, issuance of false certificates, violation of privacy of information and damage to information systems or data.

2. Prevention of Electronic Crimes Ordinance 2007

The Prevention of Electronic Crimes Ordinance, 2007 was enacted against crimes related to the confidentiality and integrity of electronic systems, networks and data, as well as the misuse of such systems, networks and data. The law, apart from providing penal sanctions against the abuse of electronic transactions, also provides the procedural regime for the investigation, prosecution and adjudication of cybercrime. The following chart represents the survey responses of Internet users in Pakistan on Internet Governance, showing their top five concerns.



The chart above not only represents the concerns of Internet users in Pakistan, but also gives an informed opinion about the state of affairs in the field of combating cybercrime in Pakistan. The huge rate of growth of Internet users and the opinions of Internet users, both corporate and individual, have been the key drivers for the creation of the electronic regime in Pakistan. The ordinance based on such feed-back penalizes the following:

- Criminal access or damage to electronic data or systems
- Electronic fraud or electronic forgery with wrongful intent
- Misuse of electronic system or device with criminal intent
- Unauthorized access to codes or passwords with wrongful intent
- Encryption of incriminating communication or data
- Spamming, spoofing or use of malicious codes
- Cyber stalking, especially against minors
- Unauthorized interception by technical means
- Use of electronic system with '*terroristic intent*'

A detailed scrutiny of the law shows that its framers intended to adopt a very broad interpretation in the definitions and explanations of the crimes. This point is evident from the title and definitions as well as the penal sections of the law. Instead of using the terms “cyber” or “computer” crimes, the emphasis is on “electronic” crimes. As far as possible all definitions and interpretations are kept open with the use of phrases like '*including but not limited to*', etc. The broad interpretation may have been adopted keeping in view the common law tradition of prosecutorial discretion providing protection against inappropriate application of the law. Furthermore, in-depth interpretation and setting up of the limits of the application of law is left to the thorough scrutiny of judicial decisions during court proceedings.

A noticeable omission in the law is the non-differentiation of “negligent” and “intended” misuse of technology. The law is criticized for not making any distinction between what is unethical and what is illegal. In the Ordinance the sections relating to spamming, spoofing and unauthorized interception allow criminal proceedings without requiring criminal intent of the person involved in such acts. Without giving due consideration to criminal intent there is a possibility of misapplication of the law either by mistake or abuse. Therefore, the intent of the offender must be considered in all circumstances before any criminal sanction is applied against that person. Only when the criminal intent of a person is established, penal proceedings should be initiated against the person. There is a need to remedy this omission by establishing criminal intent in the forefront before the application of any penal sanction.

The law has been criticized for a number of other reasons. First, the law has been condemned as a curb on the freedom of expression, especially the part relating to cyber-stalking. Distribution of photographs of persons without their consent/knowledge and display/distribution of information are issues that need clarification in this section. This explanation amounts to censorship and can prove to be a hurdle for sharing of information, healthy criticism, or even common gossip over blogs. Moreover, the definition of cybercrime as given in the law is quite vague and includes terms prone to a wide multitude of interpretation e.g. vulgar, profane, indecent, immoral, etc. Such words have an extremely wide interpretation even in dictionaries and can have different connotations for different cultures, regions, or even individuals. The law, while establishing penal sanctions, should be clear so that any person coming under the jurisdiction of the law knows what limits the law has established and what constitutes an offence.

Secondly, section 11 of the law against the misuse of encryption has been censured for coercing self-incrimination which is contrary to fundamental civil rights. This section penalizes any person who encrypts any incriminating communication or data contained in an electronic system. However, this section is against Article 13 of the Constitution of Pakistan, 1973, which provides protection against self incrimination. As this section provides a criminal penalty for concealing incriminating evidence, it coerces an offender to decrypt such evidence, which may be self-incriminating. Hence, the law violates the right of protection against self-incrimination granted by the Constitution of the country.

Thirdly, section 18 has been disapproved for putting the burden of proof on the person accused of the offence under that section. This section deals with the offences involving sensitive electronic systems and

provides greater punishment if such systems are accessed. Although the burden of proving the crime in itself, i.e. illegal access to the system, lies with the prosecution, the law presumes that the accused had the requisite knowledge that the system accessed was a sensitive electronic system. This presumption shifts the burden of proof on the accused which is against the basic norms of criminal jurisprudence, which requires the crime to be proved beyond reasonable doubt by those who bring the charges against the accused.

Finally, the most vociferous denunciation has been directed against the term ‘terroristic act’ and the penal section associated with it. The evidently broad definition and explanation of this section is vulnerable to misinterpretation as well as manipulation. It is pertinent to note that the definition and explanation of terrorism is much more restricted and specific in the Anti-terrorism Act; as such many offences that may not attract the Anti-terrorism law can be prosecuted under this law. Use of malicious code against a public entity or computer network operated by the government and “violence” against the sovereignty of the state has been included in the definition of terrorism. “Violence” has further not been elaborated and is left to the discretion of the person applying and therefore interpreting the law. In addition to this, the explanation of terroristic intent has similar flaws and is open to misapplication.

B. Comparison with Convention on Cybercrime

With regard to the definitions of offences against confidentiality, integrity and availability of computer data and systems, these have been criminalized in Pakistan as explained in the Convention on Cybercrime of the Council of Europe. Comparable criminal sanctions are available in the Prevention of Electronic Crimes Ordinance 2007 for illegal access, interference, misuse and interception of electronic data or systems. The definitions in Pakistan are comparable with the convention and have rather been kept broad to take account of any offence related to the illegal use of all electronic devices, including computers or computer data. Computer-related fraud and computer-related forgery has also been amply covered in the laws in Pakistan. The same principle has been followed that all electronic devices have been included which may be used to commit any fraud or forgery.

Regarding the content related offences, the Prevention of Electronic Crimes Ordinance has limited application. Spamming, spoofing, cyber-stalking and malicious codes, which include viruses and Trojans, etc., have been criminalized. However, these do not cover all content-related offences as enumerated in the Convention. Moreover, the laws in Pakistan do not provide any sanctions against offences described in the Additional Protocol relating to racism, hate crimes and xenophobia. The issue of child pornography is not penalized in the law, but it is argued that the sanction against cyber-stalking provides protection to minors against abuse. The section on cyber-stalking does provide protection to the extent of soliciting illegal acts, which may include sexual acts; but the section does not criminalize production, transmission or possession of child pornography. A relevant observation in this regard is that all pornography, whether child pornography or otherwise, is illegal in Pakistan.

Protection of Intellectual Property Rights is another omission in the cybercrime laws in Pakistan. Again, it is contended that Intellectual Property is protected by laws particularly drafted for the protection of the same, and the cyber laws provide protection against accessing codes and passwords for the purpose of any illegal use of electronic data.

IV. IMPLEMENTATION OF THE CYBERCRIME REGIME

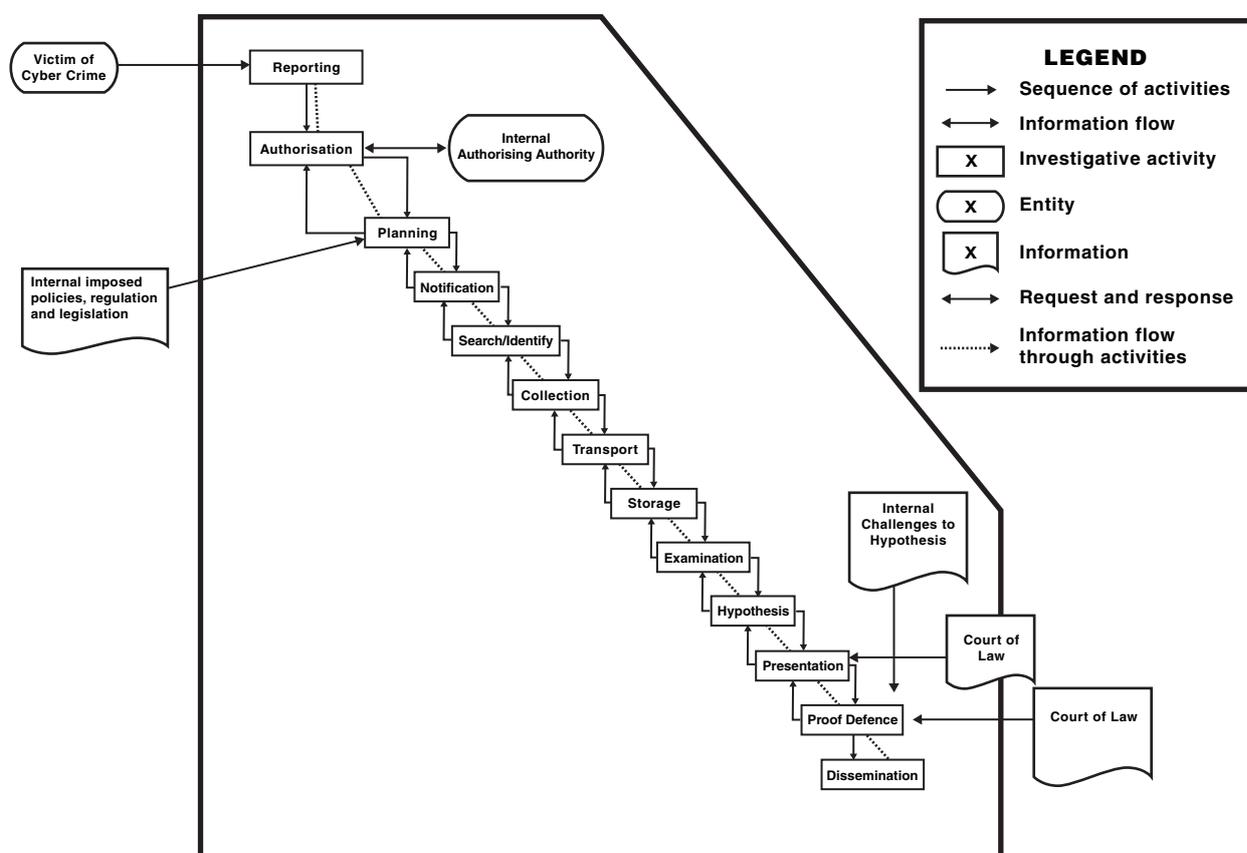
A National Response Center for Cyber Crimes has been established under the Federal Investigation Agency to deal with all issues related to cybercrimes. The functions of the National Response Center as declared by law are to ensure the enforcement of cyber laws, and to prevent, investigate and prosecute electronic crimes. The law also envisages a tribunal for the adjudication of all crimes under the Prevention of Electronic Crimes Ordinance. The National Response Center, apart from being the primary investigation agency against cybercrime, performs the following functions:

- Co-ordination with international organizations to handle trans-border cases;
- Technical support to government organizations for data and network security;
- Real-time network traffic patrolling and collection of data;
- Capacity building of law enforcement agencies in cybercrime;
- Provision of forensic services for cybercrime.

The tribunal for the adjudication of cybercrime as proposed in the law is yet to be established. All cases related to cybercrime are prosecuted in the normal penal courts as required by law until the tribunal is established.

A. Investigation

The National Response Center for Cyber Crime, which is the premier investigating agency against cybercrime, has its head office in the national capital, Islamabad, with three regional offices across the country. The centre's facilities consist of a Digital Forensic Laboratory and a cybercrime reporting and investigation centre. It provides special investigative services under the Telecom Act 1996, the Electronic Transactions Ordinance 2002 and the Prevention of Electronic Crimes Ordinance 2007. The National Response Center for Cyber Crime also provides technical support to the local police in investigations involving the use of electronic devices. Such support is provided in investigations of ordinary crimes where electronic devices or media is used in commission of the crime.



The proposed model of cyber crime investigation

A waterfall model is used for investigation of cybercrime. All activities follow each other in sequence. The model progresses from crime reporting to authorization of investigation. The next step in the process is the collection and storage of evidence. Finally evidence is examined, a hypothesis established regarding the incident and the case is prepared for prosecution in a court of law. In fact, the investigation steps require several repetitions before the case is finally prepared for prosecution. The last step of examination-hypothesis-presentation may be reiterated a number of times as the understanding of the evidence grows in connection with other relevant evidence.

However, as the whole structure established against cybercrime is still in its infancy and the processes are not formalized, The National Response Center will come across many practical and procedural challenges in due course. Experience in handling electronic crimes will help the Center to determine its future course of action in combating cybercrime. Interaction with other international agencies and further

research and development will educate those involved in this endeavour to chart out the best methods to probe electronic offences. Apart from the lack of experience in handling electronic offences, there is a lack of awareness regarding the handling of such cases, not only in the general public but also amongst those affiliated with the criminal justice system.

1. Reporting System

Electronic crimes are reported to the National Response Center, which after initial inquiry and internal authorization approves the registration of a criminal case under any of the laws governing electronic offences. The cases are registered with the police stations of the Federal Investigation Agency, which has an established network around the country and deals with a number of other specialized crimes.

The major issue with the reporting mechanism is the lack of awareness amongst victims. Electronic crimes are normally not reported for the reason that it is assumed that such crimes cannot be traced and the criminals are faceless. Moreover, the victims of electronic crimes do not know where and how to report electronic crimes. Most electronic crimes go unreported till they have reached an alarming stage, whereby the investigations are conducted on the initiative of either the National Response Center or another government agency. In certain instances, electronic crimes have been initiated in response to requests from law enforcement agencies of other countries.

2. Digital Forensics

The increasing problems of cybercrime have enhanced the importance of digital evidence and digital forensics. Digital forensics includes the preservation, identification, extraction, documentation and interpretation of digital data. As electronic evidence presents special challenges for its admissibility in courts, proper procedures are required for collection, examination, analysis and reporting of evidence. The National Response Center has established its procedures based on the above mentioned objectives.

The collection phase involves search, recognition and documentation of electronic evidence. The examination phase includes the documentation of the content and state of evidence. This phase also involves the search of any information that may be hidden or obscured. Analysis differs from examination in that it looks at the evidence for its significance and probative value to the case. Examination is the technical review that is the province of the forensic expert, while analysis is performed by the investigation team. The process is completed with a written report outlining the examination process and the pertinent data recovered. Examination notes are also preserved for purposes of discovery and testimony. The examiner may be required to testify about the conduct of the examination, the validity of the procedure and his or her qualifications to conduct the examination. In this regard, the digital forensic laboratory provides technical support for examination of evidence for prosecution of electronic crimes.

The digital forensics laboratory has the facilities for the collection, validation, identification, analysis, interpretation and documentation of data as well as its preservation as digital evidence. It has the capacity for reconstruction of corrupt data which may have evidentiary value. The laboratory is equipped with the necessary software and equipment to achieve these ends. Although the Digital Forensic Laboratory has successfully supported the investigations conducted so far, there is room for further improvement with regard to technical expertise and equipment. An issue with evidence collection from cyber space is the maintenance of traffic data by service providers. In many instances, traffic data is not available from the service providers to identify criminals or the origin of the crime.

3. Co-operation and Liaison

The National Response Center is the focal point for all cases relating to electronic crimes and electronic security. Government departments liaise with the Center for their network and data security. Pakistan Telecommunication Authority, which regulates service providers and network traffic data, also co-ordinates with the Center for the enforcement of electronic laws. The Center is the central repository for research on network security and electronic crimes. To increase awareness and understanding of electronic offences the Center also conducts training and seminars for different agencies related with the criminal justice system. The National Response Center aids local law enforcement agencies in investigations where electronic media is used in the commission of crimes. Support is provided in the examination of electronic evidence and tracing criminals through electronic media.

International co-operation for detection of cybercrime is also routed through the Center, which has established liaison with Interpol. However, international co-operation is not very forthcoming for a number of reasons. First, electronic crimes are not criminalized in many jurisdictions and network traffic data is not available in many jurisdictions. This helps cyber criminals establish spoof network addresses, which makes it difficult to detect the actual perpetrators of the crimes. Secondly, international co-operation is not very forthcoming because the victim is in another jurisdiction, therefore less importance is attached to such investigations. There is also animosity and doubt about the credibility of investigations carried out in other jurisdictions and at times problems arise due to the admissibility of evidence collected in a foreign jurisdiction by a foreign investigation agency. Furthermore, priorities differ amongst states on the prosecution of certain offences. It is for these reasons that the cybercrime law in Pakistan is based on reciprocity as far as international co-operation is concerned. Furthermore, it does not make international co-operation mandatory. Rather it allows ample discretion in assisting investigations and sharing information regarding electronic crimes and data with other jurisdictions.

B. Prosecution and Adjudication

As the infrastructure against electronic offences is in its early stages and investigations in some cases have only recently been initiated; none of these have reached the prosecution or adjudication phase. The law requires setting up a Tribunal for the adjudication of electronic crimes, which has not been established yet. Until the Tribunal, ordinary courts are empowered to adjudicate electronic crimes; the Tribunal is empowered to take cognizance of offences under the Prevention of Electronic Crimes Ordinance.

1. Jurisdiction

The law allows for a wide application of jurisdiction covering the principles of territorial, extra-territorial as well as personal jurisdictions. However, such a wide interpretation of jurisdiction of the law is not advisable and practically unrealistic. The principle of territorial jurisdiction is accepted in all criminal offences, based on the principles of respect for the sovereignty of other states. Jurisdiction is applied if the offence is committed within the territory of the state or if the offence produces its effects in the territory of the state. Even such application of limited jurisdiction leads to conflict of laws. Extraterritorial jurisdiction may result in the non-availability of evidence which may be present in the jurisdiction where the actual offence was committed. Moreover, even if, through international co-operation, evidence and the suspect are brought to the jurisdiction of the victim, the cost of numerous such investigations and prosecutions would lead the system to failure. Another issue with extraterritoriality is that an act performed in one jurisdiction may not be an offence but it may be criminalized in the jurisdiction where the act effects. Such a system is also prone to abuse, as it may be used to prosecute public officials or extraterritorial investigations may form an excuse for espionage. There is a need to establish a mechanism to settle jurisdictional conflicts through recognition of the investigative processes and evidence in other jurisdictions around the world and to standardize the priority of exercising jurisdiction.

2. Electronic Evidence Admissibility and Evaluation

The evidential issues, as already discussed, have been sorted out through the Electronic Transactions Ordinance, which has made amendments in the existing evidence laws to provide legal recognition to all electronic transactions. In addition to this, for the purpose of evaluation of evidence, the Prevention of Electronic Crimes Ordinance allows the tribunal to appoint and take assistance in technical aspects from *amicus curiae* having knowledge, experience, expertise and qualifications in information and communication technology, of which the government is bound to maintain a list.

V. CONCLUSION

In the final analysis, it is concluded that although Pakistan has taken a number of steps towards controlling electronic offences, there is room for much needed improvement. The government has shown its interest in finding solutions for recognition of electronic transactions and criminalizing electronic offences through promulgation of laws in this context. Although practical measures have also been taken to counter electronic crimes, there is a need for a more proactive approach. The enforcement of law, especially in the field of maintenance of electronic traffic data, is one aspect that requires special attention, as most of the investigations have reached dead ends due to the lack of data. Consequently, investigations remain incomplete. Another obstacle in the path of investigations is the issue of jurisdiction and international

co-operation. Till the time these issues are settled on an international level the problems will continue to obstruct the combating of electronic crimes.

Practical issues in prosecution and adjudication are yet to be encountered as none of the investigations, initiated so far, have reached that stage. As the criminal justice system in Pakistan is based on Common Law, decisions by the courts would help in interpreting and elucidating the essence of the law. Nevertheless, the legal framework needs certain clarifications, and modifications. It is hoped that practical application of the laws and further research will help in developing the legal structure and remedying its flaws.

BIBLIOGRAPHY

Commonwealth Secretariat. (2002, October). *Model Law on Computer and Computer Related Crime*. Retrieved August 3, 2008, from http://commonwealth.live.poptech.coop/shared_asp_files/uploadfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf

Constitution of the Islamic Republic of Pakistan. (1973). Pakistan.

Council of Europe. (2003). *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS 189)*. Retrieved August 15, 2008, from <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>

Council of Europe. (2001). *Convention on Cybercrime (ETS 185)*. Retrieved August 15, 2008, from <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>

Electronic Transactions Ordinance. (2002). *Gazette of Pakistan, Extraordinary, Part-I of 2002*. Pakistan.

Internet World Stats. (2008, June 30). Retrieved August 21, 2008, from <http://www.internetworldstats.com/stats3.htm>

Jamil, Z. U. (2002, September). *E-COMMERCE LAW IN PAKISTAN*. Retrieved August 20, 2008, from www.jamilandjamil.com/publications/pub_reports/IBP%20Paper%20151004.pdf

Prevention of Electronic Crimes Ordinance. (2007). *Gazette of Pakistan, Extraordinary, Part-I of 2007*. Pakistan.

United Nations. (2000). *Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders*. Retrieved August 10, 2008, from <https://www.asc41.com/10th%20un%20Congress%20on%20the%20Prevention%20of%20Crime/013%20ACONF187.10%20Crimes%20Related%20to%20Computer%20Networks.pdf>

United Nations. (1994). *The International Review of Criminal Policy: United Nations Manual on the Prevention and Control of Computer-related Crime*. Retrieved August 7, 2008, from <http://www.uncjin.org/Documents/irpc4344.pdf>

Zinnbaur, D. (2005). *Internet Governance Priorities and Practices: Pakistan*. Islamabad: United Nations Asia-Pacific Development Information Programme.

COUNTRY REPORT ON CYBERCRIME: THE PHILIPPINES

*Gilbert C. Sosa**

I. INTRODUCTION

Cybercrime goes beyond the technical, transnational dimension and involves offenders who deliberately fashion their attacks to exploit the potential weaknesses present in the infrastructure's transnational nature. It threatens the substantial and growing reliance of commerce, governments, and the public upon the information infrastructure to conduct business, carry messages, and process information.

Cybercrime is one of the fastest growing non-violent crimes in the Asian region. It takes a great deal of technical expertise and co-operation, both local and foreign, in order to address such problems. This crime affects different countries in varying degrees, depending on the extent of the legislative enactment of each country. In the Philippines, as technical and electronic landscapes change, there is a need to enact laws or amend existing laws to fully address cyber threats.

II. PHILIPPINE SITUATION

A. Government Responses

The public is aware of the importance of legislation that supports police efforts against computer crimes. Onel de Guzman, the Philippine dropout who, in August 2000, created and unleashed a remarkably dangerous computer virus called "I LOVE YOU", cost several companies, governments, and citizens billions of US dollars in damages. In August of the same year, charges against him in our country were dismissed, mainly because we had not yet passed legislation addressing the crimes he had committed. The public around the world is justifiably outraged.

1. The "I LOVE YOU" Computer Virus

The virus was received in e-mail inboxes in Hong Kong on 4 May, 2000, with subject "I LOVE YOU" and an attachment "LOVE-LETTER-FOR-YOU.TXT.vbs.". It erases or blurs the graphics and data in the computer and gets the contact addresses in the computer directory, and sends the same email to all contacts listed in that directory. Once received and opened in another computer, it replicates all that it did previously. The replication went on and on, sweeping all computers where the email was received and opened, from Hong Kong, to Europe, to the United States, infecting and damaging computers and networks of small and big companies, private and government institutions. The damage was about US\$ 5.5 billion; some reports say US\$ 10 billion.

2. Arrest of the Suspect

An international manhunt was conducted; the investigators traced the origin of the virus to its creator, a programming student (Onel de Guzman) at the AMA Computer University in Manila.

When arrested (11 May 2000), the suspect apologized to the public and said he had no intention of causing such great harm. Government prosecutors filed cases against him, but even at the first stage, the indictment was dismissed as there was no law penalizing the act at the time (May 2000) in the Philippines (*nullum crimen, sine lege*)!

3. Effect of the "I LOVE YOU" Virus

The "I LOVE YOU" virus illustrated that a person armed with a computer could, from a distant location, attack and/or disrupt computers and networks worldwide and cause severe damage.

* Chief, Anti-Transnational Crime Division of Criminal Investigation and Detection Group, Philippine National Police.

This whole episode points to the need for a domestic law to address a particular criminal act, and international/bilateral legal instruments to give “no-safe haven” to cyber-criminals (or would-be cyber-terrorists).

The Philippine Congress subsequently passed a law that penalizes computer/cybercrimes, although it did not cover cyber-terrorism.

4. Congress' Response

In order to curb the threat posed by cybercrime, the Philippine Congress enacted Republic Act (RA) 8792, otherwise known as the “Electronic Commerce Act of 2000”. RA 8792 provides for the legal recognition and admissibility of electronic data messages, documents and signatures. This was signed into law on 14 June 2000. The salient features of the Act are as follows:

- Provides for the admissibility of electronic documents in court cases;
- Penalizes limited online crime, such as hacking, introduction of viruses and copyright violations of at least Php100,000 and a maximum commensurate to the damage incurred, and imprisonment of six months to three years, among others;
- Promotes e-commerce in the country, particularly in business-to-business and business-to-consumer transactions whereby business relations are enhanced and facilitated and consumers are able to find and purchase products online;
- Aims to reduce graft and corruption in government as it lessens personal interaction between government agents and private individuals.

RA 8792 is considered the landmark law in the history of the Philippines as a legitimate player in the global marketplace. It has placed the Philippines among the countries penalizing cybercrime.

Likewise, the Supreme Court drafted the Rules on Electronic Evidence, which took effect on 1 August 2000, to emphasize the admissibility of evidence in electronic form, subject to its authenticity and reliability. This restriction intends to safeguard against accepting evidence of doubtful character.

We have also the Access Devices Regulation Act of 1998 (RA 8484) which regulates the issuance and use of access devices, prohibiting fraudulent acts committed and providing penalties and for other purposes; and, Philippine Central Bank Circular 240 dated 7 April 2000 regulating the electronic banking services of financial institutions.

While RA 8792 is already in place, it was found to have failed to address all forms of cybercrime that are enumerated in the Budapest Convention on Cybercrime of 2001, namely:

- Offences against confidentiality, integrity and availability of computer data and systems which include illegal access, illegal interception, data interference, system interference, misuse of devices;
- Computer-related offences which include computer-related forgery and computer-related fraud;
- Content-related offences such as child pornography;
- Offences related to infringement of copyright and related rights.

Furthermore, enforcing the law with the use of the existing guidelines embodied in the Revised Penal Code, as amended, may not work for cybercrime. Unlike the traditional and terrestrial crimes which deal with corporeal evidence, cybercrime involves more electronic data which are intangible evidence.

In order to cope with the daunting problem of cybercrime, the Department of Justice (DOJ) created the Task Force on E-Government, Cyber-security and Cybercrime in 2007 to deal with cyber-security issues in relation to legislation and investigation. It was created to pursue the e-government agenda, institutionalize a cyber-security regime and implement laws. The said task force worked closely with the Council of Europe, a private organization, and local experts composed of IT practitioners and other stakeholders.

Among the top priorities of the Task Force was to work for the passage of the cybercrime prevention act, and the Task Force proposes the creation of e-courts to oversee all high-tech cases of hacking or crimes committed using Internet technology. Included in its effort is capacity-building of the technical knowledge of government prosecutors and judges whose courtrooms will be designated e-courts.

A related Technical Working Group (TWG) on Cybercrime and Cyber-security consists of representatives from National Government Agencies, including law enforcement agencies like the Philippine National Police (PNP), National Bureau of Investigation (NBI), private companies and academia, which have joined hands in order to address issues relating to cyber-security and cybercrime in the Philippines. It aims to consolidate and make concrete the government's efforts on cyber-security and to successfully implement measures to fight cybercrime.

The TWG drafted and proposed a bill that will supplement the current RA 8792. The proposed cybercrime bill includes a definition of cybercrime, penalties and provisions on Internet piracy and provisions on co-operation with the international community.

The proposed bill covers not only computers and computer networks but mobile devices as well. The bill will also have anti-spam measures, and will cover SMS or text messaging for mobile phones, treating mobile phones as "communication devices".

Another added provision concerns "corporate liability" and proposes that a company can be held liable for cybercrimes like hacking or virus attacks when its computer network is utilized in the commission of prohibited acts.

The bill also proposes to create a Computer Emergency Response Council (CERC) under the supervision and control of the Office of the President to formulate and implement a national action plan to address and combat cybercrime. The CERC shall be headed by the Chairman of the Commission on Information and Communications Technology (CICT). Other members shall be the Director of the National Bureau of Investigation (NBI) as Vice Chairman and Director General of the Philippine National Police (PNP), the Head of the National Prosecution Service (NPS), the Head of the National Computer Center (NCC), the Head of the Philippine Center on Transnational Crime (PCTC), the Head of the Anti-Fraud and Computer Crimes Division (AFCCD) of the NBI and the Head of the Criminal Investigation and Detection Group (CIDG) of the PNP, as well as three representatives from the private sector involved in information security, to be appointed by the President as members.

On 26 September 2007, the Philippines signed the United Nations Convention on the Use of Electronic Communications in International Contracts at United Nations Headquarters in New York. Adopted by the United Nations General Assembly on 23 November 2005, the United Nations Convention on the Use of Electronic Communications in International Contracts aims to enhance legal certainty and commercial predictability where electronic communications are used in relation to international contracts.

In October 2007, the "Legislators and Experts Workshop on Cybercrime", led by the Commission on Information and Communications Technology (CICT), declared their support for Philippine accession to the Budapest Convention on Cybercrime and the expeditious passage of an implementing anti-cybercrime law to prevent, mitigate, and deter the commission of ICT related crimes, to foster co-operation within the ICT community, government, private sector and civil society in promoting an atmosphere of safe computing.

The United Nations Commission on International Trade Law (UNCITRAL) is the core legal body of the United Nations system in the field of international trade law. Its mandate is to remove legal obstacles to international trade by progressively modernizing and harmonizing trade law. It prepares legal texts in a number of key areas such as international commercial dispute settlement, electronic commerce, insolvency, international payments, sale of goods, transport law, procurement and infrastructure development. UNCITRAL also provides technical assistance to law reform activities, including assisting member states to review and assess their law reform needs and to draft the legislation required to implement law.

B. The Philippine National Police (PNP) Efforts

At the forefront of this cybercrime information campaign is the Anti-Transnational Crime Division (ATCD) of the Criminal Investigation and Detection Group (CIDG) of the Philippine National Police (PNP).

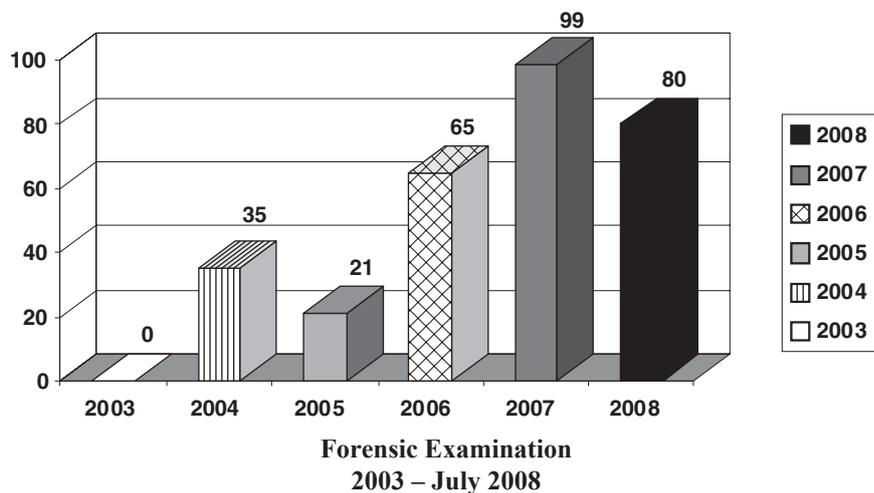
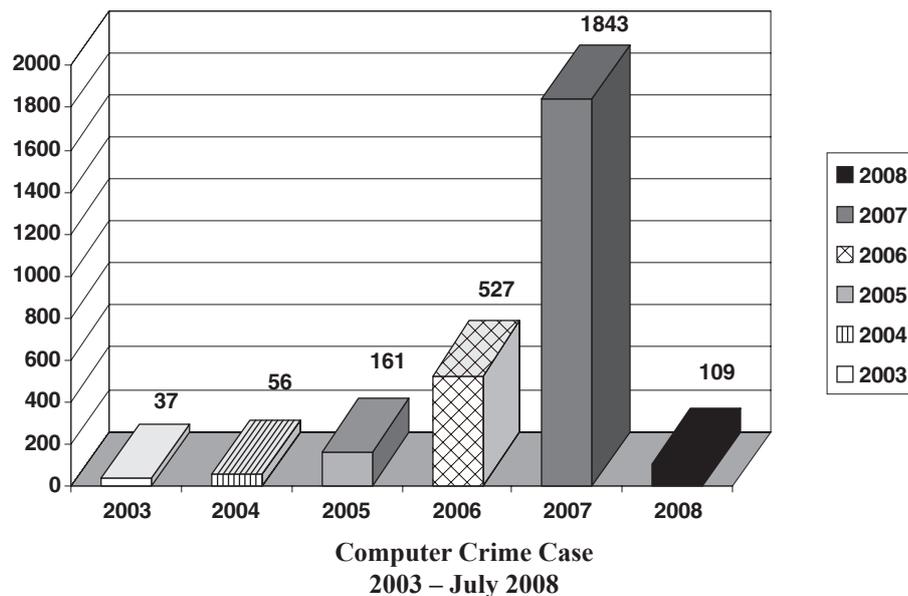
The ATCD-CIDG has a dedicated computer forensic laboratory manned by certified computer forensic examiners (EnCE) and trained computer crime investigators.

At present, numerous reports of emerging cybercrimes are emanating from the country, particularly cyber-sex and child trafficking rings.

With this development, the PNP has focused its efforts on a cybercrime information campaign within the organization. It aims to promote a deeper understanding of the impact of cybercrime and to solicit the concerns and insights of the community on cybercrime-related incidents. Likewise, it has also established links with foreign counterparts in order to successfully fight the threat posed by cybercrime operations.

The first Filipino to be convicted of cybercrime, particularly hacking, was JJ Maria Giner. He was convicted in September 2005 by Manila MTC Branch 14 Judge Rosalyn Mislos-Loja. Giner pleaded guilty to hacking the government portal "gov.ph" and other government websites. He was sentenced to one to two years of imprisonment and fined Php100,000. However, he immediately applied for probation, which was eventually granted by the court. The conviction is now considered a landmark case, as he is the first local hacker to be convicted under section 33a of the E-Commerce Law or Republic Act 8792.

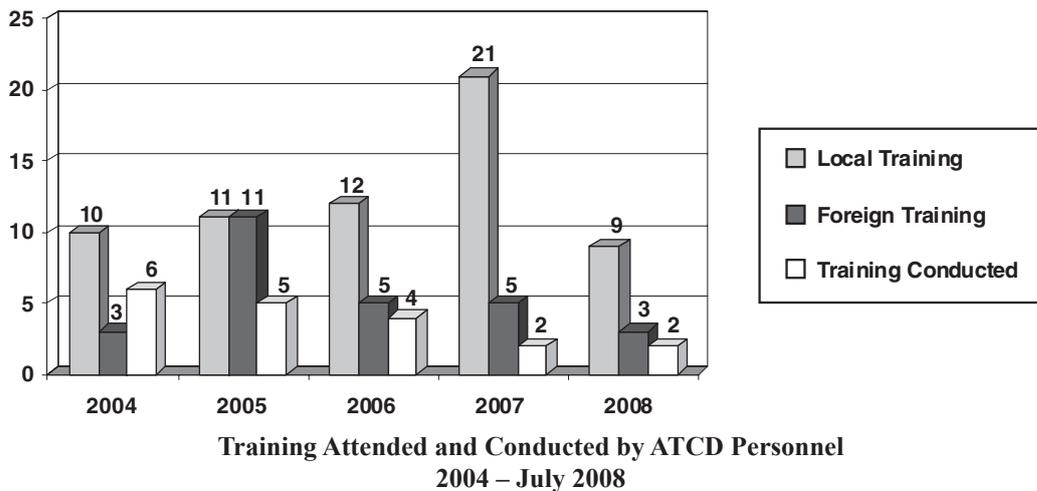
The Anti-Transnational Crime Division (ATCD) of the Criminal Investigation and Detection Group of the Philippine National Police (PNP-CIDG) was involved in the gathering of electronic evidence and the tracking down of the Filipino hacker with help from local Internet service provider Bitstop Inc., which hosted the gov. ph portal when it was attacked by Giner.



Since its creation as a Division of the CIDG in 2003, the ATCD has encountered 2,624 referred cases of computer crimes both from government agencies and private individuals nationwide. Likewise, from CY 2004 to CY 2007, a total of 195 computer forensic examinations were also conducted.

At present, based on records from the DOJ Task Force on E-Government, Cyber-security and Cybercrimes, more than 30 cybercrime cases were filed before Philippine courts on cases relating to website defacements, on-line pornography cyber-stalking, Internet libel, computer forgery, text scams, and privacy issues.

In order to beef-up its capabilities to handle various computer-related endeavours, the ATCD-CIDG personnel received a total of 67 training sessions, both local and abroad, from 2003 to 2008. Likewise, a total of 13 training sessions were conducted for 426 personnel of the PNP nationwide.



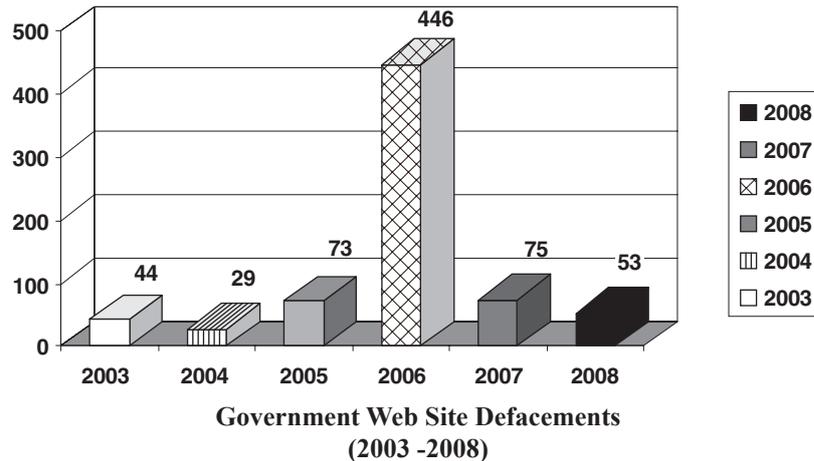
C. Philippine Emergency Response Team (PHCERT)

The first computer emergency response team or CERT in the Philippines is the PH-CERT. PH-CERT provides assistance or responses to cyber incidents locally. PH-CERT funding has to come from its membership fees and sponsorships, thus it cannot afford to have permanent staff and its services are purely voluntary. Its Concept of Operation of providing assistance is email-based and phone-based and on-site services are very minimal or do not exist. The organization has a strong co-ordination with law enforcement agencies through the conduct of technical training. However, lately, the operation of PH-CERT encountered difficulty due to lack of financial support and human resources.

D. Government Computer Security and Incident Response Team (GCSIRT)

GCSIRT was created through the Task Force on Security of Critical Infrastructure (TFSCI) and its aim is to suppress, detect and investigate computer network intrusions and other related Internet or computer crimes.

In research conducted by the GCSIRT from CY 2003 to CY 2007, there was evidence of transnational attacks on computers and the information infrastructure and a total of 667 government websites were discovered defaced, or an aggregate of 133 government websites were attacked by defacers/hackers each year, an average of 11 incidents per month. Based on this research, it was found out that 134 coded defacers (both local and international) have attacked these government websites in that five-year period. Of the attacked/hacked government websites, 507 of the 667 government websites were using the Linux operating system (OS), free and openly available software. This operating system (OS) is the most prone to attacks by defacers/hackers.



III. ISSUES

Despite the overwhelming efforts of the government and the private sector in combating cybercrime in the Philippines still much has yet to be done. The following issues hamper the effective security and protection of Philippine cyberspace:

A. Legislation against Cybercrime

The present laws are not sufficient to completely deter cyber-offenders and to protect the Philippines' cyberspace. For instance, the most important cyber-security legislation in the country, which is Republic Act 8792 or the E-Commerce Act, enacted on 14 June 2000, only penalizes hacking, cracking and piracy. It does not provide penalties for other cybercrimes such as cyber-fraud and similar offences.

B. Budgetary Constraints

Though Government spending in ICT is rising, the amount intended for the security of ICT and cybercrime prevention is very minimal.

C. Overlapping Roles of IT Government Bodies

There is no single overall government body that is mandated to address the problem of cybercrimes and to institute policies on combating such. The proliferation of different ICT committees and task forces in the government yields multiple and murky ICT directions.

D. Lack of Information Sharing, Co-ordination and Co-operation among the Stakeholders

Although there have been conferences and multilateral co-operation undertaken by the government and the private sector to develop information sharing and intelligence, still there is no established contact point for co-operation and co-ordination.

E. Lack of Proper Training of Law Enforcers

Most law enforcers do not have the proper training on computer forensics, investigation and handling of digital evidence. Worse, some do not have basic understanding of the concepts of cyber-security and cybercrime.

F. Public Awareness

Up to this time, the general public is not yet properly educated on the debilitating effect of cyber intrusions and improper computer ethics. The public should understand its role in securing the country's cyberspace.

IV. CONCLUSION

The challenge of controlling transnational cybercrime requires a full range of responses, including both voluntary and legally mandated co-operation. The government must actively pursue transnational initiatives, either voluntary, informal exchange of information, or multilateral treaties to establish a common and substantial degree of co-operation in the investigation and prosecution of cybercrime offences, since at present, there are widespread disparities among states, in the legal, regulatory, or policy environment concerning cybercrime.

With all the consolidation, revisions and filing anew of the improved version of the bills and trying to align these with the Budapest treaty, Congress has yet to act on the pending bills aimed at enacting cybercrime law in the Philippines.

Prosecutors and judges must possess technical know-how in litigating cybercrime cases.

The law enforcement agencies need specialized training and equipment in order to combat such a technical war.

Lastly, tapping all government allied agencies at the regional and international level will enhance capacity building efforts.

V. RECOMMENDATIONS

1. A law on cybercrime be enacted without delay, to supplement RA 8792, which conforms to internationally accepted standards.
2. Create a special agency with the technical expertise to monitor and regulate cyber-activities.
3. Law enforcement agencies be manned by law enforcement personnel with adequate computer skills and technical expertise and thoroughly trained to operate highly technical equipment.
4. Adequate resources be provided to law enforcement agencies in order to acquire the necessary tools, equipment and technical skills and continuously upgrade them for the defence of network systems from cybercrime attacks.
5. Technologies like firewalls, encryption and other infrastructure systems be required for all computer network systems in order to prevent intrusions.
6. Co-operation among all sectors of society to combat cybercrime.
7. Advocacy to increase awareness of the dangers of cybercrime be strengthened to include public awareness in order for everyone to become responsible and ethical users of computers and information systems.
8. Continuous efforts to lobby the members of Congress for the immediate passage of the cybercrime bill, to include the problem of cyber-terrorism.
9. Capacity building measures to ensure that law enforcement officers have a wide array of technical expertise in pursuing cybercrime-related investigations.
10. Technical equipment must also be updated, as technology is rapidly changing, in order to cope with the modern equipment of today's cybercrime offenders.
11. International co-operation like the MLAT must also be strengthened in order for member countries to address the problem of cybercrime.

THE CRIMINAL JUSTICE RESPONSE TO CYBERCRIME: THAILAND

*Santipatn Prommajul**

I. CYBERCRIME IN THAILAND

A. Current Situation

The transformation of global socio-economic structures along with the worldwide proliferation of new information and communication technologies has given rise to more forms of cybercrime, which pose threats not only to the confidentiality, integrity, or availability of computer systems, but also to the security of critical infrastructure. Furthermore, technological innovation gives rise to distinct patterns of criminal innovation: hence, different threats from cybercrime mirror differences across the spectrum of the so-called “digital divide”.

At the same time, recent rapid developments in information and communication technology, the growth of transnational transactions and the diversification of economic activities have all contributed to globalization. Together with these changes, which have created a global economic concern, the *modus operandi* of criminal groups has become more sophisticated and the scale of their activities has increased considerably.

This trend has been accelerated by the rapid proliferation of computers and the considerable increase in the number of Internet users. Advances in computer technology and Internet networks have encouraged Internet users to communicate more rapidly. While innocent users gain huge benefits from such global advancement, criminals have used the same technology to extend their activities and influence. Crimes committed using the Internet easily bypass national borders and criminals fully exploit this. At present, private security is threatened by faceless criminals.

The transnational nature of cybercrime hampers its detection and makes investigation and prosecution more difficult because investigation often requires tracing criminal activity and its effects through a variety of Internet service providers or private companies, sometimes across national borders, which may result in difficult questions of jurisdiction and sovereignty. Accordingly, international and regional co-operation would be an effective approach to assist domestic law enforcement to fight cybercrime.

Cyberspace becomes a newly powerful channel for criminals to commit illegal activities such as on-line fraud, phishing, 419 scams, identity theft, defamation, child pornography, on-line gambling and hacking or cracking. The statistics concerning computer-related offences analysed by the High-Tech Crime Center (HTCC), Royal Thai Police, reveals that from 2006 to 2008, 467 cybercrime cases were prosecuted. A large number of the offences were defamation, on-line fraud and child pornography.

In Thailand, cyber criminals have continuously developed new techniques to escape on-line tracing and police investigation. Rapid communication via the Internet allows criminals to network with transnational syndicates in committing crime in a very short space of time. As a result, techniques for collecting evidence and proving the accusations at trial are obstacles for police and prosecutors.

B. Offences Reported to the Royal Thai Police

The cybercrime cases that were reported to the Royal Thai Police after the Computer-Related Crime Act, B.E.2550 came into effect in July 2007 are categorized below.

* Deputy Superintendent, High Tech Crime Center, Royal Thai Police.

1. Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems

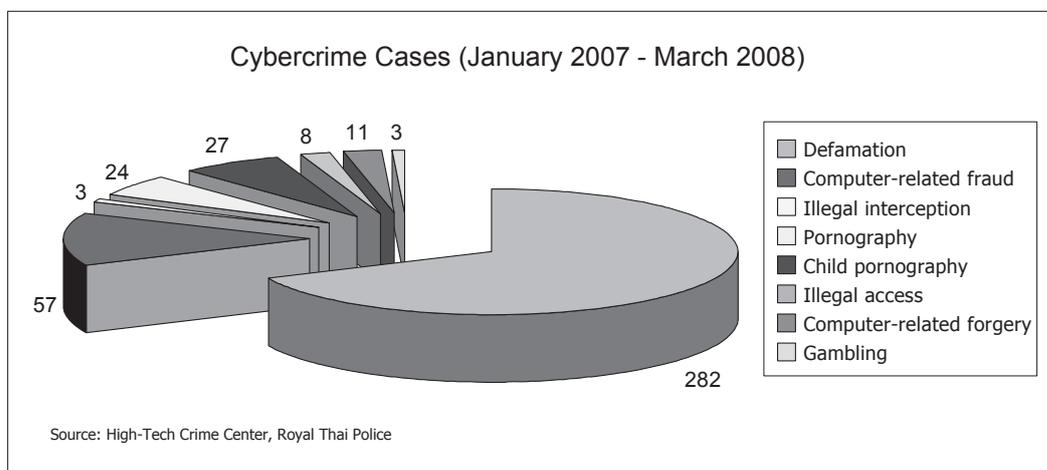
The number of such offences is low but the cost of the damage is high. The criminals employ sophisticated techniques or technology to prevent tracing by the police. Victims of these offences are the customers of Internet banking and online payment services.

2. Computer-Related Forgery and Computer-Related Fraud

These are the most serious category of cybercrime in Thailand. The criminals work mostly in-group and have no sophisticated disguising techniques. At present, there are some criminal groups from West Africa using Internet facilities in Thailand to run scams. The Royal Thai Police has set up a task force to combat these 419 scam groups.

3. Content-Related Offences

Pornographic and child pornographic websites are another category of cybercrime in Thailand. The Royal Thai Police and the Ministry of Culture have set a committee to monitor the content of websites. If they find any websites that contain obscene material or child pornography, the websites must be banned and the operators reported to the Royal Thai Police for prosecution.



II. LEGISLATION

A. Computer-Related Crime Act, B.E.2550 (2007)

The Computer-Related Crime Act, B.E.2550 entered into force in July 2007. The Act sets out the offences against computer-related crime covering hacking, unauthorized access, distributed denial of service, viruses/worms, website defacement, Internet fraud, identity theft, forgery, blackmail, gambling and pornography. It also specifies the authority of competent officials and criminal procedures. The new legislation has become a powerful tool for officers to allege, search, arrest and bring more offenders before court than in the past.

There are two chapters in this Act: Chapter One covers substantive offences; Chapter Two addresses criminal procedure.

Two main offences in Chapter One are enforced. The first are offences against the confidentiality, integrity and availability of computer systems and computer data. The second category is computer-related offences.

Chapter Two enumerates the competent officials who will lay down the procedural provisions for criminal investigations and proceedings.

The Minister of the Information and Communication Technology Ministry shall have charge and control of this Act and shall have the power to issue Ministerial Regulations for the execution of this Act (Section 4).

B. Ministerial Regulations

The Ministerial Regulations that will be issued under this Act are:

1. Ministerial Regulations regarding summonses of seizure or attachment (Section 19) – issued on 30 November 2007.
2. Ministerial Regulations regarding a list of undesirable programmes (Section 21) – not to be issued.
3. Ministerial Regulations regarding a duty of service providers to retain traffic data (Section 26) – enforced on 18 August 2008.
4. Ministerial Regulations regarding qualifications of competent officials (Section 28).
5. Ministerial Regulations regarding the form of the identity card of competent officials (Section 30).
6. Rules on guidelines and procedural methods in arresting, confining, searching, investigating and instituting criminal prosecution against the offender – to be drafted by the working group of the law enforcement agency.

C. Comparison of “Convention on Cybercrime: Council of Europe” and “Computer-Related Crime Act, B.E.2550”

On drafting the Computer-Related Crime Act, B.E.2550, Thailand had studied the Computer Crime Law or Related Law of other countries, including:

- The Electronic Commerce Act 2000 (The Philippines);
- The Computer Crime Act 1997 (Malaysia);
- The Computer Misuse Act (Singapore);
- The Unauthorized Computer Access Law 2000 (Japan);
- The Information Technology Act 2000 (India); and
- The Convention on Cybercrime: Council of Europe.

The following table shows the comparison between the “Convention on Cybercrime: Council of Europe” and the “Computer-Related Crime Act, B.E.2550 (2007)”.

Convention on Cybercrime: Council of Europe	Computer-Related Crime Act, B.E.2550
<p>Definitions</p> <p>“Computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a programme, performs automatic processing of data.</p>	<p>Definitions</p> <p>“Computer system” means a piece of equipment or sets of equipment units, whose function is integrated together, for which sets of instructions and working principles enable it or them to perform the duty of processing data automatically.</p>
<p>“Computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function.</p>	<p>“Computer data” means data, statements, or sets of instructions contained in a computer system, the output of which may be processed by a computer system including electronic data, according to the Law of Electronic Transactions.</p>
<p>“Service provider” means:</p> <p>(i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and</p> <p>(ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service.</p>	<p>“Service provider” shall mean:</p> <p>(1) A person who provides service to the public with respect to access to the Internet or other mutual communication via a computer system, whether on their own behalf, or in the name of, or for the benefit of, another person;</p> <p>(2) A person who provides services with respect to the storage of computer data for the benefit of the other person.</p>

<p>“Traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.</p>	<p>“Computer traffic data” means data related to computer system-based communications showing sources of origin, starting points, destinations, routes, time, dates, volumes, time periods, types of services or others related to that computer system’s communications.</p>
<p>Offences</p> <p>Article 2 – Illegal access</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p>Section 5</p> <p>Whoever illegally accesses a computer system that has specific security measures and such security measures are not intended for his use, shall be liable to imprisonment for a term not exceeding six months or to a fine not exceeding ten thousand Baht or to both.</p>
<p>Article 3 – Illegal interception</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p>Section 8</p> <p>Whoever illegally makes, by any electronic means, an interception of computer data of another person that is being transmitted in a computer system and such computer data is not for the benefit of the public or is not available for other persons to utilize, shall be liable to imprisonment for a term not exceeding three years or to a fine not exceeding sixty thousand Baht or to both.</p>
<p>Article 4 – Data interference</p> <p>1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.</p> <p>2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.</p>	<p>Section 9</p> <p>Whoever illegally acts in a manner that causes damage, impairment, deletion, alteration or addition either in whole or in part of computer data of other person, shall be liable to imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand Baht or to both.</p>
<p>Article 5 – System interference</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.</p>	<p>Section 10</p> <p>Whoever illegally acts in a manner that causes suspension, deceleration, obstruction or interference of a computer system of another person so that it can not function normally, shall be liable to imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand Baht or to both.</p>

<p>Article 6 – Misuse of devices</p> <p>1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:</p> <p>(a) the production, sale, procurement for use, import, distribution or otherwise making available of:</p> <p>(i) a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;</p> <p>(ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and</p> <p>(b) the possession of an item referred to in paragraphs (a) (i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.</p> <p>2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system.</p> <p>3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (ii) of this article.</p>	<p>Section 13</p> <p>Whoever sells or disseminates sets of instructions developed as a tool used in committing an offence under Section 5, Section 6, Section 7, Section 8, Section 9, Section 10 and Section 11 shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding twenty thousand Baht or to both.</p>
<p>Article 7 – Computer-related forgery</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.</p>	<p>Section 14</p> <p>Whoever commits any offence of the following acts shall be liable to imprisonment for not more than five years or a fine of not more than one hundred thousand baht or both:</p> <p>(1) that involves import to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to that third party or the public;</p> <p>(2) that involves import to a computer system of false computer data in a manner that is likely to damage the country's security or cause a public panic;</p>

<p>Article 8 – Computer-related fraud</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:</p> <p>(a) any input, alteration, deletion or suppression of computer data, (b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p>	<p>(3) that involves import to a computer system of any computer data related with an offence against the Kingdom’s security under the Criminal Code;</p> <p>(4) that involves import to a computer system of any computer data of a pornographic nature that is publicly accessible;</p> <p>(5) that involves the dissemination or forwarding of computer data already known to be computer data under (1) (2) (3) or (4).</p>
<p>Article 11 – Attempt and aiding or abetting</p> <p>1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.</p> <p>2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.</p> <p>3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.</p>	<p>The attempt, abetments or aiding is not stipulated in this Act because the Criminal Code can be applied.</p> <p>Section 15</p> <p>Any service provider intentionally supporting or consenting to an offence under Section 14 within a computer system under their control shall be subject to the same penalty as that imposed upon a person committing an offence under Section 14.</p>
<p>Article 14 – Scope of procedural provisions</p> <p>1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.</p> <p>2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:</p> <p>(a) the criminal offences established in accordance with Articles 2 through 11 of this Convention;</p> <p>(b) other criminal offences committed by means of a computer system; and</p> <p>(c) the collection of evidence in electronic form of a criminal offence.</p> <p>3. (a) Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of</p>	<p>Section 18</p> <p>Within the power of Section 19 and for the benefit of an investigation, if there is reasonable cause to believe that there is the perpetration of an offence under this Act, then a relevant competent official shall have any of the following authorities only as necessary to identify a person who has committed an offence in order to:</p> <p>(1) Issue an inquiry letter to any person related to the commission of an offence under this Act or summon them to give statements, forward written explanations or any other documents, data or evidence in an understandable form;</p> <p>(2) Call for computer traffic data related to communications from a service user via a computer system or from other relevant persons;</p> <p>(3) Instruct a service provider to deliver to a relevant competent official service users-related data that must be stored under Section 26 or that is in the possession or under the control of a service provider;</p> <p>(4) Copy computer data, computer traffic data from a</p>

offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

(b) Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

(i) is being operated for the benefit of a closed group of users; and

(ii) does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

computer system, in which there is a reasonable cause to believe that offences under this Act have been committed if that computer is not yet in the possession of the competent official;

(5) Instruct a person who possesses or controls computer data or computer data storage equipment to deliver to the relevant competent official the computer data or the equipment pieces;

(6) Inspect or access a computer system, computer data, computer traffic data or computer data storage equipment belonging to any person that is evidence of, or may be used as evidence related to, the commission of an offence or used in identifying a person who has committed an offence, and instruct that person to send the relevant computer data to all necessary extent as well;

(7) Decode any person's computer data or instruct any person related to the encryption of computer data to decode the computer data or cooperate with a relevant competent official in such decoding;

(8) Seize or attach the suspect computer system for the purpose of obtaining details of an offence and the person who has committed an offence under this Act.

Section 19

The power of authority of the relevant competent official under Section 18 (4), (5), (6), (7) and (8), is given when that competent official files a petition to a court with jurisdiction for an instruction to allow the relevant competent official to take action.

However, the petition must identify a reasonable ground to believe that the offender is committing or going to commit an offence under the Act as well as the reason of requesting the authority, including the characteristics of the alleged offence, a description of the equipment used to commit the alleged offensive action and details of the offender, as much as this can be identified. The court should adjudicate urgently such aforementioned petition.

When the court approves permission, and before taking any action according to the court's instruction, the relevant competent official shall submit a copy of the reasonable ground memorandum to show that an authorization under Section 18 (4), (5), (6), (7) and (8), must be employed against the owner or possessor of the computer system, as evidence thereof. If there is no owner of such computer thereby, the relevant competent official should submit a copy of said memorandum as soon as possible.

In order to take action under Section 18 (4), (5), (6),

	<p>(7) and (8), the senior officer of the relevant competent official shall submit a copy of the memorandum about the description and rationale of the operation to a court with jurisdiction within forty eight (48) hours after the action has been taken as evidence thereof.</p> <p>When copying computer data under Section 18 (4), and given that it may be done only when there is a reasonable ground to believe that there is an offence against the Act, such action must not excessively interfere or obstruct the business operation of the computer data's owner or possessor.</p> <p>Regarding seizure or attachment under Section 18 (8), a relevant competent official must issue a letter of seizure or attachment to the person who owns or possesses that computer system as evidence. This is provided, however, that the seizure or attachment shall not last longer than thirty days. If seizure or attachment requires a longer time period, a petition shall be filed at a court with jurisdiction for the extension of the seizure or attachment time period. The court may allow only one or several time extensions, however altogether for no longer than sixty days. When that seizure or attachment is no longer necessary, or upon its expiry date, the competent official must immediately return the computer system that was seized or withdraw the attachment.</p> <p>The letter of seizure or attachment under paragraph one shall be in accordance with a Ministerial Regulations.</p>
<p>Article 17 – Expedited preservation and partial disclosure of traffic data</p> <p>1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:</p> <p>(a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and</p> <p>(b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.</p> <p>2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>Section 26</p> <p>A service provider must store computer traffic data for at least ninety days from the date on which the data is input into a computer system. However, if necessary, a relevant competent official may instruct a service provider to store data for a period of longer than ninety days but not exceeding one year on a special case by case basis or on a temporary basis.</p> <p>The service provider must keep the necessary information of the service user in order to be able to identify the service user from the beginning of the service provision, and such information must be kept for a further period not exceeding ninety days after the service agreement has been terminated.</p> <p>The types of service provider to whom the provisions under paragraph one shall apply and the timing of this application shall be established by a Minister and published in the Government Gazette.</p> <p>A service provider who fails to comply with this Section, shall be liable to a fine not exceeding five hundred thousand Baht.</p>

<p>Article 22 – Jurisdiction</p> <p>1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:</p> <p>(a) in its territory; or</p> <p>(b) on board a ship flying the flag of that Party; or</p> <p>(c) on board an aircraft registered under the laws of that Party; or</p> <p>(d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.</p> <p>2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.</p> <p>3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.</p> <p>4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.</p> <p>5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.</p>	<p>Section 17</p> <p>Whoever commits an offence pursuant to this Act outside the Kingdom, whether</p> <p>(1) the offender be a Thai person, and there be a request for punishment by the Government of the country where the offence has occurred or by the injured person ; or</p> <p>(2) the offender be an alien, and the Royal Thai Government or a Thai person be the injured person, and there be a request for punishment by the injured person, shall be punished in the Kingdom.</p>
--	--

III. MEASURES

A. Measures to Combat Cybercrime

1. Domestic Approach

(i) Prevention

- Promote public understanding of the cybercrime situation and teach the public how to protect itself from cyber criminals.
- Enlist the co-operation of the private sector and the public in reporting illegal websites, online fraud, etc. and in the investigation process.
- Force the regulations enactment and enforce the Computer-Related Crime Act.

(ii) Suppression

- Provide investigation knowledge for local police, so that they can rapidly respond to cybercrime cases.
- Improve the investigation techniques and the skills of cybercrime investigators to specialist standard and the level accepted by the international law enforcement agencies.

2. International Approach

- Participate in international activities, meetings, training, etc. to share intelligence and experience.
- Co-operate with international law enforcement agencies and assist in solving cybercrime cases upon request. At this moment, the Royal Thai Police has assigned officers from High-Tech Crime Center to be contacts for ASEAN 24/7 High-Tech Crime, Cybercrime Technology Information Network System (CTINS) and other law enforcement agencies.

B. Our Vision in Combating Cybercrime

1. Domestic Approach

- Secure the co-operation of the private sector and public to provide information, advance technology and funding for combating cybercrime.
- Train police to achieve excellent capability in cybercrime investigation techniques.
- Develop a knowledge-base and a case management system and provide it to the public and other law enforcement agencies.

2. International Approach

- Develop co-operation among international law enforcement agencies by supporting international workshops and meetings.
- Assign a contact person for information exchange among international law enforcement agencies.

IV. ACTUAL CASE

A. 419 Scam

1. Situation

In June 2008, a Thai bank complained to the High-Tech Crime Center, Royal Thai Police, that its logo and a fake name given as its bank manager were used in spam mail. Some customers requested the bank to clarify that mail.

Spam mail informed the receiver that he or she had won US\$1,000,000 and the winner must transfer the money for tax payment and service charges including a transfer fee of about US\$10,000 to receive this fund. The bank's logo and the fake name of its bank manager were attached in the mail.

2. Investigation

The Royal Thai Police set up a task force to investigate the case led by the Central Investigation Bureau together with the Immigration Bureau, Foreign Affairs Division and High-Tech Crime Center. On investigating, the task force found following facts:

- Three e-mail addresses were used in sending the spam mail;
- The bank manager's name was fake;
- A bank account was opened to receive the transferred money. The owner was a Thai woman.
- The IP address of every spam mail came from the same place. With co-operation from the Internet service provider company, the team found the location at an Internet café in Bangkok.

A surveillance team investigated the owner of the Internet café. He informed them that an African group used his Internet café daily. The team reported that about 30 African people stayed in accommodation around that area, some in the same building as the Internet café.

Covert officers were set to work as staff of the café and manually logged the usage of computers there. The syndicate only used computers to send e-mail, not to surf the Internet.

A court order was issued to do a real time interception of traffic and content data from the Internet café. Log recorders and analysis devices were set at the gateway of the Internet café network.

On viewing the traffic data, the task force compared log records including contents and manual logs to identify the activity of the syndicate. Traffic data proved that syndicates used the café for sending spam mail and committing fraud.

3. Operation

The task force submitted a warrant of arrest for 13 suspects including one Thai woman. The court issued the warrants on 24 July 2008 and the operation was set.

About 200 police officers (uniformed and undercover) were deployed to three target areas. Eighteen suspects (17 Ghanaians and 1 Thai) were arrested.

4. Key to Success

The success of this operation was due to co-operation among the law enforcement agencies and private companies.

The co-operation of police officers from different units caused this operation to succeed. Their intention in combating cybercrime led them to share all information and to learn from each other.

SRAN Security Center provided the log recorders and traffic data analysis at the Internet café free of charge. It caused the task force to prove and present all evidence to the court for the issuing of the warrants of arrest.

Co-operation from Western Union (providing transaction data from the victims to the suspects) led the task force to identify the location of the group leader.

REPORTS OF THE COURSE

GROUP 1

ISSUES AND MEASURES CONCERNING THE LEGAL FRAMEWORK TO COMBAT CYBERCRIME

Chairperson	Mr. Syed Abbas Ahsan	(Pakistan)
Co-Chairperson	Mr. Vijith Kumara Malalgoda	(Sri Lanka)
Rapporteur	Mr. Sergio Gardenghi Suiama	(Brazil)
Co-Rapporteur	Mr. Bafi Nlanda	(Botswana)
Members	Mr. Saleh Mohammad Altawalbeh	(Jordan)
	Mr. Santipatn Prommajul	(Thailand)
	Mr. Koji Sakamoto	(Japan)
	Mr. Nozomu Suzuki	(Japan)
	Advisers	Deputy Director Takeshi Seto
	Professor Jun Oshino	(UNAFEI)
	Professor Junichiro Otani	(UNAFEI)
	Professor Tae Sugiyama	(UNAFEI)

Legal Notice: This report has been written on behalf of the group by the Chairperson and the Rapporteur on the basis of information supplied by the participants of the course. Neither UNAFEI nor any person acting on its behalf is responsible for the contents and information contained in this Report. The views expressed in this publication do not necessarily reflect the official views of UNAFEI or any person acting on its behalf. The opinions given by individual participants are based on the information available to them, their understanding of the same, and are not representative of the official stance of their respective countries.

I. INTRODUCTION

Group 1 started its discussion on 16 October 2008. The group elected, by consensus, Mr. Ahsan as chairperson, Mr. Malalgoda as co-chairperson, Mr. Suiama as Rapporteur, and Mr. Nlanda as Co-rapporteur. The group, following its assigned topic, “Issues and Measures concerning the Legal Framework to Combat Cybercrime”, agreed to conduct the proceedings in accordance with the following agenda:

1. Issues and measures relating to the criminalization of cybercrime;
2. Legal issues relating to the procedural law related to cybercrime, including admissibility of digital evidence;
3. Challenges in combating trans-border cybercrime, including issues of jurisdiction and international co-operation.

II. SUMMARY OF THE DISCUSSIONS

A. Substantive Criminal Law in Respective Countries Concerning Cybercrime, including Evaluation according to the Convention on Cybercrime

The group decided first to identify which offences have been criminalized by the countries as required by the Convention on Cybercrime. The group considered the Convention as a guideline establishing the international standards regarding this issue. Each participant of the Course had received a handout in order to clarify what offences are already included in their respective laws.

According to the participants, the current substantive criminal law of the respective countries regarding cybercrime is shown in the following table:

Country	Illegal access to a computer system	Illegal interception of data	Illegal data interference	Illegal system interference	Illegal production and distribution of devices	Computer-related fraud	Computer related-forgery	Child pornography	Copyright violations
Bangladesh	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Botswana	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

140TH INTERNATIONAL TRAINING COURSE
REPORTS OF THE COURSE

Brazil	Partially	Yes	Partially	Partially	No	Yes	Yes	Yes	Yes
Hong Kong	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Indonesia	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Japan	Yes	Yes	Yes	Yes	Partially	Yes	Partially	Yes	Yes
Jordan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mexico	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pakistan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Philippines	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes
Sri Lanka	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Thailand	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Country	Identity theft	Illegal gambling	Cyber Terrorism¹	Spam	Libel and false information	Racism and Hate Speech
Bangladesh	Yes	Yes	Yes	Yes	Yes	Yes
Botswana	Yes	No	No	No	No	Yes
Brazil	No	Yes	No	No	Yes	Yes
Hong Kong	Yes	Yes	Yes	Yes	Yes	Yes
Indonesia	Yes	Yes	Yes	No	Yes	Yes
Japan	No	Yes	No	Yes	Yes	No
Jordan	Yes	Yes	Yes	Yes	Yes	Yes
Mexico	Yes	No	No	No	Yes	No
Pakistan	Yes	Yes	Yes	Yes	Yes	No
Philippines	No	No	No	No	No	No
Sri Lanka	No	No	No	No	No	Yes
Thailand	Yes	No	Yes	Yes	Yes	No

The Chairperson, following the agenda, asked the group to discuss their national legislation regarding cybercrime. From the discussions, it was established that some countries have specific legislation on this subject, but some States do not have a separate legal framework. In such cases, they are using their prevailing legislation with amendments catering for illegal and harmful use of computer systems.

Of all the participating countries, Bangladesh, Botswana, Indonesia, Pakistan, Sri Lanka and Thailand have specific legislation against cybercrime. Brazil, Japan, Jordan, Hong Kong, Mexico and the Philippines do not have a specific legislation on cybercrime.

In Bangladesh, the Information and Communication of Technology Act (2006) covers the offences defined by the Convention on Cybercrime. According to the participant from this country, computer related fraud and forgery could be handled under the provisions of the Penal Code.

In Botswana, most of the offences have been criminalized by a specific act, except the violation of copyright. However, there is another act covering copyright offences, although this act does not mention offences committed on the Internet. The law is silent regarding electronic documents. Child pornography is criminalized (including possession).

In Pakistan, the Prevention of Electronic Crimes Ordinance was enacted to deal with cybercrime and criminalizes all the offences listed in the handout except child pornography and infringement of copyright. However, pornography of all kinds is criminalized in Pakistan through the special law against pornography; therefore, offences related to child pornography defined in the Convention are already covered in the existing legal framework. In addition, Pakistan has criminalized illegal access to computer data as a separate offence. Furthermore, the law does not criminalize copyright infringement as this is covered in a separate law.

In Sri Lanka, almost all offences defined by the Cybercrime Convention, except computer-related fraud and forgery, have been criminalized. Electronic transactions and documents are considered valid according

¹ There is no global consensus about the definition of the term “cyber-terrorism”. Therefore, the table has only considered the definition of “terrorism” provided by the national legislations.

to Sri Lankan law. However, the Penal Code already covers the offences of fraud and forgery. In addition, the Evidence Ordinance accepts computer-generated documents as evidence; hence it is possible to prosecute computer-related fraud and forgery as well. Violations of copyright and patents are criminalized and have specific provisions in the law. The Penal Code includes child pornography as a crime, including possession, distribution, sexual abuse and publication. However, there is no specific provision for such crimes when committed on the Internet.

In Thailand, all offences defined in the Cybercrime Convention except child pornography and copyright violations have been criminalized under the Computer Crime Act. Child pornography (possession included) is an offence under Child Protection Act and copyright violations are dealt under the Copyrights Act.

In Brazil, the Penal Code, the Statute of Childhood and Youth and two Federal Acts are sufficiently broad to cover most of the offences defined in the Convention on Cybercrime, except misuse of devices and access and interference in private systems.

In Mexico, the Penal Code covers most of the offences defined in the Convention.

In Indonesia, all the offences defined by the Convention are already criminalized.

In Japan, almost all of the offences are already covered by the Japanese Penal Code or special laws. There is a specific law for copyright offences. Regarding child pornography, the possession of images is not criminalized. Moreover, the production and distribution of computer viruses are not criminalized at present. Misuse of devices is partially covered by national criminal legislation.

In Jordan there are no specific laws, but the Penal Code has been modified to include computer crimes. Moreover, there is a specific law for electronic transactions. Furthermore, draft legislation is under review in the Parliament, aiming at addressing all the offences as defined in the Convention on Cybercrime. Presently, the legal framework is not sufficiently broad to cover all these offences.

In the Philippines, the E-Commerce Act criminalizes only hacking and piracy.

In Hong Kong most of the offences identified under the convention are criminalized under the Crime Ordinance, except child pornography and copyright violations. Child pornography is an offence under Publication of Child Pornography Act and copyright violations are criminalized under the Copyright Ordinance.

After the overview of the respective legal frameworks, the Chairperson proposed a thorough analysis of each article of the Convention, aiming at clarifying any ambiguity regarding the interpretation of the text of the treaty.

Beginning with Article 2, the group debated whether the criminalization of illegal access to a standalone computer (not connected to a network system) should remain optional or be mandatory for the States Parties. Mr. Sakamoto argued that the law in Japan does not consider mere access to a standalone computer a criminal matter, since mere data access is not criminalized under any circumstances. Mr. Ahsan, on the other hand, was of the opinion that the Convention makes it mandatory for all States Parties to criminalize illegal access to standalone computers. Prof. Oshino, while referring to the Convention, explained that Article 2 makes it mandatory to criminalize illegal access to a computer system, connected to a network; however, the Convention differentiates between a computer connected to a network and a standalone computer in the article, and provides an option to the States to criminalize only the first situation. The group agreed to the explanation given by Prof. Oshino, as the wording of the article allows countries to restrict their legislation to computer systems connected to another system through a network.

Professor Oshino inquired about the situation in different countries in respect of offences with the following conditions established by Article 2:

1. Committed by infringing security measures;
2. With the intent of obtaining computer data; and
3. In relation to a computer system that is connected to another computer system.

Mr. Ahsan, Mr. Nlanda, Mr. Saleh and Mr. Malalgoda declared that Pakistan, Botswana, Jordan and Sri Lanka, respectively, do not attach any conditions to the criminalization of illegal access to a computer system. Mr. Prommajul said that in Thailand, the law requires the first condition to be satisfied. Mr. Suiama noted that in Brazil, the second and third conditions have to be established for criminal sanctions. Mr. Suzuki explained that in Japan, the first and third conditions should be satisfied.

The group further discussed criminalizing illegal gambling, cyber-terrorism, spamming, libel, slander, racism and hate speech. The group did not arrive at a definite answer on these issues and decided to take further advice from the Visiting Expert Prof. Marco Gerke. Mr. Ahsan, the Chairperson, concluded on behalf of the group that individual states should be allowed to legislate on these issues according to their own standards of criminal law. This conclusion was also based on the differing constitutional obligations of the states with reference to the rights of their citizens.

B. Visiting Expert's Opinion

To take advantage of the presence of the Visiting Expert, Prof. Marco Gerke, the Chairperson proposed that the session could be dedicated to the discussion of complex issues, on which the group could not come to a definite conclusion. Mr. Ahsan further elaborated that issues thus raised could be put to Prof. Gerke to take his guidance on these questions. The proposal was accepted by the group and the discussion was focused on issues on which the group sought assistance of the Visiting Expert.

Mr. Suiama explained that the most important issue for him was jurisdiction in cybercrime, whereby we can use three approaches:

- A. Exercising extra-territorial jurisdiction, but this will raise the problems of sovereignty and breach of international law;
- B. International co-operation through mutual legal assistance treaties or multilateral treaties like the Council of Europe Convention on Cybercrime; however, this would require dual criminality and the process will be prone to unnecessary delays;
- C. Obliging the local offices of transnational companies to co-operate with the Law Enforcement Agencies.

Seconding the point of Mr. Suiama, Mr. Sakamoto proposed that the following questions should be raised by the group for Prof. Gerke on this issue:

1. Comparing the options of exercising jurisdiction vs. international co-operation; as cybercrime is a borderless crime and transcends international boundaries, how do law enforcement agencies exercise jurisdiction and what is the scope of international co-operation?
2. If the offender is in one country and the victim is in another country, is it possible for the country in which the victim resides to claim jurisdiction? And what if a service based in a country is focused on clients based in other countries?
3. If a service provider's office is located in a country, would it be advisable for the country to oblige such service provider to share data, e.g. the IP address of its users?

The criminalization of spam, libel and false information were also discussed by Mr. Prommajul and Mr. Nlanda, and then referred to the visiting expert as two separate questions:

4. What was the opinion of the Visiting Expert on the criminalization of spam?
5. Should libel and false information be criminalized with reference to cybercrime?

Additionally, Mr. Ahsan suggested that Dr. Gercke be requested to explain issues of criminalization of illegal access to data and to take his opinion on illegal access to standalone computers as well. The group also referred the issue of remote access tools used by law enforcement agencies. To this end the following questions were formulated:

6. Illegal Access to a computer in the convention does not include illegal access to data. The Convention also makes illegal access to a standalone computer an optional offence. What was the opinion of the Expert on these two issues?
7. What was the opinion of the Visiting Expert on the use of remote access tools by Law Enforcement Agencies?

The response of the Visiting Expert Dr. Marco Gercke, in the same order as the questions raised, is as follows:

1. The international co-operation approach is a better option, either directly or through the 24/7 Contact Point. Using the 24/7 Contact Point is a faster mode and the Contact Point will have all the resources and knowledge to reach the relevant person and get the necessary information and evidence at the earliest possible time. This approach has better chances of enforcement, considering that getting evidence from foreign companies, conducting investigations outside its territorial jurisdiction or arresting a suspect in a foreign country may not be easy through other means and may infringe international law. Furthermore, co-operation will not be voluntary and forthcoming to a foreign law enforcement agency but a local law enforcement agency will be better placed to enforce laws in its own jurisdiction.
2. It is possible to establish jurisdiction on the basis of the passive personality principle. Moreover, to resolve issues relating to jurisdiction, it is necessary to establish minimum standards of criminalization for all countries and also to improve international co-operation in these crimes.
3. It would not be very effective to oblige the service provider to share data and information because in some instances the service provider might just decide to close its office and leave the country. It could be more functional to use international co-operation in these matters.
4. The criminalization of spam in general is not advisable. A good example, however, is the law regarding spam in the United States, where only hiding one's identity or using spam for illegal purposes is considered a criminal offence.
5. On the issue of libel, slander and false information, it would be better to look at the general criminal law provisions and follow the same standards, noting however, that it is better to have civil remedies for such acts as applied in many countries.
6. Regarding illegal access to data, it is included in the illegal access to a system. However, as we could see from the Hong Kong example, in which a technician was given a computer to repair and copied information, it might be necessary to criminalize the illegal collection and copying of data. Although it is preferable to criminalize illegal access to standalone computers, in some jurisdictions that is not considered an offence, so a failure to criminalize would not be a serious deficiency in the law.
7. Regarding the use of remote investigative tools, in certain cases the use of such tools may be the only way to investigate a crime; therefore, the use of such tools should not be completely barred. It should be permitted according to the law of a particular jurisdiction defining the limits of the use of such tools.

C. Issues and Challenges faced by Countries concerning Procedural Law, Jurisdiction and International Co-operation

The group briefly looked at the procedural law relating to cybercrime in the participating countries. Procedural laws are available in most countries that support law enforcement agencies to investigate cybercrime, especially the general procedure on search and seizure, expedited preservation, and real time collection and interception of computer data. Most countries do not have any specific procedure on using remote investigation tools, identification requirements for Internet users, disclosure obligations or data retention obligations. The current procedural law of the respective countries regarding cybercrime is shown in the following table:

140TH INTERNATIONAL TRAINING COURSE
REPORTS OF THE COURSE

Country	Expedited preservation of computer data	Search for computer data	Seizure of computer data	Real time collection of traffic data	Real time interception of contents data	Use of remote investigation tools	ID requirement	Disclosure obligations of encryption keys	Data retention obligation
Bangladesh	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes
Botswana	Yes	Yes	Yes	Yes	No	No	No	No	No
Brazil	No	Yes	Yes	No	Yes	No	Partially	No	No
Hong Kong	No	Yes	Yes	Yes	Yes	Yes	No	No	No
Indonesia	Yes	Yes	Yes	Yes	Yes	Yes	Partially	Yes	Partially
Japan	Yes	Yes	Yes	Yes	Yes	No	No	No	No
Jordan	Not clarified	Yes	Yes	No	No	Not clarified	Yes	Not clarified	Yes
Mexico	Yes	Yes	Yes	Yes	Yes	Partially	No	No	No
Pakistan	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Philippines	No	No	No	No	No	No	No	No	No
Sri Lanka	Yes	Yes	Yes	Yes	Yes	No	No	No	No
Thailand	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

The group discussion was opened by the Chairman with a question about whether it is possible to investigate and to prosecute a person for illegal content discovered during a search and seizure process which content was not included in the scope of the judicial warrant? After analysing the issue, the group concluded that in fact such a discovery will not be in violation of the warrant, and criminal proceedings can be initiated against the person based on the discovery of incriminating content.

Mr. Ahsan then drew the attention of the group towards the issue of expedited preservation of data. Mr. Saleh stressed the necessity to have specific provisions for search and seizure and preservation of data as such tools are indispensable for cybercrime investigations. Mr. Malalgoda informed the group that Sri Lankan law states that police officers can enforce expedited preservation data for seven days. Mr. Sakamoto added that, in Japan, the process to obtain a search warrant is very expeditious, but it is still advisable to have a provision for the expedited preservation of evidence due to the fluid nature of evidence and data. The group agreed to the importance of the provision for expedited preservation of data and recommended that such a provision should be considered for legislation as evidence in cyberspace can be lost, altered or deleted with much ease.

The Chairman then requested the group members to give their opinion on the issue of admissibility of copied data in the courts and use of data available on websites as evidence. Giving the example of Pakistan, he said that specific changes have been made in the evidence laws in Pakistan to bring electronic evidence in digital format on par with other kinds of evidence; for this the Electronic Transactions Ordinance has established rules and standards of admissibility. Mr. Sakamoto in this regard mentioned that the law in Japan has provisions of search and seizure of hardware, but the law does not stipulate mere copying of digital evidence. Secondly, theoretically, data published on websites can be admissible, but it is advisable that web-based data should be duly verified by the service providers who host such data. Mr. Suiama emphasized that we have to differentiate between published content data available on websites, which can be collected directly by a forensic expert, and traffic data or communication records for which verification can be made mandatory. Mr. Prommajul explained that his experience in prosecuting such cases is that courts require data be made available in printed form where possible. Moreover, in cases involving hackers or malicious code attacks, it is necessary to set up an isolated computer network to show to the court how the crime is committed. He also added that technically it is possible to download the content of a webpage without the assistance of the ISP, but traffic data can only be obtained from an ISP if they retain such data. Summing up the discussion of the group, the Chairman said that digital evidence should be admissible in court and the law should specify a standard for the admissibility of digital evidence. He further added that the group was of the opinion that it is preferable that the standards of collection of digital evidence include certification/verification by the service providers to remove ambiguity and doubt about the evidence collected.

The group next moved to the issue of real time collection of traffic data and interception of content data. Mr. Suiama explained that in Brazil, interception of content data is possible for a maximum period

of 15 days with court orders, but it is possible to extend the time period. According to Mr. Prommajul, in Thailand, interception of content data is possible with court orders and there is no time limitation, but such interception can only be initiated in cybercrimes. Mr Suzuki added that in Japan, apart from the court overview, such methods can be used only in limited offences.

Mr. Ahsan, introducing a new topic, the obligation to retain traffic data, said that in Pakistan, the law states that ISPs must retain traffic data for 90 days. There is a penal sanction of six months for not maintaining traffic data. Mr Suiama added that Brazil has no specific obligation on this matter but the national congress is discussing a minimum mandatory traffic data retention period of two years. Mr. Suzuki, Mr. Malalgoda and Mr. Nlanda also pointed out that their countries do not have specific laws for retention of traffic data. In Thailand, Mr. Prommajul explained, the law states that the ISP must keep traffic data for at least 90 days (and a maximum of one year). If they do not comply with this obligation, they are subject to a fine. The group opined that Article 20 of the Convention supports retention of traffic data and therefore concluded that a legal framework should consider including an obligation for retention of traffic data for a minimum period of six months.

The next topic that came under discussion was the use of remote investigation tools. Mr. Prommajul described that it is possible to search and collect evidence remotely and use different remote access tools to trace criminals. However, over and above the legal issues, it is not possible to assure the integrity of evidence collected through remote means, since the investigators would have full access to the computer of the suspect. It would be difficult to use this data as evidence in a court of law. In terms of interception for the purpose of investigation only to ascertain the commission of an offence or find the location of the offender, use of key loggers and similar tools could be a good, and possibly the only, option. Mr. Suiama raised two issues: first, whether we could use the same rules for normal search and seizure in cases of remote search and seizure; secondly, is this tool a violation of privacy if performed under judicial supervision? The Chairperson was of the opinion that normal search and seizure cannot be compared to remote search and seizure as the suspect is unaware of the whole process. Secondly, if normal search and seizure is possible and the suspect identified, the need for remote search and seizure should not arise. The group agreed that the use of such tools is a controversial issue, but considered that sometimes this tool may be the only option available to the investigators. It was therefore decided that the legal aspects of the use of remote access tools required further in-depth analysis. Nonetheless, the law must define clear limits for the use of such remote access tools and the circumstances in which the use is permitted.

The group then moved to the issue of identification when accessing the Internet through a public terminal. Mr. Ahsan said that in Pakistan, there is no such obligation, and opined that such a system was not useful as the trend is towards liberalizing access to information technology as it is now the major source of knowledge and communication. Many other options are available to offenders and by such measures we will restrict the use of information technology for normal and constructive purposes. Mr. Suiama agreed that it is useless sometimes to oblige cybercafés to identify their users. On one hand, there is an ideal of free access to communication and on the other, there is a challenge in identifying crimes and suspects under difficult circumstances. Mr. Saleh thought it was important to take this measure in order to prevent cybercrime, and identify users at Internet cafés. Mr. Suiama mentioned a possibility of the use of digital identification, but added that it would result in higher costs. The Chairperson recommended encouraging Internet cafés to voluntarily use identification as a social responsibility and good practice. Mr. Suiama and Mr. Sakamoto proposed administrative regulation as another option. The group decided that the use of Internet cafés is different around the world, and although it is better to have a process for identification, the matter is left to countries to take measures suiting their circumstances.

On the issue of disclosure of passwords and encryption keys, Mr. Ahsan said that the law in Pakistan obliges the suspect to provide the password or key but this law is being criticized as a violation of the constitution and against the principle of protection against self incrimination. On the other hand, the supporters of the law argue that any self-incriminating evidence would not be admissible in court and therefore not used, but such measures would be helpful to obtain other evidence. Mr. Prommajul added that in Thailand, there is also a similar obligation, but it demands a judicial request. There is a criminal penalty if the suspect refuses to give the password (a daily fine until he or she complies). Other participants were of the opinion that a law with the possibility of self incrimination would not be possible in their countries.

The final and very important topic discussed by the group was that of jurisdiction and international co-operation. The discussion was opened by the Chairperson who explained the different types of jurisdiction and the issues faced by the international community relating to jurisdiction in cybercrime. Mr. Suiama proposed that it is necessary to go further and try to define some criteria that can be used to define jurisdiction on the Internet. Mr. Malalgoda stated that we must look at the nature of an offence in order to define the jurisdiction. Mr. Ahsan stated that the issues of jurisdiction would best be solved if we establish a proper mechanism of international co-operation. Mr. Suzuki added that there should be some minimum standards of international co-operation which should be made part of the legal framework of our own countries. As for exercising jurisdiction, a number of issues should be considered including the place where the offence was committed, the place of the victim and the ability to conduct investigation. Mr. Suiama was of the opinion that even when the international community has achieved consensus, there are still some areas of conflict (e.g. hate speech) and it is important to consider these areas. He maintained also that the country where the data is located or where the ISP has its headquarters should not be considered the only criteria to define jurisdiction, since there are many international services provided from the US that are used for nationals to commit crimes. The group agreed on the importance of international co-operation/co-ordination and recommended that minimum standards of criminalization must be established and followed to address the issue of dual criminality. In addition, standards for international co-operation in cases of cybercrime should be formulated and established.

III. CONCLUSIONS

After lively discussions, the group reached the following conclusions:

1. The group agreed that all countries may adopt some basic international standards regarding both substantive and procedural criminal law. Recognize that the Convention on Cybercrime can be used as a good reference for minimum standards that may be adopted by the participating countries. It is also necessary to move toward some basic rules regarding the collection and admissibility of evidence from foreign jurisdictions. Three participants wish to include other international conventions (especially human rights treaties) as minimum standards as well;
2. The group also agreed upon the urgent necessity to improve the investigative and judicial mechanisms of international co-operation, in order to cope with a phenomenon that is fundamentally transnational. It was also suggested that adequate procedural laws may be implemented to assure the expedited preservation of evidence also when requested by foreign jurisdictions, while the regular measures are being completed;
3. The group understands that it is necessary to improve also the mechanisms of international co-operation in terms of training and technical aid provided for members of law enforcement agencies. These training programmes may include members from all the institutions related to the criminal justice system;
4. Data espionage is not properly covered by Article 2 of the Convention on Cybercrime and according to the participants an amendment to the text of the treaty should be considered;
5. SPAM is a serious worldwide problem and the group agreed upon the necessity of repressing the diffusion of unsolicited e-mails. The group suggested that spamming may be considered a crime only in cases when the SPAM is used for illegal purposes or when the spammer hides his or her identity;
6. The general principles of substantive law in force in the respective countries may be taken into account in matters of illegal gambling, identity theft, libel, slander and false information committed in cyberspace;
7. Private communications on the Internet should be protected as a civil right. Therefore, the interception of this kind of communication as a method of cybercrime investigation should be considered in a restrictive way, subject to judicial review. Under the same circumstances, ISPs should also retain stored content data, including communication data;
8. The group agreed that the use of remote investigation tools is a very controversial issue but,

considering that sometimes this tool can be the only option available to the investigators, the legal aspects of these methods of investigation should be submitted to an in-depth analysis;

9. The national legislatures should consider including the obligation for retention of traffic data for a minimum period of 180 days, since such time is the minimum reasonable time to identify the point of Internet access;

10. About the requirement of identification of users accessing the Internet through public terminals, the group agreed that although the use of these places differ around the world, it is better to adopt measures to force the owner or the person in charge to identify the users of the terminal. The majority understands that administrative measures are sufficient to reach this aim. One member argued that it would be sufficient to encourage public terminals to voluntarily comply with the recommendation, as a matter of social responsibility;

11. On the issue of mandatory disclosure of encryption keys and passwords by the suspect, the group concluded that such measures may be considered self-incriminating and that it is possible to find a way around these measures; therefore, the group did not support such a legal obligation;

12. Our understanding of jurisdiction as defined in the Convention on Cybercrime is that jurisdiction can be exercised both from the country where the Internet has been accessed as well as where the content is hosted. Moreover, the Convention also suggests the principle of jurisdiction based on nationality, even if the act is not committed in the home country, provided the act is criminalized in both jurisdictions. It is also recommended that the principle of passive personality, i.e. the use of victim's jurisdiction, may also be considered for addition to the Convention;

13. It is important to strengthen the co-operation between local offices of transnational Service Providers and the authorities in order to identify nationals who use remote located services to commit crimes. One participant dissented and argued that even in such cases the countries should use the regular instruments of international co-operation.

GROUP 2

CHALLENGES AND BEST PRACTICES IN CYBERCRIME INVESTIGATION

Chairperson	Mr. Elcio Ricardo de Carvalho	(Brazil)
Co-Chairperson	Mr. Mirza Abdullahel Baqui	(Bangladesh)
Rapporteur	Ms. Rita Chun-fa Lam	(Hong Kong)
Co-Rapporteur	Mr. Yoichi Omura	(Japan)
Members	Mr. Hiroyuki Ito	(Japan)
	Mr. Takuya Matsunaga	(Japan)
	Mr. Gilbert Caasi Sosa	(Philippines)
	Mr. Napoleon Bonaparte	(Indonesia)
	Mr. Jesus Rodriguez Almeida	(Mexico)
	Visiting Expert	Professor Yunsik Jang
Advisers	Professor Shintaro Naito	(UNAFEI)
	Professor Ryuji Tatsuya	(UNAFEI)
	Professor Tetsuya Sugano	(UNAFEI)
	Professor Koji Yamada	(UNAFEI)
	Professor Haruhiko Higuchi	(UNAFEI)

I. INTRODUCTION

Group 2 started its discussion on 16 September 2008. The group elected, by consensus, Mr. Carvalho as Chairperson, Mr. Mirza Co-chairperson, Ms. Lam as Rapporteur, and Mr. Omura as Co-rapporteur. The Group, following its assignment to discuss “Challenges and Best Practices in Cybercrime Investigation”, agreed to conduct the proceedings in accordance with the following agenda:

1. Initial Information Gathering and Undercover Online Investigations;
2. Tracing and Identifying Criminals;
3. Digital Forensic Analysis of Evidence;
4. Cross-Border Investigative Abilities;
5. International Co-operation in Cybercrime Investigations

For the purpose of this document, the term “participating countries” refers only to the countries represented in this group.

II. SUMMARY OF THE DISCUSSIONS

A. Initial Information Gathering and Undercover Online Investigations

As for initial information gathering, all participating countries’ law enforcement agencies can directly receive reports about cybercrime from the victims or from third parties, the methods varying from reporting directly to the police stations to web pages and email addresses dedicated to receive the reports through the Internet. Japan, Mexico and the Philippines informed the group that they also conduct active cyber patrols in search of criminal activities on the Internet. In addition, Japan mentioned that the police also receive reports from the Internet Hotline Center.

The group agreed to recommend that the methods of Initial Information Gathering should be improved by:

- Educating the population about cybercrime, aiming to increase the number of reports and to improve the quality of the information contained in those reports;
- Improving the channels of communication with the victims, with training on cybercrime for police officers who receive reports and developing tools to better collect, classify and correlate the reports received from web pages and email addresses; and
- Increasing cyber patrolling activities, being more proactive in monitoring Internet sites in search of illegal activities, observing the legal limitations in each country.

Regarding undercover online investigations, there was a great debate about its definition, methods, limitations and objectives. For the purpose of this group discussion, the concept of undercover online investigation was agreed to be:

“A police officer disguising his or her own identity online or using an assumed identity online for the purpose of gaining the trust of an individual or organization to obtain information and/or evidence, subject to the domestic laws and guidelines of the implementing country and law enforcement agency.”

Other aspects which may be included under the concept of implementing undercover online investigation and which were discussed by the group *but were not agreed upon*, given the particularities of each country, were:

- Permission to change legal identity;
- Clearance to pretend to commit a crime, if necessary, when conducting the investigation;
- Ability to use the information obtained while undercover as evidence or just as intelligence information;
- Using an undercover identity to provide to a suspect the opportunity to commit a crime and charge this person for this action;
- In what type of crimes the investigators can use undercover investigation;
- The definition of reasonable grounds for conducting undercover investigation.

The participant from the Philippines asked to make it clear that his country does not allow undercover investigators to commit a crime or to give someone else an incentive to commit a crime.

Having in mind the aforementioned aspects, leaving them open for discussion within each country, respecting their particular traditions and legislation, and considering only the concept the group agreed upon, it is recommended that the participating countries try to improve their undercover online investigation capabilities, which is a very important investigative tool.

B. Tracing and Identifying Criminals

The group reached a consensus that the success of the investigation regarding the identification of the criminal relies upon the availability and the quality of the information provided by Internet service providers and telecommunication providers to law enforcement agencies. Such information can be traffic data, content data and subscriber information. Together they may allow the identification of the individual that performed a given action in a certain time and date. Then the group proceeded to discuss the current situation of the following subtopics in each country:

1. The Relationship between Law Enforcement and ISPs

Data and information held by ISPs and telecoms companies are very important for the investigation of cybercrime. Law enforcement agencies in all the participating countries have contacts with ISPs and telecoms companies in the form of regular meetings and/or inquiries about individual cases.

But no participating countries have laws to force ISPs and telecoms companies to keep data for a certain period of time. The situation varies from agreements, relying solely on the goodwill of the providers to keep the relevant data, to no agreement or regulation whatsoever. Therefore, there is a considerable risk that ISPs' data may no longer be available when investigators request it for an investigation.

2. The Relationship between Law Enforcement and Citizens

Information from citizens is also very important for investigation of cybercrimes. In particular, information from victims can be of high importance at trial.

On the other hand, there are some kinds of cybercrimes, like child pornography, in which we cannot expect information from a victim. In such cases, information provided by citizens using the Internet is very valuable in the early stages of an investigation.

3. The Anonymity of Public Access

The anonymous use of public access points, for example Internet cafés and open wireless networks, is a very serious issue, considering that a crime committed using those infrastructures may be impossible

to trace back to the perpetrator. Our countries do not have effective countermeasures to deal with this issue. Some countries mentioned that video surveillance systems are in use, but it was agreed that the identification of the criminal from such images is still a problem.

As a result of the discussion, we concluded that law enforcement agencies in our countries should have:

- New laws enforcing data retention by ISPs and telecoms providers for an appropriate period of time and restricting the disclosure of this information only to law enforcement agencies conducting an investigation;
- Measures for improvement of the relationship between law enforcement and citizens, for example, education of the population about cybercrime, what is criminalized and how serious cybercrime's influence is;
- Measures to regulate the operation of public access points, forcing administrators of those services to confirm the identification of users.

C. Digital Forensic Analysis of Evidence

The group discussed the following subtopics:

1. Specialized Units for Conducting Cybercrime Investigation/Forensics

All the participating countries either already have a specialized unit or have an organization able to conduct cybercrime investigations. It is desirable that in addition to having specialized units, the countries develop official guidelines for the work of those agencies, especially regarding the collection, preservation, examination and presentation of digital evidence, in order to have standards and procedures compatible with the best practices recognized internationally.

The group agreed that it is of the utmost importance that the countries devote resources to the capacity-building of those specialized units, with investment in personnel, equipment and training.

Considering the functioning of the specialized units, it is also advisable to follow the recommendations contained in the International Review of Criminal Policy (No's 43 and 44): United Nations Manual on the Prevention and Control of Computer-related Crime (1994), articles 198 to 209, in regard to:

1. Administrative and Organizational Security
2. Personnel Security
3. Physical Security
4. Communications-electronic security
5. Hardware and Software Security
6. Operations Security
7. Contingency Planning

2. Availability of Cybercrime Units for other Agencies/Law Enforcement Bodies

In all participating countries the cybercrime units are available to provide assistance or technical advice to other units or organizations within the country. In most countries, this assistance is provided on a case-by-case basis, without an established formal procedure or supervising relationship.

As a recommendation, the group considers that the co-operation among the cybercrime units within a specific country and between them and other governmental agencies should be co-ordinated in such a way so that a main organization could provide assistance to smaller units around the country regarding more advanced or technically demanding investigations. These measures can rationalize the expenditure of setting up forensic laboratories, which is especially important for developing countries.

3. Training

All the participant countries have some kind of training for cybercrime investigations. But the type of the training varies; some countries have only sent officers abroad to receive training, while others have specialized institutions to provide regular training on the subject. Also, most of the countries have received training from private companies. It is recommended to establish a formal and regular technical training course for dealing with digital evidence, at least on the subject of identification, collection, preservation and

presentation of digital evidence.

It is also advisable that the training not be restricted to those who will specialize in cybercrime investigation and forensics. The officers responsible for receiving the first information about the crime or making contact with the victim must also be trained in the basics of cybercrime concepts, in order to properly start the investigation.

As another recommendation, it is important that training activities be included in international co-operation programmes and efforts, improving the sharing of experience and knowledge of cybercrime among the countries.

4. Mechanisms to Exchange Information on Cybercrime

Regarding the mechanisms to exchange information on cybercrime between law enforcement and the private sector and the existence of a specialized organization to facilitate this exchange, the majority of participating countries have those kinds of mechanisms, usually in an informal way. Only a minority have specialized units to assist this exchange.

Although a dedicated organization to facilitate the exchange of information may not be required, the improvement of the relationship between law enforcement agencies and the private sector is critical to combating cybercrime. Regular meetings with the sectors involved, such as financial institutions and ISPs, should be formally established.

5. CERTs

Almost all the participating countries have a Computer Emergency Team. The nature of those CERTs varies; there are completely private CERTs, governmental CERTs and others of a mixed nature.

The group reached a consensus that the existence of a properly equipped CERT is essential for promptly responding to cyber threats, especially attacks on critical infrastructures. It is advisable that government and private sector co-operate closely in the operation of such teams, in order to avoid duplicity of work and difficulties in the communication necessary to cope with the emergency events.

D. Cross-Border Investigative Abilities

The group discussed the following subtopics:

1. Search and Seizure of Computers at the Request of Another Country

The group agreed that this is a very sensitive issue that has deep implications for national sovereignty. In the majority of the participating countries such search and seizure is possible, with some strict conditions, such as:

- Explicit government authorization;
- Criminalization of the act under the requested country's law;
- Enough evidence to open a case under the requested country's law;
- Principle of reciprocity;
- Principle of jurisdiction;
- Use of diplomatic channels for the request, such as Mutual Legal Assistance.

2. Preservation of Computer Data Evidence at the Request of Another Country

Regarding the existence of a preservation law or rule that allows for preservation of computer data evidence at the request of another country, in the majority of participating countries there is no provision for such cases. Nevertheless, in most countries it is possible to informally ask the ISP or telecoms provider in the requested country to preserve the data. The actual delivery of this data to the requesting country may be subject to the restrictions enumerated in the above subtopic.

3. Real-time collecting of Traffic Data at the Request of Another Country

Most of the countries in the group, except for Mexico and Indonesia, do not have the legal capability to engage in real-time collection of traffic data at the request of another country. Japanese investigative agencies do have such authority but have not yet exercised it in response to a request from another country. The implementation of such real-time collection is subject to the same legal requirements listed in the

discussion entitled “Search and seizure of computers at the request of another country”, above.

4. Disclosure of Header Information to Another Country

The ability to quickly disclose header information to enable the other country to trace the origin of a communication is available to a majority of the concerned countries, subject to certain legal conditions and on a case-by-case basis.

5. Provision of Secured Electronic Data from ISPs to Another Country

The ability to secure electronic data, such as subscriber information and traffic data, from ISPs or telecoms providers, and then provide it to another country, is possible in the majority of the concerned countries subject to the same legal requirements listed in the discussion of subtopic D.1 above. The provision of content data is subject to even more restrictions, due to privacy issues.

In order to come up with a workable solution to address cross-border investigation, the following are suggested:

- Requests for evidence be made under existing MLAT, MLA and/or Letter Rogatory process;
- The use of 24/7 points of contact (G8, Interpol, Regional organization);
- The utilization of locally based foreign embassies. Most countries have embassies in foreign countries. The representatives of concerned law enforcement agencies who are stationed at the relevant country’s embassy must liaise with the host country;
- Use of foreign law enforcement contacts maintained by the cybercrime unit and established through personal contacts and/or workshops, training or seminars.

E. International Co-operation in Cybercrime Investigations

The group agreed to consider the topic of international co-operation in cybercrime investigations as divisible in three dimensions:

1. Legal

2. Operational (Organizational)

3. Technical

The idea is to keep problems with difficult solutions from interfering in the discussion of solutions to problems in other dimensions. For example, the problem of search and seizure of computers in the request of a foreign country is a sensitive issue in the legal dimension. But it should not prevent discussions about how to turn this request into a real operation and how to technically conduct it. Therefore, if at some point a solution for the legal problem is found, a method for implementing the action may have already been established between the parties.

As an example of an idea to improve the operational dimension, the group discussed the establishment of a three-way handshaking protocol for the reception of collaboration requests. The motivation for this is that frequently the requests remain unanswered for some acceptable reason, but the requesting party is never notified of this reason, or some technical difficulty prevents the request from being fulfilled but the parties do not talk about how to overcome it.

A proposal for such a communication protocol, to be run on top of an Integrated Cybercrime Network,¹ would be as follows:

Step 1. The requesting country files a request containing at least the following information:

- Detailed description of the offence being investigated;
- Unit or person responsible for the request issued, to whom a reply should be directed;
- Detailed description of the requested actions.

¹ The definition and implementation details of such Integrated Cybercrime Networks are outside the scope of this document.

Step 2. The requested country, within a previously accorded timeframe, sends a reply containing at least the following information:

- Unit or person responsible for dealing with the request;
- Whether the request is to be answered promptly or demands further analysis;
- Description of legal/operational/technical issues that may arise from the request.

Step 3. The requesting country, within a previously accorded timeframe, sends back a notice acknowledging receipt of the requested country's reply.

As a result of this system, both parties would know that the other end received the message and what issues were involved, allowing for a more efficient and dynamic control of the requests and for a joint effort in overcoming possible problems.

As a suggestion to deal with technical problems, countries could discuss ways to quickly overcome the technical difficulties that arise when there is a difference between the technical capabilities of the countries. For instance, the requested country could generate images of the seized digital evidence and make it available over a secure network for the requesting country.

Another aspect of international co-operation that can happen immediately, in parallel with other legal and operational measures, is the help that developed countries can give to the capacity building of developing countries, creating a baseline for cybercrime investigation units. It would not only help the latter to deal with their internal investigations, but it would also provide for a smoother performance of practical international collaboration when receiving and executing requests from foreign countries.

As general recommendations regarding international co-operation, the group agreed that:

- All countries should implement a 24/7 hi-tech point of contact network (operational dimension);
- All countries should share cybercrime information through Interpol and other regional organizations, like ASEANAPOL (operational dimension);
- Countries should engage in international co-operation on cybercrime investigation (legal, operational and technical dimensions);
- Countries should have a legal framework that allows engagement and joint cybercrime investigation with other countries (legal dimension);
- Countries should not make direct contact to other countries' private sector entities or ISPs, but instead use the established diplomatic/international co-operation channels. But it is acceptable to contact the local office of global ISPs, when available (legal and operational dimensions).

III. CONCLUSION

Although the main theme of this group workshop was "Challenges and Best Practices in Cybercrime Investigation", it is not always possible to discuss such issues without venturing into the debate about legal frameworks, given that most procedural tools designed to overcome the challenges and some implementations of best practices need to be supported by proper legislation within each country.

Nevertheless, the group worked to identify common issues and strived to reach consensus on the recommendations towards the improvement of the fight against the threat of cybercrime. Whenever possible, those recommendations were included in the main body of this document, immediately following the discussion of the respective subject for the sake of clarity and conciseness.

PART TWO

**Work Product of the Eleventh International Training Course
on the Criminal Justice Response to Corruption**

UNAFEI

VISITING EXPERTS' PAPERS

THE UNITED NATIONS CONVENTION AGAINST CORRUPTION: ITS RELEVANCE AND CHALLENGES IN ITS IMPLEMENTATION

*Giovanni Gallo**



I. THE UNITED NATIONS CONVENTION AGAINST CORRUPTION AND ITS RELEVANCE TO CRIMINAL JUSTICE AUTHORITIES

A. Overview of the United Nations Convention against Corruption, Genesis and Structure

1. Genesis of the United Nations Convention against Corruption

In its resolution 55/61 of 4 December 2000, the General Assembly recognized that an effective international legal instrument against corruption, independent of the United Nations Convention against Transnational Organized Crime,¹ was desirable and decided to establish an ad hoc committee for the negotiation of such an instrument in Vienna, at the headquarters of the Centre for International Crime Prevention of the Office for Drug Control and Crime Prevention.²

In its resolution 56/260 of 31 January 2002, the General Assembly decided that the Ad Hoc Committee for the Negotiation of a Convention against Corruption should negotiate a broad and effective convention, which, subject to the final determination of its title, should be referred to as the “United Nations Convention against Corruption”. The text of the Convention was negotiated during seven sessions of the Ad Hoc Committee, held between 21 January 2002 and 1 October 2003.

The Convention approved by the Ad Hoc Committee was adopted by the General Assembly by resolution 58/4 of 31 October 2003. The General Assembly, in its resolution 57/169 of 18 December 2002, accepted the offer of the Government of Mexico to host a high-level political signing conference in Merida for the purpose of signing the United Nations Convention against Corruption.³ In accordance with article 68 (1) of resolution 58/4, the United Nations Convention against Corruption entered into force on 14 December 2005, nineteen days after the deposit of the thirtieth instrument of ratification, acceptance, approval or accession.

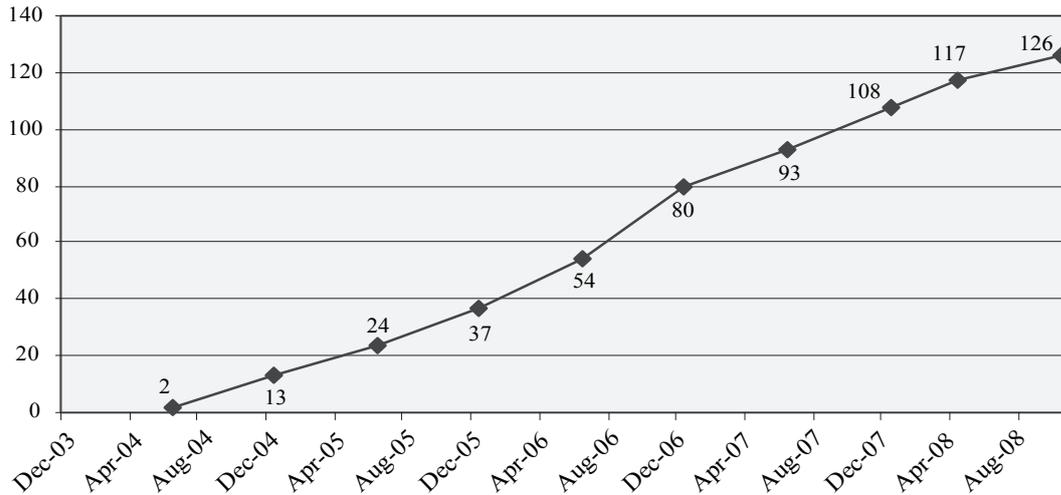
In resolution 58/4, the General Assembly also decided that the Ad Hoc Committee for the Negotiation of a Convention against Corruption would complete its tasks by holding a meeting well before the convening of the first session of the Conference of the States Parties to the Convention in order to prepare the draft text of the rules of procedure of the Conference of the States Parties and of other rules described in article 63 of the Convention, which would be submitted to the Conference of the States Parties at its first session for consideration and possible adoption. In accordance with article 63 (2) of the Convention, the first session of the Conference of the States Parties convened in Jordan from 10 to 14 December 2006, not later than one year following the entry into force of the Convention.

* Crime Prevention Expert, Corruption and Economic Crime Section, Division for Treaty Affairs, UNODC.

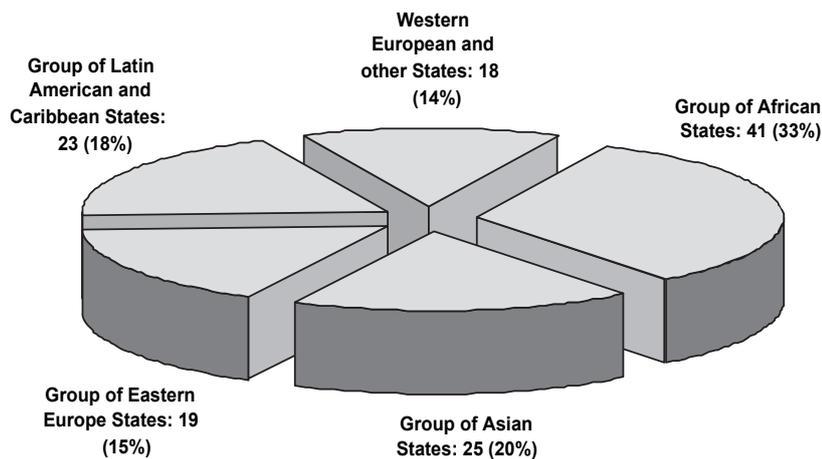
¹ Adopted by General Assembly resolution 55/25, annex I, of 15 November 2000.

² In October 2002, the United Nations Office for Drug Control and Crime Prevention was restructured and renamed the United Nations Office on Drugs and Crime (UNODC).

³ In accordance with General Assembly resolution 57/169, the United Nations Convention against Corruption was opened for signature at the High-level Political Signing Conference in Merida, Mexico, from 9 to 11 December 2003.



As at 10 October 2008, the Convention has 140 signatory States and 126 States Parties. The graphics above and below offer an overview of the Convention’s pace of adherence and of the regional distribution of its States Parties.



2. The Structure of the United Nations Convention against Corruption

The United Nations Convention against Corruption consists of 71 articles divided into eight chapters. The provisions of the Convention do not have the same level of obligation. In general, provisions can be grouped into the following three categories:

- (i) Mandatory provisions, which consist of obligations to legislate (either absolutely or where specified conditions have been met);
- (ii) Measures that States Parties must consider applying or endeavour to adopt; and
- (iii) Measures that are optional.

Whenever the phrase “each State Party shall adopt” is used, the reference is to a mandatory provision. Otherwise, if the language used is “shall consider adopting” or “shall endeavour to”, it means that States are urged to consider adopting a certain measure and to make a genuine effort to see whether it would be compatible with their legal system. For entirely optional provisions, the Convention employs the term “may adopt”.

Several articles of the Convention contain safeguard clauses that operate as filters regarding the obligations of States Parties in case of conflicting constitutional or fundamental rules, by providing that States must adopt certain measures “subject to [their] constitution and the fundamental principles of [their]

legal system” (for example, article 20), “to the extent not contrary to the domestic law of the requested State Party” (for example article 46 (17), “to the extent that such a requirement is consistent with the fundamental principles of their domestic law and with the nature of judicial and other proceedings” (for example, article 31 (8)) or “to the extent permitted by the basic principles of its domestic legal system . . .” (for example, article 50 (1)).

The eight chapters of the Convention are:

(i) General Provisions (Chapter I, Articles 1 to 4)

The purpose of this chapter is to define terms employed throughout the text of the Convention, state the scope of application and reiterate the principle of protection of sovereignty of State parties.

(ii) Preventive Measures (Chapter II, Articles 5 to 14)

Under chapter II, the Convention requires States Parties to introduce effective policies aimed at the prevention of corruption. The chapter calls for the introduction of a variety of measures concerning both the public and the private sector. Such measures range from institutional arrangements, such as the establishment of a specific anti-corruption body, to codes of conduct and policies promoting good governance, the rule of law, transparency and accountability. Significantly, the Convention underscores the important role of the wider society, such as nongovernmental organizations and community initiatives, by inviting each State party to actively encourage their involvement and general awareness of the problem of corruption.

(iii) Criminalization and Law Enforcement (Chapter III, Articles 15 to 42)

Under this chapter, the Convention requires States Parties to introduce criminal and other offences in order to cover a wide range of acts of corruption, to the extent these are not already defined as such under domestic law. The criminalization of some acts is mandatory under the Convention, which also requires that States Parties consider the establishment of additional offences. An innovation of the United Nations Convention against Corruption is that it addresses not only basic forms of corruption, such as bribery and the embezzlement of public funds, but also acts carried out in support of corruption, such as obstruction of justice, trading in influence and the concealment or laundering of the proceeds of corruption. Furthermore, chapter III also deals with corruption in the private sector. Criminalization of corrupt practices needs to be supported by measures and mechanisms that enable the actors of the criminal justice system to effectively fight corruption through detection, prosecution, punishment and reparation. In this respect, chapter III of the Convention provides for a series of procedural measures that support criminalization. These provisions are related to the prosecution of corruption offences and enforcement of national anti-corruption laws, such as:

- (a) Evidentiary standards, statutes of limitation and rules for adjudicating corruption offences (articles 28-30);
- (b) Co-operation between national law enforcement authorities, specialized anti-corruption agencies and the private sector (articles 37-39);
- (c) Use of special investigative techniques (article 50);
- (d) Protection of witnesses, victims and whistleblowers (articles 32 and 33);
- (e) Allowing the freezing, seizure and confiscation of proceeds and instrumentalities of corruption (article 31);
- (f) Overcoming obstacles that may arise out of the application of bank secrecy laws (article 40); and
- (g) Addressing the consequences of acts of corruption (article 34), including through compensating for damages caused by corruption (art. 35).

(iv) International Co-operation (Chapter IV, Articles 43 to 50)

This chapter emphasizes that every aspect of anti-corruption efforts (prevention, investigation, prosecution of offenders, seizure and return of misappropriated assets) necessitates international co-operation. The Convention requires specific forms of international co-operation, such as mutual legal assistance in the collection and transfer of evidence, extradition, joint investigations and the tracing, freezing, seizing and confiscating of proceeds of corruption. In contrast to previous treaties, the Convention also provides for mutual legal assistance in the absence of dual criminality, when such assistance does not involve coercive measures. Furthermore, the Convention puts a premium on exploring all possible ways

to foster co-operation: “In matters of international co-operation, whenever dual criminality is considered a requirement, it shall be deemed fulfilled irrespective of whether the laws of the requested State party place the offence within the same category of offence or denominate the offence by the same terminology as the requesting State party, if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States parties” (article 43, (2)).

(v) Asset Recovery (Chapter V, Articles 51 to 59)

This chapter underscores that a most significant innovation and a “fundamental principle of the Convention” (art. 51) is the return of assets. Chapter V specifies how co-operation and assistance will be rendered, how proceeds of corruption are to be returned to a requesting State and how the interests of other victims or legitimate owners are to be considered.

(vi) Technical Assistance and Information Sharing, Mechanisms for Implementation and Final Provisions (Chapter VI, VII and VIII, Articles from 60 to 71)

These Chapters of the Convention provide for training, research and information-sharing measures and contain technical provisions, such as for signature and ratification.

B. Provisions of the United Nations Convention against Corruption relevant to Criminal Justice

Authorities

1. Overview of Provisions most Relevant to Criminal Justice Authorities

The United Nations Convention against Corruption contains a number of provisions that are relevant to the actors of domestic criminal justice systems. The majority of such provisions are contained in chapter III, Criminalization and law enforcement, and chapter IV, International co-operation, of the Convention. Whilst a detailed analysis of such provisions is not compatible with the nature of the present paper, below is a non exhaustive overview of the most significant ones.

(i) Provisions relevant to Criminal Justice Authorities under Chapter III of the Convention

States Parties must ensure that the knowledge, intent or purpose element of offences established in accordance with the Convention can be established through inference from objective factual circumstances (article 28).

States Parties must establish long statutes of limitation for offences established in accordance with the Convention and suspend them or establish longer ones for alleged offenders evading the administration of justice (article 29).

In accordance with article 30, States Parties must:

- (a) Ensure that offences covered by the Convention are subject to adequate sanctions taking the gravity of each offence into account (paragraph 1);
- (b) Maintain a balance between immunities provided to their public officials and their ability to effectively investigate and prosecute offences established under the Convention (paragraph 2);
- (c) Ensure that pre-trial and pre-appeal release conditions take into account the need for the defendants’ presence at criminal proceedings, consistent with domestic law and the rights of the defence (paragraph 4); and
- (d) Take into account the gravity of the offences when considering early release or parole of convicted persons (paragraph 5).

Article 30 also mandates that States Parties consider or endeavour:

- (a) To ensure that any discretionary legal powers relating to the prosecution of offences established in accordance with the Convention maximize the effectiveness of law enforcement in respect of those offences and act as a deterrent (paragraph 3);
- (b) To establish procedures through which a public official accused of such offence may be removed, suspended or reassigned (paragraph 6);
- (c) To establish procedures for the disqualification of a person convicted of an offence established in accordance with the Convention from public office, and office in an enterprise owned in whole or in part by the State (paragraph 7); and

- (d) To promote the reintegration of persons convicted of offences established in accordance with the Convention into society (paragraph 10).

In accordance with article 31, States Parties must, to the greatest extent possible under their domestic system, have the necessary legal framework to enable:

- (a) The confiscation of proceeds of crime derived from offences established in accordance with the Convention or property the value of which corresponds to that of such proceeds (paragraph 1 (a));
- (b) The confiscation of property, equipment or other instrumentalities used in or destined for use in offences established in accordance with the Convention (paragraph 1 (b));
- (c) The identification, tracing and freezing or seizure of the proceeds and instrumentalities of crime covered by the Convention, for the purpose of eventual confiscation (paragraph 2);
- (d) The administration of frozen, seized or confiscated property (paragraph 3);
- (e) The application of confiscation powers to transformed or converted property and proceeds intermingled with legitimately obtained property (to the value of the proceeds in question) and to benefits or income derived from the proceeds (paragraphs. 4-6); and
- (f) The empowerment of courts or other competent authorities to order that bank, financial or commercial records be made available or seized. Bank secrecy shall not be a legitimate reason for failure to comply (paragraph 7).

In accordance with article 32, and bearing in mind that some victims may also be witnesses (article 32 (4)), States Parties are required:

- (a) To provide effective protection for witnesses, within available means (paragraph 1). This may include physical protection, domestic or foreign relocation, special arrangements for giving evidence;
- (b) To consider entering into foreign relocation agreements (paragraph 3); and
- (c) To provide opportunities for victims to present views and concerns at an appropriate stage of criminal proceedings, subject to domestic law (paragraph 5).

Article 33 requires States Parties to consider providing measures to protect persons who report offences established in accordance with the Convention to competent authorities.

Article 34 requires States Parties to address the consequences of corruption. In this context, States may wish to consider annulling or rescinding a contract, withdrawing a concession or similar instrument, or taking other remedial action.

Article 35 requires that States Parties ensure that entities or individuals who have suffered damages as a result of corruption have the right to initiate legal proceedings to obtain damages from those responsible.

Article 36 requires States Parties, in accordance with the fundamental principles of their legal system:

- (a) To ensure they have a body or persons specializing in combating corruption through law enforcement;
- (b) To grant the body or persons the necessary independence to carry out its or their functions effectively without undue influence; and
- (c) To provide sufficient training and resources to such body or persons.

Under article 37, States Parties must:

- (a) Take appropriate measures to encourage persons who participate or who have participated in offences established in accordance with the Convention to supply information for investigative and evidentiary purposes and to provide concrete assistance towards depriving offenders of the proceeds of crime and recovering such proceeds (paragraph 1);
- (b) To consider allowing mitigating punishment of an accused person who provides substantial co-operation in the investigation or prosecution of offences established in accordance with the Convention (paragraph 2);
- (c) To consider providing for the possibility of granting immunity from prosecution to a person who provides substantial co-operation (paragraph 3); and

(d) To provide to such persons the same protection as provided to witnesses (paragraph 4)

Article 38 requires that States Parties take measures to encourage co-operation between their public authorities and law enforcement. Such co-operation may include:

- (a) Informing law enforcement authorities when there are reasonable grounds to believe that offences established in accordance with articles 15 (Bribery of national public officials), 21 (Bribery in the private sector) and 23 (Laundering of proceeds of crime) have been committed; or
- (b) Providing such authorities all necessary information, upon request.

Article 39 requires States Parties:

- (a) To take measures consistent with their laws encouraging co-operation between their private sector authorities (financial institutions, in particular) and law enforcement authorities regarding the commission of offences established in accordance with the Convention (paragraph 1); and
- (b) To consider encouraging their nationals and habitual residents to report the commission of such offences to their law enforcement authorities (paragraph 2).

Article 40 requires States Parties to ensure that, in cases of domestic criminal investigations of offences established in accordance with the Convention, their legal system has appropriate mechanisms to overcome obstacles arising out of bank secrecy laws.

In accordance with article 41, States Parties may allow the consideration of an alleged offender's convictions in another State in their own criminal proceedings.

(ii) Provisions relevant to Criminal Justice Authorities under Chapter IV of the Convention

Article 43, paragraph 1, requires that States Parties co-operate in criminal matters in accordance with all articles in chapter IV of the Convention, that is, extradition, mutual legal assistance, the transfer of criminal proceedings and law enforcement, including joint investigations and special investigative techniques. Article 43, paragraph 2, requires that, whenever dual criminality is necessary for international co-operation, States Parties must deem this requirement fulfilled if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States Parties. The Convention makes it clear that neither does the underlying conduct of the criminal offence need to be defined in the same terms in both States Parties, nor does it have to be placed within the same category of offence.

In accordance with article 44, States Parties must ensure that offences established in accordance with the Convention are deemed extraditable offences, provided dual criminality is fulfilled (paragraph 1). If their domestic law allows it, States Parties may grant extradition for corruption offences even without dual criminality (paragraph 2). If States Parties use the Convention as a basis for extradition, they will not consider corruption offences as political offences (paragraph 4). States Parties that require a treaty basis for extradition:

- (a) May consider the Convention as the legal basis for extradition to another State Party regarding corruption offences (paragraph 5);
- (b) Must notify the Secretary-General of the United Nations on whether they will permit the Convention to be used as a basis for extradition to other States Parties (paragraph 6 (a)); and
- (c) Must seek to conclude treaties on extradition with other States Parties, if they do not use the Convention as the legal basis for extradition (paragraph 6 (b)).

States Parties with a general statutory extradition scheme must ensure that the corruption offences are deemed extraditable (paragraph 7). A State Party must endeavour to expedite extradition procedures and simplify evidentiary requirements relating to corruption offences (paragraph 9). A State Party that denies an extradition request on the ground that the person is its national must submit the case for domestic prosecution (*aut dedere aut judicare*⁴). In doing so, the State Party concerned shall ensure that the decision

⁴ See General Assembly A/CN.4/571, Preliminary report on the obligation to extradite or prosecute ("*aut dedere aut judicare*").

to prosecute and any subsequent proceedings are conducted with the same diligence as a domestic offence of a grave nature and shall co-operate with the requesting State Party to ensure the efficiency of the prosecution (paragraph 11). States Parties can discharge their obligation to submit a case for prosecution pursuant to article 44 (11), by temporary surrender (paragraph 12). If States Parties deny extradition for enforcement of a sentence on grounds of nationality, they must consider enforcing the sentence imposed under the domestic law of the requesting State (paragraph 13). States Parties must ensure fair treatment for persons facing extradition proceedings pursuant to article 44, including enjoyment of all rights and guarantees provided by their domestic law (paragraph 14). States Parties may not refuse extradition on the ground that the offence also involves fiscal matters (paragraph 16). Prior to refusing extradition, a requested State Party must, where appropriate, consult with the requesting State Party to provide it with the opportunity to present information and views on the matter (paragraph 17).

Article 46 requires States Parties:

- (a) To ensure the widest measure of mutual legal assistance for the purposes listed in article 46, paragraph 3, in investigations, prosecutions, judicial proceedings and asset confiscation and recovery in relation to corruption offences (paragraph 1);
- (b) To provide for mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to offences for which a legal entity may be held liable under article 26 (paragraph 2);
- (c) To ensure that mutual legal assistance is not refused on the ground of bank secrecy (paragraph 8).
- (d) To offer assistance in the absence of dual criminality through non-coercive measures (paragraph 9, (b));
- (e) To apply paragraphs 9 to 29 of article 46 to govern the modalities of mutual legal assistance in the absence of a mutual legal assistance treaty with another State party (paragraphs 7 and 9-29);
- (f) To notify the Secretary-General of the United Nations of their central authority designated for the purpose of article 46, as well as of the language(s) acceptable to them in this regard (paragraphs 13 and 14); and
- (g) To consider entering into bilateral or multilateral agreements or arrangements to give effect to or enhance the provisions of article 46 (paragraph 30).

States Parties may provide information on criminal matters to other States Parties without prior request, where they believe that this can assist in inquiries, criminal proceedings or the formulation of a formal request from that State Party (paragraphs 4 and 5). States Parties are also invited to consider the provision of a wider scope of legal assistance in the absence of dual criminality (paragraph 9 (c)).

In accordance with article 47, States Parties must consider the transfer to one another of criminal proceedings when this would be in the interest of the proper administration of justice relative to corruption offences, especially those involving several jurisdictions.

Under article 48, States Parties must, consistent with their respective domestic legal and administrative systems, adopt effective measures for the purposes of effective investigation with respect to the offences established in accordance with the Convention, including:

- (a) Enhancing and, where necessary, establishing channels of communication between their respective law enforcement agencies;
- (b) Co-operating with other States parties in their inquiries concerning the identity, whereabouts and activities of specific persons, and the movement of proceeds or property derived from the commission of offences and of property, equipment and other instrumentalities used or intended for use in the commission of offences;
- (c) Providing, when appropriate, items and substances for analytical or investigative purposes;
- (d) Considering bilateral or multilateral agreements or arrangements to give effect to or enhance the provisions of article 48; and
- (e) Endeavouring to co-operate in order to respond to corruption-related offences committed through the use of modern technology.

Under article 49, a State Party must consider bilateral or multilateral agreements or arrangements

regarding the establishment of joint investigative bodies, while ensuring that the sovereignty of the State Party in whose territory such investigation is to take place is fully respected.

Under article 50, a State Party must:

- (a) Establish controlled delivery as an investigative technique available at the domestic and international level, if permitted by the basic principles of its domestic legal system;
- (b) Have the legal ability to provide on a case-by-case basis international co-operation with respect to controlled deliveries, where not contrary to the basic principles of its domestic legal system; and
- (c) Where appropriate, establish electronic surveillance and undercover operations as investigative techniques available at the domestic and international level.

II. THE ROLE OF THE UNITED NATIONS OFFICE ON DRUGS AND CRIME IN PROMOTING THE RATIFICATION AND IMPLEMENTATION OF THE UNITED NATIONS CONVENTION AGAINST CORRUPTION

A. The Mandate of the United Nations Office on Drugs and Crime

In its resolution 58/4 of 31 October 2003, the General Assembly, while adopting the United Nations Convention against Corruption, requested the Secretary-General to provide the United Nations Office on Drugs and Crime (hereinafter, UNODC) with the resources necessary to enable it to promote in an effective manner the rapid entry into force of the Convention. Furthermore, in accordance with article 60 (8) of the Convention, States Parties shall consider making voluntary contributions to the United Nations Office on Drugs and Crime for the purpose of fostering programmes and projects in developing countries with a view to implement the Convention.

In its resolution 2005/18 of 22 July 2005, entitled “Action against corruption: assistance to States in capacity-building with a view to facilitating the entry into force and subsequent implementation of the United Nations Convention against Corruption”, the Economic and Social Council requested the Secretary-General to provide the United Nations Office on Drugs and Crime with the resources necessary to enable it to promote, in an effective manner, the implementation of the United Nations Convention against Corruption through, *inter alia*, the provision of assistance to developing countries and countries with economies in transition for building capacity in the areas covered by the Convention.

Subsequently, in its resolution 60/175 of 16 December 2005, entitled “Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical co-operation capacity”, the General Assembly reaffirmed the role of the United Nations Office on Drugs and Crime in providing to Member States, upon request and as a matter of high priority, technical co-operation, advisory services and other forms of assistance in the field of crime prevention and criminal justice, including in the area of prevention and control of corruption.

Furthermore, the General Assembly, in its resolution 60/207 of 22 December 2005, entitled “Preventing and combating corrupt practices and transfer of assets of illicit origin and returning such assets, in particular to the countries of origin, consistent with the United Nations Convention against Corruption”, encouraged the United Nations Office on Drugs and Crime to give high priority to technical co-operation, upon request, to, *inter alia*, promote and facilitate the ratification and implementation of the Convention and provide technical assistance to support national efforts in preventing and combating corrupt practices.

Most recently, in its resolution 2006/24 of 27 July 2006, entitled “International co-operation in the fight against corruption”, the Economic and Social Council requested the United Nations Office on Drugs and Crime to continue to assist States, upon request, with sustainable capacity-building focused on the promotion of the implementation of the Convention. The Council further invited relevant entities of the United Nations system and international financial institutions and regional and national funding agencies to increase their support to and interaction with the United Nations Office on Drugs and Crime in order to benefit from synergies and avoid duplication of efforts and to ensure that, as appropriate, activities aimed at preventing and combating corruption are considered in their sustainable development agenda and that the expertise of UNODC is fully utilized.

B. UNODC Activities to promote the Ratification and Implementation of the Convention

In the course of 2005 and 2006, the United Nations Office on Drugs and Crime conducted seven high-level regional seminars to promote the ratification and implementation of the United Nations Convention against Corruption. The seminars gathered policy-makers and practitioners from more than 130 Member States and provided a platform for sharing of experience, good practices and innovative initiatives. During such seminars, the following emerged as priority issues: (a) criminalization of the corruption offences, in particular the mandatory ones; (b) promotion of mechanisms for international co-operation, especially in the field of extradition and mutual legal assistance; and (c) development of a methodology for assessing progress in the implementation of the Convention. In addition, the seminars also highlighted a number of issues specifically related to corruption:

- (i) the need to develop and strengthen mechanisms for asset recovery;
- (ii) the importance of developing national anti-corruption strategies;
- (iii) the establishment of anti-corruption bodies with adequate political, functional and budgetary independence; and
- (iv) the central role of civil society and the media in raising public awareness on corruption.

In line with the priority issues that emerged from the aforementioned seminars, the United Nations Office on Drugs and Crime developed a strategy of interventions articulated as follows:

1. Support for States in Accession to, Ratification and Implementation of the Convention

This set of activities includes: knowledge-building and awareness-raising for leaders and policy-makers on the importance of becoming parties to the Convention, and assistance in the identification of ratification or accession requirements and in developing national action plans for ratification or accession to and implementation of the Convention.

2. Collection and Analysis of Data on Corruption

Research on and analysis of corruption patterns and trends complement and reinforce the technical assistance repertoire. Research allows for a base-line set of data to more effectively direct technical assistance and provide means to measure its impact. Furthermore, a solid knowledge base on the multi-faceted nature of corruption and its criminal dimension provides a better understanding of its root-causes, its links to other criminal activities and its adverse impact on development, hence supporting policy analysis and evidence-based decision-making. To this end, such tools as the Criminal Justice Assessment Toolkit,⁵ the Crime and Corruption Business Survey⁶ and standard survey instruments to assess justice sector capacity and integrity were produced.

3. Legislative Assistance and Legal Advisory Services to implement the UNCAC

The UNODC's assistance focuses on the criminalization of corruption offences, and the development of model legislation, model treaties and other relevant reference and training materials

This area of UNODC's work includes:

- (i) legislative assistance and advisory services to requesting States to review legislative and regulatory frameworks, identify gaps and recommend action to comply with the requirements of the Convention;
- (ii) assistance in the development or adjustment of domestic legislation for the criminalization of corruption offences established in accordance with the Convention, in particular the five mandatory ones;⁷ and
- (iii) dissemination of the Legislative Guide for the Implementation of the United Nations Convention against Corruption⁸ and the *Travaux Préparatoires* of the Convention⁹ to lawmakers. In addition, the development of a new generation of tools, guides, handbooks and model legislation is being considered. In this context, work is being conducted to develop an on-line library containing relevant

⁵ Criminal Justice Assessment Toolkit, <http://www.unodc.org/unodc/en/justice-and-prison-reform/Criminal-Justice-Toolkit.html>

⁶ Crime and Corruption Business Surveys (CCBS). <http://www.unodc.org/unodc/en/data-and-analysis/Crime-and-Corruption-Business-Surveys.html>

⁷ Articles 15, 16 (1), 17, 23 and 25.

⁸ http://www.unodc.org/pdf/corruption/CoC_LegislativeGuide.pdf

⁹ To be published by UNODC in the near future.

national legislation, policies, tools and other relevant documentation. Similarly, consideration is being given to the development of a Model Law on Asset Recovery.

4. Support in Strategic Planning, including the Development of Anti-Corruption Policies

In this area, technical assistance rendered by UNODC, includes advisory services and technical input to design, implement and monitor anti-corruption action plans at national and local levels as well as sector-specific policies for the prevention and control of corruption. To support policies aimed at enhancing transparency, accountability and governance and prevent opportunities for corruption in the public and private sectors, assistance is being rendered to review and develop:

- (i) codes of conduct for public officials;
- (ii) public complaints mechanisms;
- (iii) asset declaration systems;
- (iv) merit-based human resource management frameworks;
- (v) whistleblower protection measures and systems;
- (vi) effective management of public resources and transparent public procurement;
- (vii) access to information; and
- (viii) public education and awareness raising. To this end, the Technical Guide for the Implementation of the Convention and for policy makers and practitioners is being developed and may prove a useful tool.

5. Promotion of International Co-operation in Criminal Matters, in particular, Extradition and Mutual Legal Assistance

In this area, technical assistance activities conducted by UNODC include:

- (i) knowledge- and capacity-building for practitioners in international co-operation, with particular attention to extradition and mutual legal assistance; and
- (ii) the establishment of a directory of central authorities responsible for processing requests for mutual legal assistance.

The delivery of technical assistance in this field may be greatly facilitated by the use and further development of information technology solutions. The Mutual Legal Assistance Request Writer Tool,¹⁰ for instance, has proven so effective that a similar application is being developed in the area of extradition. An on-line directory of central authorities responsible for mutual legal assistance can help promote virtual networking, open channels of direct communication and facilitate exchange of experience, expertise and successful practices. These and other innovative solutions, such as computer-based training programmes on freezing, seizure and confiscation of criminal assets, asset recovery, law enforcement co-operation and special investigative techniques are also being considered.

6. Building Knowledge and Legal Capacities for Asset Recovery

As noted above, the chapter on asset recovery (Chapter V) is the most innovative and complex of the Convention. Besides the difficulty posed by different legal systems and normative gaps, the successful implementation of this chapter rests largely on the full understanding of its yet unexplored potential. Consolidating the knowledge base is therefore a prerequisite to the establishment of effective international co-operation mechanisms, in particular in the areas of direct recovery and mutual legal assistance for the purpose of confiscation. Furthermore, the nature of this chapter lends itself to an illustrative distinction between short- and mid-term activities necessary to implement the Convention and long-term ones. UNODC has articulated its strategy along these lines. In particular, in the short run, building knowledge and legal capacities for asset recovery is essential. Activities to this end include:

- (i) intensive promotion of awareness and understanding of asset recovery and its mechanisms among relevant stakeholders; and
- (ii) building legal capacities to enable countries to successfully recover stolen assets.

¹⁰ The Mutual Legal Assistance Request Writer Tool helps practitioners to generate effective requests and receive more useful responses. It gives access to relevant multilateral, bilateral and regional treaties and agreements and national laws and includes a case management tracking system for incoming and outgoing mutual legal assistance requests. <http://www.unodc.org/mla/>

7. Support to enable States to comply with their Legal Reporting Obligations

The under-reporting problem experienced during the first two reporting cycles of the Conference of the Parties to the United Nations Convention against Transnational Organized Crime and Protocols Thereto has demonstrated that States may have insufficient capacity to fulfil reporting obligations emanating from international treaties. To address the issue, UNODC has developed a strategy which would serve a dual purpose:

- (i) the enhancement of countries' reporting capacities in order to achieve greater compliance with the Convention and;
- (ii) a better identification, through timely, complete and accurate information, of technical assistance needs. To achieve these objectives, UNODC is providing ad hoc assistance to requesting countries through training workshops and seminars and has launched voluntary programmes to test information-gathering and review of implementation mechanisms. Also in this area, the expansion of innovative solutions, such as a computer-based self-assessment checklist,¹¹ have been considered.

8. Institution- and Capacity-building: Establishing/Strengthening Specialized Institutions prescribed by the Convention

Following the development of comprehensive preventive policies, the Convention requires States to ensure the existence of adequate bodies to implement them. Technical assistance in this area, which is also benefiting from mentors *in situ* offering on-the-job support, includes activities aimed at ensuring that anti-corruption bodies and units, financial intelligence units and central authorities responsible for mutual legal assistance be, as appropriate, operationally and politically independent, adequately staffed, trained and resourced. To this end, UNODC is giving consideration to an on-line repository with various models and approaches adopted by other countries as well as a network of both government and independent experts, readily available to provide policy advice and assistance. Also in this area, computer-based training tools, such as those on anti-money laundering and financial investigations, are proving useful.

9. Strengthening Integrity and Capacity of the Criminal Justice System

This area of work has two main aspects. Its first dimension relates to the need to enhance transparency and integrity within the justice system and reduce its vulnerability to corruption. To this end, UNODC is carrying out or considering the following activities, the effectiveness of which is being enhanced through mentors *in situ*:

- (i) advisory services to design or review human resources policies, terms of reference and codes of conduct for the judiciary;
- (ii) training on ethics and integrity standards; and
- (iii) support for national policies and measures aimed at establishing an environment conducive to the effective and independent performance of judicial functions.

The second dimension of this area relates to the need to increase the overall capacity of the criminal justice system as well as its specific ability to detect, investigate, prosecute and adjudicate corruption cases. This objective is being achieved through:

- (i) training for law enforcement on specialized investigative techniques and cross-border co-operation to detect and investigate cases of corruption; and
- (ii) training for prosecutors and judges on the Convention and on the application of domestic legislation to ensure efficient and effective adjudication of cases of corruption. Activities in this area are drawing on the Legislative Guide for the Implementation of the United Nations Convention against Corruption, the Bangalore Principles of Judicial Conduct,¹² the Commentary on the Bangalore Principles and the Training Manual on Judicial Ethics and the United Nations Handbook on Practical

¹¹ The self-assessment checklist is an innovative survey software that was launched on 15 June 2007 to facilitate the recognition of implementation efforts, the identification of implementation gaps and technical assistance needs. As of October 2008, 73 Member States have submitted self-assessment reports. Out of these, 65 are parties to UNCAC, which results in a response rate of 52%. <http://www.unodc.org/unodc/en/treaties/CAC/index.html#selfassessment>

¹² See ECOSOC Resolution 2006/23. See also Commentary on the Bangalore Principles on Judicial Conduct, UNODC, September 2007. http://www.unodc.org/documents/corruption/publications_unodc_commentary-e.pdf

Anti-Corruption Measures for Prosecutor and Investigators.¹³ To contribute to the objectives of this area, UNODC is developing a computer-based training tool on judicial ethics. Assistance in this field must receive appropriate attention as a matter of urgency, as it will require significant investment sustained over longer periods of time. The matter is directly linked with the need to consolidate and expand the realization and acceptance of the importance of the criminal justice system as a pillar of the rule of law and thus as a key developmental issue.

10. Development of Mechanisms for Asset Recovery

Following and, to a certain extent, in parallel with the establishment of the necessary knowledge-base and legal capacities, UNODC is devoting efforts to framework and institution-building. To this end, the following activities are being carried out or considered:

- (i) provision of specialized assistance to bring national legal frameworks in line with the requirements of the Convention;
- (ii) assistance to set up legislative and regulatory frameworks for the detection, seizure, freezing and confiscation of assets domestically and internationally;
- (iii) support for the adoption of preventive measures to detect suspicious transactions and the transfer of proceeds of crime;
- (iv) support for the adoption of measures for direct recovery of property and through international co-operation for confiscation, including provisions for the return of such assets;
- (v) support for a broad review of institutional arrangements in order to provide law enforcement and prosecutors with necessary investigative powers and competent judicial and central authorities with the power to process direct requests for asset recovery; and
- (vi) assistance in the creation or strengthening of specialized units, including financial intelligence units, in charge of asset recovery and international co-operation. Also in this field, innovative solutions are being explored and their expansion should be considered. The GoAML application¹⁴ developed by UNODC, for instance, is an integrated database and intelligence analysis system intended for use by financial intelligence units allowing for the collection, rule-based analysis, risk scoring, profiling and rapid dissemination of information to law enforcement agencies.

To further facilitate the development of mechanism for asset recovery, UNODC and the World Bank officially launched the Stolen Asset Recovery Initiative (hereinafter, referred to as StAR Initiative) on 17 September 2007. Work under that joint initiative includes activities to promote the implementation of the Convention, assistance to developing countries in building capacity for mutual legal assistance and partnerships to share information and expertise. To further shape the work programme of the Initiative, a number of consultation missions to identify possible pilot countries and determine their needs and political commitment have been planned and undertaken. An appropriate joint funding vehicle was established to provide assistance to States for asset recovery cases in various areas of anti-corruption policy. Other activities include the development of training tools, a library of good practices and a Web-based list of focal points.

To oversee the work of the Initiative, the two organizations created a joint StAR Secretariat housed in the offices of the World Bank in Washington, D.C., and that includes World Bank and UNODC staff. The secretariat co-ordinates all activities that fall under the StAR Initiative work programme; it acts as a central point of contact for States seeking or receiving support and for donors providing voluntary contributions, and administers funds related to the StAR Initiative. To strengthen the collective effort, the Initiative benefits from the advice and guidance of the "Friends of StAR", a small group composed of influential, experienced individuals from developed and developing countries. The group has an advocacy role in promoting the implementation of the asset recovery provisions of the Convention and co-operation between States on asset recovery.

¹³ <http://www.unodc.org/pdf/crime/corruption/Handbook.pdf>

¹⁴ GoAML is available from: http://www.imolin.org/imolin/goAML_Launch.html

III. THE CONFERENCE OF THE STATES PARTIES AND ITS INTERGOVERNMENTAL WORKING GROUPS

A. The Functions of the Conference

In accordance with article 63 of the United Nations Convention against Corruption, a Conference of the States Parties to the Convention is established to improve the capacity of and co-operation between States Parties to achieve the objectives set forth in this Convention and to promote and review its implementation. The key functions of the Conference include:

- (i) Facilitating the exchange of information among States Parties on patterns and trends in corruption and on successful practices for preventing and combating it and for the return of proceeds of crime;
- (ii) Co-operating with relevant international and regional organizations and mechanisms and non-governmental organizations;
- (iii) Making appropriate use of relevant information produced by other international and regional mechanisms for combating and preventing corruption in order to avoid unnecessary duplication of work;
- (iv) Reviewing periodically the implementation of this Convention by its States Parties;
- (v) Making recommendations to improve this Convention and its implementation; and
- (vi) Taking note of the technical assistance requirements of States Parties with regard to the implementation of this Convention and recommending any action it may deem necessary in that respect.

To discharge its functions, articles 63 (5) of the Convention states that the Conference of the States Parties shall acquire the necessary knowledge of the measures taken by States Parties in implementing this Convention and the difficulties encountered by them in doing so through information provided by them and through such supplemental review mechanisms as may be established by the Conference of the States Parties.

To this end, article 63 (6) prescribes that each State Party shall provide the Conference of the States Parties with information on its programmes, plans and practices, as well as on legislative and administrative measures to implement this Convention, as required by the Conference of the States Parties. Furthermore, the Conference of the States Parties shall examine the most effective way of receiving and acting upon information, including, *inter alia*, information received from States Parties and from competent international organizations. Inputs received from relevant non-governmental organizations duly accredited in accordance with procedures to be decided upon by the Conference of the States Parties may also be considered.

In accordance with article 63 (7), the Conference has the prerogative to establish, if it deems it necessary, any appropriate mechanism or body to assist in the effective implementation of the Convention.

To date, the Conference of the States Parties has held two sessions. The first session took place in Jordan from 10 to 14 December 2006, while the second session was held in Nusa Dua, Indonesia, from 28 January to 1 February 2008. In both sessions, the Conference adopted crucial recommendations in the fields: of gathering information on States' efforts to implement the Convention; review of implementation; technical assistance and asset recovery.

B. The Intergovernmental Working Groups Established by the Conference

1. The Intergovernmental Working Group on the Review of Implementation of the Convention

In its resolution 1/1,¹⁵ the Conference of the States Parties to the United Nations Convention against Corruption, recalling article 63 of the United Nations Convention against Corruption, agreed that it was necessary to establish an appropriate and effective mechanism to assist in the review of the implementation of the Convention and decided to establish an open-ended Intergovernmental Expert Working Group to make recommendations to the Conference on the terms of reference of such a mechanism.

In furtherance to the aforementioned resolution, the Working Group on Review of Implementation of the Convention convened in Vienna, Austria, from 29 to 31 August 2007. The report¹⁶ of the Working Group was

¹⁵ Conference of the States Parties to the United Nations Convention against Corruption, First Session, Jordan, 10-14 December 2006, Resolution 1/1.

¹⁶ CAC/COSP/2008/3.

presented to the Conference at its second session. The latter, by resolution 2/1,¹⁷

- (i) took note with appreciation of the work of the Open-ended Intergovernmental Working Group on Review of the Implementation;
- (ii) stated that effective and efficient review of the implementation of the Convention in accordance with article 63 is of paramount importance and urgent;
- (iii) requested the Working Group to prepare terms of reference for a review mechanism for consideration, action and possible adoption by the Conference at its third session;
- (iv) decided that the Working Group should hold at least two meetings prior to the third session of the Conference in order to perform its mandated tasks; and
- (v) called upon States Parties and signatory States to submit proposals to the Working Group for the terms of reference of the mechanism sufficiently in advance of the meetings of the Working Group for its consideration.

Pursuant to resolution 2/1 of the Conference, the Working Group met again in Vienna from 22 to 24 September 2008. The meeting was informed by 33 proposals submitted by States parties and signatories on the parameters of the review mechanism. During the course of the meeting, the Working Group initiated the consolidation of such 33 proposals, with a view to systematizing them while eliminating duplications. UNODC was requested to carry out the remainder of the consolidation work and to present its outcome to the next meeting of the Working Group, due to take place in Vienna from 15 to 17 December 2008, for further discussion.

2. The Intergovernmental Working Group on Asset Recovery

In its resolution 1/4,¹⁸ the Conference established the Open-ended Intergovernmental Working Group on Asset Recovery. The mandate of the Working Group is: to assist the Conference in developing cumulative knowledge; encourage co-operation among relevant existing bilateral and multilateral initiatives; facilitate the exchange of information among States by identifying and disseminating good practices; help build confidence and encourage co-operation between requesting and requested States; facilitate the exchange of ideas among States on the expeditious return of assets; and assist the Conference in identifying the capacity-building needs, including long-term needs, of States Parties in the prevention and detection of the transfer of proceeds of corruption and income or benefits derived from such proceeds and in asset recovery.

Pursuant to that resolution, the Working Group held its first meeting in Vienna, on 27 and 28 August 2007, and its report was presented to the Conference of the States Parties at its second session.¹⁹ In that context, by resolution 2/3,²⁰ the Conference decided that the Working Group should continue its work, according to its mandate as set out in Conference resolution 1/4, to advise and assist the Conference in the implementation of its mandate on the return of proceeds of corruption, and should continue its deliberations on the conclusions and recommendations contained in the report on its first meeting, with a view to identifying ways and means of translating those conclusions and recommendations into concrete action. The Conference further decided that the Working Group should explore means of building confidence, facilitate the exchange of information and ideas on the expeditious return of assets among States and encourage co-operation between requesting and requested States. Finally, the Conference requested the Working Group to continue its deliberations with a view to further developing cumulative knowledge in the area of asset recovery, especially with regard to the implementation of chapter V, entitled "Asset recovery", of the Convention against Corruption.

Subsequent to the second session of the Conference, the Working Group on Asset Recovery held its second meeting in Vienna from 25 to 26 September 2008. The Working Group discussed challenges in carrying out successful asset recovery and possible solutions, as well as the implementation of recommendations it had agreed on at its first meeting. It confirmed its commitment to supporting the

¹⁷ Conference of the States Parties to the United Nations Convention against Corruption, Second Session, Nusa Dua, 28 January-1 February 2008, Resolution 2/1 .

¹⁸ Conference of the States Parties to the United Nations Convention against Corruption, First Session, Jordan, 10-14 December 2006, Resolution 1/4.

¹⁹ CAC/COSP/2008/4.

²⁰ Conference of the States Parties to the United Nations Convention against Corruption, Second Session, Nusa Dua, 28 January-1 February 2008, Resolution 2/3 .

UNODC's activities in co-ordinating existing knowledge in this field as well as studying trends and creating new tools, such as practical guides, an electronic legal library. Furthermore, the Working Group stressed the importance of technical assistance, particularly in implementing the UNCAC chapter on asset recovery, and agreed that setting up a network of contact points, and more generally creating opportunities for exchange and dialogue concerning asset recovery, would greatly enhance successful practice in this field.

3. The Intergovernmental Working Group on Technical Assistance

In its resolution 1/5,²¹ the Conference of the States Parties to the United Nations Convention against Corruption decided to establish an interim open-ended intergovernmental working group, in accordance with article 63, paragraph 4, of the United Nations Convention against Corruption, to advise and assist the Conference in the implementation of its mandate on technical assistance. In the same resolution, the Conference also decided that the working group should perform the following functions:

- (i) Review the needs for technical assistance in order to assist the Conference on the basis of the information provided by States to the Conference;
- (ii) Provide guidance on priorities, based on programmes approved by the Conference and its directives;
- (iii) Consider information gathered through the self-assessment checklist approved by the Conference;
- (iv) Consider information, as appropriate and readily available and in the areas covered by the Convention, on technical assistance activities of the Secretariat and States, including successful practices, and on projects and priorities of States, other entities of the United Nations system and international organizations; and
- (v) Promote the co-ordination of technical assistance in order to avoid duplication.

In furtherance of the aforementioned resolutions, the first meeting of the Working Group on Technical Assistance was held in Vienna from 1 to 2 October 2007. The report of the Working Group was presented to the Conference at its second session.²² The latter, in its resolution 2/4,²³ took note of the report on the meeting of the Open-ended Intergovernmental Working Group on Technical Assistance held in Vienna on 1 and 2 October 2007, and decided that the Working Group should continue its work to advise and assist the Conference in the implementation of its mandate on technical assistance, reaffirming that the Working Group should meet during the third session of the Conference and, as appropriate and within existing resources, shall hold at least two intersessional meetings prior to the third session of the Conference. The first of such intersessional meeting is scheduled to take place in Vienna from 18 to 19 December 2008.

IV. STATES PARTIES' LEGAL AND PRACTICAL CHALLENGES IN IMPLEMENTING THE UNITED NATIONS CONVENTION AGAINST CORRUPTION

A. Methodology to Identify Legal and Practical Challenges

In its resolution 1/2,²⁴ the Conference: (a) recognized the importance of gathering information on the implementation of the Convention; (b) decided that a self-assessment checklist should be used as a tool to facilitate the provision of information on implementation of the Convention; (c) requested the Secretariat to finalize the self-assessment checklist no later than two months after the conclusion of its first session, in consultation with and reflecting input from States Parties and signatories; (d) requested the Secretariat to distribute the self-assessment checklist to States Parties and signatories as soon as possible to begin the process of information-gathering, urging States Parties, and inviting signatories, to complete and return the checklist to the Secretariat within the deadline identified by it; and (e) requested the Secretariat to collate and analyse the information provided by States Parties and signatories through the self-assessment and to share that information and analysis with the Conference at its second session.

Between February and April 2007, the Secretariat began the development of a basic survey software package, which incorporated the self-assessment checklist. For each provision to be reviewed, the software

²¹ Conference of the States Parties to the United Nations Convention against Corruption, First Session, Jordan, 10-14 December 2006, Resolution 1/5.

²² CAC/COSP/2008/5.

²³ Conference of the States Parties to the United Nations Convention against Corruption, Second Session, Nusa Dua, 28 January-1 February 2008, Resolution 2/4.

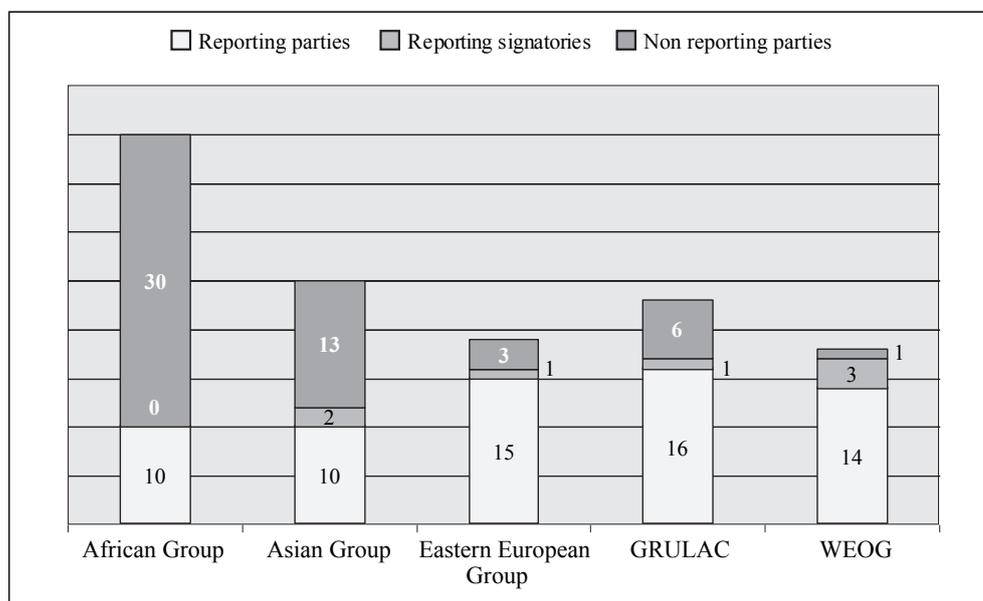
²⁴ Conference of the States Parties to the United Nations Convention against Corruption, First Session, Jordan, 10-14 December 2006, Resolution 1/2.

package offered clickable links to relevant reference material and to a summary of the main requirements against which compliance could be assessed. The development of such an innovative information-gathering tool was driven by the need: (a) to alleviate the long-lamented questionnaire fatigue, thus facilitating national authorities' fulfilment of the reporting obligation; and (b) to facilitate the Secretariat's analysis of information, thanks to the ability of the software to generate a variety of statistical data.

From 9 to 11 March 2007, an independent group of experts met in Vancouver, Canada, to review and validate the above approach. On 15 June 2007, the Secretariat distributed a CD-ROM containing the software to States Parties and signatories. On 30 June 2007, a computer-based application was made available for downloading from the United Nations Office on Drugs and Crime website.²⁵ The structure of the computer-based self-assessment checklist is such to enable the collection on information on the status of implementation of 15 selected articles of the Convention in the following thematic areas: (a) prevention;²⁶ (b) criminalization and law enforcement;²⁷ (c) international co-operation;²⁸ and (d) asset recovery.²⁹

For each selected provision, information was elicited by asking States whether they had adopted the measures required by the Convention. The available answers were (a) yes; (b) yes, in part; and (c) no. In case of full implementation ("yes"), and in order to simplify the reporting exercise, States were requested to cite, but not to provide copies of, relevant legislative information. Although optional, some 50 per cent of the reporting States excerpted or annexed copies of their legislation. An analysis of such legislation has been conducted by UNODC to the extent possible.³⁰ To substantiate reported implementation ("yes"), States were requested to provide examples of successful application of the measures cited or quoted. The optional nature of this question resulted in almost 50 per cent of the reporting States providing such examples. In case of partial compliance or non-compliance ("yes, in part" or "no"), States were requested to identify the type of technical assistance that, if available, would facilitate the adoption of the measures prescribed by the Convention.

As of 10 October 2008, 72 self-assessment reports had been received by the Secretariat, from 65 out of 126 States parties and seven signatories. The graphic below depicts the reporting status, and offers of an overview of reporting States Parties, reporting signatories and non-reporting States parties sorted by region.



²⁵ <http://www.unodc.org/unodc/en/treaties/CAC/index.html#selfassessment>

²⁶ Articles 5, 6, and 9.

²⁷ Articles 15, 16, 17, 23 and 25.

²⁸ Articles 44 and 46.

²⁹ Articles 52, 53, 54, 55 and 57.

³⁰ CAC/COSP/2008/2 and CAC/COSP/2008/2 Add.1.

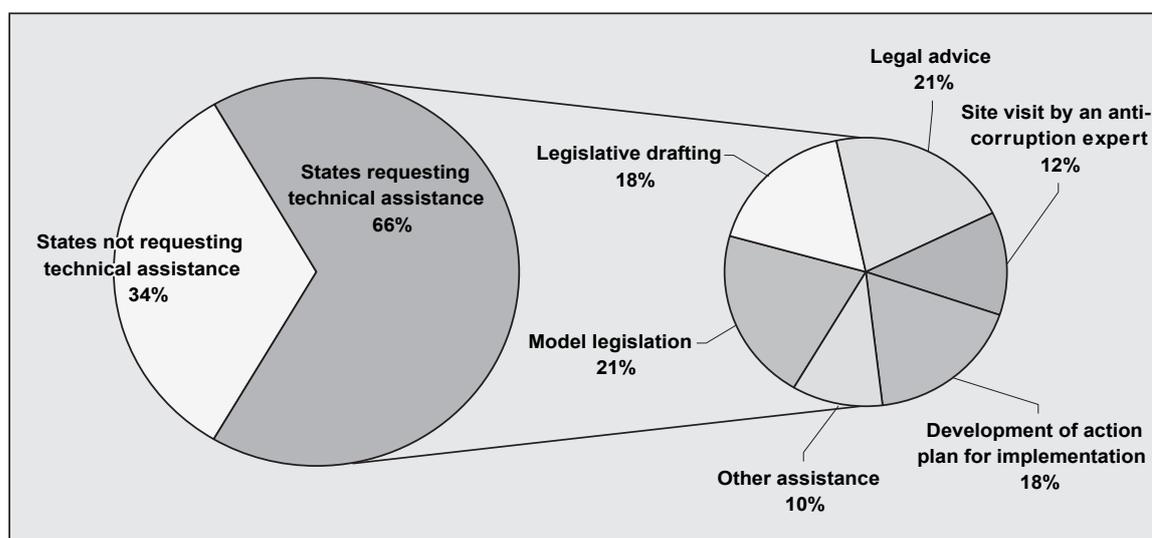
B. Identification of Legal and Practical Challenges

The above-mentioned information-gathering methodology enabled the attainment of the findings reported below:

- (i) In reporting on preventive measures (chapter II), the large majority of the reporting parties stated that anti-corruption policies (art. 5) and bodies (art. 6) had been established. The compliance rate in relation to the implementation of measures for public procurement and management of public funds (art. 9) is lower (56 per cent), with 4 per cent of the reporting parties providing no information.
- (ii) In reporting on criminalization and law enforcement (chapter III), measures providing for the criminalization of bribery of national public officials (art. 15) and embezzlement of public funds (art. 17) enjoy the highest rate of compliance (over 80 per cent for both articles). Similarly, three out of four reporting parties have criminalized obstruction of justice (art. 25). In contrast, the compliance rate for the provisions providing for the criminalization of money-laundering (art. 23) is the second lowest of the entire report, while provisions providing for the criminalization of bribery of foreign public officials (art. 16) are the least frequently implemented (49 per cent non-compliance rate).
- (iii) For international co-operation (chapter IV), since the review of implementation of measures adopted to implement chapter IV was limited to the fulfilment of notification obligations, no meaningful conclusions can be drawn.
- (iv) Lastly, for asset recovery (chapter V), out of the four chapters of the Convention under review, the compliance rate of chapter V is the lowest (less than 50 per cent), with the highest percentage of parties unable to provide any information.

Likewise, the same information-gathering methodology enabled the identification of legal and practical challenges reported below:

- (i) Of the States that reported partial compliance with chapter II (Preventive measures), 83 per cent requested technical assistance. The development of an action plan for implementation was the type of assistance most frequently requested (21 per cent), followed by requests for site visits by anti-corruption experts (15 per cent) and legal advice (13 per cent).
- (ii) Of the States that reported partial or non-compliance with chapter III (Criminalization and law enforcement), 79 per cent requested technical assistance. The provision of model legislation was the form of technical assistance most frequently requested (17 per cent), followed by the provision of legal advice (14 per cent), assistance in legislative drafting (12 per cent) and requests for on-site visits by anti-corruption experts (12 per cent).
- (iii) Of the States that reported partial or non-compliance with chapter V (Asset recovery), 83 per cent requested technical assistance. The provision of legal advice (19 per cent), model legislation (18 per cent) and support in legislative drafting (17 per cent) were the forms of assistance most frequently requested.



The overall analysis of technical assistance needs, depicted in figure above, shows that legal advice and model legislation (21 per cent each) are the forms of technical assistance most needed to implement the 15 articles of the Convention covered by the first round of review of implementation. This is followed by assistance in legislative drafting and in the formulation of action plans for implementation (18 per cent each). Site visits by anti-corruption experts (12 per cent), followed by other country-specific forms of assistance (10 per cent), are the least requested.

NATIONAL ANTI-CORRUPTION STRATEGY: THE ROLE OF GOVERNMENT MINISTRIES

*Tony Kwok Man-wai**



I. INTRODUCTION

I am honoured to have been invited to UNAFEI for the seventh time to share with you my 27 years of experience in fighting Corruption in Hong Kong, as well as my last six years of experience as an anti-corruption consultant/trainer in 19 different countries. I joined the ICAC as a junior investigator shortly after its inception in 1975 and was subsequently promoted through a number of ranks to become the first Chinese Deputy Commissioner and Head of Operations in 1996. I witnessed and participated in the successful battle to turn Hong Kong from one of the most corrupt places on earth to now one of the cleanest. Having been a pioneer corruption fighter for 27 years, I have maintained a strong passion for the anti-corruption mission and thus, since my retirement, I have been offering my consultancy service in the international arena to help fight this common enemy. Hence I am most grateful for the opportunity to participate in this most worthwhile course and share with you my experience.

II. POLITICAL WILL

From my experience and observation in a number of countries which have a serious corruption problem, I come to the conclusion that the most important element of an effective anti-corruption strategy is “political will”. Without political will at the highest level, it is almost impossible to combat corruption effectively. However, all political leaders will claim that they have the will to combat corruption. I propose that we should be able to judge whether there is genuine political will by checking the following criteria:

- Firstly, how much support has the government provided in its anti-corruption budget? In Hong Kong, we set aside 0.3 to 0.4% of our government budget for the ICAC and we believe this is quite adequate. I think no government can claim that they cannot afford to set aside such a small percentage for combating corruption, particularly when corruption is one of their major problems. However, I have witnessed that in many “corrupt” countries, their anti-corruption budget is often less than 0.01% of the national budget, and very often this is the main reason why they are unsuccessful. If a Government wants to demonstrate its political will, it should ensure that the Anti Corruption Agency (ACA) is given adequate resources.
- Secondly, is there adequate legal support for the ACA to investigate corruption? Because of its secret nature, corruption is one of the most difficult crimes to investigate, and to carry out effective enforcement an ACA needs strong power and easier-to-prove offences. The government and parliament can demonstrate their political will by passing legislation which is anti-corruption friendly.
- Thirdly, is the ACA truly independent in carrying out its enforcement work without political interference?
- Fourthly, is the government adopting a zero tolerance policy on corruption? If there is a double standard in the society, where minor corruption is tolerated or private sector corruption is tolerated, then it is impossible for the society to become a genuinely clean society.

Apart from political will, I want to point out two misconceptions about fighting corruption.

* Adjunct Professor & Honorary Course Director, Postgraduate Certificate in Corruption Studies, Hong Kong University SPACE and Former Deputy Commissioner and Head of Operations, Independent Commission Against Corruption (ICAC), Hong Kong.

- Firstly, it should be realized that there is no single solution to the problem of corruption. You need a comprehensive approach. The Hong Kong model, which is now widely accepted internationally and included in the United Nations Convention against Corruption, is to combat corruption through a three pronged approach: enforcement, prevention and education.
- Secondly, it should also be realized that you cannot rely on one single agency to combat corruption. Apart from ACA, there should be a coalition of all social partners. The most important partner is the Government, which has an important role in cleaning its own house. Other partners should include the judiciary, the parliament, the private sector, professional bodies, civil organizations, international agencies, the media and the public.

III. WHAT IS AN EFFECTIVE ANTI-CORRUPTION STRATEGY?

As a result of the success of the Hong Kong model in fighting corruption, many countries followed Hong Kong's example in setting up a dedicated anti-corruption agency. However, many such agencies have not been effective and hence there are queries as to whether the Hong Kong model can be successfully applied to other countries. The point is whether there is a thorough understanding of the working of the Hong Kong model. In my view, it consists of the following eleven components.

A. Three Pronged Strategy

As stated earlier, there is no single solution in fighting corruption. Hong Kong's ICAC adopts a three pronged approach: deterrence, prevention and education. As a result, the Commission consists of three separate departments: the Operations Department to investigate corruption; the Corruption Prevention Department to examine the systems and procedures in the public sector, to identify the corruption opportunities and to make recommendations to plug the loopholes; and the Community Relations Department to educate the public against the evil of corruption and to enlist its support and partnership in fighting corruption.

B. Enforcement Led

The three prongs are equally important, but ICAC devotes over 70% of its resources to the Operations Department. The reasons are that any successful fight against corruption must start with effective enforcement on major targets, so as to demonstrate to the public the government's determination to fight corruption at all costs, as well as to demonstrate the effectiveness of the anti-corruption agencies. Without that, the public would be reluctant to come forward to report corruption. Successful enforcement assists in identifying problem areas for corruption prevention review and can clear any human obstacle in the review. The successful enforcement stories also provide a basis for public education and deter other corrupt officials.

C. Professional Staff

Fighting corruption is a very difficult task, because you are confronting people who are probably very intelligent, knowledgeable and powerful. Thus anti-corruption agents must be very professional. The ICAC ensures that its staff is professional in its diverse responsibilities – the Operations Department has professional investigators, intelligence experts, computer experts, forensic accountants and legal experts. The Corruption Prevention Department has management/technical experts and the Community Relations Department pools together education, ethics and public relations experts. Apart from professionalism, each ICAC staff member is expected to uphold a high level of integrity and to possess a passion and sense of mission in carrying out his or her duties.

D. Effective Deterrence Strategy

The ICAC's strategy to ensure effective enforcement consists of the following components:

- An effective public complaint system to encourage reporting of corruption by members of the public and referrals from other institutions. ICAC has a 24 hour report centre – a highly publicized telephone hotline to facilitate public reporting.
- A quick response system to deal with complaints requiring prompt action. At any time, there is an investigation team standing by, ready to be called into action.
- The ICAC adopts a zero tolerance policy. So long as there is reasonable suspicion, all reports of corruption, irrespective of whether it is serious or relatively minor in nature, will be properly

investigated.

- There is a check and balance system to ensure all investigations are professionally and promptly investigated, and free from political interference.
- Any successful enforcement will be publicized in the media to demonstrate effectiveness and to deter further corruption.

E. Effective Prevention Strategy

The corruption prevention strategy aims at reducing corruption opportunities in government departments and public institutions. The general principle is to ensure efficiency, transparency and accountability in all government businesses.

The most corruption-vulnerable areas are public procurement, public works, licensing, public services delivery, law enforcement and revenue collection. These should be the priority areas to introduce corruption prevention reform as success would undoubtedly enhance government revenue and reduce wastage, hence providing the government additional resources to tackle the poverty problem.

F. Effective Education Strategy

To enlist the support of the entire community to fight corruption the ICAC has a very wide range of education strategies. These include:

- Media publicity to ensure effective enforcement cases are well publicized, through press releases, media conferences and interviews, as well as TV drama series based on successful cases;
- Media education – use of mass media commercials to encourage the public to report corruption; promote public awareness of the evil of corruption and the need for a fair and just society, and as deterrence to the corrupt;
- School ethics education programmes, starting from kindergarten up to university;
- The ICAC Club, which accepts members who wish to perform voluntary work for the ICAC in community education;
- Corruption prevention talks and ethics development seminars for public servants and the business sector;
- Corruption prevention best practices and guidelines publications;
- In partnership with the business sector, the ICAC set up an Ethics Development Centre as a resource centre for the promotion of a business code of ethics;
- Organize exhibitions, fun fairs, and television variety shows to spread the message of a clean society;
- Wide use of websites for publicity and reference, youth education and ethics development.

G. Effective Legal Framework and Anti-Corruption Law

Hong Kong has comprehensive legislation to deal with corruption. Apart from the normal bribery offences, it created three unique offences. It is an offence:

- for any civil servant to accept gifts, loans, discounts and passage from persons who have official/business relationships with the government, even if there is no related corrupt dealings, unless specific permission is given;
- for any civil servant to be in possession of assets disproportionate to his or her official income; or to live above his or her means,
- for a public official to abuse his or her authority for private gain, whether for him or herself or other persons. This is a criminal breach of the rule against conflict of interest. It includes a statutory requirement to report potential conflict of interest.

On investigative power, apart from the normal police power of search, arrest and detention, ICAC has the power to check bank accounts, intercept telephone communication, require witnesses to answer questions under oath, restrain properties suspected to be derived from corruption, and hold the suspects' travel documents to prevent them from fleeing the jurisdiction. Not only are they empowered to investigate corruption offences, both in the Government and the private sector, they can investigate all crimes which are connected with corruption.

The ICAC cases are prosecuted by a select panel of public prosecutors to ensure both quality and integrity. The judiciary of Hong Kong is a strong supporter of fighting corruption, which ensures that the

ICAC cases are handled in courts by highly professional judges with absolute fairness. The conviction rate for ICAC cases is very high, around 80%.

H. Check and Balance Mechanism

With the provision of wide investigative power, there is an elaborate check and balance system to prevent abuse of such wide power. One unique feature is the Operations Review Committee. It is a high powered committee, with the majority of its members coming from the private sector, appointed by the Chief Executive. The committee reviews each and every report of corruption and investigation, to ensure all complaints are properly dealt with and there is no “whitewashing”. It publishes an annual report, to be tabled for debate before the legislature, thus ensuring public transparency and accountability. In addition, there is an Independent Complaint Committee where members of the public can lodge any complaint against the ICAC and/or its officers and there will be an independent investigation. It also publishes an annual report to be tabled before the legislature.

I. Equal Emphasis on Public and Private Sector Corruption

Hong Kong was amongst one of the first jurisdictions to criminalize private sector corruption. ICAC places equal emphasis on private and public sector corruption. The rationale is that there should be no double standards. Private sector corruption can cause as much damage to society, if not more so, than public sector corruption. Serious corruption in financial institutions can cause market instability; corruption in the construction sector can result in dangerous structures. Effective enforcement of private sector anti-corruption measures can be seen as a safeguard for foreign investment and ensures that Hong Kong maintains a level playing field in its business environment, thus a competitive advantage in attracting foreign investment.

J. Partnership Approach

You cannot rely on one single agency to fight corruption. Every one in the community and every institution has a role to play. The ICAC adopts a partnership approach to mobilize all sectors to fight corruption together. The key strategic partner of ICAC is the government agencies. The head of government agency should appreciate that it is his or her solemn responsibility to clean his or her own house. Other important partners of ICAC include:

- (i) The Civil Service Commission
- (ii) The business community
- (iii) Professional bodies
- (iv) Civil societies and community organizations
- (v) Educational institutions
- (vi) Mass media
- (vii) International networking.

K. Top-Level Political Will

The most important factor in fighting corruption is “political will”. In Hong Kong, there is clearly top-level political will to eradicate corruption, which enables the ICAC to be a truly independent agency. ICAC is directly responsible to the very top, the Chief Executive of Hong Kong. This ensures that the ICAC is free from any interference in conducting its investigations. The strong political support was translated into financial support. The ICAC is provided with adequate resources to combat corruption on all three fronts.

IV. WHY MANY ACAs FAILED

Many countries suffering from serious corruption problems set up Anti Corruption Agencies (ACAs). Countries in Asia that have established dedicated ACAs include Singapore, Malaysia, Thailand, the Philippines, Brunei, Indonesia, Sri Lanka, Timor Leste, Papua New Guinea, Pakistan, Bangladesh, South Korea, China, Bhutan and Mongolia. However, few of them are regarded as effective in reducing corruption. In some cases, corruption worsened. By comparison with the Hong Kong Model, one can identify the following reasons why they failed:

- Lack of understanding of the causes of corruption: The causes of corruption are due to available corruption opportunities, lack of ethical values of public officials and citizens, and lack of deterrence.

Some ACAs failed to understand and hence failed to take effective action against each of the three main causes. The most common error is the belief that corruption can be eradicated through good governance reform. Some ACAs have no jurisdiction to investigate corruption and can only deal with prevention and education. On the other hand, some ACAs focus on enforcement only.

- Lack of resources: In most corrupt countries where the ACA is not seen to be effective, it usually suffers from lack of resources. Such ACAs' budgets are invariably below 0.01% of the national budget. Hong Kong's anti-corruption budget is 0.38% of the government budget, which is already adequate and such small percentage is clearly affordable by most governments;
- Lack of independence: The ACA is subject to political interference in its investigations and prosecutions. Some ACAs were perceived to be used as political tools against the opponents of the government;
- Lack of legal support: The anti-corruption law is inadequate to enable the ACA to function effectively. Some ACAs do not have power to have access bank accounts, which is essential in corruption investigations. Some ACAs do not even have the power of arrest.
- Lack of public credibility: Some ACAs do not pursue a policy to encourage public reports. Some even discourage public reporting by imposing stringent conditions. In some countries, any corruption report should be in the form of sworn affidavit before it is accepted by the ACA. Some ACAs refused to investigate minor corruption complaints or those involving political sensitivity. Some failed to observe confidentiality with the corruption reports. Some are biased in their investigation or abuse their power. They all suffered from lack of public credibility and without public support, it is impossible for them to achieve success
- Lack of coalition: The ACA appears to be fighting a lonely battle, with little support from government institutions and legislature;
- Corrupt judiciary: making it most difficult to convict corrupt offenders, hence lack of deterrent effect. To tackle this problem, some countries, such as Pakistan and the Philippines, have to set up special courts to hear corruption trials;
- Lack of professionals: Some ACAs commence their operation prematurely before they have sufficiently experienced and professional staff. Hence their ineffectiveness was highly exposed and the initial public welcome was replaced by public cynicism;
- Lack of internal control: Some ACAs are perceived to have an internal corruption problem.

The overriding factor for failure is the lack of political will. If there is strong political will and determination, most of the above problems can be resolved

V. THE ROLE OF GOVERNMENT MINISTRIES

Apart from the ACAs, the most important players in combating corruption in a country are the government ministries. I had assisted the President of the Philippines and the Prime Minister of Mongolia to run top level anti-corruption workshops for their heads of ministries. It was amazing to note that initially these heads did not consider fighting corruption as their prime responsibility. But it is interesting to note that after the workshop, they then came to have a better understanding of their internal corruption problem and their responsibilities to clean their own houses. In these workshops, they came to accept that they have the following internal problems:

- Failure by the head of ministry to accept his or her responsibility to combat inhouse corruption;
- Inadequate and ineffective in-house anti-corruption strategy and action plan;
- Lack of integrity and ethics amongst staff;
- Lack of enforcement of ethical conduct and ethical training;
- Nepotism and conflict of interest in human resource management;
- Poor public service delivery due to bureaucracy and corruption;
- Outdated regulations, resulting in lack of transparency and accountability;
- Lack of fair procurement procedures and political interference;
- Weak internal audit.

They also agreed that there were indeed many things which they can or should do. These workshops ended with a consensus on an action plan which the government ministries should implement, such as:

- Set up its own Anti-corruption Steering Group;
- Review procedures and systems to make them more transparent and accountable;

- Formulate tailor-made codes of ethics and include regulation on acceptance of gifts and entertainment;
- Introduce a declaration system for conflict of interest;
- Practice an open and fair recruitment and promotion system, and include integrity checking;
- Introduce staff training on ethics and corruption prevention;
- Leadership by example;
- Promulgate zero tolerance policy;
- Set up internal staff monitoring unit & internal audit unit;
- Enhance and promulgate a public and internal confidential complaint channel with a complaint hotline;
- Prompt referral of cases to the ACA and full co-operation with the ACA in investigation.

The government ministry should have a comprehensive corruption prevention strategy which should include enhancement in the following management systems:

- Performance Management
- Procurement Management
- Financial Management
- Human Resources Management
- Complaint Management.

Examples of some of the corruption prevention practices are:

- Identify risk in vulnerable areas and risk management;
- Streamline work procedure manuals;
- Enhance staff supervision through surprise check systems;
- Enhance internal audits;
- Maintain proper documentation for accountability;
- Information security policy;
- Job rotation policy;
- Performance indicators/performance pledges (service guarantee);
- E-government and e-procurement;
- Exercise transparency and fairness in staff recruitment, appraisal and promotion.

In both the Philippines and Mongolia, there is now a system of monitoring the annual anti-corruption plan of the government ministries, to provide professional support and to ensure its sustainability through annual review.

VI. INTERNATIONAL BEST PRACTICES

Having travelled to different countries as an international anti-corruption consultant, I have collected some examples of international best practices in combating corruption:

- In South Korea, the public sector, the business sector and civil society joined hands in forming a coalition called Korea-PACT. Over 800 organizations signed the PACT and undertook to implement the agreed action plan. The progress was reviewed annually by an international evaluation team;
- In the Philippines, an expert team is going through the government ministries one by one to carry out a comprehensive integrity audit check and to make recommendations on what measures the respective government ministries should implement to combat internal corruption problems;
- In the Philippines, all public procurement in government ministries should be conducted through a “Bids and Award Committee”, and lay observers should be appointed to represent the public in monitoring the decision making progress;
- In Canada, all public officers have a legal obligation to report corruption;
- In Pakistan, the Philippines and Indonesia, special anti-corruption courts were formed to hear corruption trials;
- Malaysia set up its own Malaysian National Integrity Index to monitor its the integrity progress.

VII. CONCLUSION

There is no single solution in fighting corruption. Every country has to examine its unique circumstances and come up with a comprehensive strategy, which should embrace the three pronged approach - deterrence, prevention and education. Ideally, there should be a dedicated and independent anti-corruption agency tasked to co-ordinate and implement such strategy, and to mobilize support from the community.

The Hong Kong experience offers hope to countries which have a serious corruption problem which appears to be insurmountable. Hong Kong's experience proves that given top-level political will, a dedicated anti-corruption agency and a correct strategy, even a most corrupt place, like Hong Kong, can be transformed into a clean society.

INVESTIGATION OF CORRUPTION CASES

*Tony Kwok Man-wai**

I. INTRODUCTION

The Hong Kong Independent Commission Against Corruption (ICAC) is popularly regarded as a successful model in fighting corruption, turning a very corrupt city under colonial government into one of the relatively corruption free places in the world. One of the success factors is its three-pronged strategy - fighting corruption through deterrence, prevention and education. All three are important but in my view, deterrence is the most important. That is the reason why the ICAC devotes over 70% of its resources to its Operations Department, which is responsible for investigating corruption. Nearly all of the major corruption cases I have dealt with were committed by people in high authority. For them, they have certainly been educated about the evil of corruption and they may also be subject to certain degree of corruption prevention control. But what inspired them to commit corruption? The answer is simply greed, as they would weigh the benefits they could get from corruption against the chance of them being discovered. If they think that it is a low-risk, high-return opportunity, they will likely succumb to the temptation. So how can we deter them from being corrupt? The only way is to make them realize that there is a high risk of them being caught. Hence the mission of the ICAC Operations Department is to make corruption a high-risk crime. To do that, you need a professional and dedicated investigative force.

II. DIFFICULTIES OF INVESTIGATING CORRUPTION

Corruption is regarded as one of the most difficult crimes to investigate. There is often no scene of the crime, no fingerprint, no eye-witness to follow up. It is by nature a very secretive crime and can involve just two satisfied parties, so there is no incentive to divulge the truth. Even if there are witnesses, they are often parties to the corruption themselves, hence tainted with doubtful credibility when they become prosecution witnesses in court. The offenders can be equally as professional as the investigators and know how to cover their trails. The offenders can also be very powerful and ruthless in enforcing a code of silence amongst related persons through intimidation and violence to abort any investigation. In this modern age, the sophisticated corrupt offenders will take full advantage of the loopholes in cross-jurisdictions and acquire the assistance of other professionals, such as lawyers, accountants and computer experts in their clandestine operations and to help them launder their corrupt proceeds.

III. CORRUPTION AND ORGANIZED CRIME

Corruption rarely exists alone. It is often a tool to facilitate organized crime. Over the years, ICAC have investigated a wide range of organized crimes facilitated by corruption. Law enforcement officers have been arrested and convicted for corruptly assisting drug traffickers and smugglers of various kinds; bank managers for covering up money laundering for organized crime syndicates; hotel and retail staff for perpetuating credit card fraud. In these cases, we need to investigate not only corruption, but some very sophisticated organized crime syndicates as well.

IV. PREREQUISITES FOR AN EFFECTIVE INVESTIGATION

Hence, there is an essential need for professionalism in corruption investigation. There are several prerequisites to an effective corruption investigation.

* Adjunct Professor & Honorary Course Director, Corruption Studies Programme, Hong Kong University SPACE and Former Deputy Commissioner & Head of Operations, ICAC, Hong Kong.

A. Independence

Corruption investigation can be politically sensitive and embarrassing to the government. The investigation can only be effective if it is truly independent and free from undue interference. This depends very much on whether there is top political will to fight corruption in the country, and whether the head of the anti-corruption agency has the moral courage to stand against any interference.

B. Adequate Investigative Power

Because corruption is so difficult to investigate, you need adequate investigative power. The HK ICAC enjoys wide investigative power. Apart from the normal police power of search, arrest and detention, it has power to check bank accounts, intercept telephone communications, require suspects to declare their assets, require witnesses to answer questions under oath, restrain properties suspected to be derived from corruption, and hold the suspects' travel documents to prevent them from fleeing the jurisdiction. Not only is the ICAC empowered to investigate corruption offences, both in the government and private sector, they can investigate all crimes which are connected with corruption. I must hasten to add that there is an elaborate check and balance system to prevent abuse of such wide power.

C. Adequate Resources

Investigating corruption can be very time-consuming and resource intensive, particularly if the cases involve cross-jurisdiction. In 2007, the HK ICAC's annual budget amounted to US\$90M, about US\$15 per capita. You may wish to multiply this figure with your own country's population and work out the anti-corruption budget that needs to be given to the equivalent of ours! However, looking at our budget from another angle - it represents only 0.3% of our entire government budget or 0.05% of our Gross Domestic Product (GDP). I think you will agree that such a small "premium" is a most worthwhile investment for a clean society.

D. Confidentiality

It is crucial that all corruption investigation should be conducted covertly and confidentially, at least before arrest action is ready, so as to reduce the opportunities for compromise or interference. On the other hand, many targets under investigation may prove to be innocent and it is only fair to preserve their reputation before there is clear evidence of their corrupt deeds. Hence in Hong Kong, we have a law prohibiting anyone, including the media, from disclosing any details of an ICAC investigation until overt action such as arrests and searches have been taken. The media once described this as a "press gag law" but they now come to accept it as a right balance between press freedom and effective law enforcement.

E. International Mutual Assistance

Many corruption cases are now cross-jurisdictional and it is important that you can obtain international assistance in the areas such as locating witnesses and suspects; money trails, surveillance, exchange of intelligence, arrest, search and extradition, and even joint investigation and operation.

F. Professionalism

All the investigators must be properly trained and professional in their investigation. The HK ICAC strives to be one of the most professional law enforcement agencies in the world. ICAC is one of the first agencies in the world to introduce the interview of all suspects under video, because professional interview technique and the need to protect the integrity of the interview evidence are crucial in any successful corruption prosecution. The investigators must be persons of high integrity. They must adhere strictly to the rule of confidentiality, act fairly and justly in the discharge of their duties, respect the rights of others, including the suspects, and should never abuse their power. As corruption is so difficult to investigate, they need to be vigilant, innovative and be prepared to spend long hours to complete their investigation. The ICAC officers are often proud of their sense of mission and this is the single most important ingredient of success of the ICAC.

G. An Effective Complaint System

No anti-corruption agency is in a position to discover all corrupt dealings by itself. They rely heavily on an effective complaint system. The system must be able to encourage quality complaints from members of the public or institutions, and at the same time, deter frivolous or malicious complaints. It should provide assurance to the complainants of the confidentiality of their reports and if necessary, offer them protection. Since the strategy is to welcome complaints, customer service should be offered, making it convenient to

report corruption. A 24 hour reporting hotline should be established and there should be a quick response system to deal with any complaints that require prompt action. All complaints, as long as there is substance in them, should be investigated, irrespective of how minor is the corruption allegation. What appears to be minor in the eyes of the authority may be very serious in the eyes of the general public!

H. Understanding the Process of Corruption

It should be helpful to the investigators to understand the normal process of corruption, and through which the investigators would be able to know where to obtain evidence to prove the corrupt act. Generally, a corrupt transaction may include the following steps:

1. Softening-up Process

It is quite unlikely that a government servant would be corrupt from his or her first day in office. It is also unlikely that any potential bribe-offerer would approach any government servant to offer a bribe without building up a good relationship with him or her first. Thus there is always a “softening up process” when the bribe-offerer builds up a social relationship with the government servant, for example, inviting him or her to dinner and karaoke, etc. Thus the investigator should also attempt to discover evidence to prove that the government servant had accepted entertainment prior to the actual corrupt transaction.

2. Soliciting/Offering of Bribe

When the time is ripe, the bribe-offerer would propose to seek favour from the government servant and in return offer a bribe to him or her. The investigator should attempt to prove when and where this had taken place.

3. Source of Bribe

When there is agreement for the bribe, the bribe-offerer would have to withdraw money for the payment. The investigator should attempt to locate the source of the funds and whether there was any third person who assisted in handling the bribe payment.

4. Payment of Bribe

The bribe would then be paid. The investigator should attempt to find out where, when and how the payment was effected.

5. Disposal of Bribe

On receipt of the bribe, the receiver would have to dispose the cash. The investigator should try to locate how the bribe was disposed, either by spending or depositing into a bank.

6. Abuse of Power

To prove a corruption offence, you need to prove the corrupt act or the abuse of position in return for the bribe. The investigator needs to identify the documents or other means proving his or her abuse of authority.

The task of the investigator is to collect sufficient evidence to prove the above process. He or she needs to prove “when”, “where”, “who”, “what”, “how” and “why” on every incidence, if possible.

However this should not be the end of the investigation. It is rare that corruption is a single event. A corrupt government servant would likely take bribes on more than one occasion. A bribe-offerer would likely offer bribes on more than one occasion and to more than one corrupt official. Hence it is important that the investigator should seek to look into the bottom of the case, to unearth all the corrupt offenders connected with the case.

V. METHODS OF INVESTIGATING CORRUPTION

Investigating corruption can broadly be divided into two categories:

- A. Investigating past corruption offences;
- B. Investigating current corruption offences.

A. Investigating Past Offences

The investigation normally commences with a report of corruption and the normal criminal investigation technique should apply. Much will depend on the information provided by the informant and from there, the case should be developed to obtain direct, corroborative and circumstantial evidence. The success of such investigation relies on the meticulous approach taken by the investigators to ensure that no stone is left unturned. Areas of investigation can include detailed checking of the related bank accounts and company ledgers, obtaining information from various witnesses and sources to corroborate any meetings or corrupt transactions, etc. At the initial stage, the investigation should be covert and kept confidential. If there is no evidence discovered in this stage, the investigation should normally be curtailed and the suspects should not be interviewed. This would protect the suspects, who are often public servants, from undue harassment. When there is a reasonable suspicion or evidence discovered in the covert stage, the investigation can enter its overt stage. Action can then be taken to interview the suspects to seek their explanation and if appropriate, the suspects' homes and offices can be searched for further evidence. Normally, further follow-up investigation is necessary to check the suspects' explanations or to go through the money trails as a result of evidence found during searches. The investigation is usually time-consuming.

B. Investigating Current Corruption Offences

Such investigation will enable greater scope for ingenuity. Apart from the conventional methods mentioned above, a proactive strategy should always be preferred, with a view to catching the corrupt red-handed. In appropriate cases, with proper authorities obtained, surveillance and telephone interception can be mounted on the suspects and suspicious meetings monitored. A co-operative party can be deployed to set up a meeting with a view to entrapping the suspects. Undercover operation can also be considered to infiltrate a corruption syndicate. The pre-requisites to all these proactive investigation methods are professional training, adequate operational support and a comprehensive supervisory system to ensure that they are effective and in compliance with the rule of evidence.

As mentioned above, corruption is always linked and can be syndicated. Every effort should be explored to ascertain if the individual offender is prepared to implicate other accomplices or the mastermind behind the scheme. In Hong Kong, there is a judicial directive to allow a two thirds reduction of the sentence of those corrupt offenders who are prepared to provide full information to ICAC and to give evidence against the accomplices in court. The ICAC provides special facilities to enable such "resident informants" to be detained in ICAC premises for the purpose of de-briefing and protection. This "resident informant" system has proved to be very effective in dealing with syndicated or high-level corruption.

VI. INVESTIGATION TECHNIQUE

To be a competent corruption investigator, an official should know many investigation techniques and skills. The following are the essential ones:

- Ability to identify and trace persons, companies and properties;
- Interview technique;
- Document examination;
- Financial investigation;
- Conducting a search and arrest operations;
- Physical and technical surveillance;
- Acting as undercover agent;
- Handling informers;
- Conducting an entrapment operation;
- Witness protection.

I will try to cover the key investigation techniques.

A. Interview Technique

As corruption is a secret crime involving parties who are often sworn to a code of secrecy and silence, a successful corruption investigator should always be a good interviewer, to break the code of silence. Interview technique always forms a very important part of the professional training of corruption investigators. Interview techniques should include the following elements:

- Proper preparation and planning before the interview: the interviewer must study the case thoroughly: the background of the interviewee, the available evidence against him or her, the list of question areas, etc. He or she should then formulate the structure of the interview.
- Ability to deal with reluctant witness: it is fully understandable that the interviewees in corruption cases are reluctant to come forward in the interview. The interviewer must have the ability to identify the reasons behind the interviewee's reluctance, whether it is due to his or her dislike of the agency, fear of intimidation, fear of going to court, his or her relations with the corrupt offenders, etc, and to use the appropriate strategy to win his or her co-operation;
- Ability to build rapport: by putting the interviewee at ease in a hospitable environment, giving him or her reassurance, and handling him or her with patience and sympathy;
- Need for active listening and to be flexible in the line of questioning, depending on what the interviewee has said;
- Maintain eye-contact and watch the body language, which often give you clue as to the truthfulness of what the interviewee is saying. Always attempt to test the truth and to identify the motive of the statements made by the interviewee;
- If the interviewee is prepared to relate the full version, ensure that maximum details are obtained – when, where, who, what and how, in chronological sequence, and most important of all, who else is also involved in the corruption;
- Always retain control in the interview.

B. Professional Investigative Support

In order to ensure a high degree of professionalism, many of the investigation techniques can be undertaken by a dedicated unit, such as the following:

1. Intelligence Section

The intelligence section is a central point to collect, collate, analyse and disseminate all intelligence and investigation data, otherwise there may be major breakdown in communication and operations

2. Surveillance Section

The surveillance section is a very important source of evidence and intelligence. The Hong Kong ICAC has a dedicated surveillance unit of over 120 surveillance agents and they have made a significant contribution to the success of a number of major cases.

3. Technical Services Section

This section provides essential technical support to surveillance and operations.

4. Information Technology Section

Rapidly advancing telecommunications techniques have created a threat to corruption investigation. Corrupt negotiation can be carried out without personal contact. It can be done through email, mobile phone, fax, all without trace. Corrupt transactions via e-banking can, with a switch of button, transfer money to overseas accounts. Paper documentation is often replaced by computer records protected by unbreakable passwords. In extreme cases, professional hackers are employed to break into the computer systems of the anti-corruption agencies to find out the progress of investigations. Counter-surveillance and counter-interception techniques are often engaged to neutralize the law enforcement effort.

However, modern information and telecommunications technology can be a great asset in corruption investigation, such as:

- Telecommunications and other technical equipment used in surveillance;
- Capability to intercept all types of telecommunication including mobile phones, Internet, fax, etc.;
- Speaker identification techniques for production of intercepted evidence;
- Mobile/Internet/ CCTV records;
- Computer forensics;
- Computer intelligence analysis techniques;
- Major enquiry/operations computer systems.

5. Financial Investigation Section

Corruption investigations these days often involve sophisticated money trails of proceeds of corruption,

which can go through a web of off-shore companies and bank accounts, funds, etc. It is necessary to employ professionally qualified investigative accountants to assist in such investigation and in presenting such evidence in an acceptable format in court.

6. Witness Protection Section

ICAC has experienced cases where crucial witnesses were compromised, one even murdered, before giving evidence. There should be a comprehensive system to protect crucial witnesses, including 24 hour armed protection, safe housing, new identity and overseas relocation. Some of these measures require legislative backing.

VII. CONCLUSION AND OBSERVATION

In conclusion, the success factors for an effective corruption investigation include:

- An effective complaint system to attract quality corruption reports;
- An intelligence system to supplement the complaint system and to provide intelligence support to investigations;
- Professional and dedicated investigators who need to be particularly effective in interviewing techniques and financial investigation;
- More use of proactive investigation methods, such as entrapment and undercover operations;
- Ensure strict confidentiality of corruption investigation, with a good system of protection of whistleblowers and key witnesses;
- International co-operation.

It is obvious that corruption and organized crime are getting more and more difficult to investigate. The offenders have taken full advantage of the high technology and cross-jurisdiction loopholes. Conventional investigation methods and current legal systems may not be adequate to win the battle against the corrupt. We should adopt a more proactive approach in investigation, such as in the wider use of undercover operations and the use of telephone interception, and to this end, we need to strike the right balance between effective law enforcement and protection of human rights and privacy.

PARTICIPANTS' PAPERS

THE CRIMINAL JUSTICE RESPONSE TO CORRUPTION – BANGLADESH PERSPECTIVE –

*Jahanara Pervin**

I. INTRODUCTION

Corruption is a global problem. It exists to a greater or lesser degree in all countries; irrespective of political and economic systems, size, or state of development.

Bangladesh is a densely populated country. The pressure of population, terrorism, poverty, illiteracy, natural disasters and corruption are some of the problems facing the country which seriously hamper its growth. Corruption in particular has made this nation unstable. However, the people of Bangladesh fight corruption continuously.

The role of the criminal justice system is crucial in the fight against corruption. Successful detection, investigation, prosecution, adjudication and punishment of corrupt offenders contribute greatly to the prevention and eradication of corruption. But these are not easy tasks to accomplish. To successfully overcome the challenges, the criminal justice authorities need to use innovative legal means, both domestically and internationally. In addition, it is of the utmost importance to ensure and maintain the integrity and necessary independence of criminal justice personnel, as a prerequisite to fulfilling their great responsibilities.

In a democratic system, the government has three wings, the executive, the legislative and the judiciary. The Bangladesh constitution ensures these three wings act separately and independently. According to constitutional obligation the judiciary has been separated. The Code of Criminal Procedure 1989 has been amended. Since 11 January 2007, there has been great attention to controlling corruption at different levels. The government of Bangladesh has taken adequate measures to curb different aspects of corruption.

II. BANGLADESH: A PARTY TO THE UNCAC

The UNCAC is the first global, legally binding instrument on corruption and a comprehensive document that includes measures on prevention, criminalization and international co-operation. Bangladesh acceded to the UNCAC on 27 February 2007. That has been a significant and symbolic step toward great reforms for good governance and is consistent with its commitment and declared strategy to fighting corruption and complying with international standards. Bangladesh acceded to the UNCAC because, together with other States Parties to the convention, it is convinced and concerned about the objectives it expects to achieve by acceding to the UNCAC. The report "UNCAC- a Bangladesh Compliance and Gap Analysis" is the result of this initiative. To convey the nation's progress in implementing the UNCAC the report was presented by the government of Bangladesh at the second conference of States Parties in Bali, Indonesia, in January 2008. The second edition of the report has already been published. Bangladesh's existing legislation covers most of the requirements for the criminalization of corruption offences and even goes beyond that, covering some elements of the offence in the non-mandatory clauses and others.

III. CURRENT SITUATION IN BANGLADESH OF CORRUPTION AND RELATED ACTS

The criminal justice system of Bangladesh is based on common law. The purpose of criminal justice is punitive. The law and justice are quite essential for keeping peace, order and civilization of the state. Prevention and eradication of corruption require a comprehensive and multidisciplinary approach.

* Director, Anti-Corruption Commission, Bangladesh.

Established in 2004, the ACC was re-constituted in 2007. Already, the Anti-Corruption Commission Rule, 2007 has been promulgated and the commission has succeeded in establishing itself as an independent body. Since then it has been working with tremendous enthusiasm, showing unprecedented activism and increasingly gaining public confidence. As of 31 August 2008, the ACC filed 1,150 criminal cases of corruption. Of those, 190 have been sent to trial and judgments have been received in 87 cases with 11 total convictions. The remainder are under inquiry and investigation. Three hundred and eighty are wealth statements asked for. However, to institutionalize this current image and effectiveness of the ACC along with the continued political will and commitment to combat corruption, an independent judiciary and other watchdog institutions are essential. In 2007, the judiciary of Bangladesh was completely separated from the executive. This is a historical achievement.

A. Bribery of National Public Officials

Chapter III of the UNCAC obligates States Parties to criminalize a wide range of acts of corruption (Articles 15-27) and to establish a series of procedural measures and mechanisms that support such criminalization (Articles 28-41).

The UNCAC obligates the States Parties to criminalize certain acts of bribery. These are active bribery of national public officials (Article 15), and passive bribery of national public officials (Article 15.b).

In Bangladesh, the Penal Code, 1860 criminalizes the act of taking by a public servant of any gratification other than legal remuneration in respect of an official act (Section 161); the act of obtaining by a public servant of any valuable thing without consideration from a person concerned in proceedings or business transacted by such public servant (Section 165); and any abetment, i.e., instigating or aiding, by any person of any such taking or obtaining (Section 165A). Moreover, according to the Prevention of Corruption Act, 1947, the act of accepting or obtaining by a public servant of any gratification other than legal remuneration in respect of an official act (Section 5(1) (a)), and the act of accepting or obtaining by a public servant of any valuable thing without consideration from person concerned in the proceedings or business transacted by such public servant (Section 5(1) (b)) amount to punishable criminal misconduct. These penal provisions adequately address the UNCAC requirements regarding active and passive bribery of national public officials.

B. Embezzlement, Misappropriation or Other Diversion of Property by a Public Official

States Parties have a mandatory obligation to criminalize embezzlement, misappropriation or other diversion of property by a public official (Article 17). Regarding embezzlement, misappropriation or other diversion of property by a public official (Article 17), the domestic standard is quite compatible with the UNCAC standard. The Penal Code criminalizes the act of dishonest misappropriation of property (Section 403) and criminal breach of trust by a public servant (Section 409). These offences, as their definitions indicate, include embezzlement, misappropriation or other diversion of property by a public official. Moreover, according to the Prevention of Corruption Act, 1947, the act of dishonest or fraudulent misappropriation or conversion by a public servant for his or her own use of any property entrusted to him or her or under his or her control as a public servant or allowing any other person so to do is punishable, criminal, misconduct (Section 5(1) (c)); on the other hand, definitions of the offences of dishonest misappropriation of property (Section 403) and criminal breach of trust (Section 406) are criminalized by the Penal Code, 1860.

IV. CORRUPTION OFFENCES AND CORRUPTION-RELATED OFFENCES IN BANGLADESH

A. Offences under the Anti Corruption Commission Act, 2004

1. Section 19: Special Powers of the Commission in Respect of Inquiry or Investigation

- (i) Any person obstructing an official legally empowered by the commission, or a commissioner in the exercise of his or her powers under this sub-section (1), or any person deliberately violating any order given under that sub-section commits a punishable offence is liable to a term of imprisonment of not more than three years or a fine or both.

2. Section 26: Declaration of Properties

- (i) If the commission is satisfied on the basis of its own information and after necessary investigation that any person or any other person on his or her behalf is in possession or has obtained ownership of property not consistent with his or her legal/known sources of income then the commission through an order in writing shall ask that person to submit a statement of assets and liabilities in the

manner determined by the commission and to furnish any other information mentioned in that order.

(ii) If any person

(a) After having received an order mentioned in sub-section (1) fails to submit the written statement or furnish the information accordingly or submits any written statement or provides any information that is false or baseless or there are sufficient grounds to doubt their veracity; or

(b) Submits any book, account, record, declaration, return or any document under sub-section (1) or gives any statement that is false or baseless or there are sufficient grounds to doubt its veracity, then that person will be sentenced to a prison term of up to three years or a fine or both.

3. Section 27: Possession of Property in Excess of Known Sources of Income

(i) If there are sufficient and reasonable grounds to believe that a person in his/her own name or any other person on his/her behalf is in possession and has obtained ownership of moveable or immovable property through dishonest means and the property is not consistent with the known sources of his/her income and if he/she fails to submit to the court during trial a satisfactory explanation for possessing that property, then that person shall be sentenced to a prison terms ranging from a minimum of three years to a maximum of ten years' imprisonment, and these properties shall be confiscated.

B. Offences under the Prevention of Corruption Act, 1947

1. Section 5, Subsection (2)

Any public servant who commits or attempts to commit criminal misconduct shall be punishable with imprisonment for a term which may extend to seven years, or with fine or with both.

C. Offences under Sections 161-169, 217, 218, 408, 409, 477A and Sections 109, 120(B) & 511 of the Penal Code, 1860 (Act XLV of 1860)

(a) Sec 161: Being or expecting to be a public servant and taking a gratification other than legal remuneration in respect of an official act. Imprisonment of either description for three years, or fine, or both;

(b) Sec 162: Taking a gratification in order by corrupt or illegal means to influence a public servant. Imprisonment of either description for three years, or fine, or both;

(c) Sec 163: Taking a gratification for the exercise of personal influence with a public servant. Simple imprisonment for 1 year or fine, or both;

(d) Sec 164: Abetment by public servant of the offence defined in the last two preceding clauses with reference to himself. Imprisonment of either description for three years, or fine, or both;

(e) Sec 165: Public servant obtaining any valuable thing, without consideration, from a person concerned in any proceeding or business transacted by such public servant. Imprisonment of either description for three years, or fine, or both;

(f) Sec 165A: Abetment of offences under Section 161 and 165. Imprisonment of either description for three years, or fine, or both;

(g) Sec 166: Public servant disobeying a direction of the law with intent to cause injury to any person. Simple imprisonment for one year, or fine, or both;

(h) Sec 167: Public servant framing an incorrect document with intent to cause injury. Imprisonment of either description for three years, or fine, or both;

(i) Sec 168: Public servant unlawfully engaging in trade. Simple imprisonment for one year of fine, or both;

(j) Sec 169: Public servant unlawfully buying or bidding for property Simple imprisonment for three years, or fine, or both and confiscation of property, if purchased;

(k) Sec 217: Public servant disobeying a direction of law with intent to save a person from punishment,

or property from forfeiture. Imprisonment of either description for two years, or fine, or both;

- (l) Sec 218: Public servant framing an incorrect record or writing with intent to save person from punishment, or property from forfeiture. Imprisonment of either description for three years or fine, or both;
- (m) Sec 408: Criminal breach of trust by a clerk or servant. Imprisonment of either description for seven years and fine;
- (n) Sec 409: Criminal breach of trust by public servant or by banker, merchant or agent, etc. Imprisonment for life or imprisonment of either description for ten years, and fine;
- (o) Sec 477A: Falsification of accounts. Imprisonment of either description for seven years, or fine, or both;
- (p) Sec 109: Abetment of any offence if the act abetted is committed in consequence, and where no express provision is made for its punishment The same punishment as for the offence abetted;
- (q) Sec 120B: Criminal conspiracy to commit an offence punishable with death, transportation or rigorous imprisonment for a term of two years or upwards. The same punishment as that provided for the abetment of the offence, which is the object of the conspiracy.
- (r) Sec 511: Attempting to commit an offence punishable with transportation or imprisonment, and in such attempt doing any act towards the commission of the offence. Transportation or imprisonment not exceeding half of the longest term, and of any description provided for the offence, or fine, or both.

D. Offences under the Money Laundering Prevention Ordinance, 2008

1. Section 4: The Offence of Money Laundering and Punishment

- (1) For the purpose of this Ordinance, money laundering shall be deemed to be an offence.
- (2) Any person who commits or attempts to commit the offence of money laundering or abets or conspires in the commission of such offence shall be punished with imprisonment for a term which may extend to seven years but not less than six months and the money or property derived from the commission of such offence shall also be forfeited to the state.

2. Section 5: Punishment for Violation of Freezing or Attachment Order

Any person who contravenes an order of attachment or freezing and account made under this Ordinance shall be punished with imprisonment for a term which may extend to one year, or with fine which may extend to five thousand taka, or with both.

3. Section 6: Punishment for Divulging of Information

- (1) No person shall, for the purpose of frustrating the investigation or making adverse influence over the investigation, divulge any information relating to investigation or other related information to any person, organization or news media.
- (2) Every person, organization or agent authorized under this Ordinance during the period of his service or appointment or on the expiry of term of service or contract of appointment shall, except for the purpose of this Ordinance, abstain from using, publishing or divulging information collected, received, retrieved and known to him.
- (3) Any person who contravenes the provisions of sub-section (1) and (2), shall be punished with imprisonment for a term, which may extend to two years, or to fine which may extend to ten thousand taka, or with both.

4. Section 7: Punishment for Obstruction or Non-co-operation in Investigation, Failure to Report or Provide Information

- (1) Any person who-
 - (i) Obstructs or refuses to assist the concerned officer engaged in investigation under this

Ordinance; or

(ii) Without reasonable ground, refuses to furnish or provide report or information required under this Ordinance shall be deemed to have committed an offence under this Ordinance.

(2) Any person who contravenes the provisions of sub-section (1), shall be punished with imprisonment for a term which may extend to one year, or with fine which may extend to five thousand taka, or with both.

5. Section 8: Punishment for Providing False Information

(1) Nobody shall knowingly provide false information relating to the source of money or the identity of any account holder or the beneficiary or nominee of the account.

(2) Any person who contravenes the provision of sub-section (1), shall be punished with imprisonment for a term which may extend to one year, or with fine which may extend to 50,000 thousand taka, or with both.

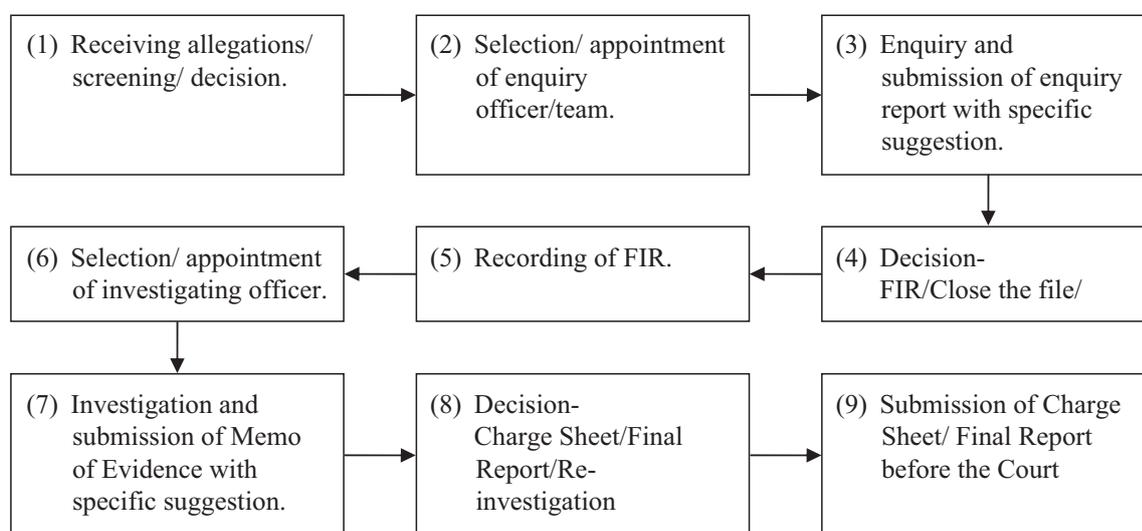
V. COMPETENT AUTHORITIES FOR INVESTIGATION, PROSECUTION AND ADJUDICATION

A. Relevant Investigating, Prosecuting and Adjudicating Authorities or Agencies of Corruption Offences and Corruption-Related Offences

The relevant laws on investigation, prosecution and adjudication of corruption cases are the Criminal Procedure Code (CrPC) 1898, the Anti-Corruption Commission Act, 2004 and the Anti-Corruption Law, 2007. The former is the general procedural law for investigation and trial of criminal cases. The latter is the special law against corruption. As far as investigations of corruption cases are concerned, if any conflict between the provisions of the aforesaid Acts is found, the provision of the latter Act will prevail. The CrPC describes under Sections 154 to 173 how offences are registered with police stations: investigations are made and the reports of investigations are submitted before the court for trial. The Anti-Corruption Commission Act dictates an investigator to conduct an enquiry before lodging/registering a First Information Report (FIR) stating the offence(s) committed. If *prima facie* evidence is established in an enquiry, an FIR is lodged with the police station and thereafter the formal investigation starts under the provisions of the CrPC. An investigation ends with submission of Investigation Report before the court. The provision of Section 20 sub-section (1) of the Anti-Corruption Commission Act, 2004 has made the commission the only investigating authority having jurisdiction all over Bangladesh to investigate the offences of corruption.

B. The Sequence of Investigation

The sequence of investigation is depicted below through a diagrammatic flow chart:

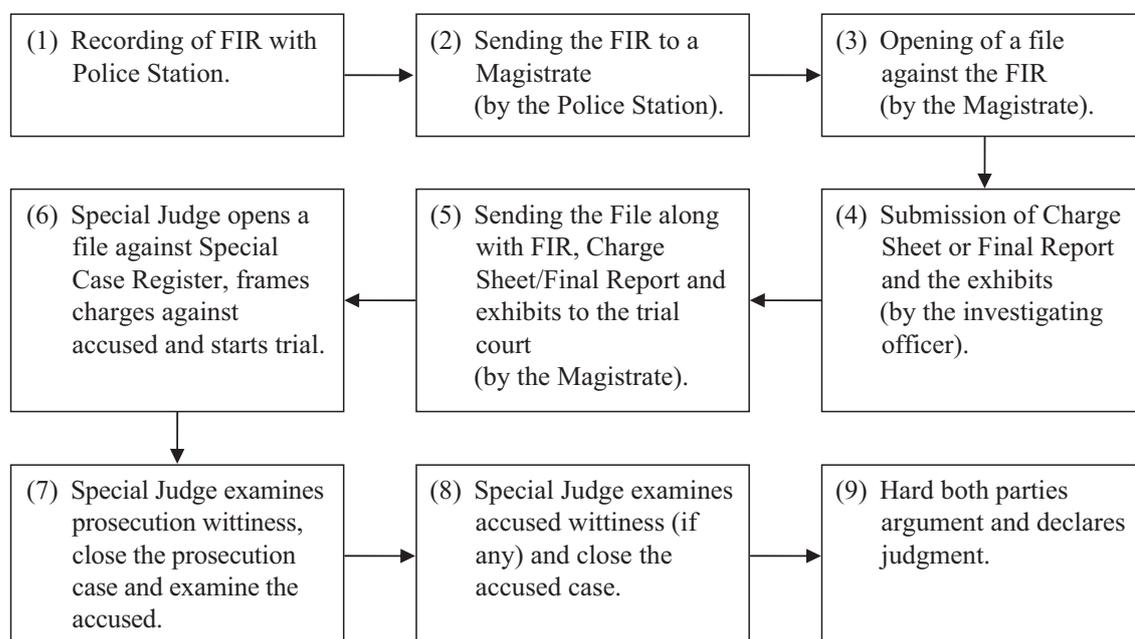


1. Any person may lodge a complaint in respect of an offence mentioned in the schedule of the Act to the commission or a police station. After receiving the complaint the screening committee will make the report and send it to the commission.
2. Then the commission will give a decision as to an enquiry and appoint an enquiry officer or a team.
3. The enquiry officer or team shall complete the enquiry within the time limit as per the Act and Rule and submit a report with specific suggestions to the commission.
4. After receiving the enquiry report the commission gives a decision to lodge the FIR or close the file.
5. According to the commission's decision the enquiry officer lodges the FIR to the respective police station.
6. The commission appoints an investigation officer.
7. After completing the investigation the officer shall submit a Memo of Evidence and draft a charge sheet or final report with specific suggestions to the commission.
8. The commission will go through the report and take a decision to accept the charge sheet or the final report or order re-investigation.
9. According to the commission's decision, the investigating officer submits a charge sheet or final report before the court.

C. Special Judges/Courts to Try Corruption Cases

Under the provision of the Criminal Law Amendment Act, 1958 and the Anti-Corruption Commission Act, 2004, corruption cases are triable by Special Judges only. A Session Judge, an Additional Session Judge and an Assistant Session Judge can be appointed as Special Judges. The Session Judges, the Additional Session Judges and the Assistant Session Judge of all districts and metropolitan areas have the authority to try corruption cases within their territorial jurisdictions, in addition to their original jurisdictions as Judges of Civil Courts and Criminal Courts. Besides, there are 21 Special Courts established exclusively for trial of corruption cases at District level and ten special courts established at Dhaka.

D. The Sequence of Prosecution and Trial



1. FIR lodged by the enquiry officer to the respective police station.
2. The police officer sends the FIR to the respective magistrate court.
3. The magistrate opens a file against the FIR.
4. The investigation officer after completing the investigation submits a charge sheet or final report with the exhibits and sanction order of the commission to the court.
5. The magistrate sends the file along with FIR and CS/FR etc. to the trial court.
6. A Special Judge (trial court) opens a file against the special case register and accepts CS.
7. If the case is ready for trial after hearing both parties it frames charges against the accused.

8. The court examines the prosecution's witnesses, closes the prosecution's case and examines the accused.
9. The court examines the accused's witnesses (if any) and closes the accused's case.
10. Having heard both parties' arguments, the judge renders a decision.

VI. PROBLEMS AND CHALLENGES IN STRENGTHENING THE CAPACITY AND ABILITY OF CRIMINAL JUSTICE AUTHORITIES AND THEIR PERSONNEL

On 11 February 2007 the Judiciary was separated from the Executive and the Code of Criminal Procedure, 1898 (Act V of 1898) was amended. The Bangladesh Judicial Service Commission Rule, 2007 and the Judicial Service (formation, appointment and suspension, dismissal and removal) Rule and (Pay Commission) Rule, 2007 were passed by the government. The Judicial Service Commission is the appointing authority of judges. They will be directly recruited by the Commission and their service will be ruled by the Commission with the consultation of Supreme Court. Now the criminal justice authorities and their personnel are independent.

A. Problems and Challenges

- (a) Lack of proper training facilities for the investigators in different investigating agencies.
- (b) Lack of adequate logistics support for investigating agencies.
- (c) Inadequate promotional opportunities for the investigating officers.
- (d) Overburdened investigating duty.
- (e) Time limit for the investigation period.
- (f) Lack of proper training for judges, magistrates and prosecutors.
- (g) Inadequate co-ordination between witnesses and prosecutors.
- (h) Taking longer to complete trials.

VII. CONCLUSION

It is expected that with the sincere co-operation of the people of Bangladesh, the recently adopted pragmatic policies and measures taken by the present government will be successfully implemented. This requires absolute separation of the judicial system from other organs of the government. Only raising a sense of moral values and integrity can lead to success and that requires both intensive and extensive mass awareness programmes. In this context, adoption of UNCAC would be a greater guideline for developing anti-corruption policies and mechanisms, public sector integrity, prevention of money laundering, controlling crimes, developing law enforcing measures and effective management of public finances. The recent changing in Bangladesh's position in the corruption scale is a good sign and a source of hope for our economy and we are to be more careful and vigilant so as to prevent the tendencies for corruption instead of waiting to resolve post corruption activities.

The government has taken initiatives to reform the legal and institutional structures to strengthen some of the key institutions of democracy and the national integrity system. The institutions that have already undergone substantive reforms include independence of the judiciary, reconstitution of the Election Commission, and establishment of the Anti-Corruption Commission and the Public Service Commission, which followed the Government's prompt decision to accede to the UN Convention against Corruption on 27 February 2007, within six weeks of taking power. A series of high profile initiatives have been taken by the caretaker government to criminalize corruption by prosecuting the allegedly corrupt individuals, irrespective of their political and other status in society. While the fate of the cases will depend on the courts, the on-going anti-corruption drive could be the strongest ever signal in Bangladesh's history that corruption is a punishable offence.

Critical to any effective anti-corruption strategy is systemic transformation. But the ultimate source of strength in the anti-corruption movement is the people: their awareness, voice raising and participation in the form of a social movement with the active support of all stakeholders, including the media. The main challenge is to create an environment in which corruption is hated and rejected by every one and pressures will come from all levels to generate the will and commitment of the leadership to strengthen the effectiveness of the key institutions.

EFFECTIVE LEGAL AND PRACTICAL MEASURES IN COMBATING CORRUPTION

*Tshering Namgyel**

I. INTRODUCTION

Corruption is a disease that is common in every country. However it varies from country to country depending upon the system of government, level of economic development, policy of the government and culture of the society. Although corruption is not seen in on an unmanageable scale it is prevalent Bhutan in all forms and at various levels, be it in government or the corporate and private sectors. Transparency International has placed Bhutan at number 46 amongst 180 countries in the Corruption Perception Index (CPI).¹

With the transition of the government to constitutional parliamentary democracy, His Majesty the Fourth King felt it very important to prevent and eliminate corruption from the very beginning of his reign and decreed the establishment of an Anti-corruption Commission (ACC) on 31 December, 2006. Accordingly on 4 January, 2007 the ACC office was set up specifically as an agency to clean up corruption in Bhutan. Since its inception, the ACC has been actively involved in tracing corruption and bringing perpetrators to task, besides carrying out preventive and educational programmes. It has mainly devoted itself to developing baseline information on corruption; investigating cases; simplifying public delivery systems and asset declaration; education and advocacy on corruption; and studying the forms, causes and consequences of corruption.²

II. POLICIES AND INITIATIVES OF THE ROYAL GOVERNMENT

His Majesty the Fourth King's development philosophy of Gross National Happiness (GNH) has been enshrined in the constitution as the goal and pursuit of the government.³ In order to pursue this noble goal, anti-corruption measures are adopted through the policies of good governance by encouraging efficiency, accountability and transparency. The fight against corruption has been featured as a national agenda in the 2005 Good Governance Plus (GG+) Report and through this report all agencies are required to take anti-corruption initiatives.

On 12 June the Prime Minister, in his address to the gathering on the Launching of the Asia Pacific Human Development Report 2008, "Tackling Corruption, Transforming Lives", assured the commitment of his government to the policy of good governance. In doing so he also stressed the participation of the people in making the government more accountable, responsible and transparent. In a later address to the nation he also assured his support for the fight against corruption and said that the government is adopting a policy of zero tolerance to corruption.

* Judge, Royal Court of Justice, District Court, Thimphu, Bhutan.

¹ Bhutan Times, Volume II, No 112 (24 September 2008).

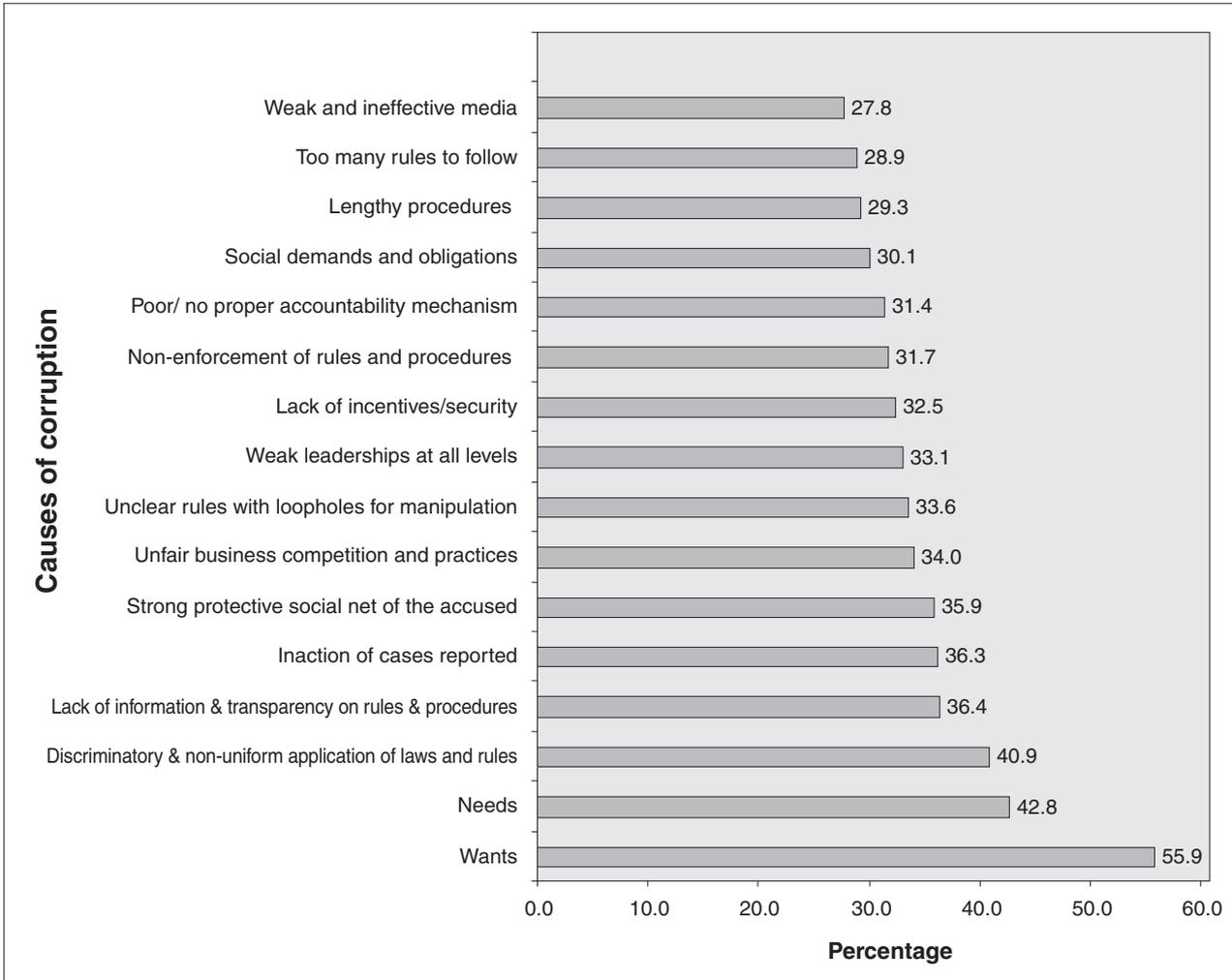
² ACC Website.

³ Article 9, section 2 of the Constitution of the Kingdom of Bhutan.

III. CAUSES OF CORRUPTION

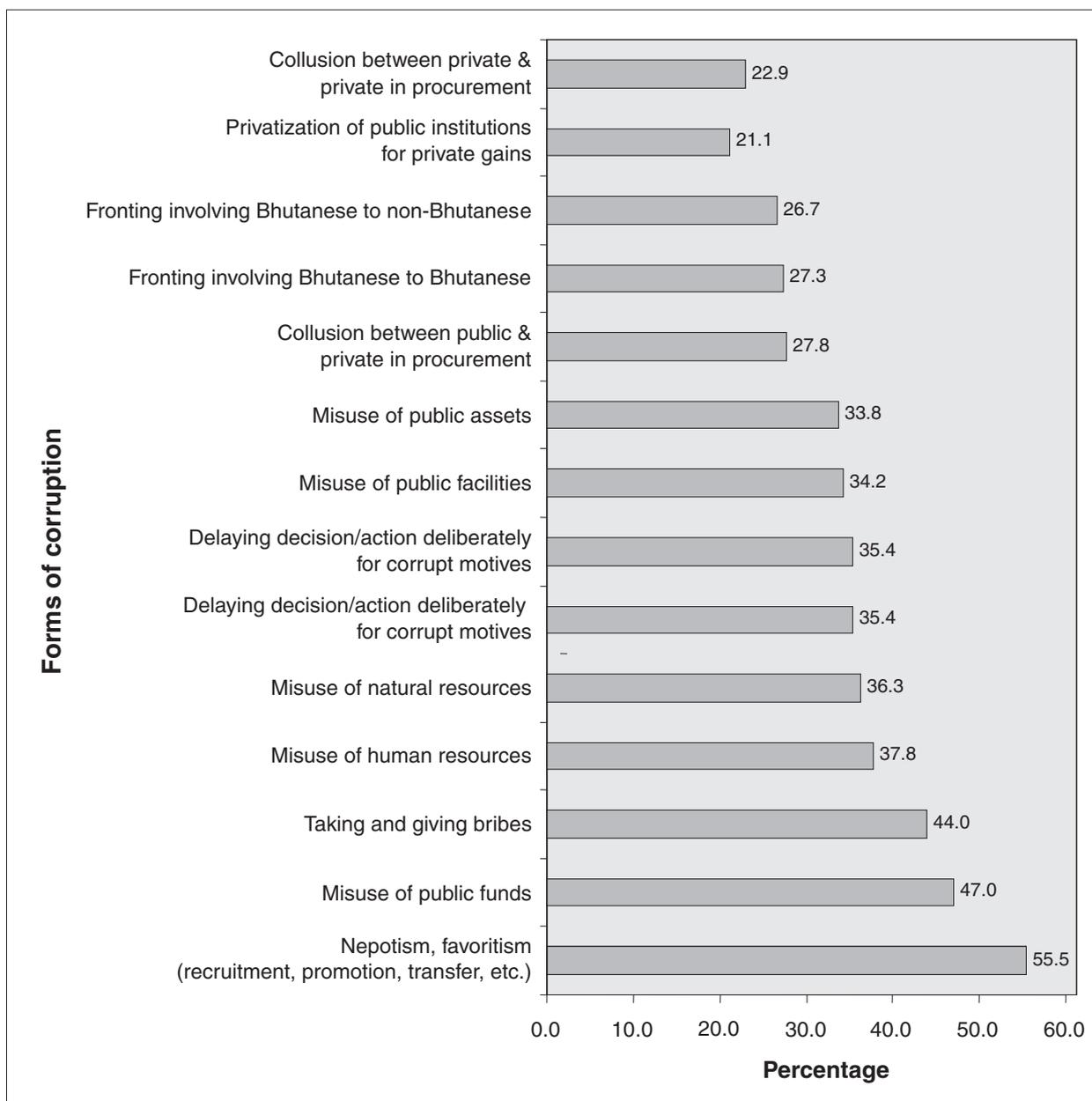
The ACC conducted a Corruption Perception Survey (CPS) in 2006 and found that the respondents viewed human wants (55.9%), needs (42.8%), and discriminatory and non-uniform application of laws and rules (40.9%), as the major causes of corruption, as shown in Figure 1.

Figure 1



IV. FORMS OF CORRUPTION

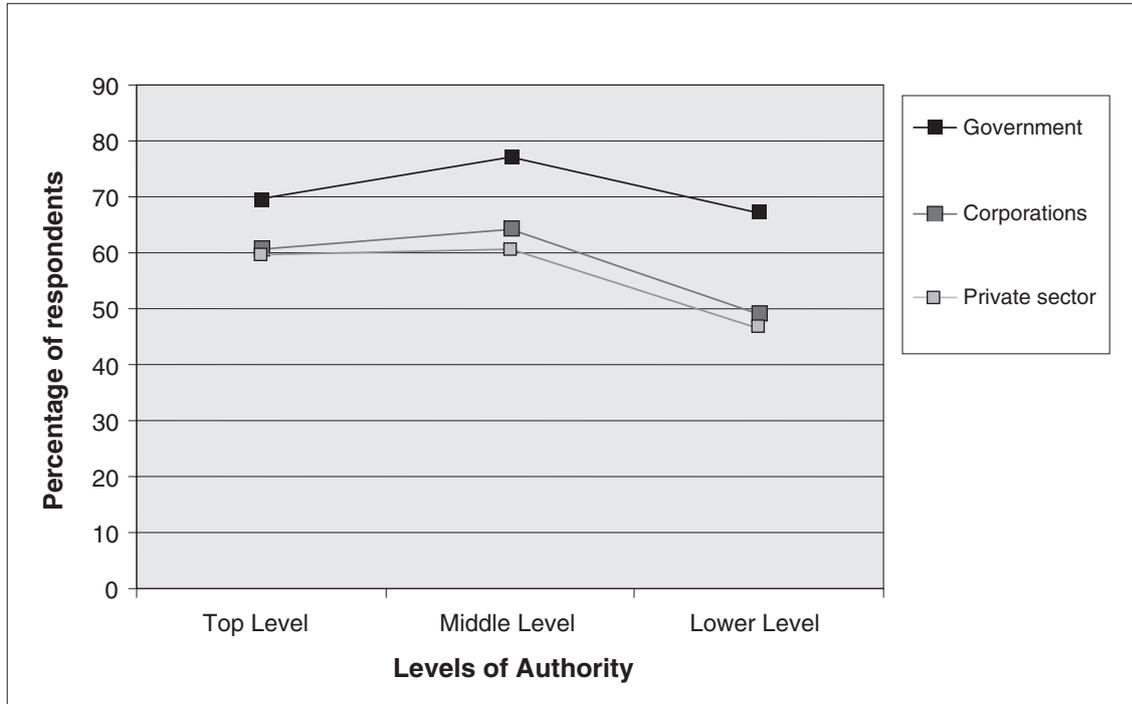
As per the CPS 2006, nepotism and favouritism are the most prevalent forms of corruption followed by misuse of public funds and bribery.



V. EXTENT OF CORRUPTION

The CPS 2006 survey also found that corruption is pervasive across all levels and sectors but is more prevalent at middle level.

Figure 3: Prevalence of corruption by level of authority



VI. COUNTER-CORRUPTION MEASURES

A. Enforcement Agencies

1. Anti-corruption Commission (ACC)

The ACC has been established as an independent body, headed by a chairperson and two commissioners to prevent and combat corruption in the country.⁴ The ACC also ensures that the reports of the Royal Audit Authority are meted out with appropriate actions by the concerned agency. Any individual can file a report with the ACC and, based on merits, the ACC takes up the case.

2. Royal Audit Authority (RAA)

The Royal Audit Authority was established in 1977 to audit the accounting systems in the country. Initially, the RAA also shouldered the responsibility of prosecuting those charged with corruption with the assistance of the Royal Bhutan Police. Today the action against the findings of the RAA is to be initiated by the line ministry and the ACC takes the case if no action has been taken against the offender.

3. Department of Revenue and Customs (DRC)

The DRC is a department under the ministry of finance primarily entrusted with the activity of collecting revenue for the government. Thus, the department also reviews whether the collection of revenue by the government agencies are properly accounted or not. Irregularities by the agencies or individuals officials are also reported to the concerned agency management.

4. Attorney General Office (AGO)

The OAG was initially established as Office of Legal Affairs in April 2000. With the passing of the Attorney General’s Act 2006, the office then became the Office of the Attorney General as per section

⁴ The Constitution of the Kingdom of Bhutan, Article 26, section 1.

3, Office of the Attorney General Act, 2006. The OAG is entrusted with the job of prosecuting and representing the government, drafting and reviewing bills, providing legal advice and other services of a legal nature as assigned by the government. Thus the OAG is entrusted with the important function of prosecuting offences in all types of corruption.

5. Royal Bhutan Police (RBP)

The RBP was established on 1 September 1965 as an independent body to maintain law and order. Its responsibility is to prevent the commission of crime and to detect crime already committed. Since it has to perform the function of prosecuting criminals in court, corruption cases are jointly prosecuted in collaboration with the concerned ministry or the OAG. The RBP also assists the ACC as and when required by the ACC.

6. Judiciary

The judiciary of Bhutan commenced functioning as separate organ from 1968 with the institution of the High Court headed by the Chief Justice of Bhutan. Presently the judiciary consists of the High Court, District Courts and Dungkhag Courts presided over by the Chief Justice, Dzongkhag Drangpons and Dungkhag Drangpons, respectively.

The Bhutanese legal system is based on Buddhist natural laws. Although the procedural system is principally adversarial, it also has certain elements of the inquisitorial system. This principle of the adversarial system is enshrined in the *Bardo thoedrel*⁵ which is also propagated to the people in the form of dance during annual festivals throughout the country.

B. Strategies Adopted by ACC

The ACC has created three divisions in order to prevent corruption. It has the Prevention Division, Public Education and Advocacy Division and Investigation Division.

The prevention division has three sections, consisting of the System Review Section, the Research Section and the Asset Declaration Section. The System Review section concentrates on organizational systemic studies aiming at both the short term as well as long term objectives. Preventive studies are based on the following sources:

- Systemic flaws discovered as a result of investigation;
- Proactive studies undertaken in corruption prone sectors;
- Findings by the Royal Audit Authority;
- Regular meetings with the senior management of government departments and public bodies and;
- Requests made by government departments or private agencies.

The Research Section undertakes research initiatives in relevant fields from local as well as global perspectives with long-term objectives such as policy changes. Research can provide useful information in formulating preventive strategies, adopting best practices, strengthening public education and supporting proactive investigation.

The Asset Declaration system provides an avenue to check the accumulation of wealth that is disproportionate to the legal source of income. This can promote trust and confidence of the general citizens in public officials occupying influential positions.

Further, the Public Education & Advocacy Division has been created to ensure the general public's awareness of corruption and its impact and influence, and to foster an attitude, behaviour and culture of intolerance towards corruption and to uphold social values and the ethics of honesty and integrity.

The Investigation Division of the Commission is mandated to investigate corrupt activities of the government, corporate and private sectors through both reactive and proactive approaches.

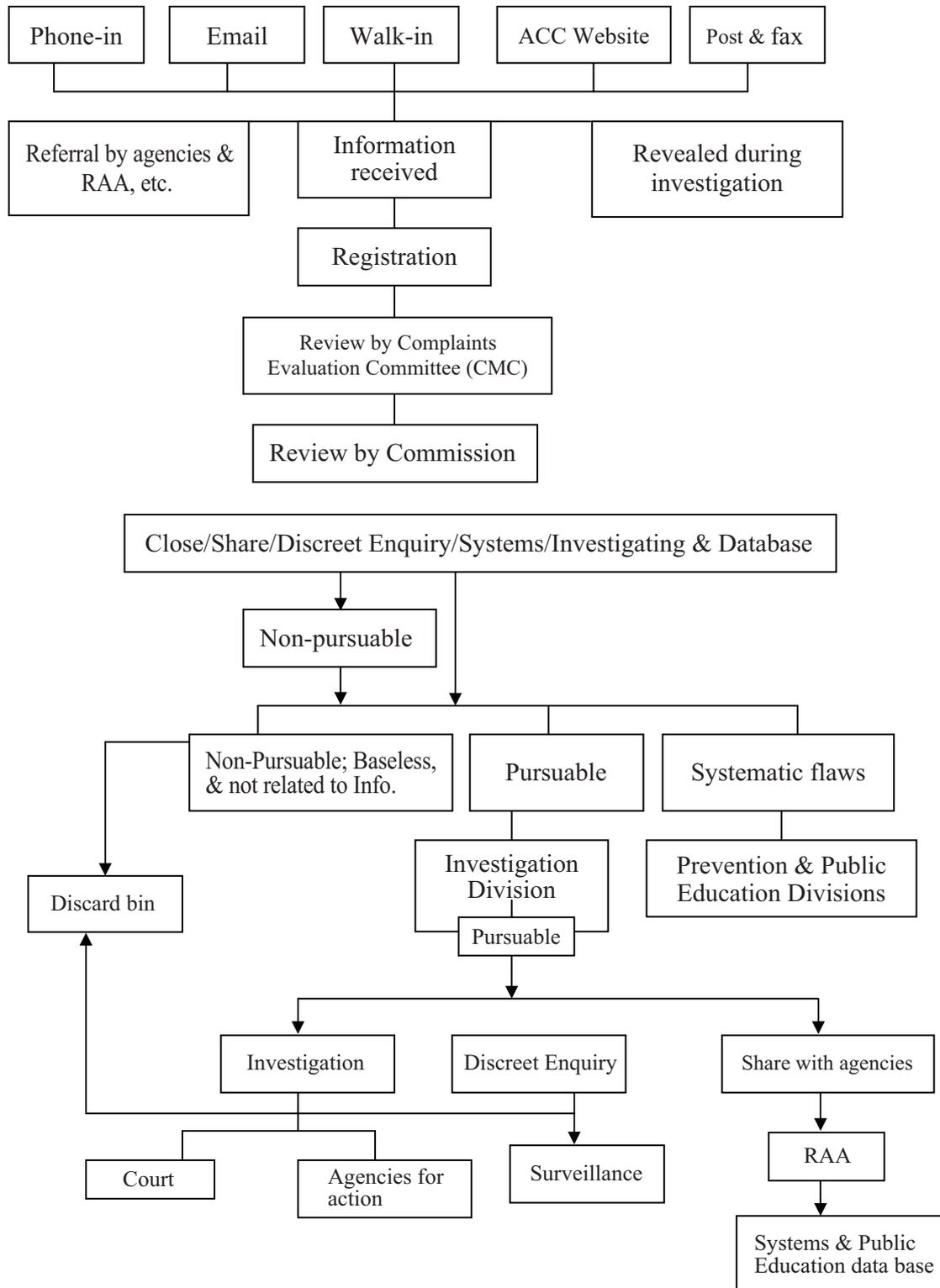
C. Filing of Complaint and Prosecution

As per section 59 of the Anti-Corruption Act of Bhutan 2006, any person can lodge a complaint with the

⁵ Book of the dead-Garud Puran.

ACC against a public servant, public entity or other person who committed or is attempting to commit an offence of corruption. Complaints, irrespective of the content, are registered by an officer and go through a rigorous process of review by the Complaints Management Committee (CMC). After the investigation, cases that warrant conviction are forwarded to the OAG for prosecution in the court of law.

The complaint management system of the ACC is as shown below:



VII. OFFENCES RELATED TO CORRUPTION

The Penal Code of Bhutan 2004 (Penal Code) has been enacted to repeal certain provisions of the *Thrimshung Chhenmo* (Supreme Law) of 1959 that are not accepted in the present day and also to cover up various offences not incorporated in the *Thrimshung Chhenmo*. Some of the provisions incorporated in the Penal Code to deal with corruption are:

- Laundering of the proceeds of crime and smuggling (Sections 277, 279 & 280);
- Embezzlement (Section 287);
- Bribery of a public official and commercial bribery (Section 289 & 292);
- Official misconduct (Section 294);
- Forgery of and tampering with public records and documents (Sections 296, 298 & 300);
- Deceptive practice (Section 309);
- Obstruction of lawful authority and public service (Section 422 & 424).

Common among the above offences charge sheeted to the court are embezzlement, forgery, official misconduct, tampering with public records and deceptive practices including fronting. The Penal Code also provides for restitution, confiscation and recovery of criminal proceeds under sections 46, 47 and 48. This could be done as provided under the criminal procedure code for freezing of accounts, seizure, etc.

VIII. CHALLENGES TO COUNTER-CORRUPTION ACTIVITIES

Bhutan has just stepped into a constitutional democratic system and its economy is still in a developing stage. Since the means has to justify the ends, it is the task of the government, corporate and private entities to provide the working class with adequate means. Further, because of globalization and growing consumerism, the dealing agencies have to manage corruption involving members of international communities.

Although civil servants are trained with modern management and administrative methods, the general tendency of complacency still persists. Besides, there is need for inculcating a business oriented culture (productivity) in government service which will remain for some time.

Bhutan is a small country with a small population where everyone is known to one another and being so, the tendency of 'Small Society Syndrome' makes the objective of bringing the corrupt to task more arduous. And one thing that hinders the assessment of bribery is the culture or the tradition of offering *Chhanjay*⁶ and receiving *Soelra*.⁷ It is difficult to draw a line between gift-giving and bribery and often the offence of bribery is overshadowed by the culture of gift-giving.

There is also a dearth of professionally trained personnel and amenities so as to effectively carry out research and investigation. The lack of adequate allowances and incentives is another factor that hinders the personnel of the agencies from effectively probing corruption.

IX. CONCLUSION

The government of Bhutan has adopted a zero tolerance policy to corruption so as to build up a strong foundation for a vibrant democracy. Since the inception of the ACC, corruption cases have multiplied to three times the former level. It has cracked down on not only on the government service employees but also on corporate employees as well as on private business industry. Although the judiciary of Bhutan is also committed to supporting the prosecution of corruption cases, not all cases of corruption could be brought to justice due to lack of evidence beyond reasonable doubt and having to play the role of an umpire as mandated by the constitution. However, smallness is also seen as an advantage considering the efforts of educating the masses and keeping watch on the functioning of the handful of government agencies, and corporate and private sector actors.

Bhutan signed the United Nations Commission against Corruption (UNCAC) in 2005 but has not yet ratified it.

⁶ *Chhanjay* is a tradition or the act of bringing gift to officials.

⁷ *Soelra* is culture or the act of giving gift by an official to a person subordinate to him or her.

THE CRIMINAL JUSTICE RESPONSE TO CORRUPTION (IN THE CONTEXT OF NEPAL)

*Rajan Prasad Bhattarai**

I. HISTORICAL BACKGROUND

After the unification of Nepal, the great King Prithvinarayan Shah declared that the bribe takers and bribe givers were the greatest enemies of the nation and deserved the death penalty. This proves that corruption prevailed in the 18th century and corruption was considered to be a serious crime. Many rulers after that took various measures to control corruption. After the political change in 1951, The Prevention of Corruption Act, 1960 was implemented to maintain good governance. Similarly, the State Cases Act, 1960 and the Evidence Act, 1974 were implemented, adopting the principles of criminal justice. These two Acts are considered milestones in the field of criminal justice. These legal provisions were further strengthened by establishing the Commission for the Prevention of Abuse of Authority as a Constitutional body in 1975. Investigation, accusation and adjudication of corruption cases were the responsibilities of the Commission for the Prevention of Abuse of Authority. After the people's movement in 1990, the constitution of the Kingdom of Nepal, 1990 provided for the establishment of a Commission for the Investigation of Abuse of Authority (CIAA). However, the CIAA was vested only with the power of investigation and accusation.

II. THE EXISTING CORRUPTION CONTROL SYSTEM IN NEPAL

The Interim Constitution of Nepal, 2007 was promulgated after the second people's movement in 2006. The Constitution provides for the Commission for the Investigation of Abuse of Authority. The president of Nepal, with the recommendation of the Constitutional Council, appoints the Chief Commissioner and other Commissioners. The term of the office of the Chief Commissioner and other Commissioners is six years from the date of appointment. They can do their work freely and fairly since they shall only be removed by an impeachment resolution passed by the parliament.¹

A. Functions, Duties and Powers of the CIAA²

The following are the functions, duties and powers of the CIAA as mentioned in the Interim Constitution of Nepal, 2007.

- To conduct inquiries and investigations of improper conduct or corruption by a person holding any public office (subject to the exception of certain public officials);
- To write to the concerned authority for warning or departmental action or other actions, if it finds that any person holding public office has misused his or her authority by improper conduct;
- To prosecute the person holding public office and other involved in the crime, if it finds that the person holding public office has committed an act defined by the law as corruption;
- To submit an annual report to the president and president will submit the report to the parliament;
- To investigate and inquire into cases of any official of a constitutional body removed from their office following an Impeachment Resolution on the ground of misbehaviour; any Judge removed by the Judicial Council on similar charges, or any person proceeded against under the Army Act after they are removed from office.

The above mentioned Constitutional provisions show that CIAA can only investigate and file the cases

* Deputy Attorney, Commission for the Investigation of Abuse of Authority, Kathmandu, Nepal.

¹ Article 119 of the Interim Constitution of Nepal, 2007.

² Article 120 of the Interim Constitution of Nepal, 2007.

against corrupt officials in 'public institutions'. The CIAA Act defines 'public institutions' as follows:³

- A company, bank or committee wholly or partly owned or controlled by the Government of Nepal;
- Universities, campuses, schools, research centres and any other academic or educational institutions run by the Government of Nepal;
- Local bodies;
- Institutions run with loans, grants or guarantees of the Government of Nepal;
- Institutions with full or partial ownership of the institutions run by the government;
- Any other institution designated as a public institution in the Nepal Gazette.

Similarly, "Improper Conduct" denotes any of the following acts committed deliberately or through negligence by the person holding a public post as defined in the Commission for the Investigation of Abuse of Authority (CIAA) Act, 1991:⁴

- Refusal to undertake any work under one's authority or undertaking any work outside one's authority;
- Not following mandatory procedure while making any decision or giving instruction;
- Use of authority vested in oneself for purposes contrary to the relevant law, decision or instruction;
- Use of discretionary power with a *mala fide* intention or selfish desire;
- Unauthorized obstruction of the work of other office, officer or employee or getting any unauthorized work done from such office, officer or employee under pressure;
- Shifting one's responsibility by sending the work to be done by oneself to another officer;
- Not fulfilling the responsibility demanded by the nature of one's position;
- Getting work done to one's own benefit under improper influence or enticement to the employee under one's influence or control; or
- Abuse of immunity, facility or concessions associated with the post.

Likewise, "Corruption" implies the guilt punishable under the prevalent law pertaining to the prevention of corruption.

The Corruption Prevention Act, 2002 has defined corruption as:⁵

- Taking or giving a bribe or agreeing to take a bribe;
- Procuring goods or services free of cost or at lower cost;
- Accepting contributions, charity, gifts and subscriptions;
- Taking commissions;
- Public servants leaking revenue;
- Working with the *mala fide* intention to incur illegal benefit or loss;
- Public servants preparing wrong documents;
- Wrong translation;
- Tampering with Government documents;
- Destroying Government or public agencies' documents;
- Breach of confidentiality of the question paper or changing the results of an examination;
- Public servants indulging in illegal commerce and business;
- Claiming positions not versed upon;
- Giving false descriptions;
- Damage to public property;
- Exerting illegal pressure;
- Giving wrong reports;
- Illegal acquisition of property;
- Committing attempts;
- Accomplice.

False certificate related cases are the most common among the above mentioned crimes filed by CIAA in the Special Court. For appointment and promotion, the public servants need higher level academic

³ Section 2 of the CIAA Act, 2002.

⁴ Section 3 of the CIAA Act, 2002.

⁵ Chapter 2 of the Prevention of Corruption Act, 2002.

certificates. Some of them submit fake certificates from Indian schools and universities.

Fake certificates for appointment and promotion create two types of problem in public administration. On the one hand, work can't be done effectively by fake certificate holders who are not qualified for the post. On the other hand, the capable candidates do not get the chance for employment and promotion. This will affect the overall development of the country.

The CIAA files the cases in the Special Court if it finds the certificates fake. According to the Preventing of Corruption Act, 2002, the fake certificates holders are sentenced to six months to one year's imprisonment and also fined depending on the degree of the offence committed. CIAA has won about 95% of cases against fake certificates holders. They are removed from their jobs after the decision according to the law.

The following are the statistics related to fake certificates cases filed in the Special Court by the CIAA in the last three years.⁶

Fiscal Year	Total registered cases	Cases related to fake certificates	Percentage
2007-2008	70	54	77.14
2006-2007	115	93	80.86
2005-2006	114	69	60.52

B. Investigation Methods of the CIAA

The CIAA uses diverse methods of investigation for improper conduct or corruption committed by a person holding any public post. It receives written complaints from various sources and starts the investigation.

1. Sources of Complaint for the CIAA

- News published in news papers;
- Official publications and reports;
- Telephone, e-mail, fax, online complaints and other information through media;
- News and information published in electronic media;
- Information collected from other sources.

The complaints collected through the above mentioned sources are handed to the two Commissioners with the opinion of the Chief of the Investigation Department. Then these complaints are investigated in two stages, preliminary and detailed investigation.

During the preliminary inquiry, complaints are analysed on the basis of their merit and available evidence. At this stage the division concerned collects records and evidence. If it appears to be a *prima facie* case, the CIAA appoints an investigation officer for detailed investigation. The investigation officer makes all necessary inquiries, records, statements of the accused, analyses the findings and submits a report to the meeting of the CIAA. Such report is reviewed by the meeting and decisions are made either to frame the case or admonition or departmental action recovery of the loss or any other action on the basis of gravity of the crime committed. In cases where the investigation leads to insufficient evidence, the case is disposed of by the CIAA. The CIAA usually makes decisions through consensus.

In the beginning, corruption-related cases used to be filed in the general courts. The government of Nepal established a Special Court in 2002 for effective and fair trial of corruption related cases. The government of Nepal, on the recommendation of the Judicial Council, appoints one chairman and two member judges from the Appellate Court. The Special Court initiates proceedings and finalizes the corruption cases. However, appeals can be filed in the Supreme Court.

⁶ 18th Annual Report of the CIAA, 2007-2008.

Here are the comparative statistics of the disposed complaints by CIAA for the last three years:⁷

Fiscal Year	Registered Complaints	Complaints decided	Complaints remaining	Decided percentage
2007-2008	2732	2135	547	78.14%
2006-2007	3564	2976	588	83.50%
2005-2006	4324	3353	971	77.54%

The comparative statistics of the cases registered in the Special Court and cases decided for the last three years.⁸

Fiscal Year	Cases registered	Cases decided	Cases won	Cases lost	Won percentage
2007-2008	70	127	95	32	74.80%
2006-2007	115	171	140	31	81.87%
2005-2006	114	109	89	20	82.00%

In addition to above mentioned works, CIAA can also perform as an Ombudsman mentioned in the Interim Constitution of Nepal, 2007 and CIAA Act, 1991. The CIAA can also give suggestions to the Government of Nepal for good governance.

III. EXISTING CRIMINAL JUSTICE SYSTEM IN NEPAL

With the promulgation of the Interim Constitution of Nepal, 2007, the concept of an independent and competent system of justice, the concept of the rule of law, and human rights and universal principles of the justice system have been introduced.

In order to uphold and implement the concept of an efficient and impartial criminal justice system, a new State Cases Act, 1992 further elaborated the procedures of investigation and prosecution. According to the Interim Constitution of Nepal, 2007 and the State Cases Act, 1992, the institutions involved in the criminal justice system are as follows:

A. Police

Under the Home Ministry, a police organization has been established, which is regulated by the Police Act, 1956. The Police Headquarters is the top organ of the police organization. Under the Police Headquarters 75 District, one Police Office has been set up in every district. This is the grassroots law enforcement unit entrusted with the responsibility to investigate crime within its territorial jurisdiction. District Police Officers are directly involved in the investigation of the crimes under the territorial jurisdiction.

B. Public Prosecutors

The Attorney General of Nepal is constitutionally responsible for prosecuting in criminal cases. The Attorney General has the power to delegate the responsibility for prosecution of criminal cases to his or her subordinates. There are 75 district level offices and 16 Appellate offices under the office of the Attorney General of Nepal.

C. Courts

The District Court is the court of first instance. It has the power to entertain all the criminal cases except otherwise provided by any law. There are 75 District Courts in Nepal. All cases in the District Courts are tried by a single Judge Bench. The Supreme Court of Nepal is the apex court. Constitutionally it is a Court of Record. The Constitution of Nepal has conferred on the Supreme Court vast and extraordinary

⁷ 18th Annual Report of the CIAA, 2007-2008.

⁸ 18th Annual Report of the CIAA, 2007-2008.

jurisdiction in order to reinforce the fundamental rights of citizens. The Supreme Court has the power to declare any legislation void for being inconsistent with any provision of the Constitution. Immediately below the Supreme Court there are 16 Appellate courts. District Courts within the territorial limitation are subject to review by the Appellate Courts on appeal.

In this way, the institutions involved in criminal justice system are the police, public prosecutors and courts. The police have the responsibility of investigation, public prosecutors have the power of prosecution and the courts give verdicts in criminal cases. However, for corruption related cases investigation and accusation are the remit of the CIAA and adjudication is the remit of the Special Court as per the Special Court Act, 2002.

IV. PROBLEMS IN CORRUPTION CONTROL

In Nepal, corruption has been considered a serious crime for a long period of time and various measures have been taken to control it. The Commission for the Investigation of Abuse of Authority has been established as the supreme institution to control corruption and it has been working continuously throughout the nation. However, the country is not able to control corruption. The number of complaints and court cases against corruption shows that corruption is deeply rooted in Nepal. The following are the major hindrances to controlling it:

- (i) Corruption in the private sector is beyond the jurisdiction of the CIAA;
- (ii) Lack of skilled personnel;
- (iii) Lack of modern equipment;
- (iv) No regional offices of its own;
- (v) Low pay scale;
- (vi) Lack of public awareness;
- (vii) United Nations Conventions against Corruption not ratified.

V. CONCLUSION

Nepal has given special priority to controlling corruption. The CIAA has been adopting punitive, preventive and promotional activities to control corruption. Because of the political instability in the country the United Nations Convention against Corruption (UNCAC), which was signed by former Chief Commissioner on 10 December 2003, has not been ratified by the parliament yet. In the present context, Nepal has been declared a Federal Democratic Republic Country. A general election for the Constitutional Assembly has been conducted. The nation is in the process of writing a new constitution. In this context, on the one hand, voices have been raised from the CIAA and various organizations to ratify the UNCAC. On the other hand, the Government of Nepal has implemented the following Acts to work according to the provisions of the UNCAC for corruption control.

The Acts are as follows:

- (i) Prevention of Money Laundering Act, 2008
- (ii) Right to Information Act, 2007
- (iii) Public Procurement Act, 2007
- (iv) Good Governance Act, 2008
- (v) Electronic Transaction Act, 2006.

In addition to these, voices have been raised to include corruption in the private sector within the jurisdiction of CIAA.

In conclusion, it is hoped that if the United Nations Convention against Corruption is ratified by the parliament, international co-operation will be gained to control corruption. Similarly, if corruption in the private sector falls within the jurisdiction of CIAA in the new Constitution of Nepal, we will be able to control corruption.

THE CRIMINAL JUSTICE RESPONSE TO CORRUPTION

*Shreelal Poudel**

I. THE NEPALESE CRIMINAL JUSTICE SYSTEM

The Nepalese criminal justice system is more or less influenced by the common law system, and operates as follows:

- A. Investigation and prosecution;
- B. Court hearing and adjudication.

A. Investigation of Crime

The Nepal Police are responsible for investigation of all criminal cases. The police function under the general supervision and control of the Ministry of Home Affairs of the Government of Nepal.

The crime investigation begins with the filing of the First Information Report (FIR) to a police post by the victims or his or her near relatives. The police investigate crime subject to the District Government Attorney's instruction. On completion of investigation, the police prepare a case file and submit it to the District Government Attorney who decides to institute or not to institute a suit.

B. Prosecution

All criminal offences to which Government is a plaintiff are defended by Government Attorneys. Government Attorneys are under the Attorney General of Nepal, who is the principal legal adviser to government of Nepal.

The Attorney General and his Subordinates are responsible for representing the Government for the protection of the rights and interest of the state. Similarly, the Attorney General is the final authority to decide whether or not to prosecute a person in a criminal offence, and for providing legal opinions to the central government agencies.

Sixteen Appellate Government Advocate Offices and 75 District Government Advocate Offices function under the Attorney General and are responsible for defending and prosecuting criminal cases.

C. Court

Under the Interim Constitution of Nepal, 2007, there are three categories of court:

(i) Supreme Court

This is the supreme court of the land. This court has both ordinary and extra-ordinary jurisdiction. Powers include hearing appeals against judgments delivered by the Courts of Appeal. The extra-ordinary power of the court includes the power of issuing the writ petitions. It also has power of judicial administration over the whole country.

(ii) Appellate Court

The Court of Appeal is the second tier in the hierarchy of the courts in Nepal. Sixteen Courts of Appeal, in various locations, are established under the Supreme Court.

The Courts of Appeal are empowered to hear appeals from the district courts under their jurisdiction, issue writ petitions and try certain cases under their respective jurisdictions.

* Section Officer, Ministry of Law, Justice & Constituent Assembly Affairs, Government of Nepal, Kathmandu.

(iii) District Courts

The District Court is located in a district, administrative unit. The District Courts are the court of first instance. The courts are responsible for trying all the civil and criminal cases.

II. CORRUPTION CONTROL LAWS IN NEPAL

A. Understanding Corruption

Corruption is a complex and multi-faceted phenomenon with multiple causes and effects, as it takes on various forms and functions in different contexts. The phenomenon of corruption ranges from a single act of activity contradicted by law to a way of life of an individual or group. It is the misuse of public goods by public officials, for private gain. This private gain is achieved by ignoring prohibitions against certain acts. This is the abuse or misuse of public offices and professional rights and duties for personal gain.

Corruption not only undermines ethical values and justice, it damages democratic institutions, the national economy and the rule of law. Corruption facilitates other forms of serious crimes, in particular transnational organized crime, human trafficking and fiscal crime such as money laundering. Corruption is also the cause of poverty and underdevelopment and diverts funds intended for development. It makes it difficult for the government to provide basic services, eliminate inequality, provide justice, and to utilize the available resources, including foreign investment and aid.

B. Corruption in Nepal

For at least 15 years, and more in recent years, the problem of corruption has been at the centre of the political agenda in Nepal. It is recognized as one of the chief causes of Nepal's under development. It is very widespread, has different manifestations. This is really a great challenge to modern Nepal. Businesspersons, politicians, government officials, academics, and even consumers, are responsible for this.

C. Corruption Control Laws in Nepal

Nepal has long made efforts to control corruption. Legislation on the control of corruption started in 1957. Recent legislation was enacted in 2002.

The main laws relating to corruption control are as follows:

1. Prevention of Corruption Control Act, 2059 (2002)

This Act has defined corruption as the following activities and penalizes:

- Taking or giving a bribe or agreeing to take a bribe;
- Procuring goods or services free of cost or at lower cost;
- Accepting contributions, charity, gifts and subscription;
- Taking commissions;
- Public servants preparing wrong documents;
- Making wrong translations;
- Tampering with government documents;
- Destroying government or public agencies' documents;
- Breach of confidentiality of the question paper or changing the result of the examination;
- Public servants indulging in illegal trade and business;
- Claiming positions which one does not hold;
- Giving false descriptions;
- Damage to public property;
- Exerting illegal pressure;
- Giving wrong reports;
- Illegal acquisition of property;
- Accomplice/inciting corruption offences.

2. Commission for Investigation of Abuse of Authority Act, 2048 (1991)

Commission for Investigation of Abuse of Authority Act, 1991 defines the abuse of authority as improper conduct. Improper conduct denotes any of the following acts committed deliberately or through negligence by the person holding a public post:

- Refusal to undertake any work under one's authority or undertaking any work outside one's authority;
- Not following mandatory procedure while making any decision or giving any instruction;
- Use of authority vested in oneself for purposes contrary to the relevant law, decision or instruction;
- Use of discretionary power with a *mala fide* intention or selfish desire;
- Unauthorized obstruction of the work of other offices, officers, or employees or getting any unauthorized work done from such offices, officers or employees under pressure;
- Shifting one's responsibility by sending the work to be done by oneself to another officer;
- Not fulfilling the responsibility demanded by the nature of one's position;
- Getting work done to own benefit under improper influence or enticement to the employee under one's influence or control; or
- Abuse of immunity, facility or concession associated with the post.

3. Anti- Money Laundering Act, 2008

The Act aims to prevent conversion of proceeds of crime into legal money. It establishes a department to administer the Act.

4. Good Governance Act, 2008

This Act aims to have good governance in the country.

5. Public Procurement Act 2007

This Act aims to maintain competition and transparency in procurements by public bodies including government bodies, Government controlled and funded bodies.

III. CORRUPTION CONTROLLING BODIES

A. Commission for the Investigation of Abuse of Authority (CIAA)

The Commission for the Investigation of Abuse of Authority, publicly known as CIAA, is a constitutional body, which serves as the investigating and prosecuting authority in corruption cases and the watchdog authority against the abuse of authority. The Interim Constitution of Nepal, 2007 provides for it in explicit terms in part 11, Article 120. Various actions, including prosecuting the concerned public official in a court of law, may be taken by the CIAA.

Pursuant to the constitution, functions, duties and powers of the commission are as follows:

- Inquiry and investigation of improper acts or corruption by a person holding public office;
- Recommending departmental action or any other necessary action against the person who has abused authority by committing an improper act;
- Filing cases against persons alleged to have committed corruption.

The CIAA, the main investigating and prosecuting body in corruption cases, filed 70 cases to the Special Court in the last fiscal year and in 28 cases the commission recommended departmental action to the concerned body. The commission called for attention in 19 cases too.

B. National Vigilance Center

National Vigilance Center (NVC), established by the Nepal Government, is a body of the government intending to control corruption and bring about good governance in the country. It is established as per chapter 4 of the Corruption Control Act, 2002. It functions under the direct control and supervision of the Prime Minister.

The main objective of the Center is to play a preventive and vigilant role to ensure good governance by controlling work delays, administrative and financial irregularities, mis-collection of public revenue and other misdeeds that exist in the various steps of the government and public sector organizations.

C. Special Court

This court hears the corruption cases filed by CIAA. This is the court of first instance in respect of corruption. Judges are deputed from the ordinary Appellate Court. It can have more than two benches.

As of 2007, the Special Court tried 142 cases related to corruption. There are four categories of corruption, according to court data: 35 cases relate to illegal property; 30 relate to decision making (at policy level); 73 are of fake certificates; and four concern bribery.

IV. ANTI-CORRUPTION NATIONAL POLICY

To prevent corruption, the following measures need to be incorporated into the draft anti-corruption national policy and strategy:

- Co-ordinating preventive anti-corruption policies and best practices;
- Collaborating with each other in the prevention of corruption;
- Disseminating knowledge on prevention of corruption;
- Ensuring anti-corruption bodies are independent and free from undue influence;
- Ensuring transparency, accountability, integrity and rule of law in the public sector, conduct of public officials, public procurement and management of public finance, including objective and transparent systems for recruitment, promotion, retirement of civil servants; legislative and administrative measures to establish criteria for candidature and election to public office; transparency in funding of candidates for elected public office and funding of political parties; standards of conduct for public officials; transparency, completion and objective criteria in decision making in public procurement and public finances;
- Strengthening integrity and independence of the judiciary and prosecution services and preventing opportunities for corruption within these institutions;
- Preventing corruption in the private sector, including provision of proportionate and dissuasive civil, administrative or criminal penalties for failure to comply with such measures;
- Public reporting and participation of society by facilitating access of the general public to information on the organization, functioning and decision making of public administration and promoting the active participation of civil society, NGOs and community-based organizations in the fight against corruption.

V. ROLE OF NON-GOVERNMENT ORGANIZATIONS IN THE PREVENTION OF CORRUPTION

NGOs have a significant role in preventing corruption by raising public awareness against corruption. There are number of NGOs in Nepal working in such a role.

VI. ARRANGEMENTS FOR IMPLEMENTATION OF THE UNITED NATIONS CONVENTION AGAINST CORRUPTION IN NEPAL

Nepal signed the Convention on 10 December 2003 in Merida, Mexico. Preparation of the administrative and legislative measures required upon becoming party to the convention are in progress.

By a Cabinet decision, the Ministry of Law, Justice and Parliamentary Affairs (the Ministry) has been given responsibility to work as a focal point and co-ordinating agency of the Convention at a national level. The Ministry is also assigned the work of the central depository of all types of treaties and conventions.

The Government of Nepal constituted a Working Committee under the chairpersonship of the Joint Secretary of the Ministry of Law, Justice and Parliamentary Affairs with the representatives of the Office of the Prime Minister and Council of Ministers, Ministry of Home Affairs, Ministry of Finance, Ministry of Foreign Affairs, the Commission of the Investigation of Abuse of Authority as members and the Under Secretary of the Ministry of Law, Justice and Parliamentary Affairs as the member-secretary. The Committee has identified an extensive list of legislative, administrative, institutional and policy reform measures required for the implementation the Convention at the national level.

Considering the Report of the above mentioned Working Committee, the Government has also constituted a high level Taskforce under the chairpersonship of the Secretary to the Ministry of Law, Justice and Parliamentary Affairs with the Joint Secretary level representatives of the Ministry of Home Affairs, Ministry of Finance, the Commission for the Investigation of Abuse of Authority, and the National Vigilance

Centre as members and the Joint Secretary to the Ministry of Law, Justice and Parliamentary Affairs as the member-secretary. The reinstated House of Representatives by its resolution dated 2063. 06.25 (11 October 2006) has also directed the Government to ratify the Convention.

VII. MEASURES TO BE TAKEN

Nepal is under a moral obligation to create a conducive environment to become a party to the Convention and to refrain from such acts which would defeat the object and purpose of the Convention. To fulfill these obligations, the following tasks are necessary.

A. Policy and Strategy Reforms

An anti-corruption policy and strategy in line with the Convention needs to be developed reflecting the principles of the rule of law, transparency and accountability. It should consist of awareness-raising of the importance of the participation of civil society, non-governmental organizations and community-based organizations, promotion of education against corruption through the development of school and university curricula, and collaboration with regional and international organizations.

B. Legislative Reforms

1. New Legislation

The Anti-money Laundering Act, Public Procurement Act, Good Governance Act, and Right to Information Act have recently been passed. The legislature must enact laws on Mutual Legal Assistance; Extradition; Protection of Witnesses, Victims or Experts; Recovery of Assets acquired through corruption/transfer of proceeds of crime; Transfer of Prisoners; Conflict of Interest; Whistle Blower Protection; Transparency; Corruption in the Private Sector; Corruption in Foreign Public Officials and Public Officials of Public International Organizations. The government must formulate policies on anti-monopoly practices; integrity in public life; public interest disclosure; other economic offences; transfer of criminal proceedings; trading in influence; execution of decisions of foreign courts; disclosure of the income and expenditure of political parties; regulation of nongovernmental organizations; and trade fraud. Some of these measures are in the process of formulation and drafting.

2. Review and Amendment of Existing Legislation

The existing Prevention of Corruption Act; Bank and Financial Institutions Act; Political Parties Act; Financial Procedures Act; Judicial Council Act; Military Act; Companies Act; Nepal Rastra Bank Act; Insurance Act; Civil Service Act; laws relating to the service and condition of the employees of public corporations/agencies; Partnership Act; Evidence Act; Private Firm Registration Act; Association Registration Act; Commission for Investigation of Abuse of Authority Act; and the Prison Act, need to be reviewed and amended.

VIII. INSTITUTIONAL REFORMS AND STRENGTHENING

The following institutions need be reformed and strengthened in light with the Convention:

1. The Commission for Investigation of Abuse of Authority;
2. National Vigilance Centre;
3. Special Court;
4. Related branch dealing with the cases of corruption within the Judicial Council;
5. Related branch dealing with the cases of corruption within the Nepalese Army.

IX. NEW INSTITUTIONS

The Anti-Money Laundering Act stipulates an Anti-Money Laundering Department. The Department will be formed soon. Similarly, Nepal Rastra Bank is entrusted to work as a financial intelligence unit under the Act.

X. CONCLUSION

Nepal's drive to prevent corruption has a long history. Despite efforts going back a long time, corruption has been not reduced but has increased furthermore. A strong legal regime against corruption, strong enforcement of general laws, development of a law-abiding culture, an end to impunity for corruption, and improvement of the socio-economic condition of government officials and also of the general public are pre-requisites for corruption control.

Legal provisions alone may not be sufficient to control corruption. Public awareness and collaboration and co-operation with the international community are also important.

With the enactment of the Prevention of Corruption Act 2003, investigation of corruption cases was speeded up. However, the speed did not remain constant. With the formation of the new government, a new opportunity has arisen to start afresh in controlling corruption.

PART THREE

**Work Product of the 141st International Senior Seminar
on the Improvement of the Treatment of Offenders through the Enhancement of
Community-Based Alternatives to Incarceration**

UNAFEI

VISITING EXPERTS' PAPERS

COMMUNITY-BASED ALTERNATIVES TO INCARCERATION IN THAILAND: CURRENT TRENDS AND FUTURE PROSPECTS

*Kittipong Kittayarak**



I. INTRODUCTION

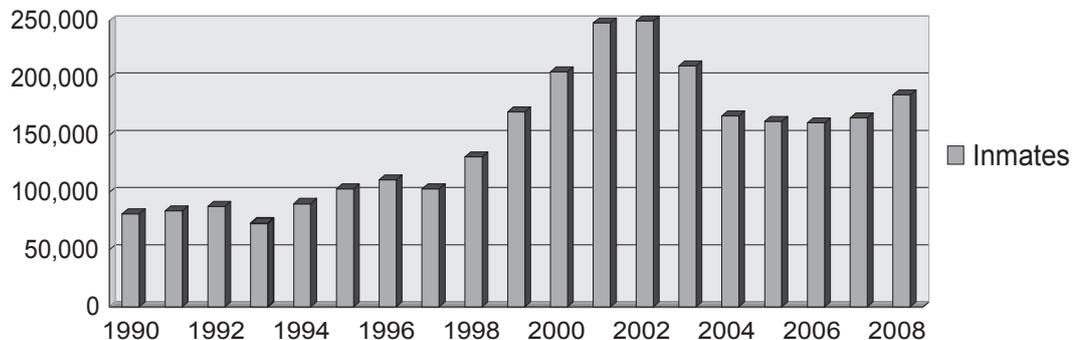
Criminal justice systems around the world have been coping with increasingly difficult challenges amid rapid changes in our political and socio-economic systems. Imbalanced development has weakened our social mechanisms, rendering them less effective in coping with economic hardships, which can contribute to the increased number of crimes. New trends also become visible where criminal activities are more and more technologically sophisticated. Failure to cope with these new challenges could have serious consequences as the functioning of the criminal justice system is at stake. Effectiveness in the treatment of offenders is one of the key indicators of healthy functioning of the criminal justice system. In order to avoid the serious issues of case backlog and overcrowding of correctional facilities, it is imperative that offender treatment systems are continuously improved and further developed.

This paper will begin with the assessment of current trends and the situation of institutional corrections in Thailand. The discussion will then focus on the community-based treatment of offenders, where current measures including drug diversion programmes whose implementation have been co-ordinated by the Department of Probation, have played a key role in reducing the number of inmates in correction facilities. The next section will discuss the role of the volunteer probation officers and community networks as key initiatives to enhance the treatment of offenders through community-based alternatives to incarceration. Finally, I will share my views on the key challenges of enhancing community-based alternatives to imprisonment in Thailand and the way forward.

II. CUSTODIAL TREATMENT OF OFFENDERS IN THAILAND: CURRENT TRENDS AND SITUATIONS

One of the most significant issues facing the criminal justice system in Thailand is coping with the extraordinary rise in prisoner numbers. From 1996 to 2002, correctional facilities in Thailand had to deal with an unprecedentedly large number of inmates. The number, which was 103,202 in 1996, jumped to 250,000 by the end of 2002. In Figure 1 the prison population for the period of 19 years is shown. Compared to other countries in the Asia and Pacific region, the number of inmates in Thailand remains high – 253 inmates per 100,000 – as shown in Table 1.

Figure 1. Prison Population in Thailand from 1990 to 2008



Source: Inmate Statistics Center, Policy Planning Division, Department of Corrections.

* Permanent Secretary Ministry of Justice, Thailand.

The rate of increase at this scale was quite unusual and cannot be accounted for under normal functioning conditions of the criminal justice system. The disproportionate increase in the inmate population since 1998 could be attributed to Thailand’s criminal policy which criminalized offences related to drug use, especially amphetamines, to deter drug-related offenders.

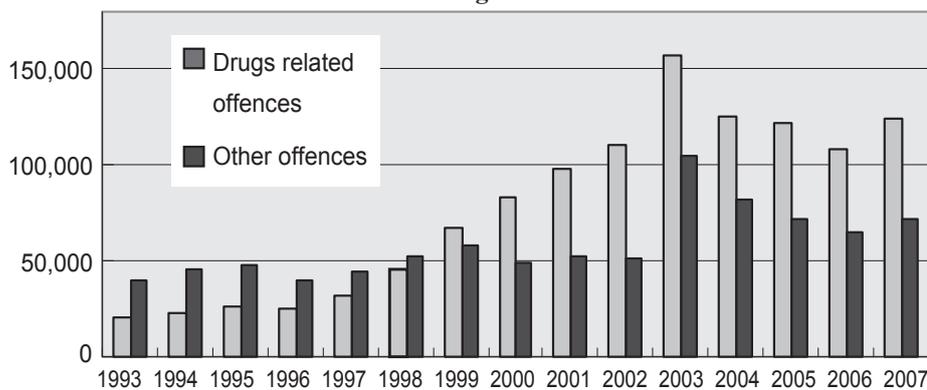
Table 1. Prison Population across Seven Countries in Asia and the Pacific in 2007

Country	Total number	Total number (per 100,000 people)	Portion of Female Inmates (percent)	Portion of Child Inmates (percent)
Indonesia	128,876	56	4.7	0.4
Macao	797	174	22.1	6.1
Malaysia	50,305	192	28.7	2.2
Myanmar	65,063	126	15.0	1.6
Sri Lanka	25,537	121	1.4	0.04
Singapore	11,768	267	10.0	4.7
Thailand	165,316	253	15.1	3.9

Source: International Centre for Prison Studies, 2008.

Figure 2 shows that the number of inmates convicted of drug-related offences has almost doubled in 15 years, while the statistics for other offenders remain mostly unchanged, leading to a conclusion that the large number of drug-related offenders is the result of severe measures while the contribution from the increase in criminal activities themselves might be only secondary.

Figure 2. Number of inmates convicted of drug offences versus other offences from 1993- 2007



Source: Inmate Statistics Center, Policy Planning Division, Department of Corrections.

There are two possible explanations for the increased number of inmates. It could signify the enhanced effectiveness of the criminal justice system in bringing those who commit the crime to justice. The implication of this interpretation is that the drug problem in Thailand has been properly taken care of since 1997. Another explanation is that by over-criminalizing the possession or consumption of amphetamines, the demand for the now drug is even higher than before, leading to higher prices and more profit-making, thus more people who are willing to risk trading them. This graver theory signifies that severe punishment as a deterrence measure has been far from achieving its policy objectives.

Tables 2, 3 and 4 illustrate the inmate population profile according to their categories, types of offences and terms of imprisonment. Based on these current statistics, it is clear that a large portion of Thailand’s correctional resources is being used to provide custodial treatment for convicted offenders, while suspects awaiting trial or final judgment constitute the second largest group of the population, contributing to the current rate of imprisonment prior to conviction of nearly 30%. This rate implies that the criminal process

THE 141ST INTERNATIONAL SENIOR SEMINAR
VISITING EXPERTS' PAPERS

has not yet been able to provide a timely response to those awaiting trial and who must be assumed to be innocent. Table 5 provides regional comparative data on this category of inmates, which shows that Thailand is among the countries at the top of the list for having a large percentage of inmates on remand. When viewed by type of offence, inmates who have been convicted of offences related to drug use constitute the largest group, almost 60%. It should also be noted that about half of the total population in prisons are currently those serving relatively short terms (less than five years).

Table 2. Overall population of the Thai prison system according to major categories (As of 1 September 2008)

Categories	Male	Female	Total	Percentage
1. Convicted	112,464	18,594	131,058	70.825
2. On-remand	44,744	7,538	52,282	28.25
2.1 pending appeals	22,354	3,541	25,895	13.99
2.2 awaiting trial	9,576	1,495	11,071	5.98
2.3 awaiting investigation	12,814	2,502	15,316	8.28
3. Children and youths under detention	401	3	404	0.22
4. Relegated persons	11	1	12	0.01
5. Detainees	1,128	185	1,313	0.71
Total	158,748	26,321	185,069	100

Source: Inmate Statistics Center, Policy Planning Division, Department of Corrections.

Table 3. Prisoners Statistics by Type of Offences

Type of Offences	Male	Female	Total	Percentage
1. Offence against property	25,911	1,647	27,558	22.25
2. Offence against narcotics law	56,689	15,349	72,038	58.16
3. Offence against life	8,798	277	9,075	7.83
4. Bodily harm	3,552	83	3,635	2.93
5. Offence against social security	216	11	227	0.22
6. Others	5,031	496	5,527	4.46

Source: Corrections in Thailand 2008 - an annual report published by the Department of Corrections, Thailand.

Table 4. Prisoners Statistics by Sentence Terms

Sentence Term	Male	Female	Total	Percentage
Less than 3 months	899	96	955	0.77
3- 6 months	2,889	382	3,271	2.53
6 months – 1 year	7,930	1,263	9,193	7.12
1 – 2 years	16,164	3,173	19,337	14.97
2 – 5 years	32,700	4,274	36,974	28.63
5 – 20 years	38,018	6,836	44,854	36.22
20 – 50 years	10,149	2,142	12,291	7.83
Life imprisonment	1,653	218	1,871	1.51
Death penalty	113	7	120	0.09

Source: Corrections in Thailand 2008 - an annual report published by the Department of Corrections, Thailand.

There are numerous factors that contribute to the current picture of correctional treatment in Thailand. Lack of coherent and effective criminal policy has been one of the key factors, hindering any systematic attempt to implement alternative approaches for parties of conflicting interests to get access to justice. Social norms, as can be seen from the public attitude towards offenders, tend to be negative, and there is a strong inclination among

Thais to rely on formal criminal processes or legal action as means to solve their problems. These factors also play significant parts in shaping the current situation of the Thai correctional system. Further, at the root of the problem, the symptoms of which can be seen from the severe drug problems and high rate of crime, is the inability of the society to cope with the negative impact of globalization. Various institutions such as family, community, educational systems, and spiritual faith have been faced with new types of challenges and threats.

Table 5. Numbers of offenders awaiting trial in several countries in Asia in 2007

Country	Total Number of Inmates	Total Number of Inmates On-Remand	Percentage of Inmates On-Remand
Indonesia	128,876	387	0.3
Iran	158,351	39,271	24.8
Macao	797	176	22.1
Malaysia	50,305	14,438	28.7
Myanmar	65,063	7,417	11.4
Mongolia	6,593	1,305	19.8
Hong Kong	10,440	1,409	13.5
Japan	81,255	9,751	12.0
Taiwan	60,346	7,181	11.9
Brunei	486	35	7.2
Laos	4,020	40	1.0
Singapore	11,768	812	6.9
Thailand	165,316	43,313	26.2

Source: International Centre for Prison Studies, 2008.

Lack of co-ordinated effort to systematically deal with these challenges has put the entire criminal justice system under considerable pressure. The overcrowding problem has not only affected the corrections system, but also the police, the prosecutors, and the courts. The burden caused by the anomalously sharp rise in inmate numbers has been enormous. Despite the attempt to allocate new budgets to expand or build new prisons, most very soon become crowded, worsening the living conditions for prisoners in terms of space, hygiene and overall prison environment.

Despite the overcrowding situation, the number of correctional staff has remained almost the same, even during the peak period of 1997-2006, and the current ratio of corrections officers to inmates is 1:32, while the international standard is 1:5. This leads to a heavy workload for staff, which affects both their morale and the quality of work to meet the treatment needs of inmates.

In order to respond to problems faced by the corrections system, especially the serious issue of overcrowding, various measures to introduce community-based alternatives to imprisonment have been considered and put to work under the management of the Department of Probation. In the next section some of these key measures will be highlighted to illustrate the current situation and the direction for future development.

III. COMMUNITY-BASED NON-CUSTODIAL TREATMENT IN THAILAND: CURRENT TRENDS AND SITUATIONS

In Thailand, probation measures for adult offenders were provided for by the Penal Code of 1956 but they were not actively implemented due to the lack of a specialized agency or probation officers to carry out the court order. In 1979, the law on probation was proposed and a specialized agency was created and probation officers were appointed to carry out court orders imposing conditions for the supervision and rehabilitation of offenders under suspended or deferred sentences. This law thus marked the beginning of the community-based treatment of offenders in Thailand, under the responsibility of probation officers, volunteer probation

officers, and civil organizations based in the community. In 1992, the Department of Probation was established to handle all adult probation nationwide.

During the first two decades of its operation, the Department of Probation focused its work on providing probation programmes for offenders whose imprisonment terms were suspended. The programmes mainly consisted of the supervision of offenders which could be combined with other types of support such as education, counselling, rehabilitation, community service, and other social welfare. The overall objective of these activities is to assist offenders in their effort to rehabilitate and successfully reintegrate into society to become productive members of society without lapsing into reoffending.

Although the Department of Probation has done excellent work in providing successful adult probation programmes, it was unable to expand its scope of work to cover new, community-based alternatives to incarceration. Lack of overall criminal justice policy planning, lack of interagency co-operation and co-ordination among key actors, and inadequate funding were among the major reasons hampering the successful introduction of community-based treatment as an alternative to the long-held practices based mostly on retributive, custodial measures.

The overhaul of the criminal justice system which began in 1996 and culminated in 2002, when the Ministry of Justice was reorganized and repositioned as the focal point for justice administration, also paved way for the application of community-based treatment. In addition, changing policy on drug problems had also opened the way for community-based treatment of drug abusers, who constitute more than half of the number of defendants in criminal cases and inmates in correctional facilities. The government recognized the necessity of a new policy which took into account both the rehabilitation needs and the need to lessen the pressure within the criminal justice system.

The growing interest in the concept of restorative justice is another factor that has a direct impact on the promotion of community-based treatment of offenders in Thailand. As restorative justice emphasizes informal methods of dealing with crime, particularly with the increasing the roles of victims, offenders, and the community, it supports community-based treatment options.

One of the key milestones for such development was the cabinet resolution of 10 July, 2001 which specified clear guidelines on how to reduce case backlogs and overcrowding. The so-called "July 10 Resolution" recommended several non-custodial and community-based treatment measures as desirable approaches, and thus served as a road map for future development of community-based treatment measures in Thailand. Some of the key initiatives include the setting up of community mediation centres to settle certain kinds of disputes within communities; the encouragement of the use of prosecutorial discretion not to prosecute, subject to certain kind of conditions; the initiation of drug diversion programmes; and the expansion of the scope of probation to include juvenile offenders as a new target group. The new policy has proved effective not only by introducing new approaches for diversion of cases from the formal criminal justice process, but also by providing alternatives to imprisonment that are more efficient in returning the offenders to society.

The Department of Probation, under the Ministry of Justice, has been the key organization in the implementation of the July 10 Resolution. Its scope of work has been expanded to include probation programmes for all types of offenders: juveniles and adults. Its probation programmes now cover all stages of the criminal process, including the pre-trial, trial, or post-conviction stages. With a specialized agency in charge of all the probation work for the suspect and offenders at all stages of the criminal process, the probation system in Thailand is more focused and can benefit more from unified policy objectives, compared to the past.

With the expanded scope of probation work from traditional probation based on investigation of information about offenders and supervision, to the new frontier of prevention and diversion, the Department of Probation has been forced to come up with innovative ideas to carry on its new assignments and, at the same time, maintain the quality of its traditional functions. Apart from its original work of providing community-based programmes for only adult probationers, after the 2002 reform it has become a key agency administering community-based rehabilitative measures and aftercare services to youth and adult probationers and parolees, providing compulsory treatment programmes for drug addicts, and working to promote effective crime control and prevention through local community networks.

Figures 3 and 4 indicate the clear growth in the responsibility of probation officers in recent years, as seen from the change in the total number of cases handled by probation officers during the past 30 years and the number of offenders who enter the probation system in comparison with those put in the custody of prisons for the same period.

Figure 3. Number of cases handled by the Department of Probation in the past 30 years. The number represents cases coming from all types of work except community justice.

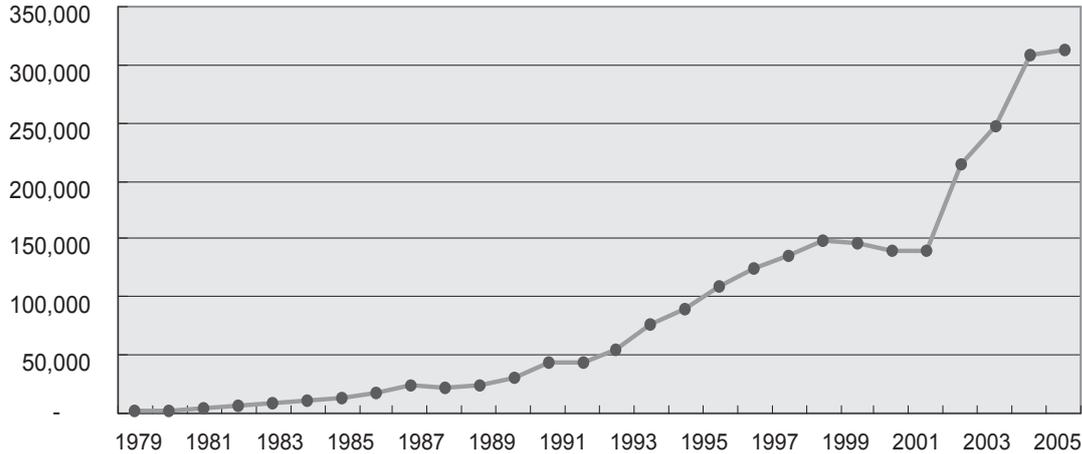
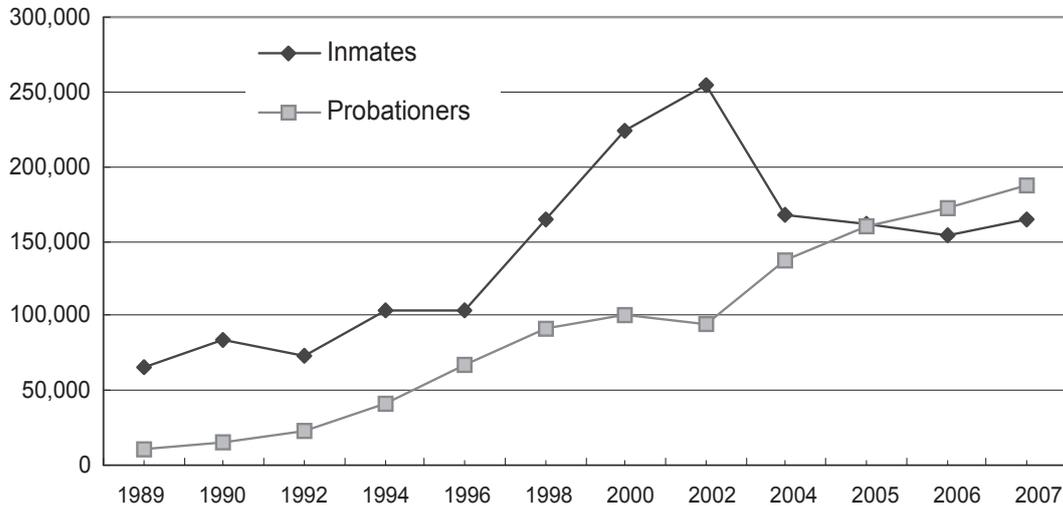


Figure 4. Number of offenders entering the probation system versus that of offenders placed under custody for the past 30 years.



From its moderate inception in 1979, the probation system has now overseen more than 1.5 million offenders, with less than 20% recidivism after probation, indicating that most of the offenders who have been through treatment programmes can successfully reintegrate into society (see Table 6 for more detailed statistics).

Table 6. Numbers of offenders who reoffended under probation programmes during 2004-2007.

Year	Total number of offenders under probation	Number of reoffenders under probation	Percentage of reoffenders under probation
2004	176,799	23,867	13.50
2005	126,974	10,590	8.34
2006	128,954	16,622	12.89
2007	137,178	20,988	15.30

Source: Annual Reports of the Department of Probation for the period of 2004-2007.

IV. SELECTED COMMUNITY-BASED MEASURES CO-ORDINATED BY THE DEPARTMENT OF PROBATION

Here are some of the community-based treatment measures that have been implemented by the Department of Probation.

A. Probation of Adult Offenders

The current adult probation system in Thailand consists of:

1. Social Investigation

Social investigation in Thailand, in accordance with the Penal Code 1979 (B.E. 2522) Section 56, is conducted by probation officers in the pre-trial phase. Probation officers then have to prepare a pre-sentence report required by the court before a sentence is imposed. The overall aim of social investigation is basically to gather facts related to the offender and offence, and to make recommendations for courts on appropriate sentences.

A report contains the offender's social background, circumstances of the offence, the risk the offender is likely to pose to the public and advice on suitable probation measures for individual offenders. The likelihood of individual reform is also taken into account. Another essential part of the social investigation is the Risk/Need Assessment to be included in the pre-sentence report.

During the social investigation, as a result of need assessment, probation officers may address the offender's needs and provide assistance, where appropriate, such as helping them with bail matters, meal allowance, transportation assistance, etc. More importantly, at that stage, probation officers may also work with victims of crime to give them a voice in the process, and provide them with support based firmly on restorative justice principles.

2. Supervision

The supervision of adult offenders is an offender rehabilitation process. Probation officers will apply many different techniques. Those include:

- (i) The supervision of adult probationers with the use of counselling techniques as a rehabilitative tool;
- (ii) The use of community-based rehabilitation programmes that are appropriate to individual offenders; and
- (iii) Provision of assistance.

Supervision is a procedure to supervise, treat, support, and give counselling to probationers within the community. Probationers will be given a helping hand to amend their habits, assist them to reintegrate into the community as law-abiding citizens, and discourage them from reoffending or continuing their criminal lifestyles.

When courts impose suspended sentences or suspension of sentence with probation conditions, probation officers will make an arrangement with the offender to fulfill the court order. The arrangement is based largely on the outcome of risk and need assessment of each offender. The conditions could be modified or reduced or the probation may be terminated early before the specified date. Probation officers will comment on this when reporting the progress of probation. Additionally, the probation and supervision plan will be reassessed every three to six months. The supervision is also to give offenders an opportunity

to compensate for the harm done by the crime they commit, and to be encouraged to stop reoffending.

3. Specific Rehabilitation Programmes

Concerning treatment programmes, the Department of Probation has initiated a wide range of rehabilitative interventions and activities. The strength of our rehabilitation is the way in which probation rehabilitative practices are integrated with local resources and work in partnership with other government and non-government agencies. Various constructive programmes have been implemented. Explicit examples include 'Buddhist Ordination', 'Dharma activities' (religious training), 'Ethical Camps', 'Anti Drink-Driving Campaign', etc.

In attempting to create innovative rehabilitation programmes, the department encourages probation officers to work jointly with multi-agencies, volunteer probation officers (VPO), psychologists, social workers, social welfare officers, religious organizations (Buddhist, Islamic, Christian), etc. Moreover, the department also works closely with the Victims of Drunk Driving Club whose members are seriously-injured or handicapped victims of drunk-drivers.

4. Basic Assistance

Probation officers are to provide basic assistance for all offenders - the offender under social investigation, adult probationers, juvenile delinquents, parolees, and ex-probationers, including ex-prisoners. Basic assistance will be provided in accordance with the result of need assessment.

Basic assistance is generally to do with vocational training, helping with higher education, job finding, job application, and other matters beneficial for rehabilitation. This is for the offenders to be able to support themselves and manage to integrate back into society.

B. Probation of Youth Offenders

The probation of juvenile delinquents in Thailand is the responsibility of two agencies: the Department of Juvenile Observation and Protection and the Department of Probation. The Department of Juvenile Observation and Protection deals with the social investigation of young offenders and oversees those in the delinquent detention centres. The Department of Probation supervises young offenders subject to probation orders imposed by the courts and those released from detention centres nationwide for a specific period of time. Since 2004, the Department of Probation has run the Juvenile Rehabilitation Program which incorporates a number of related projects aimed at strengthening co-operation with community civil society organizations, empowering the family and the community, and capacity building for the probation officers in their work for the children. To provide a venue for counselling and for creative activities by the children within the community, a number of community centres for juveniles have been established to serve as a forum for co-ordinating help and support for the children in the community as well as for introduction of useful programmes and activities for the children in the community.

C. Probation of Parolees

After serving one third or at least 10 years of an imprisonment period, inmates may be given a parole or remission order. Also, those who have been serving a sentence of life imprisonment are eligible for early release if the Parole Board so agrees. Before the decision is made, probation officers will propose a post-sentence investigation report to the Parole Board. A report consists of relevant information about the inmate and his/her behaviour during the imprisonment and details of supporters. Probation officers may also include in the report the views of the victim, the offender's neighbours, and the community leaders.

The supervision of parolees has its own purpose, and practices principles similar to the supervision of adult probationers. However, what makes it different is the way in which parolees are approached, and the programme requirements. This is partly due to the fact that they have been in custodial institutes for some time, and certain inmates find it rather difficult to adapt back into their community and even their own family.

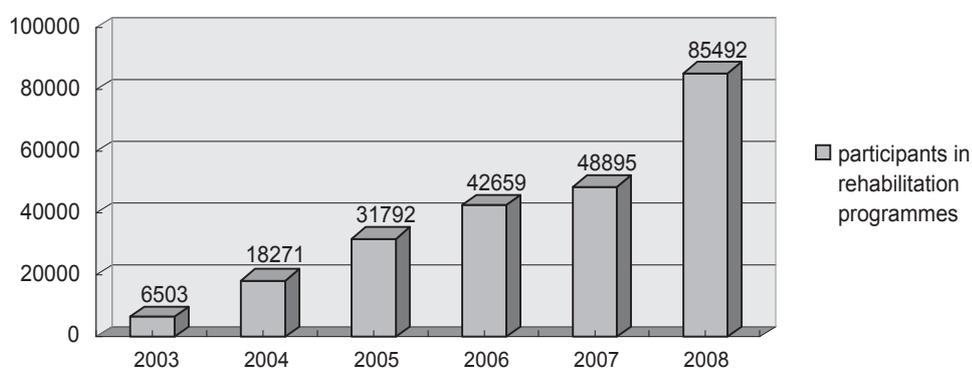
D. The Compulsory Rehabilitation of Drug Addicts: A Major Scheme to reduce Overcrowding in Thailand

Since 2002 the Thai government has adopted a new policy to tackle narcotic drug problems. The new emphasis is on the enhancement of preventive measures. Under the policy, drug users and drug addicts, who previously had been prosecuted as criminal offenders, are to be regarded as patients who need rehabilitation

treatment. In 2002, the law on Drug Rehabilitation was revised to provide a new legal framework for the integrated treatment of drug-related offenders in Thailand. Under the new scheme, all related government agencies have to work closely together to provide integrated responses to the treatment of drug offenders. These agencies include the Office of the Narcotic Control Board, the Royal Thai Police, the Department of Corrections, the Department of Juvenile Observation and Protection, the Courts of Justice, the Royal Thai Army, the Royal Thai Navy, the Royal Thai Air Force, the Ministry of Public Health, the Ministry of Interior, and the Bangkok Metropolitan Administration, with the Department of Probation serving as the focal point.

The Drug Rehabilitation Act 2002 can be regarded as a revolutionary piece of Thai legislation. The 2002 Act makes clear that drug addicts are not 'criminals', but 'patients' who are in need of effective treatment. The enforcement of the Act undeniably contributes to thousands of drug cases being diverted from courts, and shifting the public view of drug dependents in Thailand. After assuming the responsibility, the Department of Probation did not hesitate to take a more holistic approach by introducing various drug rehabilitation programmes to assist drug addicts in rebuilding a new life. The number of drug addicts who have been treated under the scheme from 2003 to present is shown in Figure 5.

Figure 5. Number of participants in compulsory rehabilitation programmes from 2003 - 2008



The 2002 Drug Rehabilitation Act stipulates that the person charged with “drug addiction”, “drug addiction and possession”, “drug addiction and possession for disposal”, or “drug addiction and disposal,” if the amount of possession is less than the limitation of the law, is to be transferred to the court within 48 hours, and in the case of young persons 24 hours. The court then will be able to divert the case from the traditional criminal justice system and refer the person to designated facilities for drug assessment. The evaluation will be conducted by the regional Sub-committee of Narcotic Addict Rehabilitation, chaired by the chief provincial public prosecutors, who will make a decision on whether the person is a drug addict. Apart from this, the committee is given statutory power to supervise drug abusers/addicts during the assessment and rehabilitation, refer the person to drug rehabilitation centres, consider the extension or reduction of the rehabilitation period, and grant temporary release during detention. If the evaluation result shows that the person is a drug abuser/addict, he or she will be required to attend treatment programmes for a specific period of time.

If he or she is assessed as being addicted, the prosecutor will suspend the prosecution and the person has to undergo one of the two compulsory systems: the “custodial” or “non-custodial” rehabilitation programme.

E. Custodial Rehabilitation

There are two types of custody options available for the participants of the rehabilitation programmes, depending on the needs to limit freedom of each participant: the full custody arrangement, and the partial custody arrangement. In either case, the first four months into the rehabilitation scheme are dedicated to the intensive medical treatment of each drug addict. The difference is the differing degree of custody during that period. At present, there are two designated facilities that are equipped to run rehabilitation programmes under full custody treatment: the Lat Lum Kaeo Community Treatment Center in Pathum Thani province, and the Jirasa Air Force Base Center operated by the Royal Air Force. In case of partial custody requirements, the four-month rehabilitation programmes are based on the integration of four key

components, namely: family, alternative treatment activities, self-help, and therapeutic community, or FAST MODEL, and are available at facilities under various government agencies, including military camps, naval camps, and the medical treatment centres of the Ministry of Public Health. In case of partial custody, there is more variety depending on the emphasis and available resources of the participating agencies.

Upon completing the intensive rehabilitation programme, each participant will be released and allowed to live within his or her community under probation for another two months. The Department of Probation is the central agency overseeing this process where emphasis is placed on preparing each participant for reintegration into society. After completing probation, the participants will be periodically monitored by the volunteer probation officers or the volunteer public health officers for another 12 months to evaluate if they are successfully rehabilitated. Successful participants on the scheme are then exempt from criminal prosecution.

F. Non-Custodial Rehabilitation

In the case where no custody is required during the intensive treatment, participants who are diagnosed as addicts may or may not be admitted as patients at hospitals or other rehabilitation centres, to receive the appropriate treatment. This step lasts from four to six months. In the case where the participants are deemed merely drug users, they will receive treatment provided by the Department of Probation for six months. The remaining two-month probation period and the one-year monitoring period are implemented in the same way as the scheme for rehabilitation under custody.

In addition to the implementation of the rehabilitation scheme, the Department of Probation has also come up with a number of initiatives to assist drug-related offenders in their effort to successfully reintegrate, such as the following:

1. Basic Educational Support

The idea is to provide the drug addicts who undergo the rehabilitation programme with the opportunity to receive basic education. The programme is run by the Department of Probation in collaboration with the Ministry of Education, where special curricula equivalent to that of the regular elementary or primary schools are provided to each participant depending on his or her needs. It is hoped that by fulfilling the educational gap for these drug-related offenders, they will be in better shape for future employment in the real world or to pursue higher education of their choice upon the completion of the programme.

2. Enhancement of Family Support

The initiative involves educating family members of drug addicts on how to support the rehabilitation effort, and counselling services for family members as well as the participants of the rehabilitation programme. The rationale for this initiative is that the rehabilitation will be effective only when it extends to cover all stakeholders and that therefore family members of each drug addict can play significant roles. In order to ensure the smooth and happy reintegration of offenders back into society, support and understanding on the part of his or her family is deemed indispensable.

The initiative has proved very effective in equipping both the rehabilitants and their families with understanding of the importance of the community-therapy, the fostering of bonds among family members, and the importance of having the right mindsets in dealing and supporting the rehabilitation of the offenders. It was found the participants whose family members also took part in the initiative had a higher rate of successful rehabilitation.

3. Buddhist Teaching for Drug Addicts

This initiative aims at applying relevant Buddhist principles and guidelines to help the drug addicts in developing their mental strength to rehabilitate. The Department of Probation has been able to gain support from three Buddhist temples willing to provide a pilot programme under the initiative.

G. Restorative Justice Interventions

In Thailand, there are several criminal justice agencies implementing restorative justice interventions. To begin with, the Department of Juvenile Observation and Protection has been implementing a restorative justice conference since 2003. It is taken in form of a 'Family and Community Group Conference' (FCGC), conducted in the pre-trial stage as a channel of diversion. From the beginning of the programme in June 2003

to February 2008, there were 21,490 cases where an FCGC was conducted, of which 18,128 cases were approved for non-prosecution by public prosecutors. In addition, the Department of Probation also has also initiated programmes on restorative justice intervention since 2003. The programme is known as 'Restore-Relationship Conferencing', conducted at the pre-sentence/social investigation stage. Due partly to the legislative limitation, the initiative does not place an emphasis on diversion. Rather, the outcome of restorative justice conferences proves beneficial for judges in giving appropriate sentences. This is particularly when judges examine the extent to which offenders feel guilty and if any reparation is made for the committed crime.

Restorative justice has begun to gain wider acceptance in Thailand. Recently, the Criminal Court has also initiated a pilot project on criminal mediation based on restorative justice principles. Draft legislation on diversion of small criminal cases at the police and prosecutors stages have also been proposed for consideration by the parliament.

1. Restorative Justice in Response to Domestic Violence

In recent years, domestic violence (DV) has been recognized as another serious issue that threatens the stability of the family in Thai society. The traditional view is that domestic violence is a private matter and it is inappropriate for outsiders to interfere. This has resulted in the situation where domestic violence tends to be closely related to violence against women, since the female counterparts, who are normally the victims, are reluctant to bring the matter to the authorities. This has in some cases resulted in repeated incidents of DV by the male partners.

The Department of Probation, in co-operation with the Royal Thai Police, the Rama Hospital, the Bangkok Metropolitan Administration, the Women Empowerment Association, (an NGO which provides emergency shelters for female victims of violence), and the Friends of Women Foundation, has designed an integrated DV response system where the concept of restorative justice is used in conjunction with the law enforcement and rehabilitation programmes organized by the interdisciplinary professional organizations to provide assistance to the victims of such violence, and to the offenders in their effort to change their behaviour and stop using violence.

The restorative justice concepts have proven effective in providing a suitable ground for resolving disputes within the family in a way that tries to maintain the relationships among the family members. In bringing the parties in conflict to dialogue and trying to reach an agreement, emphasis is placed on responding to the needs of the victims as well as holding the offenders accountable. Restorative justice has therefore provided an effective alternative to the formal criminal justice process in response to DV.

When violence occurs between a married couple, the partner who has been the victim of violence can exercise his or her right to bring a criminal case against the offender by first reporting it to the police. Under the restorative justice initiative, he or she can request that a dialogue with the partner be arranged with mediation by a probation officer, a psychologist, or a social welfare worker. If the two sides can reach an agreement, the charge against the offender will be suspended on the condition that he or she participates in a rehabilitation programme under the supervision of the probation officer for an agreed upon period of time. During that period, the participants will be able to receive various kinds of assistance from the Department of Probation, including legal aid counselling, occupational training, and accommodation support. If the participant has been well behaved and not violent, the charge will be completely dropped. Within the prescription period of the offence, if the attempt proves unsuccessful, the victim can at all times request that the prosecution against the partner will be resumed.

H. Aftercare Services

Certain offenders under probation are considered socially disadvantaged and they have also lost their potential to abide the rule of law. Aftercare services aim to regain their reformatory potential and self-improvement. These are available for ex-probationers who have completed the probation term within one year.

For aftercare services, Department of Probation has applied the use of 'halfway house' to help offenders in need of accommodation. Halfway houses are there to help them adjust and be prepared to get back to their family/community. As a temporary accommodation, there are a variety of routine activities and programmes in the halfway houses including occupational training, spiritual counselling, and various skill development

programmes. In running the temporary residences, Department of Probation attempts to integrate various sciences, local and traditional know-how, traditions, cultures, and religions, altogether. Thus the halfway house can be considered as a boundless work among the probation departments, religious institutes, and the community at large.

At present, there are several halfway houses operated by the Department, which are located in provinces such as Nakhon Sawan, Amnat Charoen, Maha Sarakham, Kamphaeng Phet, and Phatthalung, providing services for not only offenders under probation orders, but also drug addicts under the diversion initiative. Various activities are offered, including Buddhist therapy, drug rehabilitation programmes, and supervised community service.

While new initiatives are considerably more diverse and group-specific, to implement such treatment programmes effectively on a large scale requires enormous resources which is far beyond the normal capacity of any government agency. Therefore, recruitment of volunteers and active participation by the community itself are of great importance as they provide sustainable resources for implementing the community-based correctional programmes. It is also important to empower each community to develop its own mechanism of crime prevention by means of knowledge sharing. Some of the ongoing initiatives aimed at community empowerment are the topics of the next section.

V. INITIATIVES TO PROMOTE COMMUNITY-BASED TREATMENTS

A. Community Participation: A Key to Success

The Department of Probation recognizes the importance of community networks as valuable community-based resources for sustainable correctional programmes. It is important to empower each community to develop its own mechanism of crime prevention. Therefore, the Department has emphasized equipping the communities with knowledge before engaging them in taking an active role in crime prevention and community-based rehabilitation of offenders. Some of the ongoing initiatives aimed at community empowerment are the following:

1. Volunteer Probation Officers Programme

The initiative to allow community members to actively take part in probation service has been in place since 1986. From the beginning, the volunteer probation officers have had an integral role in the probation system since they provide a linkage between the State and the general public. They also serve as multiplying factors in the attempt by the Department of Probation to reach out to the community, either through various schemes to disseminate information, to educate people, or to sensitize the public to various issues, including certain types of criminal offences. One of these important roles is to provide effective monitoring for the offenders who are serving the probation orders within the community to ensure their conduct is in accordance with the conditions set by the court.

In performing such duties, these volunteers are also responsible for providing help to, and assessing the progress made by these offenders – an indispensable element of a successful probation system. Thus, the volunteer probation officers make an invaluable contribution to foster effective reintegration of the offenders back into society, in particular through their roles in narrowing the gaps that exist between the life of offenders and that of normal citizens, and helping offenders to overcome the alienation they feel upon their return to society.

The following list comprises the basic qualification requirements for those interested in joining as a volunteer. Candidates must:

1. Be at least 20 years of age;
2. Live in a permanent residence;
3. Be literate;
4. Be a person of integrity and honesty;
5. Have suitable income;
6. Maintain law-abiding behaviour;
7. Have completed required training courses as provided by the Ministry of Justice;
8. Have no criminal record except for petty offences or negligence.

As of 30 September 2008, there are about 9,430 volunteers currently registered throughout the nation. In 2008, the number of offenders under the supervision of volunteer probation officers who have successfully completed the probation programmes without reoffending is as high as 98.9 percent, supporting the claim that volunteer probation staff have become a vital contributing factor in the success of the reintegration scheme by Thailand's probation system.

To encourage community of practice among the volunteer probation staff, an Association for Volunteer Probation Officers has been established under the support of the Ministry of Justice to provide assistance to volunteer probation officers as well as to foster networking and sharing of information among the volunteers.

2. Community Justice Networks

Starting from 2003 as a pilot project, the initiative has been the first attempt by the Department of Probation to put the theory of community justice into practise. This kind of network developed because the Department of Probation felt the need to have a broader base of community support to be able to cope with much more demanding responsibilities, especially in the rehabilitation of drug addicts. Through the concept of 'community justice' where the community can work in 'partnership' with the government, it was hoped that the community could join hands to help during rehabilitation and reintegration of drug addicts into society. The pilot project proved successful and the idea of working in 'partnership' with the community has been expanded to other areas beyond drug rehabilitation.

In rural Thailand, the concept of people in the community joining hands with the authorities in law enforcement and providing justice has long been a tradition. This tradition was neglected once the modern criminal justice agencies were established. The pilot project initiated by the Department of Probation has been successful in utilizing this hidden strength of the community. It was found that through the unity and bonding between members in the community, it was possible to bring about positive outcomes in terms of helping and caring for the needy in society. By empowering the community to be more active and get involved in day-to-day justice activities, community resources and social capital can be fully utilized to achieve the end result.

In other words, the community justice network is an important initiative by the Department of Probation with an aim of strengthening public participation in the field of criminal justice by creating a network of civil society groups within the community to work closely with the government. Key activities include training for probation officers so they can develop the necessary skills to work with or within the community to promote community justice; educating the general public so that they are aware of the roles and functions of various agencies within the criminal justice system, the importance of surveillance in crime prevention, how to file complaints, how to protect their rights and liberties guaranteed by the law; alternative dispute resolution including mediation; as well as various approaches - such as community workshops - for the community-based treatment of offenders.

Under the initiative, a community justice centre is established within the community where the members are recruited from the general public as volunteers. These volunteers will receive training from the Department before they get together to commence their functions, such as hearing complaints and organizing meetings to deal with disputes. Community justice newsletters and other periodicals, combined with frequent exchange of site visits, are used to strengthen and maintain the close relationship between the networks and the Ministry of Justice. From 2005 to present, community justice networks have grown into a large network of 56,433 volunteers who can join their efforts through various activities organized around the 530 community justice centres all over the country.

B. Making Probation Work More Visible

1. Drink-Don't-Drive Campaign

The Drink-Don't-Drive Campaign is one of the most popular nationwide campaigns aimed at reducing the numbers of deaths and injuries caused by road accidents during long vacations such as the New Year and *Songkarn* (Thai traditional New Year) holidays. During such holidays, a large number of people may return home or travel. According to statistics, during the five to seven days of the *Songkarn* holidays of 2002-2004 there were more than 35,000 injuries and around 550-650 deaths as result of road accidents. Statistics showed that around 35 percent of the accidents were caused by drunk driving. Although drunk driving in

Thailand is a criminal offence punishable by up to six months' imprisonment, in reality, where there is no major injury involved, the drivers would normally receive only a fine. Such light punishment does not deter drivers from repeating the offence.

In 2005, the Department of Probation joined the campaign. It has successfully persuaded the courts to put drunk drivers on probation. In this initiative, drunk drivers were given suspended sentences and put on probation with the requirement that they perform community service. The Department of Probation selects community service activities designed to sensitize drunk drivers to the kinds of injuries they might cause themselves or others. They include assisting victims of car accidents, working in hospitals, volunteering for road accident emergency rescue units, and campaigning against drunk driving during the New Year holidays and *Songkarn* Festival.

The initiative combines a specific type of community service with public education in co-operation with a network of civil society organizations to create an effective campaign against drunk driving in Thailand. The Department of Probation works closely with the Thai Health Promotion Foundation, the Drink-Don't-Drive Foundation, the Department of Disaster Prevention and Mitigation, the Road Accidents Prevention Network, and the Traffic Police Head Quarters, to educate drivers, the general public, and the mass media, and sensitize them to the damage caused by traffic accidents, including the criminal offence of drunk driving. The campaign also aims at instilling a sense of social responsibility among drivers.

The Drink-Don't Drive campaign, with the message "Drunk drivers will not only be fined but will also be put on PROBATION" was one of the most successful campaigns. The campaign received wide media coverage: news of the campaign was on the front pages of every newspaper and on primetime TV across all stations. As a result of working hard to get the campaign's message to the public, a poll conducted in 2006 by Assumption University in Bangkok found that 91 percent of those polled agreed with the idea that drunk drivers should receive community service orders. When asked whether they had heard of the Department of Probation, once the least known organization in the criminal justice system, 83 percent of the respondents said yes, a steep rise from the 48 percent in a 2000 survey.

VI. KEY CHALLENGES AND WAYS FORWARD FOR COMMUNITY-BASED TREATMENT IN THAILAND

In order for community-based treatment to serve as an alternative for the treatment of offenders, it is important that well-focused criminal justice policy regarding the non-custodial treatment and reintegration of offenders across the criminal justice process is in place. It is also highly desirable that all stakeholders and responsible government agencies, especially the Department of Probation, continue their efforts to improve and enhance the capacity of their staff. This entails providing the staff with training and opportunity to acquire and develop new skills to cope with their expanding responsibilities; improving work conditions; and enhancing the overall efficiency of the work system. This is particularly important when one considers the fact that there will always be a certain degree of constraint at the high policy level to reduce the size of the bureaucratic system, making it very difficult for the public agencies to employ additional staff to match the increased workload.

It can be said that the community-based approach has begun to take root in the criminal justice system, and Thai society. Yet, for this new alternative approach to survive and attain more maturity, a number of key challenges will have to be adequately dealt with. Here are some of the challenges and ways forward.

A. Explosive Growth in Scope of Work

Figure 4 shows the number of cases that fall under the responsibility of the probation officers, while Figure 5 traces the number of probationers entering the system during the past 30 years. Here the explosive growth in responsibility of probation staff in recent years is clearly visible.

The increase is not only in the quantity of work, but also the variety of missions. New laws that have been in force in recent years have paved the way for the expanded scope of probation work from the traditional intensive probation based on investigation and supervision of offenders, to the new frontier where probation work becomes an essential instrument for diversion and crime prevention. The introduction of

innovative techniques, such as electronic monitoring for treatment of offenders in the community, has also led to a significant increase in the workload of probation officers. The expanded scope of work has had a considerable impact on the probation staff already stressed by chronic under-staffing. So far, the Department of Probation has introduced numerous measures to improve the working system, including the introduction of information technology and innovative approaches with an aim to enhance the efficiency of work. Still, all this will not be enough to effectively address the overwhelming problem of workload increases and its impact on the morale of the staff, unless the government takes this issue seriously and comes up with a systematic way to provide sufficient support. What is needed is sufficient funding and support to cope with the expanded scope of work with the guarantee that the quality of the probation programme will not suffer.

B. Need for Enhanced Visibility

Probation work, where most of the activities take place within the community, tends to be less visible in the eyes of the general public compared to institutional treatment. One serious implication for this relatively low visibility is the difficulty in trying to convince the decision makers, who might not be able to see the tangible results of probation work, to provide essential support both in terms of policy advocacy and financial support.

Thus, in order to gain the understanding and appreciation of the general public, the Department of Probation will have to make more strategic efforts to ensure as clear and concrete as possible outcomes to the probation programmes. So far, the Department has been successful in raising the visibility of probation treatment for drunk-drivers. The campaign was successful in sending out a clear message to the public that community services, such as working in hospital or providing care for victims of drunk-driving accidents, are more effective as a means to help the offenders to reconsider the impact of their action and refrain from repeating it, and thus a more effective enforcement of the law against drunk driving. The Court was also convinced to make more use of community service orders as alternatives to fines. More needs to be done to increase the visibility of probation work with respect to more types of offences.

C. More Effective Treatment Programmes

In order for the community-based treatment of offenders to become a viable alternative to incarceration there is urgent need for the Department of Probation to come up with effective programmes of treatment to ensure rehabilitation of offenders and reduction of reoffending. This requires a good system of risk assessment that allows probation and parole officers to effectively distinguish between the high and low risk groups of offenders and apply appropriate rehabilitation programmes that take into account public protection. In this connection, the Department of Probation should put more emphasis on designing effective offending behaviour programmes that enhance thinking or cognitive skills of offenders. There should also be more variety of programmes which should respond to the specific needs of each particular group of offenders, such as anger management, domestic abuse, sex offenders' programmes, etc. As most of the social issues and causes of crime become more and more complicated, there is a constant need for probation staff to improve their efficiency and to acquire new knowledge and skills so that they can cope better with more sophisticated demands when supervising and providing assistance to offenders that effectively addresses their problems at the fundamental level.

In the early days, especially when the Department of Probation was under the direct control of the judiciary, the main responsibility of probation officers was to prepare the so-called social inquiry reports for judges to use as pre-sentencing information. There was less emphasis on turning probation programmes into an effective alternative to the prevalent forms of punishment. So far, the Department of Probation has been successful in developing programmes specific to the treatment of drug addicts as well as drunk driving offenders. More customized treatments will be necessary for quality probation programmes of the future.

D. More Focus on Reintegration

At the heart of any quality treatment is the ultimate goal of reintegration of offenders into society. Measures must be tested and monitored for their effectiveness in terms of providing assistance to offenders so they can attain such a goal. With the reform of 2002, the task of ensuring smooth reintegration of offenders, under both parole and probation, is the responsibility of the Department of Probation. In reality, it is difficult for these socially disadvantaged groups to start a new life without further assistance with reintegration. It is thus important that more attention should be paid to aftercare services which will enable offenders to regain their reformative potential and self-improvement. In this connection, the Department

of Probation has recently applied the use of ‘halfway houses’ to help offenders in need of accommodation. Halfway houses are there to help them adjust and be prepared to get back to their families and communities. As a temporary accommodation, there are a variety of routine activities and programmes in the halfway houses, including occupational training, spiritual counselling, and various skill development programmes. In running the temporary residences, the Department of Probation attempts to integrate various sciences, local and traditional know-how, traditions, cultures, and religions altogether. Thus the halfway house can be considered a boundless work among the probation departments, religious institutes, and the community at large. Currently there are several halfway houses operated by the Department which are located in provinces such as Nakhon Sawan, Amnat Charoen, Maha Sarakham, Kamphaeng Phet, and Phatthalung, providing services for not only offenders under probation orders, but also drug addicts under diversion initiatives. It is important that the Department of Probation continues with this important initiative and puts greater effort into involving all stakeholders, including the community, in this significant mission.

E. More Embrace of Innovations

In many cases, innovative approaches to the treatment of offenders can prove very effective. Currently, Thailand is exploring a number of intermediate sanctions, including intensive probation, home detention, weekend detention, periodic detention or curfew, and electronic monitoring. If such a variety of innovative options are available, it is more viable to extend the use of alternatives to incarceration, such as probation, to a higher risk group of offenders. Additional innovative approaches might include pre-sentencing probation, assistance programmes for victims of crime, and the implementation of restorative justice measures. In this connection, it is necessary that there are amendments to the existing legal framework to incorporate these new sentencing options.

In response to the need to systematically embrace more innovative approaches, some might look for the establishment of a new agency to be responsible for the new demand. Still, in my opinion, it might be more productive to consider assigning such new missions to the Department of Probation, considering that its staff have had considerable real work experience and are equipped with the necessary fundamental knowledge and skills. Each probation officer, provided that they are properly trained, will have at least three significant qualifications, namely: 1) being knowledgeable with respect to law and the criminal justice system; 2) having good background knowledge of psychology and social welfare; and 3) having intensive work experience with all key stakeholders in the criminal justice process - police, public prosecutors, offenders, victims, or the members of the local community. Therefore, we only need to build more on the well-laid foundations.

F. More Partnership and Networking

The Department of Probation’s success in promoting public participation in the criminal justice process of Thailand has inspired decision-makers at the top policy levels to apply this model of volunteers and community justice networks to address other key criminal justice issues, especially to develop a community-based system of responses focusing on alternative dispute resolution and access to legal assistance. So far, the volunteer probation officers’ initiative, as well as the prototyped networking initiatives by the Department of Probation, has had great success in mobilizing public support for and understanding of the work of offender treatment, which results in more effective implementation of treatment programmes and after-release assistance programmes within the community. My experience in working to promote public participation in the treatment of offenders has confirmed the fundamental belief that direct engagement of the community members, either through the form of volunteer probation officers or a broader-based criminal justice network, is indispensable for the effective implementation of alternative treatments. It is the most efficient way to make use of resources within the local community, and other forms of social capital, to support probation work, as well as other functions relating to law and justice. In the context of Thailand’s political system, direct participation from the local community also contributes to on-going efforts with respect to decentralization of administrative power from the central government, as mandated by the Constitution. As present, there are over 6,700 *Tambon* Administration Organizations, the smallest units of local government, throughout Thailand, with increasing independence in terms of policy planning and budget management. The success in promoting community involvement in the treatment of offenders should be expanded to include the form of partnership agreements with these local administrations, which, in my opinion, will provide a more sustainable solution to the chronic problems of budget constraints and lack of support for assistance programmes for the reintegration of offenders into society.

VII. CONCLUSION

Community-based treatment in Thailand has come a long way since it was first introduced 30 years ago as an alternative to custodial treatment for adult offenders. It has become a well-accepted option for diversion of criminal cases from mainstream treatment programmes based on incarceration. There have been a number of new measures for specific groups of offenders to better serve their needs. Public participation and community engagement have become an integral part of a system where rehabilitation and reintegration are the ultimate goals. Some innovative measures, such as restorative justice with an emphasis on a role for the victim, have become increasingly popular. Finally, the working style where community networking and partnership are absolute ingredients of programmes has become the norm. All these are good signs for the sustainable development of the community-based approach.

Since its inception 30 years ago, now is perhaps the most crucial time for community-based treatment measures in Thailand. With stronger support at the policy-making level, and with more important tasks at hand, it is important that the Department of Probation, which shoulders the responsibilities of implementing community-based measures, puts great effort into monitoring and evaluating the outcome of such programmes, while maintaining the quality of work, despite rising demands. Through decades of hard work, the Department of Probation has been successful in introducing and firmly establishing the system of community-based treatment of offenders in Thailand. However, if these community-based alternatives to incarceration are to be more widely accepted and utilized, it is necessary that full support be urgently given to the Department of Probation. Viewed as a cheaper alternative, community-based treatment measures in many countries, including Thailand, are facing the same problems of chronic lack of funding and inadequate personnel resources. Although community-based options may in fact be a cheaper alternative, this does not mean that they can survive without adequate funding and support. To ensure successful results, it is necessary that due consideration be given to providing full support to probation work during this important period for continuing growth and maturity.

COMMUNITY-BASED ALTERNATIVES TO INCARCERATION

*Christine Glenn**



I. INTRODUCTION

This paper will concentrate in the main on community-based penalties but the account would be incomplete without the broader picture of sentencing and penal policy across the justice system in England and Wales.

II. GOVERNMENT POLICY

Government policy is that prison should be reserved for serious and dangerous offenders, and that others are normally better punished in the community. To this end, the Ministry of Justice has been working with the courts and others to try to bring down the prison population, which is at record high levels.

III. PURPOSES OF SENTENCING

Our whole sentencing framework was rewritten in the Criminal Justice Act 2003. For the first time, there was a statutory definition of the purposes of sentencing. These are (as set out in section 142 of that Act):

- The punishment of offenders;
- The reduction of crime (including its reduction by deterrence);
- The reform and rehabilitation of offenders;
- The protection of the public and;
- The making of reparation by offenders to persons affected by their offences.

This definition does not apply to offenders under 18 at the time of sentencing and certain categories of sentences for the mentally ill. Other than those few categories, the purposes of sentencing are now so defined.

IV. SERIOUSNESS OF THE OFFENCE

Whilst courts are obliged to have regard to these principles, sentences will generally be determined according to the seriousness of the offence. Seriousness is made up of:

- harm caused by the offence; and
- culpability of the offender in committing it.

There is also a presumption that recent and relevant previous convictions make an offence more serious. There are thresholds of penalty based on seriousness:

- offences that are so serious that only custody will represent a sufficient response;
- offences that are serious enough to warrant a community sentence.

If neither of these thresholds is reached then a fine or a discharge will be appropriate.

* Chief Executive, Parole Board of England and Wales.

V. COURT JURISDICTION

There are three types of offences:

- summary, which may only be tried in the magistrates' courts;
- indictable, often known as "either way", which may be tried in either the magistrates' courts or the Crown Court; and
- indictable only, which may only be tried in the Crown Court.

Penalty levels vary depending on the court trying the offence. The magistrates' courts may not impose more than six months' imprisonment for a single offence nor generally fine more than £5,000.

VI. FINES

Fines are available to punish all offences (other than where mandatory minimum sentences apply, such as for murder). In general, the maximum fine that can be imposed by a magistrates' court is defined in terms of level. There are five levels, currently set as follows:

- Level 1 £200
- Level 2 £500
- Level 3 £1,000
- Level 4 £2,500
- Level 5 £5,000

In practice, fine levels are generally much less than the maximum as courts must take account of offenders' means when deciding on the amount to impose. The Crown Court may fine an unlimited amount.

VII. COMMUNITY SENTENCES

Since the implementation of the Criminal Justice Act 2003, there has been a single community order for offenders aged 18 or over that can comprise up to 12 requirements depending on the offence and the offender. These are:

- unpaid work (formerly community service/community punishment) – a requirement to complete between 40 and 300 hours' unpaid work;
- activity – e.g. to attend basic skills classes;
- programme – there are several designed to reduce the prospects of reoffending;
- prohibited activity – requirement not do something that is likely to lead to further offences or nuisance;
- curfew – electronically monitored;
- exclusion – not much used as no reliable electronic monitoring yet available;
- residence – requirement to reside only where approved by probation officer;
- mental health treatment (requires offender's consent);
- drug rehabilitation (requires offender's consent);
- alcohol treatment (requires offender's consent);
- supervision – meetings with probation officer to address needs/offending behaviour;
- attendance centre – three hours of activity, usually on Saturday afternoons, between a minimum of 12 hours and a maximum of 36 in total.

Typically, the more serious the offence and the more extensive the offender's needs, the more requirements there will be. Most orders will comprise one or two requirements but there are packages of several available where required. The court tailors the order as appropriate and is guided by the probation service through a pre-sentence report.

VIII. BREACH

Offenders who commit more than one unacceptable failure to comply with the terms of a community order within a 12 month period are returned to court. If the breach is proven, the court is obliged to make

the order more punitive, or it may re-sentence, including to custody.

IX. CUSTODY

The picture on custody is complicated as there are different sentences for 18 to 21 year olds and for older adults; and depending on whether sentence is under the Criminal Justice Act 2003 or its predecessor, the Criminal Justice Act 1991.

Eighteen to 21 year olds are sentenced to detention in a young offender institution and older adults to imprisonment but to all intents and purposes here, they can be considered to be the same thing.

Maximum penalties are specified for all offences according to the seriousness of the offence. Generally, the maximum will fall into one of the following bands:

- 1 month
- 3 months
- 6 months
- 12 months
- 2 years
- 5 years
- 7 years
- 10 years
- 14 years
- life.

One of the characteristics of the criminal law in England and Wales is that offences are defined very broadly. Robbery, for example, can be the snatching of a bar of chocolate from one schoolboy by another or a multi-million pound gold bullion heist. Hence penalties tend to cluster much lower than the maxima.

X. SHORT SENTENCES – UNDER 12 MONTHS

Those sentenced to under 12 months (still made under the Criminal Justice Act 1991) spend the first half of their sentence in prison and are then “at risk” for the remaining period. This means they are under no positive obligations and do not report to the probation service but, if they commit a further imprisonable offence during the at risk period, they can be made to serve the remainder of the sentence in addition to the punishment for the new offence. The exception to this is those aged 18 to 21 who have a minimum of three months’ supervision on release.

XI. CUSTODY PLUS

The Criminal Justice Act 2003 sought to replace short sentences with custody plus, a new sentence that would comprise a short period (2 to 13 weeks) in custody followed by a period under supervision in the community (similar to a community order). This was because the recidivism rate for short sentences is particularly high and one of the reasons for that is because offenders receive no supervision or support on release. Resource constraints have prevented the introduction of this sentence, which remains on the statute book.

XII. SUSPENDED SENTENCE ORDERS

The government has implemented suspended sentence orders, which enable a court to suspend a sentence of up to six months for a period of up to two years subject to the successful completion of requirements in the community. The courts have used this substantially – we think to up-tariff from community sentences. As breach of a suspended sentence order leads very often to custody, this is having an unfortunate effect on the prison population. The government tried to legislate in the Criminal Justice and Immigration Bill to restrict the use of the order to indictable (including either way) offences but had to give up on account of lack of time for the parliamentary process. They will probably return to this in future legislation.

XIII. SENTENCES OF 12 MONTHS OR OVER

A. Criminal Justice Act 1991

The provisions of the 1991 Act for sentences of more than 12 months have been replaced by those of the 2003 Act but there are still some prisoners sentenced under the 1991 Act who are working their way through the system.

The 1991 Act created a distinction between short-term – those serving under four years – and long-term – those serving sentences of four years or over – prisoners.

Short-term prisoners are those serving between one and four years and spend the first half of their sentence in prison; the third quarter on licence and the final quarter at risk.

Long-term prisoners serving determinate sentences spend the first half of their sentence in prison and then may apply for parole to the independent Parole Board. Parole may be granted at any time between the half-way point and the two-thirds point of the sentence, and will only be granted if the Parole Board considers that the offender is a sufficiently safe bet to release. The test is that the prisoner will not commit a further offence of any kind within the parole window. The offender is on licence from the point at which he is released until the three quarter point of sentence and then at risk for the final quarter. In the Criminal Justice and Immigration Act 2008, the government legislated to treat long-term prisoners (as defined by the 1991 Act) who have been convicted for non-sexual non-violent offences as if they were standard determinate sentence 2003 Act prisoners. These provisions commenced on 9 June 2008 and apply only to prisoners who have yet to reach the half-way point of their sentence on that day.

Life sentences, as their name suggests, last for the remainder of the offender's life. When sentencing, the judge sets a minimum period – normally known as the tariff – that the offender must serve as a punishment before being considered for release. Once this minimum period has elapsed, the offender may be released by the Parole Board but only if it considers that to be an acceptable risk to public safety. The test is different from the one described above – here, the Board must decide whether the prisoner would commit an offence which would harm “life and limb” – this is usually a sexual or violent offence.

B. Criminal Justice Act 2003

The 2003 Act abolished the distinction between short- and long-term prisoners and instead created one between standard determinate sentences and public protection sentences.

Offenders sentenced to a standard determinate sentence serve the first half in prison and the second half in the community on licence. The at-risk period no longer applies.

Offenders convicted of a sexual or violence offence may be sentenced to a public protection sentence. In such cases, the court has to determine whether the offender is dangerous to the extent that he or she is likely to cause serious harm to the public through the commission of a further sexual or violent offence. If the court does consider that to be the case, it may impose a public protection sentence. There are three such sentences:

- life – which should be used where it is available by statute and where the particular crime warrants it;
- imprisonment for public protection (IPP) – where the maximum for the offence is ten years or more and where life is not available or appropriate. An offender sentenced to an IPP serves the tariff as set by the judge and then is eligible to be released if considered safe by the Parole Board. The only significant distinction between life and IPP is that, whereas life sentences last for the whole of the offender's life, the Parole Board can bring an IPP licence to an end after 10 years in the community following release;
- extended sentence – where the maximum for the offence is less than 10 years. An extended sentence comprises the normal custodial period plus an extension period. The offender may be released at any time between the half-way point and the end of the normal custodial period and is on licence until the end of the extension period.

The Criminal Justice and Immigration Act 2008 changed the provisions so as to give judges more

discretion over the use of public protection sentences; for use of public protection sentences to be restricted to offences for which two years' real time is justified; and for release from an extended sentence to be automatic at the half-way point of the custodial period with licence extending then until the end of the extension period. These changes apply to cases sentenced on or after 14 July 2008.

XIV. LICENCE

For the duration of the licence, an offender is obliged to comply with the terms of that licence. These may include requirements to report to the probation service, restrictions as to where he or she may live and what work he or she may undertake, and requirements to attend programmes. If an offender breaches his or her licence he or she is liable to recall to prison, potentially until the end of his or her sentence.

XV. EARLY RELEASE

Offenders serving under four years who meet various criteria may be released up to 4.5 months before they would otherwise be released, on home detention curfew, subject to an electronically monitored curfew.

Alternatively, offenders who meet other criteria may be released up to 18 days earlier than they would otherwise have been released on end-of-custody licence.

XVI. OFFENDER MANAGEMENT

Alongside these matters around sentencing, we must also consider offender management, now the job of the National Offender Management Service. The National Offender Management Model is said to be consistent with the best available evidence on what works in reducing reoffending.

This service encompasses both the probation and prison services, for the first time seeking to harmonize and co-ordinate sentence planning and management under a single umbrella. The principles are as follows:- Resources should follow risk – the evidence suggests that efforts should be focussed on those offenders who are at medium/high risk of reoffending;

- Supervisory practices should incorporate elements of pro-social modelling where the offender is actively engaged in the sentence and is motivated, supported and encouraged to change his or her offending behaviour;
- The relationship between the offender and the offender manager is critical with consistency of supervision promoting the development of a trusting working relationship;
- Supervision and referrals to other agencies for interventions should vary according to the assessed risk levels and needs of the offender; and
- Referrals to partner agencies can be beneficial for offenders with multiple needs and for offenders who would otherwise not have received community supervision. However, the evidence here is mixed.

The objective of the service is for the C's to be delivered – continuity, consistency, commitment and consolidation. Risk is then matched to resources using a tiering mechanism based on four approaches. Tier 1 is punish and includes monitoring and “signposting” to the offender. Tier 2 is Help and includes in addition helping and brokering support for the offender who will fit the low risk and low seriousness criteria. The help may be with health problems, accommodation, employment or learning skills, for example. Tier 3 adds an additional element of personal change on top of the Tier 2 elements and Tier 4 adds Control. These offenders may be regarded as dangerous and/or prolific, who need additional restrictions and controls to manage their risk.

More than half of community and suspended sentence orders ran their full course or were terminated early in the first quarter of 2008. But 36% of community sentences terminated for negative reasons and 1,860 offenders were in custody in August 2008 for breaching a court order. These numbers need to be considered alongside those for persons in prison for breaching their licence following release. In 2007/08, 11,756 determinate sentenced prisoners were recalled to prison – an increase of 5% on the previous year. In the same period, 926 parolees were recalled – a drop of 24% from 2006/07. The parole rate remained the

same at 36%. These figures show a continued trend of “back end sentencing” – a consequence of legislative changes and the increased focus and efficiency of the Probation Service in enforcement of licences.

XVII. RISK ASSESSMENT

Risk assessment is at the heart of offender management and underpins sentence planning, resource allocation, targeting of interventions designed to reduce reoffending and community supervision of offenders. It is defined as “The systematic collection of information to determine the degree to which harm (to self and others) is likely at some future point in time.”

For all involved in offender management, making a full and accurate assessment of risk is crucial to decision making. In understanding the boundaries of risk assessment, it must be recognized that the processes do not conform to an exact science and that no environment is risk-free. Assessment refers to the prediction of future reoffending (in the UK this is normally measured by reconviction) and the prediction of the harm, to both an offender and their victim, that reoffending is likely to cause.

Typically, risk assessment measures two types of risk factor- “static” and “dynamic” and methods of assessment are actuarial or clinical in nature. Static factors are the unchangeable historical characteristics of an offender – such as gender, age and previous criminal convictions associated with higher rates of reoffending. Actuarial risk prediction relies on assessment of these factors. It calculates the probability that an individual will reoffend based on the average reoffending rate calculated from a sample of offenders who match that individual on relevant static factors. Clinical risk prediction in contrast is less structured and relies on interviews and observations of social behavioural environmental and personality factor related to previous offending. These factors are considered dynamic in nature as they are amenable to change via treatment and offender management.

Both actuarial and clinical approaches are limited when used alone. Actuarial assessment cannot identify which offenders will go on to reoffend, merely into which group an individual falls. Clinical assessment can be more prone to bias as it relies upon judgment and can be influenced by an assessor’s opinion of the relative importance of different risk factors. A number of tools are available, many of which have been validated on UK populations and these are used as part of risk assessment processes. Some are actuarial, some clinical and others a combination of both. A number of tools predict specific types of reoffending, for example sexual or violent, others are designed for general application. The most prominent tool now used is the Offender Assessment System (OASys), which is used to assess risk of general offending, likely degree of harm and degree of need posed by an offender in a range of areas. Other widely used tools are Risk Matrix 2000 which predicts the risk of sexual reoffending and Historical Clinical List – 20 (HCR-20) which measures the risk of violent reoffending. Risk assessment in England and Wales is undergoing substantial re-development. The current OASys reoffending predictor will be replaced in the spring by a refined actuarial measure. The new measure scores on dynamic factors which research has shown to be most predictive of non-violent reconviction, such as drug misuse, and accommodation needs, which in addition to criminal history were the best individual predictors of non-violent reconviction. A separate actuarial predictor of violence will also be included and this will be used to form the basis for further judgments regarding risk of serious harm. A further tool is being piloted to examine dynamic risk factors for sexual offenders being managed in the community, building on the Stable and Acute 2007 tool developed in Canada.

XVIII. PROBATION SUPERVISION INCLUDING HIGH RISK OFFENDERS

The number of offenders starting community orders remains relatively stable – 33,200 started such a sentence in the first quarter of 2008. Fifty one percent of these community orders had just one requirement, 14% had 3 or more requirements. Three percent more offenders were being supervised under community orders on 31 March 2008 than a year earlier, up from 98090 to 101,250. Thirteen percent had no previous convictions or cautions – 18% had 15 or more.

The number of offenders starting pre- or post-release supervision increased by 4% to 11,870. The total number of offenders being so supervised was 97,080 at March 2008. This is an increase of over 22% from December 2002 and is largely a result of the changes brought in by the 2003 Act, which means

that offenders now spend longer on licence. High risk offenders are supervised under Multi-Agency Public Protection Arrangements (or MAPPA). These are arrangements set up locally to assess and manage offenders who pose a risk of serious harm. National guidance indicates the use of three levels of management. Level 1 involves ordinary agency management; Level 2 is where the active involvement of more than one agency is required to manage the offender. Most offenders assessed as high or very high risk of serious harm can be managed effectively at Level 2 where the management plans do not require the oversight and commitment of resources at a senior level. The highest level is Level 3 where it is determined that the management issues require conferencing and senior representation from the agencies. The few cases referred at Level 3 – sometimes known as the critical few – are those whose management is so problematic that multi-agency co-operation and oversight at a senior level is required, together with the authority to commit significant resources.

In 2007/08, there were 12,806 Level 2 and 3 offenders. During this period, 79 serious further offences were committed by these nominees. The major aim of MAPPA is public protection. Relevant agencies have a statutory duty to co-operate in the arrangements.

There is also the Prolific and other Priority Offender (PPO) Programme which targets those offenders who commit most crime in the area, or whose offending causes the most damage to the local community. The three strands of the programme aim to:

- Catch and convict offenders who commit most crime in their locality or whose offending causes most harm to their community. There is no standard national definition of PPO. Local areas devise their own selection criteria based on key principles set out in national guidance. PPO's are subject to intense police supervision;
- Rehabilitate and resettle: this involves working with offenders to stop their offending by offering a range of supportive interventions addressing identified needs and risks of further offending. The opportunity to rehabilitate is backed by a swift return to court if offending continues;
- Prevent and deter: to stop the most active young offenders escalating into tomorrow's prolific offenders through youth justice interventions and continued post-sentence support.

Recent research supports a positive assessment of the PPO programme. A comparison of total convictions before and 17 months following the programme showed a 43% reduction by PPO offending, and a comparison from the start of the scheme to 17 months after the start showed a 62% reduction in convictions and a sharp reduction in PPO offending following entry on to the scheme. These reductions cannot necessarily be attributed to the PPO programme as we do not know what would have happened to these offenders had the scheme not been introduced.

A new initiative is integrated offender management, the aim of which is to reduce reoffending. It approaches target offenders in the community who present the highest risks to their communities, especially those short sentence offenders released from prison with no statutory supervision. There are five pilot areas. No evaluation has yet taken place but research is being built into the pilots which were announced in July 2008 and which will run for two years. The schemes are multi-agency partnerships.

XIX. SENTENCE DISPOSAL PATTERNS

Fines are the most common disposal with 941,500 handed out in 2007 – accounting for 66.6% of all sentences. Community sentences accounted for 196,400 cases: 13.9% of all sentences, up 3% from 1997. Immediate custody was given to 6.7% (95,200), up from 93,800 in 1997, but a similar proportion of all sentences. This does not tell the whole story. Use of the fine for indictable offences has dropped dramatically in the last 10 years – falling from 27.6% in 1997 to 15.8% in 2007. Over the same period, the use of community sentences for these offences has risen by 5.3% to 33.7%. The immediate custody rate for indictable offences has remained relatively stable over the past decade, rising slightly from 22.5% to 23.7% in 2007. This does point to the increase in breach and recall numbers being at the heart of the increase in the prison population. In 2007, almost 136,000 were sentenced to custody, immediate and suspended – the highest figure in a decade and up 40% on 1997 numbers. Other disposals include conditional discharges (94,100 in 2007), absolute discharges – 11,000 over the same period down from 18,200 in 1997 and compensation orders – 165,900 in 2007.

The fine became a less popular disposal from the 1990s as enforcement became less effective. Much effort and investment went into improving enforcement and this has paid off in results. In 2007/08, the new amount of fines imposed was £376 million (including transferred fines from previous years). In the same year, £256 million was collected and £106 million was cancelled. The paid and cancelled amounts do not necessarily relate to the fines imposed in that year but could be collected against any fine outstanding regardless of age. The fine has started to be restored as a credible sentence as a result of the efforts to improve enforcement which have resulted in a steady year on year rise in payment rates since 2003 – from 73% in 2003/04 to 90% in 2006/07. In the six years to 2006, there has been a 23% reduction in the number of offences committed by offenders within one year of commencing a court order under probation supervision. In 2006, 36% of offenders commencing a court order under probation supervision committed at least one offence in the following year – down from 40% in 2000. In this period, there has been no change in the number of most serious offences committed within a year by offenders commencing court orders under probation supervision.

Similar trends emerge from those released from prison. In the same six years, there has been a 15% reduction in the number of offences committed by offenders within one year of discharge from custody. In 2006, 46% of offenders released from prison committed at least one offence the following year – down from 51% in 2000. The greatest reductions have been made with offenders sentenced to over one year in prison – over 40% in terms of the number of offences committed.

XX. PROBLEMS AND CHALLENGES OF COMMUNITY-BASED SENTENCES

The first problem – and the most important – is that of public confidence in these sentences, which can be seen as soft options. The British Crime Survey (BCS) shows that crime has fallen by 10% in the last year, representing a million fewer crimes. Police recording of crimes has improved while victim reporting of crime has remained fairly stable since 1997.

Despite this, high numbers of people believe that the crime rate has risen. People have more positive perceptions of crime in their own area than nationally – 65% thought that crime in the country as a whole had increased in the past two years compared with 39% who thought that crime in their home area had increased.

Sentencing has become more complex over recent years. When I appeared before the Parliamentary Public Accounts Committee last October, one MP asked me for a definition of honesty in sentencing – I replied that this was about a sentence being clear and transparent and readily understandable to all. The legal labyrinth which sentencers have to navigate and which practitioners then have to enforce makes such a concept aspirational. If I had a magic wand, I would use it to clarify sentencing so that people understood it. This lack of understanding is in my view the biggest barrier to improving public confidence in the system. Unfortunately, the media does little to help.

We must not underestimate the media influence on public confidence. The trend now seems to be about blame and scapegoats when things go wrong – as they inevitably will. I am certainly not suggesting even for a moment that officials and agencies should not be accountable – but trial by television or newspaper in the absence of many of the facts is not the most mature way of proceeding in these cases. Sadly, in the UK, the public does not accept the facts about the fall in crime and often, according to research polls, regards published statistics as at best incomplete and misleading, and at worst dishonest. This research indicates that people are more likely to believe local rather than national estimates. This is not a quick fix cure but it is not enough to look only internally and not engage and try to inform the community about your work – and to agree to some press interviews and coverage to try and balance reporting where possible.

I go back to my magic wand. I would also use it to put in place an IT system that was common across the criminal justice agencies and which would enable good research to be carried out, as well as for information to be effectively shared. The public just can't understand why, for example, one police service has information that isn't accessed and acted on by police in another area and which may have prevented a high-profile offence.

There is also the issue of judicial confidence – it is vital that the judiciary is independent and is seen to be so. Some parts of the 2003 Act – notably the IPP sentence – were crafted so as to take away judicial discretion and when judges did what they had to do in following the statute with unfortunate consequences, there was public criticism. It has taken over three years for the worst excesses of this sentence to be put right by the 2008 Act. What is a great advance is that in those years there is now a proper agreement between the Secretary of State for Justice and the Lord Chief Justice – the concordat. Communication and understanding have greatly improved and this bodes well for the future.

And then there are resources. We were already facing budget pressures before the downturn in the global economy. All interventions require funding. Our prison population is estimated to increase to between 83,400 and 95,800 by 2015. Community orders too are projected to go up to 258,500 by 2010/11. The increase in knife crime and the expectation to prosecute rather than caution these offenders and for sentencing tariffs here to increase may increase these estimates further. The impact of increased radicalization as well as the impact of technology on crime will also be challenges. What impact will the credit crunch have on crime too?

What has been encouraging is the success of partnership work between agencies. I spoke earlier about MAPPA and integrated offender management as well as the provisions for dealing with the persistent and prolific offender. There are other such partnerships – crime and disorder reduction partnerships and community safety partnerships. These are locally based and involve local government, listening to local people and aiming to be responsive to local needs and make local people feel safe in their communities. There are moves to build on the work so far, including having directly elected chairs of these partnerships and scrutiny committees which will provide people with a way to influence their local police service and hold it to account.

There are also unique opportunities – such as UNAFEI courses and seminars – where we get the opportunity to learn and understand what is happening elsewhere, what has been successful and what has not. This should enable us to make the best possible use of resources as these come under increased pressure.

IMPROVING THE TREATMENT OF OFFENDERS THROUGH THE ENHANCEMENT OF COMMUNITY-BASED ALTERNATIVES TO INCARCERATION: THE PHILIPPINE EXPERIENCE

*Ismael Juanga Herradura**



I. INTRODUCTION

A. Background

In the Philippines, the treatment of offenders and individuals who are in conflict with the law is undertaken by the government through the Department of Justice (DOJ), the Department of the Interior and Local Government (DILG), and the Department of Social Welfare and Development (DSWD).

The DOJ supervises and manages the national penitentiaries (for prisoners serving the penalty of imprisonment for more than three years) through the Bureau of Corrections (BuCor). There are at present seven national penitentiaries with a total population of approximately 40,000 inmates. Through the Board of Pardons and Parole (BPP) and the Parole and Probation Administration (PPA), the DOJ formulates, implements and monitors programmes and activities for offenders on probation and parole, and those granted conditional pardon with parole conditions through executive clemency by the President. As of December 2008, the PPA was supervising 34,796 probationers, 13,762 parolees and 852 pardonees, or a total of 49,410 clients, through its 15 regional offices, 99 provincial field offices and 128 city field offices, or a total of 227 field unit offices.

The DILG, through the Bureau of Jail Management and Penology (BJMP), supervises and controls city, municipal and district jails. The Philippine National Police (PNP), also under the supervision of the DILG, manages the municipal jails that cannot yet be supervised by the BJMP, including lock-up jails or precinct jails that are used as temporary detention centres for arrested individuals under investigation. The Offices of the Provincial Governor, also under the DILG, manage the provincial jails which, by law, keep convicted offenders with prison sentences that range from six months and one day to three years. In all, there are 79 provincial jails, 25 sub-provincial or extension jails, 135 district jails, 85 city jails and 1,003 municipal jails nationwide.

The DSWD operates and monitors rehabilitation centres nationwide for juveniles in conflict with the law (JICL) whose cases are still pending in court. There are 11 rehabilitation centres for JICL in the country. For the calendar year 2008, DSWD served a total of 1,532 CICL/youthful offenders comprising 1,416 males and 116 females.

As described, it is the PPA that is given the task of treatment of offenders through community-based programmes of probation, parole and/or conditional pardon. The BPP is simply concerned with policies on the grant of parole and on the recommendatory measures to the President in cases of executive clemency. Upon the grant of parole or conditional pardon, the offender is referred by the BPP for supervision to the PPA. Offenders on probation are referred by the courts of justice.

B. Purpose of the Paper

In the hope of enhancing clarity, simplicity and focus in presentation, the paper will attempt to:

1. Describe the current situations, problems and challenges in the treatment of offenders who are under probation, parole or conditional pardon;

* Administrator, Parole and Probation Division, Department of Justice, Philippines.

2. Present the measures to improve the treatment of offenders through the enhancement of community-based alternatives to incarceration; and
3. Present the highlights of other community-based alternatives outside the jurisdiction of the Parole and Probation Administration.

C. Legal Bases

1. Probation

Adult probation as a post-sentencing disposition was adopted in the Philippines on 24 July 1976 under Presidential Decree No. 968. Section 2 of the Decree enumerates the purpose of the law, as follows:

- a. Promote the correction and rehabilitation of an offender by providing him with individualized treatment;
- b. Provide an opportunity for the reformation of a penitent offender which might be less probable if he were to serve a prison sentence; and
- c. Prevent the commission of offences.

Of special interest is Section 28 of the law which provides that “to assist the Probation (and Parole) Officers in the supervision of probationers, the Probation Administrator may appoint citizens of good repute and probity to act as probation aides.”

2. Parole

The purpose of Act No. 4103, as amended, otherwise known as the Indeterminate Sentence Law, is “to uplift and redeem valuable human material to economic usefulness and to prevent unnecessary and excessive deprivation of liberty.” Under Section 5 of said Act, it is the duty of the Board of Pardons and Parole to look into the physical, mental and moral record of prisoners who have served the minimum of their prison sentence and to determine the proper time of release of said prisoners on parole.

3. Conditional Pardon

Under Section 19, Article VII of the Philippine Constitution, the President may grant executive clemency with the objective of preventing a miscarriage of justice or correcting a manifest injustice. Such grant may be exercised by the President *motu proprio* or upon recommendation of the Board of Pardons and Parole or of any other agency. Conditional pardon may be extended to a prisoner who has served at least one-half of the minimum of the original indeterminate and/or a definite prison term.

D. Organizational Mandate of the Parole and Probation Administration

1. Vision Statement

A model component of the Philippine correctional system that shall enhance the quality of life of its clients through multi-disciplinary programmes and resources, an efficient organization, and a highly professional and committed workforce in order to promote social justice and development

2. Mission Statement

To rehabilitate probationers, parolees and pardonees and promote their development as integral persons by utilizing innovative interventions and techniques which respect the dignity of man and recognize his divine destiny.

3. Goals

The Administration sets to achieve the following goals:

1. Promote the reformation of offenders and reduce the incidence of recidivism; and
2. Provide a cheaper alternative to the institutional confinement of offenders who are likely to respond to individualized, community-based treatment programmes.

4. Organizational Outcome

Rehabilitation of Offenders in a Community-Based Setting and Reduction of Crime Incidence.

II. CURRENT SITUATIONS, PROBLEMS AND CHALLENGES

A. The Treatment Paradigm



Figure 1. PPA's Harmonized Rehabilitation Programme

As shown in Figure 1, the PPA treatment paradigm has three major components: 1) Restorative Justice (RJ) as the philosophical foundation or conceptual framework, represented by the frame and handle of the umbrella; 2) Therapeutic Community (TC) as treatment modality, represented by the panelled canopy of the umbrella showing the distinct but overlapping treatment categories, namely: behaviour shaping/behaviour management; emotional/psychological aspects; intellectual/spiritual aspects; and vocational/survival skills; and 3) the Volunteer Probation Aide as the lead community resource, represented by a figure holding up the umbrella in co-operation with the Probation and Parole Officer. The umbrella matrix also highlights the extension of support to both victim and offender and their respective families/communities in the overall spirit of reconciliation and healing.

1. Restorative Justice Practices as Adopted by the PPA

By way of Memorandum Order No. 12, S.2003, dated 16 July 2003, the PPA promulgated a policy on adopting RJ practices as a major component of its treatment programme.

The Agency policy defines RJ as a philosophy and a process whereby stakeholders (offender, victim and the community) in a specific offence resolve collectively how to deal with the aftermath of the offence and its implications for the future.

As a philosophy, RJ treats crime as a violation of people and relationships. It creates obligations to make things right through involvement of the victim, the offender and the community in searching for solutions which promote repair, reconciliation and reassurance (Van Ness quoting Zehr, 2002).

As a process, RJ resolves conflicts in a manner in which the response to the crime would be not to add to the harm caused by imposing further harm on the offender, but to do as much as possible to restore the situation. The community offers aid to the victim; the offender is held accountable and required to make reparation. Attention would be given not only to the outcome, but also to evolving a process that respects "the feelings and humanity of both victim and the offender" (Martin Wright, quoted by Van Ness, 2002). Thus, its application entails meetings or a series of meetings attended by all stakeholders – the offender, the victim/s and the members of the community. RJ seeks to achieve the following: 1) reparation for the victim; 2) reconciliation of the offender, the offended and the community; 3) reassurance to the offender that he or she can be reintegrated into society; and 4) enhancement of public safety by activating the offender, the victim and the community in prevention strategies.

The PPA's choice of RJ as a conceptual framework of its rehabilitation programme is an affirmation of a

practice that began in 1978 upon the operationalization of the substantive provisions of the Probation Law. The consultation of the offended party and the community upon the offender's petition for probation was a requirement for investigating probation officers on the basis that the inputs of the offended party, the petitioner's family and some responsible members of the community could be very critical in the release and reintegration of the offender in the same community where he or she committed the offence. Moreover, the theory and practice of RJ is very indigenous in Philippine culture which, historically, maximizes the use of mediation and conciliation in solving community conflicts. This is highlighted by the adoption of the *Katarungang Pambarangay (Barangay Justice System)* in settling disputes at the village level.

The operationalization of RJ in the community is best illustrated through the "Circle of Support" which was used by the VPA Field Training Laboratory (FTL) team in a village of San Pedro, Laguna. Please refer to Appendix A for the full-length copy of the article entitled "The Circle of Support: RJ in Community Engagement and Volunteer Resource Development" by Cecilia G. de la Cruz, Chief Facilitator, National Field Training Laboratory, PPA.

In the main, the RJ practice generally proceeds in the following manner:

(a) Investigation Stage

The investigation conducted by the Probation Officer includes the statement of the victim/offended party and of the general community towards the crime, the offender and suggestions for his/her/its reparation. At this stage, the investigating officer tries to ascertain the victim's readiness for reconciliation with the offender and the community as well as the community's capacity to provide support.

(b) Supervision Stage

The offender's supervision treatment plan (STP) shall include the need for RJ intervention as may be needed and appropriate. The RJ process may proceed in this way:

- 1) The parties should be brought within the programme of their own free will. Parties should have the right to seek legal advice before and after the restorative process.
- 2) Before agreeing to participate in the restorative process, the parties should be fully informed of their rights, the nature of the process, and the possible consequences of their decisions.
- 3) Neither the victim nor the offender should be induced by unfair means to participate in restorative justice processes or outcomes.
- 4) Where no agreement can be made between the parties, the case should be withdrawn from the restorative process.
- 5) In the event agreement is reached by parties, it should be put in writing to give substance/essence to the agreement. The failure to implement any provision of the agreement made in the course of the restorative process is a basis for the withdrawal of the case from the programme; and
- 6) Discussions and disclosures made during the process shall be treated with strict confidence and shall not be disclosed and used against the parties involved.

2. Outcome of the RJ Practices and Processes as Components of the PPA Programme

As shown in Table 1, the RJ practices used by PPA include mediation and conferencing, specially the "Circle of Support." The outcomes centered largely on the conduct of Community Work Service (CWS) for clients, the payment of civil liabilities by the offenders and, in certain instances, the reconciliation between the clients and their respective victims.

These results suggest that through these RJ practices adopted by PPA field offices, the clients, the offended party and the community are able to see their respective roles in reconciling and restoring broken relationships. In this context, all the stakeholders have heightened their sense of responsibility and accountability in pursuing an attitude that is inclined towards restoration and healing, rather than punishment and revenge.

THE 141ST INTERNATIONAL SENIOR SEMINAR
VISITING EXPERTS' PAPERS

Table 1. Status Report on Restorative Justice Outcomes (CY 2008)

Region	Total Supervision Caseload	RJ Process Used			Numbers Involved		Outcome
		Mediation	Conferencing	Circle of Support	Clients	Victims	
I	2,139	24	15	18	87	94	CWS of 56 clients; 13 clients paid; CL of PhP59,809
II	1,046	19	32	0	47	50	CWS of 40 clients; partial payment of CL by 9 clients
III	2,592	45	40	12	50	37	CWS of 45 clients; 45 paid CL of PhP147,569
IV	5,897	45	77	10	348	128	CWS of 191 clients; 49 clients paid PhP8,000
V	2,270	13	27	1	72	37	CWS of 37 clients
VI	4,193	56	70	13	305	226	CWS of 126 clients; 35 clients paid PhP1,500
VII	5,276	14	43	0	193	128	CWS of 190 clients; 25 clients paid CL of PhP520,243.10
VIII	2,748	5	15	0	171	48	CWS of 159 clients
IX	1,622	15	105	0	382	16	CWS of 290 clients
X	3,367	28	8	0	70	53	CWS of 15 clients; Rest. – 9
XI	2,265	24	34	1	110	69	CWS of 30 clients; Rest. – 5
XII	1,549	2	23	0	27	24	Reconciliation of 2 clients with victims
XIII (CARAGA)	1,416	2	5	0	62	23	CWS of 36 clients; 3 clients paid CL
CAR	699	6	16	2	27	22	CWS of 10 clients; dropping of countercharges of client
NCR	12,331	14	11	8	35	22	CWS of 5 clients
TOTAL	49,410	312	521	65	1,986	977	

B. The Therapeutic Community (TC) as a Treatment Modality

TC is a specialized self-help learning treatment modality founded on such precepts as “responsible love and concern,” “honesty,” “humility,” “forgiveness,” “pride in quality,” “no free lunch,” and others. Its overall goal is to move the client from “wrong living” to “right living.”

The adoption of TC as the treatment modality in PPA's community-based programme began in 1998 after a series of training programmes conducted by Daytop International, Inc. New York, through funding from the Bureau of International Narcotics and Law Enforcement Affairs (INL), U.S. Department of State. A total of 141 PPA officials and personnel in three batches completed the training.

Efforts were made to suit the treatment modality to the needs of Filipino clients, without disturbing the essence and structure of the modality. Thus, the graduates of the Daytop programme led by the respective RDs/ARDs formed committees and conducted echo seminars in their respective regions. A national Committee was organized and tasked to come up with training modules, session plans, and other training materials to be used.

For calendar year 2008, the TC action plan centered on five areas, namely: 1) programme implementation; 2) capacity-building; 3) programme and materials development; 4) social marketing; 5) resource generation; and 6) monitoring and evaluation.

1. Outcome of TC Implementation

As of September 2008, substantial accomplishments were reported and monitored by the 15 regional offices, as presented in Table 2.

Table 2. Status of TC Implementation (as of September 2008)

Region	Field Offices Involved		Clients Involved	
	Number	%	Number	%
I	7/13	54	342/2,139	15.99
II	9/9	100	459/1,046	43.88
III	13/14	92	334/2,592	12.88
IV	27/27	100	1,081/5,897	18.33
V	11/14	78	658/2,270	28.97
VI	26/26	100	1,590/4,193	37.92
VII	21/21	100	1,309/5,276	24.81
VIII	12/12	100	398/2,748	14.48
IX	11/13	84	209/1,622	12.88
X	16/16	100	1,158/3,367	34.39
XI	12/12	100	194/2,265	8.56
XII	12/12	100	528/1,549	34.08
XIII	9/9	100	452/1,416	31.92
CAR	8/8	100	370/699	52.93
NCR	21/21	100	1,205/12,331	9.77
TOTAL	215/227	94	10,287/49,410	20.82

Table 2-a. Status of Capacity-Building in TC (as of September 2008)

Region	Training/Activity Title	Participants			Funding Source
		PPOs	VPAs	Total	
I	1. Demonstration Training on Drug Testing	3	-	3	Donation from officers Local government units (LGU) PPA Regional Office funds
	2. Basic Training on TC for VPAs		29	29	
	3. Review of Materials and Roles in TC Implementation	17	-	17	
	4. Refresher Course on Drug Testing	25	-	25	
	5. TC Trainers' Training	7	5	12	
II	1. Basic Training for VPAs	8	11	19	Regional funds Donation from officers
III	1. TC Reorientation Seminar	53	3	56	Regional funds
	2. TC Basic Training for Implementers	11	-	11	
	3. Specialized Training on TC, RJ and Volunteerism	-	60	60	
IV	1. TC Training for VPAs	-	33	33	Regional funds

THE 141ST INTERNATIONAL SENIOR SEMINAR
VISITING EXPERTS' PAPERS

V	1. Orientation on the TC Programme 2. Family Therapy Trainers' Training	8 2	- -	8 2	LGU funds NGOs
VI	1. Orientation on VPA Organization and TC Programme 2. Refresher Course on Drug Testing 3. Managing Resistant Clients and Case Conferencing 4. Orientation Seminar on TC	2 54 25 -	21 - - 19	23 54 25 19	Regional funds LGU funds Donation from officers and VPAs
VII	1. Cluster Meeting on PPA Community-Based Programme 2. Residential Training on TC	325 -	2 7	327 7	LGU funds Donation from officers And VPAs
VIII	1. TC Orientation Seminar for VPAs 2. Information Dissemination on TC	- 3	132 46	132 49	LGU funds
IX	1. Residential Seminar on TC (Orientation Phase) for Clients 2. TC Training for VPAs	- 2	4 25	4 27	Regional funds LGUs Donation from officers
X	1. Regional TC Committee Meeting 2. Educational Trip to Cocoon Drug Rehab Center 3. TC Enhancement Training	6 15 43	- - -	6 15 43	Regional funds
XI	1. Orientation Seminar on TC for Parents of Clients 2. Phase One 5-day Residential Training 3. Specialized Training on RJ and TC for VPAs 4. Cluster Meeting for TC Concerns	8 8 5 11	3 2 19 -	11 10 24 11	Regional funds LGUs
XII	1. TC Orientation Course 2. Seminar on Life Skills for Drug Prevention	- 32	3 -	3 32	Regional funds
XIII	1. Realigned TC Seminar 2. Seminar on Life Skills for Drug Prevention	17 34	4 -	21 34	Regional funds LGUs
CAR	1. TC Enhancement Training	39	-	39	Regional funds
NCR	1. TC Enhancement Training 2. Seminar on Management of Drug Cases 3. Orientation on TC	57 3 3	- - 25	57 3 28	Regional Funds LGUs

Under the Programme and Materials Development component of the TC Action Plan, the following were accomplished:

1. Translation of Programme Materials into Filipino and other local languages;
2. Preparation of session plans, visualization exercises, and other teaching aids such as songs, games, etc;
3. Production of other IEC materials for information drives;
4. Designing an evaluation questionnaire for programme monitoring and evaluation.

With regard to social marketing, the accomplishments included the following:

1. Formal information drive using print and media, integrating the three components of the PPA programme of TC, RJ and VPA;
2. Symposiums/Forums in schools and villages;
3. Organization of Family Associations;
4. General assembly of clients and immediate family members;
5. Meeting with the Anti-Drug Abuse Councils, Provincial/City/Municipal Development Councils, Peace and Order Councils/Members of the other pillars of the criminal justice system;
6. Publication/distribution of newsletters/primers on the programme;
7. Integrating the programme in community-service projects like tree planting, cleanliness drives, sports festivals, and the like;
8. Extending assistance, specifically on training, to other agencies such as the LGUs, BJMP, DOH and DSWD upon their request.

Under the Resource Generation component of the Programme, the following accomplishments were reported:

1. Submission of proposals to LGUs for financial/technical assistance;
2. Co-ordination with community resources, for use of seminar venues for free or at discounted rates;
3. Fund-raising activities with the help of VPAs and other community partners;
4. Review of the Memorandum of Agreement with DSWD, DILG, NAPOLCOM, PNP, NPS, PNVSCA, *Liga ng mga Barangay*, VSO-Bahaginan, Rotary Club, Lions Club and PAVE; and
5. Top level advocacy with the Department of Budget and Management for an additional budget for the Programme.

As to monitoring and evaluation, the following activities were undertaken:

1. Improvement of the Agency's reporting system;
2. On-site observation of the rehabilitation programme in randomly selected field offices;
3. Revision of the Performance Evaluation System to give due weight to the PPA Rehabilitation Programme.

C. The Volunteer Probation Aides (VPAs) as the Lead Community Resource

The enlistment and training of VPAs started in 1977 while the Agency was preparing for the operationalization of the national probation programme which was to begin on 3 January 1978.

Towards 1980, the VPA programme dwindled from around 2,123 VPAs to only 100, due to budgetary limitations in the reimbursement of travelling expenses.

Beginning in 2003, through the technical and financial assistance of UNAFEI, PPA revitalized its VPA system with due consideration of its past experience. Later, with the support of JICA, a three-year In-Country Training Programme on the Holistic Approach to Volunteer Resource Development was undertaken from 2006 to 2008. The Project was extended for another two years as a technical co-operation project until 2010.

D. VPA Programme Objectives

In light of the provisions of Executive Order No. 468 of the President of the Philippines, promulgated on 11 October 2005, directing the PPA to revitalize its VPA programme and as enunciated in the Policy Guidelines on the VPA Programme of the Agency, duly approved by the Secretary of Justice on 26 October 2006, the following objectives are pursued:

1. To amplify the extent of services rendered to clients in an effective yet economical means through the use of volunteers;
2. To develop a competent corps of VPAs who will assist the PPA officers in the effective supervision of clients;
3. To inculcate greater citizen awareness and understanding of the criminal justice system;
4. To enhance community participation in crime prevention, treatment of offenders and criminal justice administration; and
5. To foster an attitude of meaningful involvement in the social, economic, cultural and political affairs of the community.

E. Functions and Responsibilities of VPAs

A VPA is expected to perform the following functions:

1. Work in close consultation and co-operation with the Supervising PPO;
2. Keep all information about the client in strict confidentiality;
3. Maintain an honest recording and monthly reporting of activities to the Supervising PPO;
4. Devote substantial and quality time for supervision of clients and perform the following tasks:
 - 4.1 Offer advice and guidance;
 - 4.2 Act as job placement officer;

THE 141ST INTERNATIONAL SENIOR SEMINAR
VISITING EXPERTS' PAPERS

- 4.3 Refer clients to pertinent agencies for spiritual, mental, economic, social or health needs;
- 4.4 Implement treatment objectives as provided for in the supervision treatment plan; and act as a resource individual;
- 5. Endeavour to help the PPO in extending RJ interventions to the client's situation; and
- 6. Attend TC, RJ and other activities as may be required.

F. The Roles of VPAs

The role of the VPA may be classified into two categories:

1. Direct Supervisor

The VPA should undertake the following:

- 1.1. Supervise a maximum of five clients at any given time;
- 1.2. Work Closely with a PPO and discuss the treatment plans and status of clients; and
- 1.3. Submit a monthly accomplishment report to the PPO.

2. Resource Individual

The VPA may act as a:

- 2.1 Resource speaker during training activities, information drives, etc.;
- 2.2 Counsellor;
- 2.3 Donor, sponsor or resource manager during fund-raising activities;
- 2.4 Programme co-ordinator of client activities; and a
- 2.5 Mediator, RJ Implementer, TC Facilitator.

G. Current Status of VPA Programmes

Tables 3-a, 3-b, and 3-c present the current status of the VPA programme in the Philippines:

Table 3-a. Number of Appointed VPAs Given Training

Region	No. of VPAs Appointed	No. of VPAs Trained	% Trained
I	298	277	93
II	242	129	53
III	1,154	605	52
IV	1,283	852	66
V	138	109	79
VI	725	550	76
VII	671	555	83
VIII	346	219	63
IX	435	308	71
X	388	216	56
XI	288	189	66
XII	223	150	67
XIII (CARAGA)	318	92	29
CAR	297	196	66
NCR	562	249	44
TOTAL	7,368	4,696	64

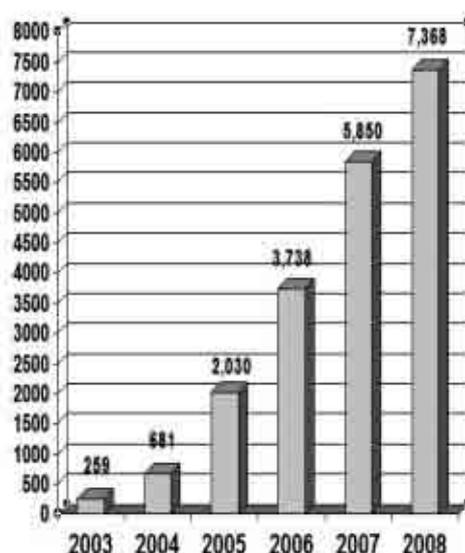
Table 3-b. Number of VPAs with Clients and Number of Clients Served (CY2008)

Region	No. of VPAs with Clients	No. of Clients Served
I	38	185
II	95	185
III	191	384
IV	317	1,051
V	94	303
VI	360	783
VII	170	846
VIII	69	192
IX	239	461
X	216	821
XI	129	452
XII	146	582
XIII (CARAGA)	113	346
CAR	109	200
NCR	116	337
TOTAL	2,402	7,128

Table 3-c. Total Number of Members per VPA Association

Region	No. of Association	No. of Members
I	12	61
II	7	102
III	13	803
IV	11	498
V	6	96
VI	20	424
VII	15	521
VIII	6	281
IX	7	371
X	5	108
XI	9	217
XII	4	97
XIII (CARAGA)	8	135
CAR	7	205
NCR	1	312
TOTAL	131	4,231

Figure 2. Growth of the PPA Programme, 2003-2008



1. Problems and Challenges

In a survey conducted in February 2008 by the Strategic Pathway on Harmonized Rehabilitation Programs, aimed at finding out how far along the 227 field offices were in the harmonized implementation of the TC, RJ and VPA components of the programme, it was revealed that TC obtained the highest score in implementation, VPA second and RJ a close third. Using a self-evaluation questionnaire, the respondents were asked to rate his or her office implementation of the programme through a 10-point scale with 1 as the lowest and 10 the highest. The summary of findings showed that, on the issue of sustainability, the average score ranged from 6 to 8, which was interpreted to be “good enough”, for starters. On the degree of harmonization, very few field offices gave equal attention and emphasis to all the three programme components. One reason advanced by the Study Committee was the issue of control and focus. Specifically, it was pointed out that in TC, the field officer/implementer deals primarily with the client over whom he/she has lot of control. In the VPA agenda, the implementer does not have as much control as in TC, including the fact that VPAs’ grasp of the programme might not be that full yet. In RJ, the implementer deals with some stakeholders over whom he has little control and who might be lukewarm or indifferent to the programme, if not downright hostile.

Table 4. Comparative Performance of Field Offices in the Implementation of the Rehabilitation Programme

Region	SCORE		
	Low	Middle	High
I	No data	No data	No data
II	RJ 6.176	VPA 7.277	TC 8.778
III	RJ 7.400	VPA 7.700	TC 8.200
IV	VPA 6.380	RJ 6.670	TC 8.720
V	No data	No data	No data
VI	RJ 6.460	VPA 7.310	TC 7.420
VII	VPA 7.200	RJ 7.650	TC 8.100
VIII	VPA 4.545	RJ 4.545	TC 6.500
IX	RJ 6.800	TC 7.000	VPA 7.700
X	VPA 5.640	RJ 6.000	TC 7.710
XI	RJ 6.550	VPA 7.270	TC 7.910
XII	RJ 4.700	VPA 6.300	TC 7.200
XIII (CARAGA)	RJ 6.000	VPA 8.000	TC 8.000
CAR	RJ 6.286	VPA 7.000	TC 8.143
NCR	RJ 6.710	VPA 7.290	TC 8.950

The Study Committee advanced its interpretation of the findings as follows:

2. Why TC Got a High Rating

The reasons given for the rating given to TC were:

1. Belief in the effectiveness of the programme;
2. Availability of manuals and other training materials;
3. Adequate training and commitment of implementers;
4. Programme is well-structured, continuous and with definite schedules;
5. Involvement of VPAs; full support of the community; financial support of LGUs; and
6. An effective monitoring system.

3. Why VPA Got a Moderate Rating

The moderate score given to the VPA programme was due to the following reasons:

1. Inability of some VPAs to fix a common time for meetings, training, etc. due to other tasks;
2. Funds for VPA training and travel are not easily available;
3. Minimal community support; ineffective recruitment strategy; and
4. Inadequate training and commitment and strong resistance of some implementers.

4. Why RJ Obtained a Low Rating

Below were the reasons given for the low rating given to RJ:

1. Inability of many clients to participate in RJ processes, including the payment of civil liabilities, due to poverty, distance of residence, and fear;
2. Non-participation/lack of co-operation of victims due to antagonism, distance, cultural barriers, and general conditions of peace and order;
3. Lack of personnel and a heavy caseload vis-à-vis RJ as a long and tedious process needing a lot of preparation;
4. Inadequate training for implementers; programme guidelines and mechanics not clear; and
5. Lack of support of some community stakeholders.

III. MEASURES TO IMPROVE THE TREATMENT OF OFFENDERS THROUGH THE ENHANCEMENT OF COMMUNITY-BASED ALTERNATIVES TO INCARCERATION

In 2006, an inter-agency collaboration effort was made by the pillars of the criminal justice system (CJS) in the Philippines to come up with a comprehensive study and discussion on how the criminal justice system can respond to the need to focus on the demand side or on how the poor and the disadvantaged can have access to justice. The fruit of the effort is the Medium-Term Development Plan for the Criminal Justice System (2007-2010). It was formulated with the participation of representatives from the five pillars. With funds provided by the United Nations Development Programme, the project was led by the Supreme Court of the Philippines which engaged the University of the Philippines' National College of Public Administration and Governance Centers for Policy and Executive Development (UP NCPAG-CPED) for technical support.

The pertinent problems and issues raised for the corrections pillar and their corresponding strategies are summarized in Table 5.

Table 5. Measures to Improve the Non-Institutional Treatment of Offenders

Problems/Issues	Recommendations/Strategies
1. Prohibitive fees and charges in securing clearances for offenders applying for probation, parole and other forms of release.	1.1 Strengthen inter-agency agreements to reduce fees 1.2 Lobby for pertinent legislation

THE 141ST INTERNATIONAL SENIOR SEMINAR
VISITING EXPERTS' PAPERS

2. Inadequacy of services for detainees/ probationers/ parolees.	2.1 Sustain the revitalization of the Volunteer Probation Aide (VPA) programme, including provision for travel, e.g., discounted bus fare, and institutionalize the same. 2.2 Expand partnership/co-operation with private sector/ individuals. 2.2.1 Enhance the aftercare programmes, particularly among drug dependents.
3. Enactment of laws relative to community-based alternatives to incarceration.	3.1 Amendment of certain provisions of Probation Law: 3.1.2 Changing the name of VPA to Volunteer Probation Officer or enactment of a VPO Law 3.1.2 Expanding the coverage of probationable penalties from 6 years to 12 years 3.2 Merger of the PPA and the Board of Pardons and Parole 3.3 Enactment of a Recognizance Law to allow poor litigants who cannot post bail to be released on recognizance. 3.4 Enactment of a law to unify the correctional system or establishment of an inter-agency monitoring/assessment system to unify the thrusts of the corrections pillar.
4. Lack of public information on how corrections work.	4.1 Maximizing existing information drives 4.2 Engagement of the <i>barangay</i> information system

In the context of the survey conducted by the Strategic Pathway on Harmonized Rehabilitation Programme mentioned earlier, and of the outputs in the Monitoring and Evaluation Seminar of the PPA-JICA Technical Co-operation Project conducted from 12-16 January 2009, the following sets of measures appear urgent in the improvement of the non-institutional treatment of offenders.

Table 6. Measures to Improve the VPA Agenda in the PPA Harmonized Programme

Key Result Areas	Strategies/Activities
1. Sustained integration and Harmonization of TC, RJ and VPA as major components of the PPA programme	1.1 Continued adoption of the umbrella matrix as a treatment paradigm 1.2 Clear-cut definition of the PPA rehabilitation programme 1.3 Harmonization of the reporting system of the rehabilitation programme 1.4 Continued training of the VPAs in TC and RJ processes 1.5 Continued involvement of VPAs in the conduct of TC sessions and RJ processes for clients
2. Improved recruitment and appointment system for VPAs	2.1 Continued conduct of massive information drives using the IEC materials produced by the NFTL team 2.2 Continued and strengthened partnership with the community
3. Continuing system of training of VPAs	3.1 Conduct at least one basic training for FO/cluster per year 3.2 Continued inclusion of VPAs in specialized training like TC and RJ practices
4. Empowerment of VPA Associations	4.1 Early affiliation of VPA association with the national federation (AVPAP) 4.2 Continued organization of at least one association per field office level 4.3 Conducting team-building workshops for members
5. Supervision workload of VPAs	5.1 Arrangement by each field office to ensure that VPAs are assigned at least one client for supervision at any given time
6. Monitoring and evaluation of the VPA Agenda	6.1 Submission of required reports by VPAs 6.2 Regular visit and observation of field offices by the Regional Director/ Assistant Regional Director/ Administrator 6.3 Documentation of activities to make all assessments and evaluation evidence-based

IV. OTHER COMMUNITY-BASED ALTERNATIVES TO IMPRISONMENT

The other community-based alternatives to incarceration in the Philippines are mostly provided under Republic Act (RA) No. 9344, otherwise known as the Juvenile Justice and Welfare Act of 2006, and are applicable to juveniles or children in conflict with the law (JILC/CICL). These alternatives are outlined below.

A. Intervention Programme for CICL Exempt from Criminal Liability

Section 20 of RA 9344 provides that “if it has been determined that the child taken into custody is 15 years old or below, the authority who will have initial contact with the child has the duty to immediately release the child to the custody of his/her parents or guardians, or in the absence thereof, the child’s nearest relative. Said authority shall give notice to the local social welfare and development officer who will determine the appropriate programs in consultation with the child and the person having custody over the child.”

The intervention programme may include counselling, skills training, education and other activities that will enhance the child’s psychological, emotional, and psycho-social well-being.

B. Diversion for CICL who acted with Discernment

It includes the process of determining the responsibility and treatment of a CICL on the basis of his or her social, cultural, economic, psychological or educational background, without resorting to formal court proceedings.

The diversion programme includes mediation, family conferencing and conciliation and, where appropriate, indigenous modes of conflict resolution in accordance with the best interest of the child, with a view to accomplishing the objectives of restorative justice and the formulation of a diversion programme.

The following factors shall be considered in formulating a diversion programme:

1. The child’s feelings of remorse for the offence committed;
2. The parents’ or guardians’ ability to guide and supervise the child;
3. The victim’s view about the propriety of the measures to be imposed; and
4. The availability of community-based programmes for rehabilitation and reintegration of the child.

C. Release on Bail or Recognizance

Release of the CICL on bail or on recognizance or his or her transfer to a youth home or youth centre in cases where he or she is not suitable for diversion or where diversion is not acceptable to his or her parents or is not appropriate as per assessment and recommendation of the social worker.

D. Automatic Suspension of Sentence

Section 38 of RA 9344 provides that if the CICL is found guilty of the offence charged, the court shall determine and ascertain any civil liability; however, instead of pronouncing conviction, the court shall place the CICL under suspended sentence without need for application.

E. Probation

Probation for a CICL who failed to rehabilitate while under suspended sentence.

F. Exemption

Exemption of the CICL from prosecution for crimes of vagrancy, prostitution, mendicancy, and sniffing of rugby. Instead, the CICL shall undergo an appropriate counselling and treatment programme.

V. CONCLUDING STATEMENT

The treatment of offenders in the Philippines through the enhancement of community-based alternatives to incarceration has been reformed in the last few years. The trend is towards using the holistic approach in strengthening the individualized community-based programme, in close adherence to the United Nations Standard Minimum Rules for non-custodial measures, also known as the Tokyo Rules. The journey has

THE 141ST INTERNATIONAL SENIOR SEMINAR
VISITING EXPERTS' PAPERS

been attended by some barriers but with the overall commitment, capability and collective effort of all stakeholders, specifically, the human resources of the PPA, and the full support of its partners, local and foreign, much headway has been achieved.

The signals are quite clear that with the issues of continuity and sustainability duly addressed, the ultimate goal of improved crime prevention and treatment of offenders will be within reach in the very near future. As this happens, the PPA will be ready to execute the idea of establishing a research and training institute that would largely focus on the effective modes and strategies of engaging the community in the treatment of offenders and in the prevention of crimes.

APPENDIX A

THE “CIRCLE OF SUPPORT”: RJ IN COMMUNITY ENGAGEMENT AND VOLUNTEER RESOURCE DEVELOPMENT

*Cecilia G. Dela Cruz**

In 2003, the Parole and Probation Administration decided to revitalize its programme, which had dwindled due to multiple factors. With the possibility of long-term support for the programme from JICA (Japan International Cooperation Agency) and UNAFEI (United Nations Asia and Far East Institute [for the Prevention of Crime and the Treatment of Offenders]), the agency set up a pilot project (that was later converted into a Field Training Laboratory) that validated the processes and systems for volunteer resource development.

I. COMMUNITY ENGAGEMENT AND THE RECRUITMENT OF VOLUNTEERS

When the team first went to the communities covered by the project in four municipalities in Laguna, i.e. San Pedro, Biñan, Sta. Rosa (now a city) and Cabuyao, the members were daunted. While it was easy to go through the process of recruitment and training of individual volunteers, and later organizing them into teams, they realized that the programme needed to have a context. Community engagement then became a necessary process. This was also experienced by the other Field Training Laboratory set up in Bataan.

The team had to sort through different approaches and strategies to begin the process of community engagement. At one point, they decided that it would be best to have as point of entry the issue of grassroots participation. The difficult part was the identification of a conceptual framework on which to anchor the engagement.

After consultations, it was decided that the best conceptual framework would be Restorative Justice (RJ). Initially, the idea was simply floated in the communities, especially during the information drives and dialogues with local community institutions. After enough curiosity had been aroused, more detailed discussions of the concept were conducted. In these discussions, those involved realized that not only was RJ a desirable objective, it was also identified as the most feasible focus for grassroots participation. Although the form and process were not easy to determine, it was clear to see that as a concept, it would be easy to operationalize because the communities saw that it was inherent in Filipino psychology and culture.

In the *kapwa* psychology of the Filipino, the “shared inner self” is pivotal in all interpersonal transactions. Even in its ethics and philosophy, which is a combination of the behaviorist and humanist approaches, the personhood or inner self is of paramount importance. The idea of reconciliation as an end part of justice was not difficult to accept; the Filipino believes that whatever he does to his fellow man is reflected unto himself. This therefore paved the way for community engagement in pursuit of Restorative Justice.

The restorative process is relatively new in application, but it has existed as a principle ever since human beings thought of grouping themselves into communities. Restorative processes are particularly evident in indigenous cultures. It was only with the influx of Western thoughts and values into indigenous cultures like ours that there was a change in attitudes towards crime and offenders. Yet later on, the need arose for a more humane system of dealing with crime. People began to recognize that there is a need to restore relationships within a community.

Some advocates of RJ in different cultures worldwide had developed models in which they applied restorative processes and values. Some of these are mediations, family group conferences, circles and

* The author is a registered social worker who was Chaplaincy Program Assistant at the Bureau of Corrections for eight years. She is a Chief Administrative Officer at the Parole and Probation Administration where she has been working for the last twelve years. She is also the Chief Facilitator for the In-Country Training Program for Volunteer Resource Development of the PPA.

community services. In the Philippines, there are groups advocating for the adoption of the restorative process in dealing with crime. Just as other countries have seen the inadequacy of the retributive system, there is now more enthusiasm for RJ in this country. The probation system has also considered adopting this approach.

The pilot project on the holistic approach to the rehabilitation of offenders used RJ as the conceptual framework. It was determined that RJ is an important concept in rehabilitation because it involves the community, which is the core characteristic of community-based corrections. By involving the community, the broken relationship, which is a consequence of an offence, can be repaired and restored. The Volunteer Probation Aides (VPAs) who participate in CS provide the empirical objectification of "community".

But the restorative process remained a concept for some time. The main activities of the project team focused on introducing the concept at the grassroots level. The responses towards the alternative knowledge were very good. However, its application remained quite vague.

So far, the only form that has been tried in the pilot areas is the "Circle of Support". In the model that was developed, the offenders were involved in drug abuse and illegal fishing. Although these cases are labeled as "victimless crimes," that is not exactly correct because whole communities were actually victimized by the effects of these offences. The concept was crystallized with the help and advice of the prime advocate of Restorative Justice in the country, Brother Rudy Diamante. CS defines restoration as moving forward, as a time to start healing. To foster healing means to have support. Around this thought revolves the idea of the "Circle." The volunteers from San Pedro, Laguna created a hybrid model that should be suitable for a particular community and the particular crime and persons involved. In that sense, this circle model brought together clients of one community with similar offences. The team used one *barangay* in San Pedro as the locus for the process. The problem in this community was drug-related.

The idea of the "Circle" is to bring about reconciliation between the offender and the community through dialogue.

II. OPERATIONALIZING THE 'CIRCLE' AT GRASSROOTS LEVEL

The idea of the "Circle" is to bring about reconciliation between the offender and the community through dialogue. The "Circle" is composed of the offender/s and two or more three persons of their choice who can provide them with moral support during the dialogues, community representatives from the sectors most affected by the offence, the offender/s' Volunteers Probation Aide/s (VPA) and Parole and Probation Officer/s (PPO), and local government officials who could provide follow-through rehabilitation services for the offenders.

The restorative process began by preparing the participants of the Circle. Here, the offender will take responsibility for the negative effects of the crime he or she committed. Then, he or she may decide to make amends for it in ways agreed on by the victims/community. Restoration thus begins.

A. The "Circle" in San Pedro, Laguna

The first "Circle" was organized by the team in a *barangay* in San Pedro, Laguna. It involved three offenders from the community involved in drug abuse. They each had one or two "supports." Representatives from the local Catholic church, school and residents, as well as *barangay* officials and the VPA and PPO, composed this "Circle". As agreed, they met every other Saturday at the community chapel after Mass (a Catholic religious service). There were a total of six sessions each, one of which lasted for an hour.

The first session was like a forum for all participants, especially for the community members. An orientation on the concept, nature, goals and processes of Restorative Justice was conducted. The *barangay* captain, probation officers as facilitators, volunteer probation aides (some of whom were *barangay* council members), a representative from the local Catholic church, and representative from the local school attended the said session.

In the second session, two client-offenders attended together with the members of their personal support system. One brought his brother; the other brought her cousin who is a Protestant pastor. The volunteer probation aides handling their cases were also present. The process was held just after the 5:30 p.m. Mass in the San Roque chapel. The circle was comprised of 19 participants. The facilitator started with asking how the commission of crime affects anyone in the circle.

“It made me quiver as I walked back and forth inside the house while my son would bang himself against the door of our house. I felt much fear”, said a participant-mother speaking about a son who was taking drugs and who had brought its ill effects upon his family.

Other members soon spoke about their own plights. One shared her feeling as an aunt with a nephew who turned violent every time he had hallucinations brought about by drugs. Others talked about other effects of drug-related offences on the community. At one point, a volunteer went out of the room when he heard noises outside the chapel and reported back that there was a drug peddler on the run. This incident made the group see more closely the negative effects of illegal drugs on the community. More of the participants expressed their individual sentiments. Having seen the impact of the offence, all of them realized that they had a responsibility to be involved even in small ways in countering this kind of crime.

A discussion followed with the unfolding of a client’s experiences. He talked about his own dilemma of being tagged as a drug-user. Some of his personal plans were disrupted, he said, because of his hesitation brought on by the fear that he might be rejected by others once they found out about his wrongdoing in the past. He said that it was like having a “*lamat*”, or a flaw or stain on his personality.

Two volunteer probation aides even disclosed their previous addiction to drugs. They told about the hardship they underwent to change for the better. They stressed the value of self-motivation and support from outside and noted that if they had been able to change, others could do it as well. They professed that they can be used as instruments to teach a lesson to those who are taking drugs and to help them change. The discussion was fruitful. Only one client did not talk because of her personal reservations. The session, which lasted about two and a half hours, closed with a challenge for the clients to continue to change. The principle of confidentiality, which applies to every word spoken within the circle, was reiterated to the participants and upheld at all times.

Two weeks later, the third session was conducted. The same participants attended, with the addition of a client and two representatives from the school and the absence of the two clients from the last session. The facilitator started with the questions: “Is this activity worthy to be continued? Do you find any value in undergoing this? Is there a need for this Circle?” The responses were all favourable. The participants saw the need to address the effects of drug addiction in their area. Aside from realizing the help that they could extend simply by giving oral support towards an offender’s continuing change, the participants also saw the Circle as a venue to air and resolve grievances.

In restoring the relationships broken by a crime, the offender should start with ownership and assuming responsibility for the crime he or she committed. The victim and community then recognize this admittance of failure on the part of the offender. Stigmatization would thus be eliminated. When the different parties achieve openness, and total understanding of one another, making amends is then possible. The community members had very positive takes on making amends. In fact, several members of the circle encouraged a client to let the community see what she was doing to show that she had already changed. One suggestion was for the offender to give testimonies about her experience with drugs; for instance, addressing pupils/students in classrooms, to serve as an example to the rest of the community. The client was hesitant, however, to do something so public, and the rest of the circle participants understood and affirmed the value of voluntary action on the part of everyone, including the offender.

On the other hand, drug abuse is the main offence classified as a victimless crime. Naturally, it is the offender him or herself who is seen to have suffered from taking illegal drugs. But the external effects of drug abuse also eventually affect the taker’s immediate family as well as the other members of the community. It was thus decided that the community itself is victimized by this offence.

B. The “Circle” in Orion, Bataan

A “Circle” was also organized in a fishing community in Orion, Bataan. The offenders were all involved in illegal fishing. Participants in the circle were members of the community such as the “*Bantay Dagat*”, the local police and a representative from the Mayor’s Office, as well as the VPAs and PPOs of the offenders.

In the initial session of this “Circle,” the offenders were quite belligerent and initially insisted that they merely resorted to illegal means of fishing in order to survive. It was easy to see that the issue was a conflict between the law and what the offenders perceived as a right. This “Circle” holds regular sessions, even after the offenders have asked for forgiveness for their offence, with the hope that there will eventually be closure in terms of an agreement between the offenders and the service providers on what specific services they need as follow-through for their rehabilitation process.

As in the CS in San Pedro, the community church members in Orion had a strong influence in changing the initial belligerence of the offenders to humility and *hiya*. Most of the offenders and their families became involved in church fellowships. Slowly, Christian doctrine became fused with the idea of Restorative Justice.

The CS, as a model of Restorative Justice process that was tried and developed by the Field Training Laboratories (FTL), is now being shared with other unit offices of the agency. Several more “Circles” have been organized by the FTL in Laguna and have on-going sessions. The CS has thus evolved from a theoretical model into an initiative started within a community. With the participation of the community members and their responses to the process, the goal of having a peaceful society is deemed realizable by reconciling and restoring relationships. After all, our indigenous culture of eternal and communal support towards each other has existed a long time. It is all a matter of looking back to our roots.

III. SUMMING UP: BUILDING COMMUNITIES THROUGH PARTNERSHIP WITH VPAs

Based on the experiences in the Laguna and Bataan FTLs, the following insights were gained:

1. There is a set of preparatory activities that need to be carried out before starting a “Circle of Support”, such as the following:
 - a. Client’s orientation on the process and expectations;
 - b. Meeting with VPAs;
 - presentation of client’s concerns and issues;
 - identification of community members who will participate in the “Circle”;
 - c. Enlisting the support of the other participants in the process;
 - d. Setting the first session in a venue that is conducive to serious discussion;
 - e. Engaging the community with the VPA as a participant.
2. The following roles of the VPA in the process were identified:
 - a. In establishing the “Circle”:
 - identify and recommend the proper authorities and community members who will comprise the “Circle”;
 - assist the PPO in advocating and co-ordinating the preparations;
 - assist in preparing the clients for the sessions.
 - b. In sustaining the process:
 - act as moderator and facilitator;
 - act as a resource person;
 - be a catalyst for community support;
 - be part of the client’s support system.
3. Prospects
 - a. It is possible to turn over the “Circle” to the community with the VPAs as facilitators;
 - b. A real community engagement takes place when the community has realized that it is responsible for sustaining the initial steps taken by the client towards reformation.

4. Long-term impact
 - a. Full reintegration of the client into community life;
 - b. Prevention of crime and recidivism.

In essence, the CS is all about relationships. Persons bond with one another through their common humanity. But when someone commits a crime, harm is done and links are broken. The victim reacts with resentment, and often, with fury. People in the community usually stigmatize the offender. For many years, the answer for every crime committed has always been punishment. As a result, the offenders were often isolated from the rest of the community. This is the retributive system of justice. Looking at it superficially, it is very logical to be punitive. But as people became more understanding of each other's humanity, alternative ways of thinking flourish, such as that of Restorative Justice.

The RJ perspective says that "crime is suffering, and the end of crime is possible only with the end of suffering." Thus, the answer to crime is not punishment, but healing and restoration.

REFERENCES

Catholic Bishops Conference of the Philippines – Episcopal Commission on Prison Pastoral Care (2004). “Restorative Justice: A Source Book,” 2004.

Co, Manuel G. (2008). “An Assessment of RD’s Restorative Justice Program in the Parole and Probation Offices of Bataan, Sta. Rosa City and Baguio City.” Unpublished Master’s Thesis, National Defense College of the Philippines, Quezon City, October 2008.

Diamante, Rodolfo S. and Cesar G. Banaag, eds. (2007). Justice that Heals: Forgiveness and Reconciliation. Manila: Coalition Against Death Penalty (CADP).

National Police Commission – Technical Committee on Crime Prevention and Criminal Justice (2008). 2008 National Crime Prevention Plan.

Parole and Probation Administration (2008). Operational Plan for Calendar Year 2008.

Parole and Probation Administration (2008). 2008 Annual Report, January 2009.

Parole and Probation Administration National TC Team. “Realigned Therapeutic Community Program: Revised TC Manual, Phase I to IV,,” A Manual for Agency Implementers, 2005.

Perfas, Fernando (2002). The Process of Building a Therapeutic Environment. New York: By the Author.

Presidential Decree No. 968. “Establishing a Probation System,” July 24, 1977.

Presidential Decree No. 1508. “Establishing a System of Amicably Settling Disputes at the Barangay Level.” June 11, 1978.

Republic Act No. 9344. “An Act Establishing A Comprehensive Juvenile Justice and Welfare System,” April 28, 2006.

Supreme Court of the Philippines (2003). “Strengthening the Other Pillars of Justice through Reforms in the Department of Justice.” A Diagnostic Report, February 2003.

Supreme Court of the Philippines (2006). “Medium-Term Development Plan for the Criminal Justice System (2007-2010)”. Final Report, December 2006.

Toch, Hans, ed. (1980). Therapeutic Communities in Corrections. New York: Praeger Publishers.

COMMUNITY-BASED ALTERNATIVES IN SENTENCING

*Bala Reddy**



I. INTRODUCTION

Punishment in the modern context has acquired a profound, new meaning. It has evolved into a concept encompassing traditionally favoured principles of deterrence, retribution, prevention, and the presently popular principles of rehabilitation and restorative justice. In 1965, the dominant sentencing philosophy in Singapore was observed to be retributionist, with greater emphasis given to the objectives of retaliation against the accused and deterrence than to the needs and reformation of the offender.¹ Some fifteen years later, the sentencing philosophy was observed to have remained largely the same.²

Experience has shown that this approach led to an extremely high rate of recidivism.³ Furthermore, such an approach is no longer adequate in light of changing social trends; it does not address the underlying issues in the increasing number of offences arising from those trends, such as attempted suicides, teenage promiscuity and mental illness and disability in offenders.

Therefore, our response has been to adapt our penal philosophy to include rehabilitation as an equally important objective.⁴ In fact, we go as far as to recognize that the need to address the injury caused to the victims and community is also as important as the reformation of the offender. A restorative justice approach which advocates the use of community-based alternatives to custodial sentences was thus factored into the skein of our sentencing principles. The Community Court, which was launched in June 2006, was especially created to give greater scope for the court to give effect to our current penal philosophy.

The ethos of offender rehabilitation is not merely confined to the courts; it permeates the other components of our penal system. Our biggest correctional agency, Singapore Prison Service, has in place a sophisticated and carefully thought through offender rehabilitation programme which continues to assist the offender even beyond the prison walls. For these measures and programmes to be successful, there has to be “a progressive attitude towards ex-offenders”.⁵ The Yellow Ribbon Project was therefore set up in 2004 to educate the public on the need to give ex-offenders a second chance. Recidivism is a key measure of our efforts and I am glad to say that we have one of the lowest recidivism rates in the world.⁶ Our penal system also enjoys the confidence of the public because its approach secures justice, not only for the State and the Community, but also for the offender.

To merely describe the present approach and the measures implemented without first understanding “why punish?”⁷ would be a vacuous exercise because punishment is no longer an end in itself but rather a means to achieving a myriad of objectives. Therefore, an examination of the basis of sentencing an offender is necessary.

* Principal Senior State Counsel, Head, State Prosecution Division, Attorney General’s Chambers, Singapore.

¹ Professor Tommy Koh, “*The Sentencing Policy and Practice of the Singapore Courts*” (1965) 7 Mal. L.R. 291, at p. 294.

² Peter English, “*Sentencing in Singapore*” (1981) 23 Mal.L.R. 1, at p.24.

³ “*Our History*”, Singapore Prison Service, http://www.prisons.gov.sg/our_history.html

⁴ K.Shanmugam, Law Minister, “*Singapore’s Penal Policy (Review)*”, Singapore Parliamentary Report Vol.85 Sitting No.7, Oral answers to questions, 19 Jan 2009 – attached in Annex A.

⁵ Per Chief Justice Chan Sek Keong, Opening address at the Yellow Ribbon Conference 2006, 27 September 2006.

⁶ K Shanmugam, op cit n.4 above.

⁷ Adapted from *Why Punish?* by Nigel Walker, (Oxford University Press, 1991).

II. WHY PUNISH?

The classic principles of sentencing philosophy have been succinctly encapsulated in four words: retribution, deterrence, prevention and rehabilitation⁸ and adopted with much approval by courts in Singapore.⁹ Each principle has generated much theoretical discussion which attempts to find a basis for punishment as a response to the question, “why punish”? Perhaps the most instinctive, if not primal, response to the question is retribution.

A. Retribution

To express the retributive principle simply, punishment is justified because the offender deserves it or as the Old Testament puts it, “an eye for an eye, a tooth for a tooth, and a life for a life”.¹⁰ Within the brutally clear message are overtones of censure as the offender is held accountable for his or her misdeeds. Hence, it has been suggested that retribution is the notion of getting the offender to pay for what he or she owes, that is, his or her debt to society.¹¹ However, this is by no means restorative justice because sentences imposed with retribution as a primary concern generally do not make offenders liable personally to the victim for the injury their actions have caused since the emphasis is on hitting back at the offender¹² rather than to address the injury caused to the victims.

B. Deterrence

Related to the principle of retribution is deterrence. An important component of the retributivist principle, censure when expressed through the imposition of court-sanctioned punishment *deters* people from committing offences since doing so defines them as criminals.¹³ What this incidentally demonstrates is the paramount objective of deterrence: people refrain from committing offences because of their aversion to the consequences.

Two types of deterrence exist: specific deterrence and general deterrence. Specific deterrence focuses on the offender him or herself and aims to deter the offender from repeating his or her criminal conduct¹⁴ by instilling in him or her the fear of reoffending through the threat of punishment he or she will receive for doing so.¹⁵ General deterrence, on the other hand, is directed at educating and deterring members of the general public,¹⁶ either through the form of legislation sanctioning punishment for specific offences or the imposition of a substantial sentence for certain offences, both of which are designed to convey the message that offences of a particular nature will not be tolerated.¹⁷

It is obvious that the emphasis of the deterrence principle is on its ability to benefit the greater good and punishment is therefore justified, even if harm is caused to the offender, so long as the harm it seeks to prevent is greater than the harm caused to the offender when punishment is imposed on him or her. It is accepted that penalties do deter but because scant regard is given to the type of punishment which *ought* to be imposed on the offender, only the symptoms and not the root cause of the problem are dealt with. Kleptomaniacs would keep on stealing and unhappy neighbours would continue feuding even if sentences are enhanced.

C. Prevention

Perhaps the most fearsome principle is the principle of prevention because sentencing based upon prevention as a primary consideration necessarily results in harsher punishment. The policy is that of selective incapacitation: offenders who are deemed dangerous or persistent in reoffending are incarcerated, usually for extended periods, in order to protect the public and to reduce crime. The notion of prevention is

⁸ *R v Sargeant* [1975] 60 Criminal Appeal Reports 74 at p.77.

⁹ *PP v Tan Fook Sum* [1999] 2 SLR 523. *Chua Tiong Tiong v PP* [2001] 3 SLR 425; *PP v Goh Lee Yin* [2007] SGHC 205.

¹⁰ Exodus 21:23 – 27.

¹¹ Nigel Walker, *Why Punish?* (Oxford University Press, 1991), p.73.

¹² “*The Expressive Function of Punishment*”, *A Reader on Punishment*, Joseph Feinberg (ed. Anthony Duff and David Garland, Oxford University Press, 1994) p.76.

¹³ “*Censure and Proportionality*”, *A Reader on Punishment*, A. von Hirsch (ed. Anthony Duff and David Garland, Oxford University Press, 1994) p.120.

¹⁴ *PP v Tan Fook Sum* [1999] 2 SLR 523.

¹⁵ *PP v Law Aik Meng* [2007] 2 SLR 814 per Justice V.K. Rajah.

¹⁶ *Meeran bin Mydin v PP* [1998] 2 SLR 522.

¹⁷ *Xia Qin Lai v PP* [1999] 4 SLR 343.

reflected in punishment policies such as mandatory minimum sentences, preventive detention and corrective training.¹⁸ Such offenders are removed from society for long periods and they are therefore the category of offenders who require more assistance towards reform and reintegration than the average offender.

D. Rehabilitation

Under the rehabilitation principle, crime is perceived to be the symptom of a social disease and the objective of rehabilitation is to cure that disease. Unlike the three sentencing principles discussed thus far, rehabilitation involves an examination of the offence so that the appropriate punishment can be imposed with a view to changing the offender's values so that he or she will learn that such conduct is wrong and refrain from committing offences in the future. After all, it is undisputed that a substantial proportion of the prison population hail from the lower socio-economic strata and because of their social circumstances like poverty and lack of education, they are sometimes led to crime. Recognizing this, the Singapore Prison Service's strategy has been to invest heavily in education and training to keep offenders on the right path after their release.

It is therefore clear that the benefits of rehabilitating offenders accrue not only to the individual, but also to society at large.¹⁹ It is unsurprising that rehabilitation has come to enjoy considerable support as an alternative to conventional methods of punishment since it produces a win-win situation: lower rates of recidivism translate into a safer environment for all to live in, while higher rates of ex-offenders engaging in gainful employment facilitate better economic progress for the nation.

E. Restorative Justice

There has been much emphasis in recent times on restorative justice. However, restorative justice is by no means a recent concept and is in fact "grounded in traditions from ancient Arab and Western civilizations and in Hindu, Buddhist, and Confucian traditions".²⁰ In Arab civilizations, there is the Pentateuch which specified restitution for property crimes in Israel, and the Code of Ur-Nammu (c.2060 BC) required restitution for offences of violence in Sumer. As for Western civilizations, there is the Roman Twelve Tables (449 BC), the Irish Brehon Laws, the German tribal laws under King Clovis I (496 AD), and the English Laws of Ethelbert of Kent (c.600 AD) which all required some form of restitution for offences.

It is obvious by now from the ancient examples that an approach based on restorative justice goes beyond the reform and rehabilitation of the offender. The concept of restorative justice is a fine balance of a multitude of objectives: a balance between the therapeutic and retributive models of justice; a balance between offenders' rights and victims' needs and a balance between the need to rehabilitate the offender and the duty to protect the public.

Recognizing this, the courts started to incorporate restorative justice processes into their sentencing philosophy. These processes are largely non-custodial in nature and include victim-offender mediation, family group conferencing, restorative or community conferencing, community restorative committees and restorative circles which assist the offender in his or her successful transition back to the community.

Community-based alternatives have received the stamp of approval by the United Nations since 1990 through its Standard Minimum Rules for Non-custodial Measures – the Tokyo Rules.²¹ While Singapore is not a signatory to the Rules, the sentencing approach is very much in line with its philosophy which promotes the use of non-custodial measures. A commonly used measure is probation because it rehabilitates the offender effectively, with maximum involvement of the offender's family or the community, and reintegrates the offender into mainstream society as a socially responsible and law-abiding person.²²

¹⁸ Sentencing Practice in the Subordinate Courts, Ch 3: General Objects of Sentencing.

¹⁹ *PP v Goh Lee Yin* [2008] 1 SLR 824, 863.

²⁰ J Braithwaite, "Restorative Justice", *Handbook of Crime and Punishment* (edited by Michael Tonry, NY: OUP, 1998), p.323 – 344.

²¹ United Nations Standard Minimum Rules for Non-custodial measures (The Tokyo Rules) adopted by General Assembly, Resolution 45/100 of 14 December 1990.

²² Chomil Kamal, then Chief Probation Officer, MCYS, "The Probation Service in Singapore", www.unafei.or.jp/english/pdf/PDF_rms/no67/04_Ms.Kamal_p61-p74.pdf

One such example is the approach taken in late 2005 in the case of the 17-year-old blogger²³ who was convicted of making racist remarks against Malays. Instead of imposing a custodial sentence, the court imposed 24 months' supervised probation with unique features to address the accused's offending behaviour. The offender was tasked to perform community service at centres specifically catering to the needs of Malays, the very people he insulted.

A very different fate befell the 18-year-old offender²⁴ with an IQ of 58 whose appeal was decided in the High Court just three weeks before the blogger's case. The teen was a repeat offender and was once again convicted for molestation in the Subordinate Courts. The unrepresented teen then appealed against his sentence to be spared the cane. However, in view of the seriousness of the offence, he was not spared the cane and his sentence of imprisonment and caning was enhanced. The decision drew much public attention and even sparked off a parliamentary debate on how the courts should treat mentally disabled offenders.

The call for a more updated sentencing approach which does more than merely punish finally culminated in the setting up of the Community Court, the symbol of Singapore's endorsement of the ethos of using community-based alternatives to custodial sentences.

III. THE COMMUNITY COURT

A. Profile

The Community Court was set up in June 2006 as a specialist court to respond to the needs of the community²⁵ and social trends which have translated into crime. More teenagers are engaging in sexual activities. Neighbourhood spats have increased. There is also the disturbing increase in attempted suicides. As demonstrated before, there was also the call for rehabilitation or sentencing options which provide help rather than mere punishment for offenders with mental disabilities and disorders.

Conventional custodial sentences or fines would clearly not make these problems go away since they do not strike at the heart of the 'disease'. Therefore, the Community Court's approach is "a problem-solving one that combines criminal justice and community resources for a comprehensive response" to deal with such social problems. Cases under the Community Court include youthful offenders aged 16 to 18 whom by reason of their age are not within the purview of the Juvenile Court, carnal connection offences by youth offenders, offenders with mental disabilities or disorders, neighbourhood disputes, attempted suicides, animal cruelty, cases which have impact on race-relations and selected cases involving offenders above 65 years old.

B. Sentencing Options

The Community Court is like any other court of law in Singapore. However, as its sentencing considerations are different, it makes use of sentencing options such as probation, deferred sentences, conditional discharge and community service orders in addition to conventional sentences of imprisonment or fine. Other features of the restorative justice model are employed by the Community Court to achieve its desired goal in sentencing. Through Community Court Conferences facilitated by a case manager, issues such as victim-offender mediation, family group conferencing and restorative conferencing are addressed.

C. Proposal to Increase Community-Based Sentencing Options

There has been encouraging public support for the efforts of the Community Court and its innovative and sensitive treatment of offenders and victims of crime, an approach which is endorsed by the Government.²⁶ In fact, the Community Court's efforts have been so successful that the Ministry of Law recently announced its proposal²⁷ to increase community-based sentencing options to include:

²³ *PP v Gan Huai Shi*, reported 24 November 2005 in "Today".

²⁴ *Iskandar Muhamad Nordin v PP*, [2005] SGHC 207, decided on 4 November 2005.

²⁵ Chief Justice Chan Sek Keong, Keynote Address, 15th Workplan 2006/2007.

²⁶ Associate Professor Ho Peng Kee, Senior Minister of State for Law for the Deputy Prime Minister and Minister for Law, "Criminal Procedure Code and Probation of Offenders Act (Review)", Singapore Parliamentary Report, Vol.83, Sitting No. 9, Start Col: 1328; End Col: 1331, 27 August 2007.

²⁷ Public Consultation on Criminal Procedure Code Bill, 2009 http://notesapp.internet.gov.sg/_48256DF20015A167.nsf/LookupContentDocsByKey/GOVI-7M6ETJ?OpenDocument

1. Mandatory Treatment Orders

To allow the Courts to order an offender to undergo psychiatric treatment in lieu of imprisonment. No such power exists currently.

2. Short Detention Orders (SDO)

To give first time low-risk offenders a short experience (about one week) of detention. The SDO is less stigmatizing than imprisonment and limiting the detention period will prevent contamination. More importantly, the SDO will not dislodge the offender from his family and job. At the same time the “clang of the prison gates” helps deter reoffending.

3. Day Reporting Orders (DRO)

To require an offender to report to a Reporting Centre on a regular basis and be electronically tagged, if necessary. This imposes some discipline and aids in rehabilitation as the offender’s progress is monitored closely. It can be used very effectively in combination with an SDO. Other countries have used such orders to positive effect.

4. Community Work Orders (COMWO)

Modelled after the “Corrective Work Order” for litterers, to allow for a wider range of offences and types of work to be mandated. The type of community work should have some nexus to the offence committed. The proposed maximum length of the COMWO is up to 40 hours.

5. Expanded Community Service Orders (CSO)

To allow offenders aged 16 and above to make reparation to the community while being punished for their misdeeds. This will require tying up with Voluntary Welfare Organizations which can put the offenders’ service to good use. The proposed length of the CSO is 40 to 240 hours.

6. Expanded Conditional Discharge

To allow the Courts to specify conditions such as participation in programmes or an MTO as a requirement. The maximum term for a conditional discharge is proposed to be extended from the current 12 months to 24 months to allow sufficient time for participation in programmes.

The proposals reflect the intention to enhance the present approach of using community-based rehabilitation options by introducing greater flexibility and allowing more graduated sentencing options for minor offences. Offenders can be imprisoned for short terms yet be adequately punished without disruption to family life or loss of job.

D. Two Years On: The Cases dealt with Thus Far

Please refer Annex B.

IV. BEYOND THE COMMUNITY COURT

A. The Singapore Prison Service: Complementing the Objectives of the Modern Approach

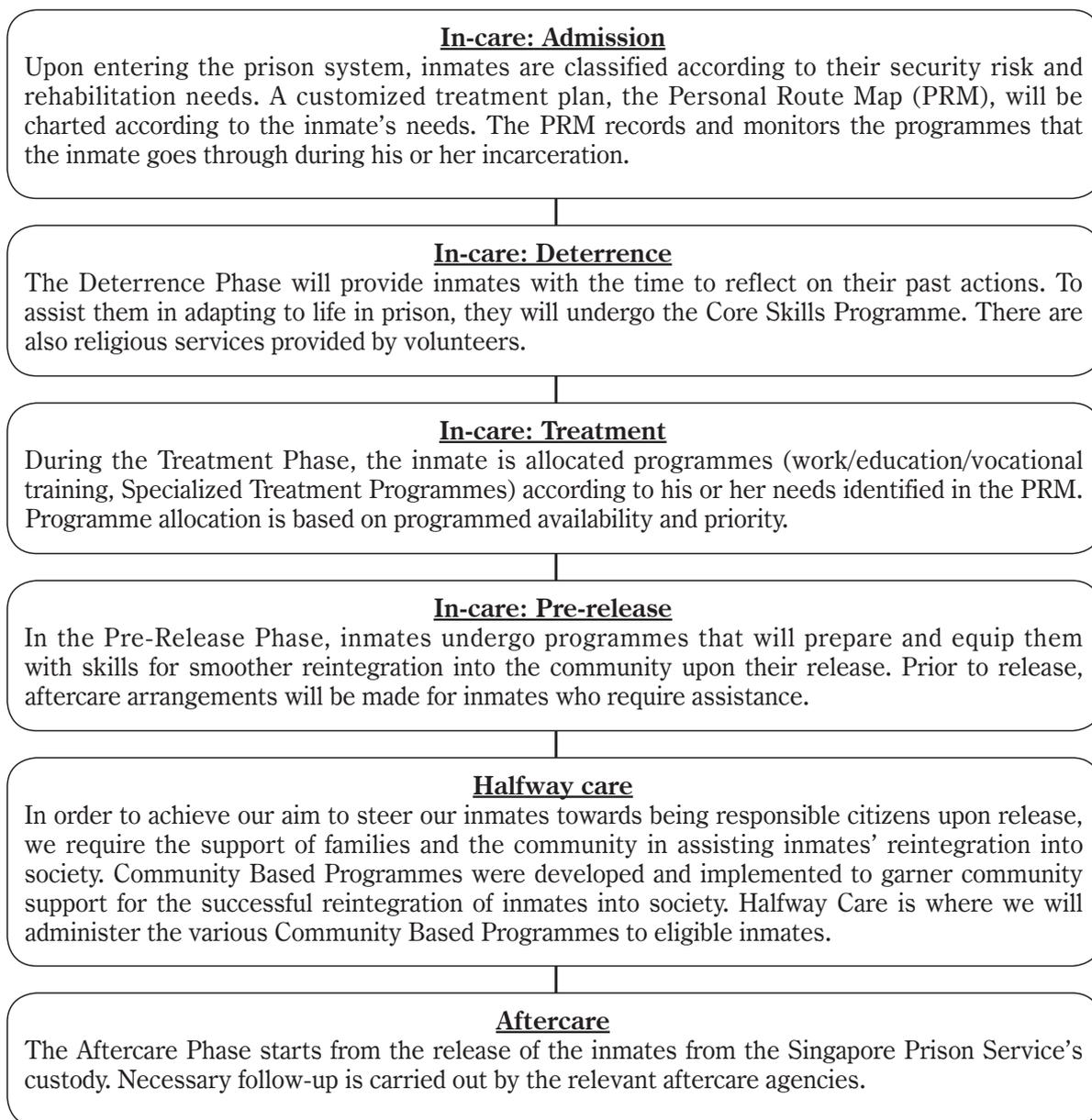
1. Integral to the success of reform is the criminal justice system, the chief components of which are the police, the prosecution, the courts and the correctional agencies.²⁸ Prison is by far the most important component in the system towards achieving the objectives of prevention and rehabilitation since it is the biggest correctional agency and the most direct agency which enforces the sanctions imposed by the courts.
2. Rehabilitation was recognized as equally significant as punishment and correction as early as 1895 by the very people who created prisons – the British. In 1895, the Gladstone Committee was formed to survey the effectiveness of prisons. Unsurprisingly, it found that a prison system created solely for the purpose of punishment reduces neither crime nor recidivism. In fact, it only “made for the deterioration and degradation of the prisoners and their eventual release into society neither

²⁸ K.V Veloo, *Rehabilitation of Offenders in Singapore: Volume 1* (Department of Social Work and Psychology, Faculty of Arts and Social Sciences, National University of Singapore, 2004) at p.10.

deterred nor reformed, but brutalized and embittered".²⁹

3. Since its institutionalization in 1946, the Singapore prison system has evolved progressively from a basic facility adopting chiefly Victorian punitive methods into one providing a comprehensive rehabilitation service which can "stand proudly with some of the better [prisons] in other parts of the world".³⁰ An overview of the rehabilitation process in diagram 1 reveals a rigorous programme put in place for the offender at every stage from the very moment of his or her admission to the period after his or her release.

DIAGRAM 1
Singapore Prison Service's Rehabilitation Process³¹



²⁹ *The Treatment of Offenders in Britain*, Central Office of Information Reference Pamphlet, London, (Her Majesty's Stationery Office, 1960) at p.5.

³⁰ Foreword to *Rehabilitation of Offenders in Singapore: Volume 2*, K.V Veloo, (Department of Social Work and Psychology, Faculty of Arts and Social Sciences, National University of Singapore, 2004) at p.3.

³¹ Singapore Prison Service, Rehabilitation Process, <http://www.prisons.gov.sg/restart.html>

4. The contemporary system is not meant to make life any easier for the offender than traditional methods which only focused on the punitive aspects. Rather, it is a sophisticated system which not only serves to reduce crime and recidivism but also to deliver justice to the offenders by treating them not as criminals but worthy individuals capable of having better lives.
5. A cursory examination of the prison's programmes will reveal that the underlying objectives complement that of the Community Court and the Tokyo Rules, that is, to promote among offenders a sense of responsibility towards society and encourage greater community involvement.
6. Brief Profile of Singapore Prison Service's Schemes and Programmes.

(i) Education

It is undisputed that a substantial part of the prison population is made up of offenders from the lower socio-economic strata³² and are sometimes led into crime because of their circumstances. In line with rehabilitation objectives, further education is offered to the offenders with a view to increasing opportunities and creates a new pathway for them. This way, the offender's ability to reintegrate into the community is enhanced, which in turn should keep them from lapsing into their old ways and returning to prison. Hence, the Singapore Prison Service has been keenly investing in education.

Programmes available in prison are diverse: formal academic courses - GCE 'N', 'O' and 'A' levels, vocational courses, e.g. computer literacy and technology courses, enrichment activities e.g. choir, drama, etc., religious and moral education, social skills courses, family-focussed courses and community reintegration courses.

To accelerate and enhance inmates' literacy level, the Literacy Education Accelerated Programme (LEAP) was implemented in April 2004. The following table³³ shows a consistent enthusiasm in participation thus far.

Educational levels/course	Apr 2004 to Dec 2004	Jan 2005 to Dec 2005	Jan 2006 to Dec 2006	Jan 2007 to Dec 2007	Jan 2008 to Dec 2008
Basic Literacy Courses	NA	650	983	1366	585
BEST	45	402	185	178	79
GE	531	995	462	145	87
GCE N	126	160	171	147	117
GCE O	93	135	154	131	127
GCE A	33	33	33	34	22
Total	828	2375	1988	2001	1017

(ii) Work

Work is an important, if not the most important, component in the rehabilitative process for offenders.³⁴ It instils discipline, responsibility and work ethics which will help them rejoin the workforce and reintegrate into the community upon release. Through the Singapore Corporation of Rehabilitative Enterprises (SCORE), offenders receive a variety of on-the-job training based on their interests. Offenders typically receive vocational training in the areas of electronics, food preparation, cleaning, etc.

In fact, some of the workshops within the prisons are leased to and run by private firms who work with SCORE³⁵ e.g. "Connect Centre", a call centre operating in Changi Women's Prison since 2005 which

³² Chief Justice Chan Sek Keong, op cit n.5 above.

³³ Courtesy of Singapore Prison Service.

³⁴ Singapore Prison Service, Rehabilitation Process, <http://www.prisons.gov.sg/restart.html>

³⁵ <http://www.score.gov.sg/Industrial%20Space%20Leasing.html>

employs about 40 inmates.³⁶

The Prison Service continues with the offender's work programme even after his or her release. Under the 'Place and Train' Scheme, industries which require manpower support and are keen to hire ex-offenders are identified so that offenders upon their release will be able to find employment. The Prison Service together with SCORE has engaged companies such as NTUC, NParks and Building & Construction Association. Another scheme which provides aftercare support in relation to work is the 'Prepare and Place' Scheme which is essentially a job fair. All these measures are aimed at facilitating the offender's integration with the community after his or her release.

(iii) Early Release

(a) Home Detention Scheme

Another measure which involves the community is the Home Detention Scheme (HD). Offenders on this scheme would be less likely to find themselves coming back to the community as an alienated individual. Under the HD Scheme, which was implemented in May 2000, offenders who are about to be released and identified as suitable will be released early to be detained at home and will be monitored through electronic tagging. The offenders are to abide by the curfew hours stipulated in the HD Order. They will be able to commute to work or further their studies during the period that they serve out their sentence at home.

Offenders convicted of serious and violent crimes are not released on home detention.³⁷ Maximum placement on the scheme is 12 months and an offender has to be sentenced to a minimum of four weeks' imprisonment to be eligible. Eligibility also depends on an offender's progress and response to rehabilitation and level of family support.

(b) Completion & Recidivism Rates

Since 2000, a total of 11,534 inmates have been placed on the HD scheme and as of 2008, 10,995 inmates had successfully completed the programme. As can be seen from the following table,³⁸ recidivism rates have steadily fallen among offenders as compared with the general population. Thus, the scheme has been lauded as an example of the success of the sound and practical principles of our penal system, which advocates rehabilitation and reintegration.³⁹

Recidivism rates of HD inmates who have completed the programme		
	HD inmates who have completed the programme	General population
2001 cohort	3.8%	35.3%
2002 cohort	6.1%	31.2%
2003 cohort	10.8%	24.9%
2004 cohort	11.3%	23.7%
2005 cohort	10.3%	24.2%

(iv) Work Release Scheme

The Work Release Scheme (WRS) allows an offender to serve the last months of his sentence in a work release camp or halfway house under supervised conditions. Offenders who lack family support are most suited for this programme. Under this programme, inmates are closely guided by staff at the camp or halfway house. The same objectives adopted by the work programmes in the prison (instilling discipline, responsibility and work ethics which will help offenders rejoin the workforce and reintegrate into the community upon release) also apply in WRS.

³⁶ <http://www.connectcentre.com.sg/security/who.htm>

³⁷ See Schedule to the Prisons Act for the offences for which a person has been convicted will not qualify for home detention.

³⁸ Courtesy of Singapore Prison Service.

³⁹ K Shanmugam, op. cit. n.4 above.

(a) Completion Rates

A total of 3,779 inmates have been emplaced since 2000 and as of 2008, 3,099 inmates had successfully completed the programme. As can be seen from the following table,⁴⁰ recidivism rates have fallen significantly among offenders on the scheme since its inception.

Recidivism rates of WRS inmates who have completed the programme		
	WRS inmates who have completed the programme	General population
2002 cohort	13.3%	31.2%
2003 cohort	22.7%	24.9%
2004 cohort	19.0%	23.7%
2005 cohort	18.9%	24.2%

B. Raising Awareness: The Yellow Ribbon Project

The efforts by the Community Court and the Prison Service cannot exist in a vacuum. Successful rehabilitation of offenders and ex-offenders “must be accompanied by a progressive societal attitude towards ex-offenders”.⁴¹ In 2004, the Yellow Ribbon Project was launched to raise awareness of the stigma faced by ex-offenders and to educate the public to show compassion to them. Efforts to raise awareness include “Wear A Yellow Ribbon Day”, concerts, conferences, exhibitions, etc. The widely successful project has received accolades from international experts and a very honourable mention at the 2007 United Nations Grand Award.⁴² It continues to garner greater acceptance of ex-offenders by the community⁴³ and contributes to the development and implementation of reintegration programmes for ex-offenders.

V. CONCLUSION

Experience has shown that the conventional methods of imposing custodial sentences and fines with only considerations of retribution, deterrence and prevention are not effective in the long run. They also do not satisfactorily deal with crimes which have arisen out of changing social trends. A criminal justice system worthy of public confidence must respond to these needs. Singapore has adapted accordingly as reflected by the efforts of the Community Court and the Prison Service. Thus far, the Community Court’s holistic approach towards its treatment of offenders has yielded positive results and has been well received by the community. The modern approach of combining rehabilitation and restorative justice with the traditional principles of sentencing is set to gain greater use with the likely increase in sentencing options. With that, a low crime rate can be achieved while maintaining custodial sentences as a last resort.

⁴⁰ Courtesy of Singapore Prison Service.

⁴¹ Chief Justice Chan Sek Keong, *op.cit.* n.5 above.

⁴² K Shanmugam, *op.cit.* n.4 above.

⁴³ http://www.yellowribbon.org.sg/pages/conference_2008.html

ANNEX A

I. PP v JOHN ONG GEOK YEOW

The offender was convicted on one count of voluntarily causing hurt to a public officer with the intention of deterring the latter from discharging his duty. In the course of committing the offence, John landed several blows to the body of the police officer.

In sentencing the offender to imprisonment for a period of two months with the added condition that he undergo police supervision for 12 months after the expiration of the sentence, the Court took into account the report from the Institute of Mental Health (IMH). The IMH report stated that John suffered from schizophrenia. Further, the report also indicated that John was likely to have been in a state of acute relapse during the time of the offence.

The sentence imposed by the Court was arrived at after balancing the need for deterrence and the importance of rehabilitation in this case. Incarceration of John – at least for a short period – was required to drive home the message that attacking a public officer constitutes a serious offence. Yet, the short period of incarceration, together with the imposition of police supervision, demonstrates the Court's focus upon the importance of rehabilitating the root cause of John's offence.

II. PP v YEO GEOK HUAY

Mdm Yeo committed the offence of voluntarily causing hurt to a police officer with the intention of deterring the officer from discharging his duty. At the time of the offence, the police officer was responding to a complaint from Mdm Yeo's neighbour that the music from her home was too loud. Upon arrival at Mdm Yeo's unit, the police officer was charged upon by Mdm Yeo and punched in the head and body.

The Court had called for a report from the IMH prior to sentencing. The report reflected Mdm Yeo's psychiatric history dating back to 2003. The psychiatrist's diagnosis stated that the offender suffered from Major Depressive Disorder: a condition which causes heightened levels of aggression. Noting that Mdm Yeo's offences were all inextricably linked to her depressed mood, the Court recommended that she undergo medical treatment upon her release from six weeks' imprisonment.

Just like in the preceding case involving John's assault on a public officer, Mdm Yeo was similarly sentenced to a short period of imprisonment. Considerations of deterrence aside, the focus upon rehabilitation is evident by the Court's recommendation that she undergo medical treatment upon her release.

III. PP v CHEONG AH SIEW

Mdm Cheong was convicted of committing a rash act so as to endanger the personal safety of others. Her actions in throwing several items out of her ninth storey flat constituted the criminal offence in question.

The IMH report called for by the Court diagnosed Mdm Cheong as having a long history of Schizoaffective Disorder. One characteristic of this disorder is to cause sufferers to act rashly and impulsively.

The judge ordered conditional discharge for 12 months. In his judgment, the district judge stated that the existence of a serious mental disorder is a relevant factor in determining the type of sentence which an offender receives. His Honor also stated that in the process of coming to his decision, he had considered the impact of the disorder upon the offender. Further, he was of the view that rehabilitation – through psychiatric treatment – was the predominant sentencing consideration in this case as it was fundamental to preventing Mdm Cheong from committing offences in the future.

IV. PP v HONG CHEE MENG

Mr. Hong was convicted of the same offence as Mdm Cheong. He was arrested for throwing several items out of the kitchen window of the HDB flat. He had a history of previous admissions into IMH, and had been diagnosed as a danger to the public due to alcohol induced brain damage. Prior to sentencing, the Court called for an IMH report. The diagnosis of Mr. Hong stated that alcohol intoxication and brain damage caused him to have impaired judgment and loss of impulse control during the time of the offence. The report also stated that in the absence of alcohol consumption, it was likely that he would not have committed the offence.

The judge granted Mr. Hong conditional discharge for a period of 12 months in view of his potential for rehabilitation. Further, his parents were bound in the sum of \$1,000 to ensure his good behaviour throughout the duration of those 12 months.

V. PP v MOHAMAD SANI MD SAID

The accused person pleaded guilty to one count of committing a rash act so as to endanger the personal safety of others. He had thrown several items, including a BMX bicycle metal frame, from the 4th floor of a HDB block.

The IMH report called for by the Court stated that he had been suffering from Schizophrenia since 1984, and that his IQ level of 67 rendered him mildly retarded. Unable to work, he was a vagrant sleeping in a HDB corridor and begging for food. The psychiatrist's recommendation was that the accused be placed in a Welfare Home.

The judge ordered conditional discharge for 12 months and for the accused's aunt to execute a bond amounting to \$1,000. The Court opined that a custodial sentence would fail to achieve the aims of general deterrence. Further, the judge also stated that punishment or probation would be inappropriate in this case as the accused did not have the financial means to support himself, much less pay a fine. Taking into account the accused person's medical condition, and the need for psychiatric treatment, the judge consulted with the IMH psychiatrist to work out a treatment plan for the accused. In relation to his destitution, liaison with the MCYS resulted in a programme under which the accused person would be admitted into a Welfare Home for six months while he underwent rehabilitative and vocational training.

From the outcome of the sentencing process, it is evident that the main objective of the Court in this matter was to ensure that the accused gains access to the services necessary for him to be a useful citizen integrated into society.

VI. PP v CHONG KUET CHIEN

The accused person pleaded guilty to using criminal force on the victim with the intention to outrage her modesty. He had used his right index finger to touch the victim's thigh.

The IMH report reflected that the accused suffered from schizophrenia, and was in a state of relapse during the time of the offence. In the psychiatrist's opinion, the illness probably contributed to the accused's criminal conduct during the time of the offence. The psychiatrist also recommended that the court mandate long term treatment of the illness as part of the sentence imposed.

Having considered the report from the IMH, the judge sentenced Mr. Chong to five weeks' imprisonment and police supervision for 12 months following the expiration of the term of imprisonment. On top of which, the accused agreed to reside at the Helping Hand Halfway House under the supervision of a social worker by the name of Freddie Ho. Further, he was to adhere strictly to a treatment plan prescribed by Dr. Kenneth Koh of the IMH.

From the sentence imposed, it is evident that retribution for the suffering of the victim – in the form of a custodial sentence – was balanced by the aims of reformation of Mr. Chong through psychiatric treatment.

VII. PP v MUHAMMAD FAUZI BIN MASOOD

The accused was 17. He committed the offence of housebreaking when he and an accomplice decided to look into flats for any items which could be stolen. Fauzi chanced upon a hand phone near the window and he took the phone by sliding his hand through the open window. Despite his youth, the accused had previously committed several offences including snatch theft and housebreaking by night to commit theft. For those offences, he had been ordered to reside in the Muhammadiyah Welfare Home for three years. It must be noted that the offence in question was committed when he had absconded from the Home.

The MCYS was requested to provide a psychological report on the accused. Their assessment was that the accused was within the mild intellectual functioning range. Given his condition, he was susceptible to negative influence from his peers. Other than his intellectual condition, lack of parental supervision and management, as well as lack of personal responsibility, contributed to his risk of engaging in future criminal conduct. The psychologist made several recommendations to alter the course of his future. First, that he attends offence specific treatment programmes which are tailored to his learning ability. Secondly, it was pertinent that he be taught peer refusal skills. Finally, in order to ensure greater parental supervision over him, the accused's father was asked to attend parenting sessions.

The Court took heed of the recommendations by the MCYS and imposed a sentence of 18 months' supervised probation. Attached to the probation order were the following conditions: firstly, that the accused resides at the Muhammadiyah Welfare Home; secondly, he was to remain indoors from 9pm to 6am; thirdly, that he be enrolled in a suitable educational institution and abide by all rules and conditions imposed by the school and relevant authorities; fourthly, that he be taught peer refusal skills and lastly, that his father executes a bond of \$5,000 to ensure that the accused person's conduct is in compliance with all conditions of the probation order.

The sentence aimed to rehabilitate the accused person by ensuring that he was placed in environments conducive to reformation. Mandating that he reside at the Welfare Home as well as attend an educational institution not only ensured that he received education in a disciplined environment, it also prevented him from being exposed to negative influences. Further, enlisting the help of his father certainly increased the probability that the accused would have access to greater parental control – which is an indispensable element in nurturing good behaviour.

VIII. PP v LIM KENG SENG

The accused person was a male aged 62. He pleaded guilty to a charge of being in possession of a knife without lawful authority or purpose.

The IMH assessed that at the time of the offence, Mr. Lim was suffering from depression. He had been brooding over the fact that he had been diagnosed with cancer.

The Court ordered that the accused be given a conditional discharge for 12 months. In light of the need to ensure his good behaviour, the accused person's son was ordered to execute a bond of \$1,000, on top of which the latter also undertook to send his father for treatment for his depression.

ANNEX B

Parliament No: 11
 Session No: 1
 Volume No: 85
 Sitting No: 7
 Sitting Date: 2009-01-19
 Section Name: ORAL ANSWERS TO QUESTIONS
 Title: SINGAPORE'S PENAL POLICY (Review)
 MPs Speaking: Mr Lim Biow Chuan; The Minister for Law (Mr K Shanmugam)

SINGAPORE'S PENAL POLICY (Review)

5. **Mr Lim Biow Chuan** asked the Minister for Law whether there is any need to review Singapore's penal policy in view of the statement in the latest issue of the *Law Gazette* by the President of the Law Society of Singapore Mr Michael Hwang that Singapore is sadly lacking a principled and transparent penal policy.

The Minister for Law (Mr K Shanmugam): Sir, I thank Mr Lim for his question. Mr Hwang, the President of the Law Society, in his article in the *Law Gazette* asserts that detailed statistics on crime and punishment should be published and that not publishing such statistics has prevented social scientists from undertaking adequate research on the causes of crime and the effects of current penal policies on prisoners. And he says that this has resulted in our system being unprincipled, and rigorous regular research with full access to relevant information will help us decide on issues like the effectiveness of capital punishment.

I will deal with each of the three assertions.

About statistics not being published - this assertion is questionable for two reasons. First, Mr Hwang does not make clear what data (which would help in penal research) that he is referring to as not having been published. Second, law enforcement agencies such as the Singapore Police Force and Central Narcotics Bureau do publish crime and drug offence statistics regularly. Where there is public interest to be served, additional relevant information is collected and disseminated.

In addition, it should be noted that Home Team departments also undertake qualitative and quantitative research, often in collaboration with independent researchers, on topics relating to crime, punishment and criminal behaviour. Further, as a matter of practice, assistance is also given to researchers, including students, who wish to do serious research and such research has been done. To suggest to that, there are inadequate published statistics and that that has prevented proper research is therefore quite untenable.

I will now deal with the second of his assertions - has a lack of statistics led to our penal system being unprincipled?

Since the basis of his assertion - that we do not publish statistics - is itself not clear, this further conclusion is equally questionable. Further, any objective analysis of our penal system will show that the system is based on sound practical philosophy and principles, which have been made clear several times.

While we take a tough stand on crime, we also believe strongly in compassion and rehabilitation. These principles underpin our approach to:

- (i) principles of prescribing punishment and sentencing;
- (ii) treatment and rehabilitation of prisoners when they are in prison; and
- (iii) reintegration of ex-offenders back into society.

Let me deal with punishment and sentencing. The Government's approach to prescribing punishments

is a matter of public record. During the Second Reading (in 2007) of the amendments to the Penal Code, our approach was again restated clearly. In brief summary, these are:

- (i) the type and quantum of punishment should provide sufficient flexibility to the Courts to mete out an appropriate sentence in a particular case;
- (ii) the prevalence of the offence;
- (iii) the proportionality of the penalty to an offence, taking into account its seriousness; and
- (iv) the relativity in punishment between related offences.

On sentencing, our Courts have set out the applicable principles. Our former Chief Justice, Mr Yong Pung How, had published over 882 judgments during his time on the Bench, several of which relate to criminal offences. Our current Chief Justice has been equally prolific. Subordinate Court judges publish *Sentencing Practice in the Subordinate Courts*, which is a sentencing guide, making accessible the sentencing approach for a wide range of offences. This approach is not based exclusively on either deterrence or retribution alone. Rather, the approach to sentencing an offender is to consider both these aspects, and also take into account other considerations such as potential for rehabilitation, suitability of the punishment for each individual offender and the nature of the offence committed.

Hence, both in prescribing punishments and sentencing offenders, much thought has been given to how justice can be best secured for each individual offender. The Government is also at present exploring Community Based Sentencing options, which will further equip our penal framework with the best tools to advance justice in each particular case.

Let me deal with treatment and rehabilitation of prisoners in prison. As stated earlier, we believe strongly in rehabilitation and we believe that that process should start even while the sentences are being served. Thus, during incarceration, inmates who are genuinely willing to change are given education, training and rehabilitative opportunities that will better help them reintegrate into society after their prison sentences.

Our focus on reintegration of ex-offenders back into society continues after the prisoners are released. The Yellow Ribbon Project (YRP), set up to create awareness on giving second chances to deserving ex-offenders and generate acceptance of ex-offenders back into the community, has been widely lauded by international experts, and has received an honourable mention at the 2007 United Nations Grand Award. Coupled with the YRP was the setting up of a Yellow Ribbon Fund which contributes to the development and implementation of reintegration programmes for ex-offenders.

A key measure of the success of our rehabilitation and reintegration programmes is our recidivism rate, which is now one of the lowest in the world.

Another example of the successful rehabilitation and reintegration programmes for offenders is the Home Detention Scheme. Deserving inmates are released earlier, at the tail-end of their sentences and placed on electronic monitoring to work or study. Prisoners on Home Detention have lower recidivism rates compared to the general population.

Thus, far from being unprincipled, our penal philosophy has been carefully thought through and has been articulated publicly several times. Theoretical arguments on our penal policy, bereft of any reference to these key aspects in our system, may make for good sound bites. But they do not have any real merit. In evolving our policies, we take into account the views of parties involved in the administration of justice, including the courts, law enforcement agencies, civic interest groups, the legal profession, academia and the Law Society.

I will now deal with Mr Hwang's final assertion relating to capital punishment. His suggestion is that publication of detailed statistics will lead us to a possibly conclusive answer to the debate on capital punishment.

The debate on capital punishment, Sir, is not going to be settled on the basis of statistics. Leaving aside the fact that it is not clear, from what Mr Hwang says, as to what statistics are said to be lacking, I should point out that all capital punishment cases are matters of public record in Singapore and the media usually

widely covers such cases. Each criminal case heard before a court is also a matter of public record.

On the issue of capital punishment itself, the reality is that there is no universal consensus on such punishment, and there is unlikely to be any such consensus, anytime soon. Serious and bitter debate on capital punishment has raged on in many countries. The philosophical and ideological chasms that separate the proponents and opponents of capital punishment are quite unbridgeable. Both sides marshal powerful arguments.

On an issue like this, the Government has to take a stand. And the Government believes that death penalty should be retained. A *Straits Times* survey conducted a few years ago reported that 95% of Singaporeans supported the retention of the death penalty.

Our firm position on crimes and the considerable benefits of such a stand to our society can be illustrated by reference to the drug situation. In a region where drug is a very serious problem, Singapore has kept the problem very much under control and is in fact almost unique in battling it successfully so far. Members know that in the last 15 years, the drug situation has been getting from bad to worse in many countries, both in this region, and in the world.

Why have we succeeded so far, when so many others have not? It is because we took a practical, hard headed approach to the problem and tackled it decisively. In this context, the introduction of the death penalty for drug trafficking has, we believe, had the deterrent effect. There are no widely prevalent syndicated drug activities linked to organised crimes in Singapore, in contrast to the hierarchical and organised drug syndicates and cartels in various countries. As a result of our policies, thousands of young people have been saved from the drug menace.

Singaporeans appreciate the safe environment here. And the international community has taken note of our success in maintaining law and order. In 2008, the Institute for Management Development (IMD) World Competitiveness Yearbook ranked Singapore first in personal security and private property.

Sir, in closing, let me assure Members that our approach to penal policy is both principled and transparent. And, quite fundamentally, the approach has been shown to work, ensuring the safety and security of our citizens. We will continue to review our approach and ensure that it remains relevant and effective.

PARTICIPANTS' PAPERS

THE IMPROVEMENT OF THE TREATMENT OF OFFENDERS THROUGH THE ENHANCEMENT OF COMMUNITY-BASED ALTERNATIVES TO INCARCERATION

*Boitumelo Makunga**

I. INTRODUCTION

The states of Africa are diverse and multifarious; they are sovereign independent states in their own right, with differing histories, cultures, traditions, languages and institutions. However, for all their diversity they do share some commonalities; i.e. the international conventions and agreements to which all or most of them are party and existence of their respective criminal justice systems. In spite of this, commentators have pointed out that the concept of prisons is an alien model and a form of punishment unknown to most societies of pre-colonial Africa in dealing with offenders (Moroka 2008, Mujuzi 2008).

II. BOTSWANA'S PRE-COLONIAL JUSTICE SYSTEM

In Botswana the traditional/indigenous criminal system focused on "reclaiming" the offender from the crime, and the punishment was meant to fit the offence. Moroka points out that at the core of the system was an obligation to "restore the victim and undo the harm done" without condemning the offender to permanent criminal being. The author further states that punishment aimed at "taking the offence out of the offender and not the offender out of society" (4: 2008). The indigenous criminal code was made of two classes: *Crimina in se* i.e. murder, rape, theft, robbery etc. and *crimina prohibita* i.e. hunting outside the hunting season, starting bush fires, ploughing or harvesting out of season, adultery, disrespect for elders, etc.

Offenders were tried at the main community or *Kgotla*. The family, immediate clan and the community at large all had a role to play in dealing with deviant and offensive behaviour that threatened social order. Their participation in the proceedings was crucial in that the offender was given the opportunity to make restitution and the victim would be able to request the type of restorative punishment he or she believed served adequate justice. Moroka maintains that only after several attempts by the community to restore order by employing corrective action would an offender be banished from the community – this would be a last resort where an offender did not attempt to mend her/his ways (2008). There were no institutionalized forms of punishment.

III. THE DUAL LEGAL SYSTEM IN BOTSWANA

During the British colonial era, African Customary law and the Roman-Dutch law co-existed. The "received" law was individualistic and was put in-place to govern the colonial settlers. The customary law governed the indigenous African communities. This co-existence hinged on a "repugnancy clause", i.e. for as long as the Customary Law was not an offence to the colonial administration it was allowed to exist. However, in due course the "received" law became territorial: where the indigenous people broke the settlers' rules, they were governed in accordance to the settlers' laws. This resulted in the *Kgosi* (chief) losing jurisdiction of most criminal and civil matters; the *Kgosi* would mainly preside over all family law matters that involved the indigenous populations or criminal matters between tribesmen. In 1964 the Penal Code came into existence as the set standard to establish a code of criminal law. Significantly, none of the indigenous communities were consulted regarding its conception; i.e. it was "accordingly imposed." One reason for this status quo could have been that Traditional/Customary law was not written. It was encoded in the psyche of the people and passed down by oral tradition. Moroka (2008) asserts that S.10 (8) of the

* Alternative Sentencing Initiative/ Wellness Coordinator, Attorney General's Chambers, Botswana.

Constitution “drove the last nail” into the dignity of the Customary Law by stating: “No person shall be convicted of a criminal offence unless that offence is defined and the penalty therefore is prescribed in a written law: Provided that nothing in this subsection shall prevent a court of record from punishing any person for contempt of itself notwithstanding that the act or omission constituting the contempt is not defined in a written law and the penalty therefor is not so prescribed.”

And thus the way was paved for the current dual legal system as it exists at present in Botswana.

In Botswana the Customary Courts are established under an act of Parliament. Customary Law according to this means: in relation to any particular tribe or tribal community, the customary law of that tribe or tribal community so far as it is not incompatible with the provisions of any written law or contrary to morality, humanity or natural justice. Customary courts have powers to sentence people to imprisonment, and in the exercise of the provision may be guided by the Penal Code of Botswana. Section 18 of the Customary Courts Act provides for the sentences that may be administered and also provides for imprisonment in S. 23. (Refer to Appendix C). The Customary Courts also impose suspended sentences; impose fines and order compensation.

In reference to what has been stated above; it has been asserted that the State became the fundamental player in prosecuting criminal cases; while the role of the communities dwindled. As communities were pushed further and further to the periphery, the fight against crime became the responsibility of the police. Furthermore, *di-Kgosi*¹ who normally preside over cases in the customary courts had to interpret complex statutory law in which they had no training.

In administering criminal justice, the Magistrates Courts also sentence people to imprisonment in accordance with the provisions of S. 60 of the Magistrates Courts Act. Sentences may be suspended according to the discretion of the presiding magistrate. The High Court of Botswana has appellate jurisdiction from any decision of the Magistrate Court and Customary Courts in Botswana; and has power to confirm or amend or set aside any judgment, decision or order and also to impose such punishment whether more or less severe than the court of the first instance. In terms of the law the High Court also has jurisdiction in certain crimes, such as treason and murder, and may impose appropriate sentences accordingly. The Court of Appeal is also established under the provisions of Cap. 04:01 of the Laws of the Republic of Botswana. In terms of S. 7 of the Act, the Court of Appeal shall have, in addition to any other power, authority or jurisdiction conferred by the Act or the Constitution, the power and jurisdiction vested in the High Court. On appeal against conviction the Court of Appeal may set aside a conviction on grounds that it is unreasonable or may quash the conviction (S. 13).

The Prisons Service is the custodian of all the offenders sent by the above-mentioned courts.

IV. THE PROBLEMS OF IMPRISONMENT

The aims of incarceration are retribution, deterrence, protection of the society (i.e. by incarceration), and rehabilitation of the offender. In Botswana, imprisonment is a form of punishment that derives its legitimacy from the Constitution. Section 5 (1) states: “No person shall be deprived of his or her personal liberties save as may be authorized by law in any of the following cases, that is to say (a) in execution of the sentence or order of a court, whether established for Botswana or some other country, in respect of a criminal offence of which he or she has been convicted”.

However, imprisonment as a preferred method of punishment has a number of disadvantages that have an effect on the offender, family, community and national policy. These disadvantages include the following:

- Stigmatization and humiliation of the offender; resulting in prospects that the offender may never regain her or his self-respect and dignity within the community.
- Creation of an environment where offenders “forget” those they have harmed and regard themselves as victims; this in turn creates a sense of bitterness and this builds a culture of vengeance.

¹ *Kgosi* means Chief/ Community Tribal Leader. *Di-Kgosi* is the plural of *Kgosi*.

THE 141ST INTERNATIONAL SENIOR SEMINAR
PARTICIPANTS' PAPERS

- The desire to avenge often leads to further crime, after the offender has been released.
- Since the majority of offenders are adults, imprisonment robs families of the presence and support of key family members and often leaves children without adequate support and parental guidance.
- Imprisonment never takes the interests and the concerns of the offender into consideration.
- Lack of juvenile prison facilities in Botswana results in young people being incarcerated with older “hardened” offenders who pass on their wilful and unruly behaviour to these young and impressionable people. Thus the cycle of crime continues.
- Maintaining offenders in prisons is costly and diverts valuable resources that can be used for other national development projects.

In essence, imprisonment appears not to solve problems, it seems to cause more problems. It fails to achieve deterrence and reform.

V. THE BOTSWANA PRISONS ACT – CAP 21:03

Under the provisions of S.97 of the Prisons Act, courts may order extra-mural labour for offenders. With consent, the offender may be employed under the immediate control and supervision of the public authority on public work or service outside prison. Officers-in-charge have the ultimate control of offenders doing extra-mural labour. The Commissioner of Prisons or an official visitor may also order extra-mural labour for offenders. The disadvantage of ordering extra-mural labour for offenders in Botswana is that it is only available to offenders who have been sentenced to a term of imprisonment not exceeding 12 months. It would be of great assistance to alternative sentencing if the condition of sentencing exceeds 12 months to include a longer period, depending on the gravity of the offence.

VI. JUVENILE JUSTICE SYSTEM

The Juvenile Courts are governed by Sections 22 to 33 of the Children’s Act – Cap 28: 04. A magistrate’s court or customary court may sit for the purpose of hearing a charge against a juvenile (S. 22 (1) a). Section 22 (2) of the Act further states that: “A juvenile court shall not have jurisdiction to hear and determine any charge against any person other than those persons who are between the ages of seven years and 18 years”.

Section 28 of the Act provides that where a child or juvenile is found guilty of an offence the following may be considered:

- (a) dismissing the charge;
- (b) discharging the offender on his entering into a recognizance;
- (c) placing the offender on probation for a period of not less than six months or more than three years;
- (d) sending the offender to a school of industries for a period not exceeding three years or until he attains the age of 21 years; or
- (e) ordering the parent or guardian of the offender to pay a fine, damages or costs.

The Minister of Labour and Home Affairs may establish and maintain shelters for juveniles who have been charged with offences and are waiting to appear before the Juvenile Court. Currently there is a school of Industry that has the capacity to shelter 100 male juvenile offenders. However, there are no facilities for juvenile female offenders, who are currently sheltered with the general female adult prison population.

A. Current Types of Introduced Community-Based Alternatives to Incarceration in Botswana

TYPE OF SENTENCE	DESCRIPTION	ADVANTAGES	DISADVANTAGES	COMMENTS
Extra Mural Labour	Supervised unpaid public work/service carried on outside the prison for not more than 8 hours by an offender whose sentence is not more than 12 months. Or where an offender has to pay a fine not exceeding P800.	* The offender can partake in the decision of whether or not to consent to extra-mural labour. * Offender re-pays debt to society.	* The final decision is taken following an assessment by the parole board – (the decision can be subjective). * Prison officers may be short-staffed with regard to supervising offenders sentenced to extra mural labour.	See Prisons Act Cap 21:03 S.97 – 104.
Corporal Punishment	Caning with a cane approved by the court. The number of caning strokes do not exceed 12 and not more than six for an offender under the age of 18.	The offender re-pays debt to society.	* Only male offenders under the age of 40 are sentenced in this manner. * It is agonizing, both physically and emotionally.	See Penal Code Cap 08:01 S.28 and The Criminal Procedures & Evidence Act Cap 08:02 - S.305
Fines	The offender may be requested to pay a fine in lieu of imprisonment at the discretion of the court.	This can be combined with compensation to the injured party or restitution of the injured party's stolen property.	The offender may not be able to pay the requested amount of money to pay the fine; due to financial constraints. Where the offender is of a high socio-economic status he or she may be under the mistaken believe that he or she can manipulate the justice system to his or her advantage.	See Penal Code Cap 08:01 S.29 and The Criminal Procedures & Evidence Act Cap 08:02 - S.316 & S.318
Discharge without punishment	The offender's charges are dismissed at the discretion of the court following the consideration of the character, antecedents, age, health or mental condition of the accused; or the trivial nature of the offence or the extenuating circumstances in which the offence was committed.	The offender is given the opportunity to redeem him or herself.	The offender may repeat the offence especially where his or her environment contributed to his or her offence.	See Penal Code Cap 08:01 S.32
Discharged into the care of an appointed custodian	An offender who is under the age of 18 is released into the care of a designated suitable person for a specific period. This may be combined with corporal punishment.	The offender receives support & guidance from those close to him or her; and can be counselled formally by the relevant professionals.	The offender may repeat the offence especially where his or her environment contributed to his or her offence.	See The Criminal Procedures & Evidence Act Cap 08:02 - S.304

VII. AUTHORITIES AND AGENCIES WITH COMPETENCE FOR INVESTIGATION OF OFFENDERS

A. The Botswana Police Service

The Botswana Police Service is established by an Act of Parliament – the Police Act Cap 21:01 of 1979. With regard to the general powers and duties of a police officer, S. 6(1) and S. 16(5) of the Police Act states that: “It shall be the duty of every police officer at all times to protect life and property, prevent and detect crime, repress internal disturbance, maintain security and public tranquillity, *apprehend offenders, bring offenders to justice, enforce all written laws* with which the Service is directly charged and generally maintain the peace.”

The main challenge facing the Botswana Police Service is the shortage of qualified personnel to interpret the complex statutory law; this can result in poor quality investigations.

B. The Botswana Local Police

The Botswana Local Police Service is also established by an Act of Parliament – the Local Police Act Cap 21:04 of 1972. With regard to the general powers and duties of a local police officer, S. 8(c) of the Local Police Act states that a Local Police Officer shall: “preserve the public peace, prevent the commission of offences and *apprehend all persons in respect of whom he holds a valid warrant of arrest.*”

Furthermore, S.9 states that a Local Police Officer: “shall at all times co-operate with the Botswana Police Force and shall, if the President so directs in writing, be subject to the Orders of the Commissioner of Police.”

This gives Local Police the power to in effect operate in the same manner as Botswana Police Officers. However, the main challenge facing the Botswana Local Police Service is the shortage of qualified personnel who are able to interpret the complex statutory law; this can result in poor quality investigations.

C. The Directorate of Corruption and Economic Crime

The Directorate of Corruption and Economic Crime (DCEC) is established by an Act of Parliament – the Corruption and Economic Crime Cap 08:05 of 1994. With regard to the general powers of the Directorate, S.6 (a. – d.):

The functions of the Directorate shall be

- (a) to receive and investigate any complaints alleging corruption in any public body;
- (b) to investigate any alleged or suspected offences under this Act, or any other offence disclosed during such an investigation;
- (c) to investigate any alleged or suspected contravention of any of the provisions of the fiscal and revenue laws of the country;
- (d) to investigate any conduct of any person, which in the opinion of the Director, may be connected with or conducive to corruption

The main challenge facing the DCEC is potential for corruption within the organization; this can result in poor quality investigations.

D. Customs and Immigration

The Customs sector investigates issues of customs, i.e. the regulation of exportation and importation of goods. Immigration investigates issues pertaining to the regulation of the movement of individuals crossing Botswana's borders.

VIII. AUTHORITIES AND AGENCIES THAT HAVE COMPETENCE FOR THE PROSECUTION OF OFFENDERS

The Directorate of Public Prosecutions (DPP) is headed by the Director of Public Prosecutions appointed in terms of Section 51A of the Constitution. Section 51A (3 - 4) states that: “The Director of Public Prosecutions shall have power in any case in which he or she considers it desirable -(a) to institute and undertake criminal proceedings against any person before any court (other than a court martial) in respect of

any offence alleged to have been committed by that person; (b) to take over and continue any such criminal proceedings that have been instituted or undertaken by any other person or authority; and (c) to discontinue, at any stage before judgment is delivered, any such criminal proceedings instituted or undertaken by himself or herself or any other person or authority.”

In relation to this, Section 51A (4) states that: “The powers of the Director of Public Prosecutions under subsection (3) may be exercised by him or her in person or by officers subordinate to him or her acting in accordance with his or her general or special authority.”

The primary mandate of DPP is the prosecution of criminal cases before all courts of the land and criminal applications and appeals arising from criminal litigation.

Prior to 1 October 2005, there was no Directorate of Public Prosecutions and prosecutorial functions were vested squarely and exclusively in the Attorney General. The 1 October 2005 saw the coming into effect of the Constitution (Amendment) Act No. 9 of 2005, which provided for the appointment of a Director of Public Prosecutions with an entrenched tenure of office and constitutional protection.

Parallel to the Constitution (Amendment) Act came into effect the Constitution (Amendment) Consequential Provisions Act No: 14 of 2005, covering at least 30 statutes dealing with criminal prosecution. In terms of the Constitution Amendment Act, in carrying out his or her professional mandate, the Director of Public Prosecutions shall not be under the control or direction of any person, a position consistent with international best practice.

A. Primary Statutes

The primary penal statutes used by the Directorate in criminal prosecution are the Penal Code Cap 8:01 of 1964 and the Criminal Procedure and Evidence Act Cap 8:02 of 1939, which give guidance on general matters of procedure in criminal litigation. However, the prosecutorial mandate extends broadly to all such other legislation as creates penal offences, except where statute provides for trial by court martial. In the prosecution of the Director’s mandate the Director is constitutionally obligated to consult with the Attorney General on matters considered by the latter to be of national importance. The final decision on whom and whether or not to prosecute remains that of the DPP.

However the Director remains under the administrative supervision of the Attorney General (AG) for institutional accountability.

IX. AUTHORITIES AND AGENCIES THAT HAVE COMPETENCE FOR THE ADJUDICATION OF OFFENDERS

Please refer to Part III “THE DUAL LEGAL SYSTEM IN BOTSWANA” (above).

X. TYPES OF TREATMENTS DESIGNATED AND IMPLEMENTED FOR OFFENDERS IN BOTSWANA

The Penal Code came into existence in 1964; it is an Act to establish the code of criminal law. Under Ss. 25 – 33, the Penal Code defines² different punishments as follows: “The following punishments may be inflicted by a court - (a) Death; (b) Imprisonment; (c) Corporal punishment; (d) Fine; (e) Forfeiture; (f) Finding security to keep the peace and be of good behaviour or to come up for judgment; (g) Any other punishment provided by this Code or by any other law.”

XI. CHALLENGES WITHIN THE CRIMINAL JUSTICE SYSTEM IN BOTSWANA

As part of the preparation of compiling this report I interviewed colleagues and people who either worked directly with offenders or within the criminal justice sector. The objective was to obtain their

² Please refer to Appendix A for a description of the above-mentioned punishments in accordance of the Penal Code Ss. 26 -33. Please refer to Appendix B for a description of the above-mentioned punishments in accordance of the criminal procedures and Evidence Act Ss. 298 -315.

views on the current system and to determine their appreciation of community-based alternatives to imprisonment. These officers included:

- Senior Prison Officers
- A Senior Police Officer
- A Chief Magistrate
- A *Kgosi* who presides in the Customary Courts
- The Deputy Director of Tribal Administration
- The Principal of the Ikago School of Industry (who is a professional social worker).

A. Senior Prison Officers

The Prison Officers presented a picture of an effective but under-staffed and under-resourced environment.

- Emphasis was on rehabilitation of offenders. Through the assistance of, and assessment by, the Employment Allocation Committee (EAC) comprising of a team Rehabilitation Officers, offenders are offered employment and skills development while incarcerated. They are employed in areas of agriculture and industry (e.g. welding). However, only a certain number of offenders can be employed because there are more offenders than there are jobs; and the waiting list is long.
- All offenders are treated humanely in accordance with the Prisons Act – Cap 21:03; even where offenders are problematic they are still treated humanely.
- The most familiar alternative to incarceration facilitated by the prison system is extra-mural labour. The offender is supervised by prison officials and is provided with meals in the form of a dried-food ration on a weekly basis. The extra-mural labour is ordered either by the Commissioner of Prisons, a magistrate or any of the courts.

Nelson (2008) asserts that the prison system environment worldwide is isolated and is removed from public attention. This suggests that the environment that prisons operate in, and the challenges faced by prison administrators, are both misunderstood. The author states that:

“The role that they perform is neither obvious nor easily explained to the political leaders and the general public prisons are most often ignored in discussions of mainstream legal and criminal justice matters and reform initiatives; furthermore, they are not considered a priority for funding in comparison to other social and economic challenges that governments face. The absence of increased funding for other criminal justice reforms, such as harsher and longer prison terms for certain offences and significant limitations on the use of non-custodial measures, have significantly impacted on the number of persons incarcerated. While the number of offenders continues to grow in prisons; prison administrators are simply expected to manage.” (Power point pres. 2008)

This observation summarizes my contact with the Botswana Prison Officers; on explaining the purpose for the exercise I was conducting, they were very polite and really wanted to assist but I felt that they withheld vital information. They stated that they were bound by confidentiality; despite that fact I explained that I would treat all information as confidential and would not disclose names or locations. This poses a serious problem because I found out that even attorneys or members of the general populace relied on hearsay from the media, or NGOs who monitor incarcerated offenders' welfare. For example, AIDS NGOs have pointed out that the issue of HIV and AIDS affects the prison population as much as it does the general public; as a result, male offenders should be provided with HIV/AIDS prevention education and condoms because it transpires that male prisoners have unprotected sex with other men (MSM) and this can only exacerbate the spread of HIV and AIDS. This was an issue that is not discussed openly by prison officials.

B. Senior Police Officer

The police officer (who was also a prosecutor) was aware of the current alternatives to imprisonment in Botswana, but felt that the stumbling block within the criminal justice system was the “mandatory minimum sentence” which required sentencing officers to consider incarceration as a first option. Furthermore, he believed that the victim was never adequately considered, focus was mainly on the offender. He believed

that the answer for a solution lay in “a robust public education [*campaign*] on non-imprisonment alternatives to sentencing.”

C. Chief Magistrate

The Chief Magistrate asserts that: crime violates the relationship between the offender, the victim, his or her next of kin and the greater community. It is these relationships that need to be mended if order and peace are to prevail in any society. The answer lies in restorative justice; therefore:

- There is urgent need to review our laws to make our criminal justice system less offender-focused and more victim-focused;
- There is also need to involve the greater community more directly in the criminal process;
- A reparative model of criminal justice is needed which focuses on reparation to the victim by the offender;
- There is need to urgently review the role of customary courts to make them part of the solution and not a part of the problem.

The Chief Magistrate believes that the fragmentation of Botswana’s criminal justice system has contributed to the status quo.

D. Kgosi and Deputy Director Tribal Administration (Customary Courts)

As stated previously; customary courts have powers to sentence people to imprisonment and in the exercise of the provision may be guided by the Penal Code of Botswana. Section 18 of Customary Courts Act provides for the sentences that maybe administered and also provides for imprisonment in Section 23. The Customary Courts also impose suspended sentences, impose fines and order compensation. However, *di-Kgosi** who normally preside over cases in the customary courts have problems in interpreting the complex statutory law in which they have no training. The Deputy Director – Tribal Administration stated that this has resulted in a 70% backlog of cases waiting to be tried at the Customary Court of Appeal. The Deputy Director also stated that the powerlessness of the Customary Courts was also due to the fact that there was little or no collaboration between the Customary Courts and the Administration of Justice Division.

The *Kgosi* expressed concern over “excessive” modernization which has resulted in disorderliness in communities, especially among young people. The *Kgosi* believed that building on a justice system that starts in *di-kgotlana* (village wards), i.e. adults guiding each other and young people, would assist in cutting down on crime. Major cases would be the ones tried at the main *Kgotla* under Customary Law.

Regarding corporal punishment being regarded as “degrading and inhumane” (refer to *Petrus and Another v State. 1984*; as well as *Desai & Others v State. 1987* - Botswana Law reports); the *Kgosi* stated that communities believe it to be a just punishment.

Ultimately, the main challenges facing the Customary Courts are lack of capacity building of the sentencing officers and an inadequate relationship with the mainstream justice system.

E. Principal – Ikago Centre: School of Industry

Ikago Centre, the only school of industry in Botswana, is situated about 50km from the capital city Gaborone. It was established in 2001 to shelter male juveniles charged with horrific crimes ranging from murder to rape to robbery. The Centre has the capacity to house 100 juveniles aged 14 to 18 years. At the time of compiling this report there were 30 male juveniles accommodated there. Ikago does not have facilities for female juveniles. The staff complement is 46. Twenty-two are professional officers and 14 are auxiliary members of staff.

1. Daily Routine

Though the daily routine is fairly structured, the residents at the Centre are reluctant to wear uniforms because of perceived stigma (on their part) by members of the community; therefore it is not compulsory. The daily routine is as follows:

- The day commences at 06:00
- Breakfast – 06:30

THE 141ST INTERNATIONAL SENIOR SEMINAR
PARTICIPANTS' PAPERS

- Assembly – 07:30 (Gives the staff and boys the opportunity to start the day together. Morning talk emphasizes motivation and development of life-skills.)
- The workday begins – 08:30
- Lunch – 12:30 to 14:00

Monday, Wednesday and Friday are Workshop Education days. The Centre residents are taught a number of practical vocational skills which include auto-mechanics, welding, woodwork, etc.

Tuesday and Thursday are mentoring and social skills development days. Led by the social workers and the school nurse, activities include: psychosocial therapy, individual counselling and healthcare education. On alternative Tuesdays and Thursdays the Centre residents work in the community under the supervision of the social workers and the Centre's technical staff.

There is an entertainment hall where the residents can play snooker or watch satellite TV. The Centre also boasts a *marimba* band and the residents are being encouraged to form a traditional dance ensemble.

2. Challenges in Effective Functioning of Ikago Centre

The Principal at the Centre draws attention to the issues that hampered effective functioning of the Centre. These included:

- Unless the Centre administration makes an effort to establish linkages with magistrates in the various jurisdictions, there is no formal linkage between the Centre and the justice system. As a result, many juveniles are sent to the Boy's Prison where they ultimately associate with people hardened by crime.
- It appears that the Centre was established on the spur of the moment and as result it is "a white elephant" that breeds juvenile criminals and does not rehabilitate them. The Centre is not "categorized" as a prison, school or reformatory. The name "School of Industry" is redundant.
- Rehabilitation is only emphasized in the written word, not practically, because the staff members are not qualified in this area. There are occasions were the members of staff have failed as role-models.
- Due to being under-staffed and lack of training, the members of staff are employed on a 07:30 – 16:30 basis, going home at the end of the day. As a result, the Centre residents are left to their own wilful ways during the night under the supervision of security guards hired from an external security company.
- Security is lax. The Centre's boundaries are marked by a high fence with barbed wire on the top to create a "normal" environment as well as to deter the residents from leaving the premises. However, the residents cut through the fence at night to leave the Centre to "entertain" themselves out in the community and engage in disorderly behaviour until the early hours of the morning.
- Due to lack of staff qualified in the area of rehabilitation and due the extreme anger of some of the Centre's residents, vandalism of the Centre's property is commonplace.

In conclusion, the purpose for having Ikago as a juvenile rehabilitation facility is defeated because it has a poor resource base and lacks qualified members of staff ensure its efficient functioning.

Lastly, as a professional working in Botswana's justice system, I would like to draw attention to the fact that, in my experience, the main down-fall of our sentencing systems at present is lack of physical infrastructure, lack of financial resources and lack of human resources to ensure an efficient and effective system.

BIBLIOGRAPHY

Moroka, L. 2008. *The Challenges Of Punishment In A Dual Legal System In Botswana*. (Paper presentation)

Mujuzi, J. D. 2008. *Working With The Media In The Search For Public Support For Alternative Sentencing*. (PowerPoint presentation)

Nelson, R. H. 2008. *Alternative Sentencing Commonwealth Small States Southern Africa Region Programme*. (PowerPoint presentation)

Laws of Botswana last electronic update 31 December, 2006.

Botswana Law Reports 1984 – 2007 (1)

APPENDIX A

THE PENAL CODE Cap 08:01

PART I

General Provisions (ss 1-33)

Punishments (ss 25-33)

26. Sentence of death

(1) When any person is sentenced to death, the sentence shall direct that he shall be hanged by the neck until he is dead.

(2) Sentence of death shall not be pronounced on or recorded against any person convicted of an offence if it appears to the court that at the time when the offence was committed he was under the age of 18 years, but in lieu thereof the court shall sentence such person to be detained during the President's pleasure, and if so sentenced he shall be liable to be detained in such place and under such conditions as the President may direct, and whilst so detained shall be deemed to be in legal custody.

(3) Where a woman convicted of an offence punishable with death is found in accordance with the provisions of section 298 of the Criminal Procedure and Evidence Act to be pregnant, she shall be liable to imprisonment for life and not to sentence of death.

27. Imprisonment

(1) Sentence of imprisonment shall not be passed on any person under the age of 14 years.

(2) A person convicted of an offence punishable with imprisonment for life or any other period may be sentenced for any shorter term.

(3) A person convicted of an offence punishable with imprisonment may be sentenced to pay a fine in addition to or instead of imprisonment.

(4) Notwithstanding any provision in any enactment which provides for the imposition of a statutory minimum period of imprisonment upon a person convicted of an offence, a court may, where there are exceptional extenuating circumstances which would render the imposition of the statutory minimum period of imprisonment totally inappropriate, impose a lesser and appropriate penalty.

28. Corporal punishment

(1) Subject to the provisions of subsection (4), no person shall be sentenced to undergo corporal punishment for any offence unless such punishment is specifically authorized by this Code or any other law.

(2) A sentence of corporal punishment shall be inflicted once only. The sentence shall specify the number of strokes, which shall not exceed 12, nor, in the case of a person under the age of 18 years, six.

(3) No sentence of corporal punishment shall be passed upon any of the following persons-

(a) females;

(b) males sentenced to death;

(c) males whom the court considers to be more than 40 years of age.

(4) Where any male person under the age of 40 is convicted of any offence punishable with imprisonment, other than an offence listed in the Second Schedule to the Criminal Procedure and Evidence Act, a court may, in its discretion but subject to the provisions of section 27(1), order him to undergo corporal punishment in addition to or in substitution for such imprisonment.

(5) Where it is provided that any person shall be liable to undergo corporal punishment such punishment shall, if awarded, be inflicted in accordance with the provisions of section 305 of the Criminal Procedure and Evidence Act.

29. Fines

(1) Where a fine is imposed under any law, then in the absence of express provisions relating to such fine in such law the following provisions shall apply-

(a) where no sum is expressed to which the fine may extend, the amount of the fine which may be imposed is unlimited, but shall not be excessive;

(b) in the case of an offence punishable with a fine or a term of imprisonment, the imposition of a fine or imprisonment shall be a matter for the discretion of the court;

(c) in the case of an offence punishable with imprisonment as well as a fine in which the offender is sentenced to a fine with or without imprisonment, and in every case of an offence punishable with a fine only in which the offender is sentenced to a fine, the court passing sentence may, in its discretion-

(i) direct by its sentence that in default of payment of the fine the offender shall suffer imprisonment for a certain term, which imprisonment shall be in addition to any other imprisonment to which he may have been sentenced or to which he may be liable under a commutation of sentence; and also

(ii) issue a warrant for the levy of the amount in accordance with the provisions of section 303 of the Criminal Procedure and Evidence Act.

(2) In the absence of express provisions in any law relating thereto, the term of imprisonment or corporal punishment ordered by a court in respect of the non-payment of any sum-

(a) imposed as a fine;

(b) ordered to be forfeit to the State;

(c) ordered to be paid under the provisions of any other law,

shall be such as in the opinion of the court will satisfy the justice of the case, but shall not exceed in any such case the maximum fixed by the following scale-

Amount of fine Maximum

Not exceeding P200 14 days or 6 strokes

P 200-P1000 One month or 9 strokes

P 1001-P10,000 Six months or 12 strokes

Exceeding P10,000 Two years imprisonment.

30. Forfeiture

The provisions of this Code with respect to the forfeiture of property to the State shall be in addition to and not in derogation from the provisions of sections 58 and 319 of the Criminal Procedure and Evidence Act.

31. Security for keeping the peace or to come up for judgment

(1) A person convicted of an offence not punishable with death may, instead of, or in addition to, any punishment to which he is liable, be ordered to enter into his own recognizance, with or without sureties, in such amount as the court thinks fit, on condition that he shall keep the peace and be of good behaviour for a time to be fixed by the court, and may be ordered to be imprisoned until such recognizance, with sureties, if so directed, is entered into; but so that the imprisonment for not entering into the recognizance shall not extend for longer than one year, and shall not, together with the fixed term of imprisonment, if any, extend for a term longer than the longest term for which he might be sentenced to be imprisoned without fine.

(2) When a person is convicted of any offence not punishable with death the court may, instead of passing sentence, discharge the offender upon his entering into his own recognizance, with or without sureties, in such sum as the court may think fit, on condition that he shall appear to receive judgment at some future sitting of the court or when called upon.

32. Discharge of offender without punishment

(1) Where, in any trial before a magistrate's court, the court thinks that the charge is proved but is of the opinion that, having regard to the character, antecedents, age, health or mental condition of the accused, or to the trivial nature of the offence, or to the extenuating circumstances in which the offence was committed, it is inexpedient to inflict any punishment, the court may, without proceeding to conviction, make an order dismissing the charge.

(2) An order made under this section shall, for the purpose of re-vesting or restoring stolen property, and enabling the court to make any order under the provisions of sections 318 and 319 of the Criminal Procedure and Evidence Act have the like effect as a conviction.

33. General punishment for offences

When in this Code no punishment is specially provided for any offence, it shall be punishable with imprisonment for a term not exceeding two years or with a fine, or with both.

APPENDIX B

THE CRIMINAL PROCEDURE AND EVIDENCE ACT Cap 8:02 PART XVIII

Punishments (ss 298-315)

298. Sentence of death upon a woman who is pregnant

(1) Where a woman convicted of an offence punishable with death alleges that she is pregnant, or where the court before which a woman who is so convicted thinks fit to order, the question whether or not the woman is pregnant shall, before sentence is passed on her, be determined by the court.

(2) The question whether the woman is pregnant or not shall be determined on such evidence as may be led before the court either on the part of the woman or on the part of the State, and the court shall find that the woman is not pregnant unless it is proved affirmatively to its satisfaction that she is pregnant.

(3) Where in any proceedings under this section the court finds that the woman in question is not pregnant, the woman may appeal to the Court of Appeal and the Court of Appeal, if satisfied that for any reason the finding should be set aside, shall quash the sentence passed on her and, in lieu thereof pass on her a sentence of imprisonment for life.

299. Manner of carrying out death sentences

(1) No sentence of death shall be carried into effect except upon the special warrant of the President, to whom a record of all proceedings in the case shall be forwarded as soon as may be after sentence together with a report upon the case from the officer presiding at the trial.

(2) Such special warrant shall be issued to the Sheriff or his deputy who shall, as soon after the receipt of such special warrant as fitting arrangements for the carrying out of the sentence can be made, execute such special warrant in the place appointed therein:

Provided that the Sheriff or his deputy shall not execute the warrant aforesaid if at any time the President by written notice under his hand to the Sheriff or Deputy-Sheriff intimates that he has decided to grant a pardon or reprieve to the person so sentenced or otherwise to exercise the prerogative of mercy with regard to him. Any notice by the President under this proviso shall be construed for all purposes as a cancellation of the warrant aforesaid.

300. Cumulative or concurrent sentences

(1) When a person is convicted at one trial of two or more different offences, or when a person under sentence or undergoing punishment for one offence is convicted of another offence, the court may sentence him to such several punishments for such offences or for such last offence (as the case may be) as the court is competent to impose.

(2) Such punishments, when consisting of imprisonment, shall commence the one after the expiration, setting aside or remission of the other, in such order as the court may direct, unless the court directs that such punishments shall run concurrently.

301. Conviction of other charges pending

Where an accused person is found guilty of an offence, the court may, in passing sentence, take into consideration any other charge of a similar offence then pending against the accused if the accused admits the other charge and desires it to be taken into consideration and if the prosecutor of the other charge consents.

302. Imprisonment in default of payment of fines

Whenever a court has imposed upon any offender a sentence of a fine without an alternative sentence of imprisonment, and the fine has not been paid in full or has not been recovered in full by a levy, the court which passed sentence on the offender may issue a warrant directing that he be arrested and brought before the court which may thereupon sentence him to such term of imprisonment as could have been imposed

upon him as an alternative punishment in terms of section 29 of the Penal Code or other written law.

303. Recovery of fine

(1) Whenever an offender is sentenced to pay a fine, the court passing the sentence may, in its discretion, issue a warrant addressed to the Sheriff or messenger of the court authorizing him to levy the amount by attachment and sale of any movable property belonging to the offender although the sentence directs that, in default of payment of a fine, the offender shall be imprisoned. The amount which may be levied shall be sufficient to cover, in addition to the fine, the costs and expenses of the warrant and of the attachment, and sale thereunder.

(2) Such warrant when issued by the High Court may be executed anywhere within Botswana.

(3) Such warrant, if issued by a magistrate's court, shall authorize the attachment and sale of the movable property within the local limits of the jurisdiction of such magistrate's court, and also without such limits when endorsed by the magistrate having jurisdiction in the place where the property is found.

(4) If the proceeds of sale of the movable property are insufficient to satisfy the amount of the fine and the costs and expenses aforesaid the High Court may issue a warrant, or in the case of a sentence by any magistrate's court may authorize such magistrate's court to issue a warrant, for the levy against the immovable property of the offender of the amount unpaid.

(5) When an offender has been sentenced to pay a fine only or, in default of payment of the fine, to imprisonment, and the court issues a warrant under this section, it may suspend the execution of the sentence of imprisonment and may release the offender upon his executing a bond with or without sureties as the court thinks fit, on condition for his appearance before such court or some other court on the day appointed for the return to such warrant, such day not being more than 15 days from the time of executing the bond; and in the event of the amount of the fine not having been recovered, the sentence of imprisonment shall be carried into execution at once.

(6) In any case in which an order for the payment of money has been made on non-recovery whereof imprisonment may be awarded and the money is not paid forthwith, the court may require the person ordered to make such payment to enter into a bond as prescribed in subsection (5), and in default of his doing so may at once pass sentence of imprisonment as if the money had not been recovered.

(7) When an offender has been sentenced to pay a fine only or, in default of payment of the fine, to a period of imprisonment, and before the expiry of that period any part of the fine is paid or levied, the period of imprisonment shall be reduced by a number of days bearing as nearly as possible the same proportion to the number of days to which such person is sentenced as the sum so paid and levied bears to the amount of the fine. An amount which would reduce the imprisonment by a fractional part of a day shall not be received. No payment of any sum under this section need be accepted otherwise than during the ordinary office hours.

304. Manner of dealing with convicted juveniles

(1) Any court in which a person under the age of 18 years has been convicted of any offence may, instead of imposing any punishment upon him for that offence (but subject to the provisions of section 26(2) of the Penal Code) order that he be placed in the custody of any suitable person designated in the order for a specific period:

Provided that such order may be made in addition to the imposition of corporal punishment; and provided further than no order made in terms of this subsection shall direct that the convicted person shall remain in the custody in which he has been placed after he attains the age of 18 years.

(2) Any person who has been dealt with in terms of subsection (1) and who absconds from the custody in which he was placed may be apprehended without warrant by any policeman and shall be brought as soon as may be before a magistrate of the district in which he was apprehended.

(3) When any person is brought before a magistrate under the provisions of subsection (2) the magistrate shall, after having questioned the absconding person as to the reason why he absconded, order-

- (a) that he be returned to the custody from which he absconded;
- (b) that he be placed in the custody of another person for the remaining period of the original order; or
- (c) that he be committed to prison for the remaining period of the order made under subsection (1).

305. Corporal punishment

(1) When a person is sentenced to undergo corporal punishment such sentence shall be a sentence of caning and shall be in accordance with the following provisions-

(a) the caning shall be carried out in a manner and with a cane of a type approved by the Minister, who may approve different types of cane for different classes of person;

(b) no caning shall be inflicted on any convicted person until he has been certified by a medical officer to be fit for such punishment; caning shall only be inflicted in the presence of a medical officer, or, if one is not available, in the presence of a magistrate; the medical officer or magistrate shall immediately stop the infliction of further punishment if he considers that the convicted person is not in a fit state of health to undergo the remainder thereof and shall certify the fact in writing;

(c) whenever under the provisions of paragraph (b) any medical officer or magistrate has certified that any prisoner sentenced to undergo caning is not in a fit state of health to undergo the whole or the remainder thereof he shall immediately transmit his certificate to the court which passed the sentence or to a court having jurisdiction which may substitute another punishment in lieu of the sentence of caning; such prisoner may lawfully be kept in custody pending the decision of the court to which the medical officer or magistrate has transmitted his certificate as hereinbefore provided;

(d) no sentence of caning shall be carried out by instalments;

(e) where at any one sitting of a court more than one sentence of caning is imposed on any person, the sentences so imposed shall be deemed to be one sentence for the purposes of subsection (2) of section 28 of the Penal Code.

(2) Every sentence of corporal punishment shall be carried out privately in a prison: Provided that in the case of a person under 18 years of age the court before which such person is convicted may direct that the punishment be administered by such person and in such place as it may specify and in such case the parent or guardian of such first mentioned person shall have the right to be present.

(3) The Minister may by statutory instrument make an order specifying such places as he may consider proper for administering corporal punishment in traditional manner with traditional instruments.

306. Recognizances to keep the peace and be of good behaviour

If the conditions upon which any recognizance or security under section 31 of the Penal Code was given are not observed by the person who gave it, the court may declare the recognizance or security to be forfeited and any such declaration or forfeiture shall have the effect of a judgment in a civil action in that court.

307. Payment of fine without appearance in court

(1) When any person has been summoned or warned to appear in a magistrate's court or has been arrested or has been informed by a peace officer that it is intended to institute criminal proceedings against him for any offence, and an officer holding a rank or post to be designated by the Minister from time to time for the purposes of this section by order published in the *Gazette*, has reasonable grounds for believing that the court which will try the said person for such offence will, on convicting such person of such offence, not impose a sentence of imprisonment or corporal punishment or a fine exceeding P200, such person may sign and deliver to such officer a document admitting that he is guilty of the said offence; and-

(a) deposit with such officer such sum of money as the latter may fix; or

(b) furnish to such officer such security as the latter deems sufficient, for the payment of any fine which the court trying the case in question may lawfully impose therefor, not exceeding P200 or the

THE 141ST INTERNATIONAL SENIOR SEMINAR
PARTICIPANTS' PAPERS

maximum of the fine with which such offence is punishable, whichever amount is the lesser, and such person shall, subject to the provisions of subsection (8), thereupon not be required to appear in court to answer a charge of having committed the said offence.

(2) Such person may at any time before sentence is passed upon him in terms of subsection (5) submit to any person in charge of the aforesaid document an affidavit setting forth any facts which he desires to bring to the notice of the court in mitigation of the punishment to be imposed for the said offence, and such affidavit shall be submitted together with the said document to the court which is to pass the sentence.

(3) An officer designated as aforesaid, if he is not the public prosecutor attached to the court in which the offence in question is triable, shall, as soon as practicable after receiving a document referred to in subsection (1), transmit it to such public prosecutor.

(4) Whenever such public prosecutor has received any such document he shall transmit it to the clerk of the said court: Provided that before doing so he may report the matter to the Director of Public Prosecutions and ask him for his directions thereon.

(5) After receiving such document the clerk of such court shall cause it to be numbered and filed consecutively in the records of that court in a file to be known as the criminal record (admission of guilt) file, which file shall for the purposes of any written law be deemed to be a criminal record book of that court and the person in question shall, subject to the provisions of subsection (8), thereupon be deemed to have been convicted by such court of the said offence, and such court shall pass sentence upon such person in accordance with law: Provided that such court may decline to pass sentence upon him and may direct that he be prosecuted in the ordinary course, and in that case, if the said person has been summoned or warned in terms of subsection (1), he shall be summoned afresh to answer such charge as the public prosecutor may prefer against him.

(6) If the court imposes a fine on such person such fine shall be paid out of any sum deposited in terms of paragraph (a) of subsection (1), or if security has been given in terms of paragraph (b) of subsection (1) and the fine has not been paid in accordance with the terms of the security, the latter, if corporeal property, may be sold by public auction and the fine paid out of the proceeds of the sale: Provided that if the whereabouts of such person are known, written notice of the intended sale and of the time and place thereof shall be given to him not less than three days before the sale takes place.

(7) If any balance remains of any such deposit or of the proceeds of any such sale, after payment of such fine, such balance shall be paid over to the person who made such deposit or gave such security and if such deposit or such security is insufficient to pay the fine imposed, the balance remaining due shall be recovered from the person upon whom the fine was imposed in the manner provided in this Act.

(8) At any time before sentence has been passed upon the person in question under subsection (5), the Director of Public Prosecutions may direct that no action be taken in the matter under subsections (5), (6) and (7), but that such person be brought to trial in the ordinary manner: Provided that in that case, if such person has been summoned or warned in terms of subsection (1), he shall be summoned afresh to answer such charge as the Director of Public Prosecutions may direct.

(9) If at the conclusion of the trial referred to in subsection (8) the person tried is sentenced to pay a fine, the provisions of subsections (6) and (7) shall apply.

(10) If at the conclusion of any proceedings against any person under this section, no fine is imposed upon him, the money or security deposited by or on behalf of such person shall be returned to the person who made the deposit.

308. Powers as to postponement and suspension of sentences

(1) Whenever a person is convicted before the High Court or any magistrate's court of any offence other than an offence specified in the Second Schedule, the court may in its discretion postpone for a period not exceeding three years the passing of sentence and release the offender on one or more conditions (whether as to compensation to be made by the offender for damage or pecuniary loss, good conduct or otherwise) as the court may order to be inserted in recognizances to appear at the expiration of that period,

and if at the end of such period the offender has observed all the conditions of the recognizances, the court may discharge the offender without passing any sentence.

(2) Whenever a person is convicted before the High Court or any magistrate's court of any offence other than an offence specified in the Second Schedule, the court may in its discretion pass sentence, but order that the operation of the whole or any part of the sentence be suspended for a period not exceeding three years, which period of suspension, in the absence of any order to the contrary, shall be computed in accordance with the provisions respectively of subsections (3) and (4). Such order shall be subject to such conditions (whether as to compensation to be made by the offender for damage or pecuniary loss, good conduct or otherwise) as the court may specify therein.

(3) The period during which any order for the suspension of a part of a sentence, made under subsection (2) and affecting a sentence of imprisonment shall run, shall commence on the date upon which the person convicted was lawfully discharged from prison in respect of the unsuspended portion of such sentence, or if not then discharged because such person has to undergo any other sentence of imprisonment, such period shall commence upon the date upon which such person was lawfully discharged from prison in respect of such other sentence. If any portion of such other sentence is itself suspended, the periods of suspension of all such sentences shall, in the absence of any order to the contrary, run consecutively in the same order as the sentences.

(4) The period during which any order for the suspension of the whole of a sentence of imprisonment shall run, shall commence-

(a) where the convicted person is not serving another sentence, from the date from which the sentence wholly suspended was expressed as taking effect, or took effect; and

(b) where the convicted person is serving another sentence, from the date of expiration of that sentence including any period thereof which may be subject to an order of suspension.

(5) If during the period of suspension of the whole of a sentence the convicted person is sentenced to imprisonment the portion then remaining of the sentence wholly suspended shall be deemed to be consecutive to the sentence of imprisonment subsequently awarded.

(6) If the offender has, during the period of suspension of any sentence under this section, observed all the conditions specified in the order, the suspended sentence shall not be enforced.

309. Commencement of sentences

Subject to the provisions of section 308, a sentence of imprisonment shall take effect from and include the whole of the day on which it is pronounced unless the court, on the same day that sentence is passed, expressly orders that it shall take effect from some day prior to that on which it is pronounced.

310. Payment of fines by instalments

Whenever a person is convicted before the High Court or any magistrate's court of any offence other than an offence specified in the Second Schedule, the court may in its discretion order that any fine imposed on such person be paid in instalments or otherwise on such dates, and during such period not exceeding 12 months from the date of such order, as the court may fix therein. If on such date or dates the offender has made all payments in accordance with the order of the court, no warrant shall be issued committing the offender to prison to undergo any alternative imprisonment prescribed in the sentence in default of payment of the fine.

311. Consequences of failure to comply with conditions of postponement or suspension of sentence

(1) If the conditions of any order made, or recognizance entered into, under the provisions of section 308 or section 310 are alleged not to have been fulfilled, the local public prosecutor may, without notice to the offender, apply to any magistrate's court within the local limits of whose jurisdiction the offender is known or suspected to be, for a warrant for the arrest of the offender for the purpose of bringing him before the court to show cause why such offender shall not undergo the sentence which has been, or may be, lawfully imposed.

(2) Any application made under subsection (1) shall be supported by evidence in the form of an affidavit or on oath, that the order or recognizance is still binding upon the offender and that such offender has failed, in a manner to be specified, to observe the conditions thereof.

(3) The court to which application is made under subsection (1) may, if it is satisfied that the offender ought to be called upon to show cause why he shall not undergo the sentence which has been, or may be, imposed, grant a warrant for the arrest of such offender for the purpose of bringing him to court to show cause as aforesaid.

(4) The court, before which any offender appears in consequence of an application under subsection (1), shall read, or cause to be read, to the offender, such application and the evidence given in support thereof, and shall thereupon call upon the offender to say whether he opposes such application.

(5) If such offender does not oppose the application and admits that he has not fulfilled the conditions of the order made, or recognizance entered into, the court may order that the offender shall undergo the sentence which was, or is then, imposed upon him or may make an order under section 312 if the original order was made under section 308(2) or under section 310.

(6) If the offender denies the allegations and opposes the application, the court shall proceed to hear the matter in accordance with the principles generally applicable to criminal trials under this Act, and if it finds that the offender has not fulfilled the conditions of any order made, or recognizance entered into, the court may thereupon order that the offender shall undergo the sentence which was, or is then, imposed upon him, or may make an order under section 312 if the original order was made under subsection (2) of section 308 or under section 310.

312. Further postponement or deferment of sentence

The court before which an offender appears may, if the original order related to the suspension of a sentence under section 308(2), or to the payment of a fine by instalments or otherwise under section 310, and if the offender proves to the court's satisfaction that he has been unable through circumstances beyond his control to fulfil the conditions of such order, in its discretion grant an order further suspending the operation of the sentence or further deferring payment of the fine, subject to such conditions as might have been imposed at the time the original order was made.

313. Magistrates' courts not to impose sentences of less than four days

No person shall be sentenced by a magistrate's court to imprisonment for a period of less than four days, unless the sentence is that the offender be detained until the rising of the court.

314. Discharge with caution or reprimand

Whenever a person is convicted before the High Court or any magistrate's court of any offence other than an offence specified in the Second Schedule, the court may in its discretion discharge the offender with a caution or reprimand, and such discharge shall have the effect of an acquittal, except for the purpose of proving and recording previous convictions.

315. Regulations

The President may make regulations, not inconsistent with this Act, as to all or any of the following matters, namely, the appointment, powers and duties of persons (to be known as probation officers) to whom may be entrusted the care or supervision of offenders whose sentences of imprisonment have been suspended under this Act, the circumstances under which courts of law may entrust such care or supervision to probation officers, the conditions which shall be observed by such offenders while on probation and the varying of such conditions, and generally for the better carrying out of the objects and purposes of this Part.

APPENDIX C

CUSTOMARY COURTS ACT CAP 04:05

12. Criminal jurisdiction

(1) Subject to the provisions of section 13, a customary court shall have and may exercise criminal jurisdiction to the extent set out in its warrant in connection with criminal charges and matters in which the charge relates to the commission of an offence committed either wholly or partly within the area of jurisdiction of the court.

(2) No customary court shall sentence a person to a period of imprisonment in excess of the period of imprisonment authorised in its warrant.

(3) In the exercise of the jurisdiction under the provisions of this section customary courts may be guided by the provisions of the Penal Code.

(4) In any prosecution in a customary court the prosecutor may be either the person who has a right to bring such prosecution under customary law or the Director of Public Prosecutions or any person authorized thereto by the Director of Public Prosecutions.

(5) Notwithstanding the provisions of subsection (2), the President may, by order under his hand, authorize an increased jurisdiction in criminal cases to be exercised by any customary court to the extent specified in the order.

(6) No person shall be charged with a criminal offence unless such offence is created by the Penal Code or some other written law.

13. Cases excluded from the ordinary jurisdiction of customary courts

Subject to any express provision confirming jurisdiction, no customary court shall have jurisdiction to try-

(a) cases in which the accused is charged with-

- (i) treason, riot or any offence involving the security or safety of the State,
- (ii) an offence in consequence of which death is alleged to have occurred,
- (iii) bigamy,
- (iv) any offence under Division II of Part II (Offences against the Administration of Lawful Authority) of the Penal Code with the exception of offences under sections 108, 119, 123, 125 and 128 of the said Division,
- (v) bribery,
- (vi) an offence concerning counterfeit currency,
- (vii) robbery, where the person accused is of or above the age of 21 years,
- (viii) extortion by means of threats,
- (ix) an offence against insolvency law or company law,
- (x) rape,
- (xi) contravention of prohibitions relating to precious stones, gold and other precious metals,
- (xii) such other offences as may be prescribed;

(b) any cause or proceeding whereby divorce or a declaration of nullity of marriage or an order for judicial separation is sought where such marriage has been contracted other than in accordance with customary law;

(c) any cause or proceeding-

- (i) arising in connection with a testamentary disposition of property,
- (ii) arising in connection with the administration of a deceased estate to which any law of Botswana applies,
- (iii) arising under the law relating to insolvency, or
- (iv) involving matters of relationships to which customary law is inapplicable;

(d) cases relating to witchcraft without the general or special consent of the Director of Public Prosecutions.

18. Punishments

(1) Subject to the provisions of subsections (2), (3) and (4) and section 21 and to the provisions of any other law for the time being in force a customary court may sentence a convicted person to a fine, imprisonment, corporal punishment or any combination of such punishments but shall not impose any punishment exceeding those set out in its warrant.

(2) No customary court shall sentence any female or any person who is, in the opinion of the court, of the age of 40 years or over to corporal punishment.

(3) Where any person under the age of 40 years is convicted of any offence, a customary court may, in its discretion, order him to undergo corporal punishment in addition to or in substitution for any other punishment:

Provided that this subsection shall not apply to-

(a) any offence in respect of which a minimum punishment is by law imposed; and

(b) any conspiracy, incitement or attempt to commit any offence referred to in paragraph (a).

(4) No customary court shall subject any person to any punishment which is not in proportion to the nature and circumstances of the offence and the circumstances of the offender.

THE CRIMINAL JUSTICE RESPONSE TO CRIME PREVENTION - GUYANA

*Fay Ingrid Clarke**

I. INTRODUCTION

The subject of crime and the quest for prevention continues to evoke varying responses at every level of society all over the world.

General responses range from emotive to some level of consternation as new types of criminal activity continue to ravage societies and acts which appear senseless often leave victims carrying the pain of their loss for very long periods. Many victims never overcome the trauma of their experience. In recent years, unfolding changes in the general criminal landscape have exposed the devastating effects of the number of heinous crimes now perpetrated by gangs and youth. Additionally, the impact of those who have built empires based on the manufacture, export and sale of illicit narcotics cannot be understated.

The narcotics trade is often accompanied by the export and sale of illegal weapons and ammunition.

The result is that the vast financial base of those parts of the underworld which are involved in illicit drugs, arms and ammunition trafficking have developed structures comprised of a national, regional and trans-national nature. In countries like Guyana, with fragile economies and large segments of the population living in poverty, the lure of 'easy money' makes it difficult, if not impossible, for any one component of the justice system to address in a comprehensive manner the current levels of crime.

As decision makers grapple with the ever evolving, expanding and dynamic nature of crime, many are beginning to recognize that the fight must take a paradigm shift to compensate for the new variables being presented and utilize multi-dimensional responses to confront the situation. Evidence of this global issue has already led world leaders to expand alliances to confront the challenges of crime in the twenty first century.

In many countries, politicians and the general public demand responses which they feel could improve their sense of safety. Lawmakers respond by drafting legislation which increases the length of sentences and imposes new mandatory minimum sentence requirements. The results are burgeoning prison populations which give rise to increased prison fights, unrest, inadequate staffing levels, ineffective or non-existent rehabilitation aims, and unsuccessful reintegration regimes which ultimately result in very high recidivism levels. Guyana has also experienced varying levels of the crime phenomena demonstrated worldwide, and the consequential effects of these realities. However, in spite of limited resources, Guyana's decision makers have undertaken a number of proactive measures to confront the often alarming displays of crime in the nation.

The region's crime situation is not much different from Guyana. Between 1990 and 1999 there were 7,621 murders in Jamaica whilst for the same period, Guyana had 1,100 murders. In 2001, a Barbados Extended Bulletin indicated that Barbados had an increase in crime over the last five years. A Washington report on the Hemisphere, noted Trinidad and Tobago's increasing violent crime rate, of which 70 percent involved drugs, while police in Curacao also noted an increase in murders, of which most were execution style killings. The diagnosis of the source of the crime upsurge in Guyana must thus factor in the 'regional' variable.

This paper will provide a brief overview of the criminal justice system, give insight into the Executive and specific Ministerial responses to the topic, and discuss where we are and the way forward in our efforts to expand present methods and implement new initiatives with specific attention to the introduction of alternative sentencing, community custody and civil society collaboration to confront crime, as pivotal to

* Superintendent of Prisons, Officer in Charge of Training, Welfare & Corrections, Guyana.

crime prevention strategies.

II. BRIEF OVERVIEW OF THE CRIMINAL JUSTICE SYSTEM

The nation of Guyana has three branches of Government, consisting of the Executive, Parliament and Judiciary.

The Judicial system is a hierarchy of Courts comprised of Magistrates, High/Supreme Court, Full Court of the Supreme Court and the Court of Appeal, which is the court of last resort. There are 37 Courts, of which 23 are of the Magistracy and 13 are of the High Court. Guyana also subscribes to the Caribbean Court of Justice based in Trinidad and Tobago, where persons may seek redress for certain kinds of matters for which they failed to obtain victory at the Court of Appeal.

The legal tradition on which the Criminal Court of Appeal law is based consists of the English Common Law and a series of indictable and summary offences, all heard in the Magistrates Court. After a preliminary hearing is held in a Magistrate's Court, indictable matters are heard in the High/Supreme Court. Appeals go to the Full Court of the Supreme Court and finally to the Court of Appeal. Civil practice and procedure is based on the English common law as well as Statutory Law (High Court/Court of Appeal). The majority of civil litigation cases take place in the Supreme Court.

III. BRIEF OVERVIEW OF THE GUYANA PRISON SERVICE

As a colony of the British, Guyana's penal system was known as Her Majesty's Penal Service. The name was changed to The Guyana Prison Service (GPS) in 1957. There are five prisons spread over the northern part of the country; three are in Region Four, where the capital city is also to be found. The GPS is headed by a Director of Prisons who has overall responsibility for the prisons and a Deputy Director responsible for Operations. A Senior Superintendent of Prisons heads the main prison (Georgetown) and a Superintendent of Prisons has responsibility for Officers and Prisoners' Training, Welfare and Corrections.

Other ranks include Assistant Superintendent of Prisons, Cadet Officers, Chief Officers, Principal Officers II, Prison Trade Instructors, Principal Officers I, Prison Officers and Assistant Prison Officers who perform administrative, clerical and custodial duties.

The total prison population now averages 2,900 daily, representing 26 percent of the national population of 770,000, spread over Guyana's ten regions, comprised of over 83,000 square miles, and of whom the majority live on the coast. The main prison now has an average of 1,000 prisoners daily, an increase of approximately 40 percent over the last 18 months and of which close to 60 percent are remand prisoners. The legal responsibility of the GPS is ended when the prisoner is released upon completion of his or her sentence.

The GPS and Parole Board are both within the ambit of the Ministry of Home Affairs and whereas the GPS was established by Prison Act No. 26 under the Laws of Guyana, the Parole Board was established by Parole Act 24/1991 and aimed to promote rehabilitation of offenders through early release on specific conditions of supervision and after-care. The Parole Board is expected to liaise with the Probation Service for home study, the police for records, visit prisons, meet with legal personnel and relatives of prospective parolees. They also have to engage family and other members of the community where the crime occurred, to sensitize them to the parolee. On the granting of parole, the Board also schedules the required contact meetings for the parolee. Additional bodies who supplement rehabilitation efforts of prisoners are Prison Visiting, who have wide-ranging power to intervene in all aspects of prisoners' welfare and treatment as well as make recommendations to the authorities, and the Discharge Aid Committees who assist indigent and needy prisoners on their discharge from prison. In spite of these checks and balances, from time to time, there are known and alleged cases of prisoner abuse and injuries which prison inmates incur due to fights, especially when prisons are overcrowded.

A. Mission Statement of the Guyana Prison Service

"The Guyana Prison Service has the responsibility of custody and retraining of prisoners committed to the prison and to engage in economic and other social programs supportive to National Objectives".

B. Profile of the Prison Population

A large number of the non-indictable and petty crimes are committed by recidivists who account for approximately 50 percent of the prison population. Many of these prisoners are illiterate and come from poor backgrounds, while 30 percent are drug related crimes and 8 percent of the total prison population are awaiting trial for murder.

Current Prison Statistics

Georgetown	New Amsterdam	Mazaruni	Lusignan	Timehri
468 Convicted 570 Remanded	235 Convicted 131 Remanded 83 Females	76 at Mazaruni 114 at Sibley Hall	86 Convicted 4 Remanded	142 Convicted 1 Remanded
32 on Death Row	1 Female on Death Row	N/A	N/A	N/A
Overcrowded by 45 percent	Overcrowded by 50 percent	Overcrowded by 40 percent	Overcrowded by 15 percent	Overcrowded by 30 percent

Due to limited staff and resources as well as prisoner classifications, less than 40 percent of the total prison population receives structured technical and/or vocational, or other, instruction. Moreover, priority is given to security and training is often suspended and officers are assigned custodial duties when staff is limited due to illness or vacation.

IV. ESTABLISHED GPS REHABILITATION PRACTICES

A. Vocational Skills

In exercising its functions, the Guyana Prison Service has historically included a variety of rehabilitation efforts in addressing the mandate expressed in the Mission Statement. The activities related to skills training included literacy, numeracy, tailoring, carpentry, joinery, masonry, building construction, farming, baking, animal husbandry, and the use of a printing press. A large segment of this training was done on a limited scale by skilled tradesmen in the organization who were eventually promoted to the rank of Prison Trade Instructor, as well as by some who were hired with the skill acquired from a Trade Institute or by being sponsored by the GPS to study at a trade school.

B. Coping and Commercial Skills

Other efforts at rehabilitation included periodical instruction on a variety of topics, given by Social Workers, with the aim of achieving behavioural change.

Moreover, a substantial amount of motivational and religious instruction is provided by the main religious bodies (Christian, Muslim and Hindu), which subsequently are often helpful in the prisoners' reintegration process.

In addition, a steel band called the Republican Steel Orchestra was formed and the instruction was given by a prisoner who knew the art. This band produced over a thousand players since its inception, and has even won national competitions and proven to be a sustainable programme. This band was the popular choice of a particular foreign Emissary for performing at several functions held by the British High Commission.

An additional success story is the Republican Boxing Gym which has produced a number of boxers who have made the service proud, both locally and internationally, by winning medals in every class. During their annual week of activities showcasing the Guyana Prison Service, the prisoners beam with a sense of pride on hearing and seeing the admiration of spectators who view the high quality evident in the wood, leather and other crafts made for display to the public. By the female prisoners, intricate expressions are revealed in crocheted items, clothing, pickles, etc.

C. Community Interaction

The Guyana Prison Service has also practiced being involved in the community by providing annual assistance in 'clean up' campaigns at schools, senior citizens' homes, the compounds of the courts, and in painting pedestrian crossings near schools. The Republican band provides musical renditions at various functions and there was formerly an annual concert called "Prisons In Concert" which there are plans to reactivate.

D. Prisoners' Incentive Scheme

A fund referred to as the Prisoners Incentive Scheme (PRISS) was developed to assist prisoners to accumulate money for work undertaken during their incarceration. The principle applied was that the prisoner was assigned one third of whatever he or she earned, one third was assigned the GPS and the final third was placed in a fund used for to purchase items which could be of benefit to the prisoners' welfare.

V. RECENT EXPANSION OF REHABILITATION

Over the past ten years, rehabilitation efforts were expanded to establish a base whereby structured components were developed to ensure that a larger number of prisoners could acquire a marketable skill for use on release as well as provide the coping skills to facilitate successful reintegration.

Expanded Administrative components of this thrust included the design and development of entry poll forms which provide personal, medical and academic data on the prisoner and risk assessment for the selection of prisoners to work within or outside the prison, for classification as trustees or orderlies.

Exit poll forms were designed to obtain data on how the prisoner evaluated his or her experience and to determine whether he or she had a family to return to and their likelihood of successful reintegration.

Structured components of training curricula were developed which focused on addressing major behavioral issues such as, anger management, conflict resolution, sex offenders' rehabilitation, goal setting, building self esteem, overcoming adversity, counselling for addicts, and HIV/AIDS awareness.

Underpinning the foregoing was the developing of a signature project called "Prisoners of Purpose" (POP) established in 2001 by the writer, which saw dramatic change in the formerly violent prison environment at the main prison. The strategy of this project utilizes the peer education concept, and those who successfully participate in the foundational Behaviour Change Program, and display vastly improved attitudes, are then selected as leaders to promote the concepts they were taught and then lead teaching sessions for other prisoners.

Prisoners who were part of this programme shared the principles at other locations when they were transferred.

Over the past ten years, the recidivism rate of those who have attended and participated in the POP programme has been less than five percent. Moreover, none of these prisoners have participated in unrest or major conflict.

A. New Initiatives

The following classes were conducted on a structured manner to the prisoners at various locations, whereby the curricula were prepared in a modular method. All of these programmes were run by committed, external facilitators. Efforts are underway to have the programmes accredited.

The topics were: automobile maintenance, ceramics, barbering, music (keyboard and guitar), making of mulch, upholstery, how to use the computer, electrical installation, small appliance repairs, CXE English, and CXE Spanish.

B. Recruitment of Welfare Officers

Two Welfare Officers were recruited in 2006, and in 2007, a Prison School Teacher who is a graduate of the Cyril Potter College of Education and has nine years' experience as a Senior Master at a High School, joined the GPS Also coming on stream was a skilled Welder/Machinist Fitter. A number of other skilled personnel are expected to join the plan for comprehensive rehabilitation later in 2009.

VI. CHALLENGES TO CHANGE

It is common knowledge that people dislike change and that management faces resistance when change is introduced. The absence of a Change Management Strategy has made the efforts somewhat tedious as people prefer their 'comfort zones'. Moreover, accounts are the same in other countries where the punitive method of prison management was or is practiced. The orientation of persons in 'prison' structures are that prison is not supposed to be nice or comfortable.

In many cases, aggression is the means of control and personnel are trained to have a 'them' against 'us' mentality. These mindsets must be addressed in full awareness that the change cannot or will not happen overnight. This attitude is inherent in the concept held by many that prison should be punitive and retributive in nature. The focal strategy is to provide relevant training for all levels of staff who can be made to see that viable rehabilitation increases safety in the prison environment and for the community when the prisoner is released.

VII. THE WAY FORWARD: COMPREHENSIVE REVIEW OF REHABILITATION IN GPS

The Hon. Minister of Home Affairs, Mr. Clement Rohee MP has consistently demonstrated an intense interest in the subject of prisoners' rehabilitation and has converted that interest to serious actions to make his concern a reality. In addition to approving the hiring of new staff, he (in late 2008) requested that a thorough evaluation be made of the entire system, with a view to creating the conditions whereby every prisoner would be exposed to some skill and behaviour change training. He also gave a commitment to see that increased expenditure is allocated in the 2009 budget to see the refurbishing, equipping and retooling of trade shops at all locations. These increases would result in the acquisition of competently skilled staff and facilities equipped with the relevant machinery for effective training.

A. Education Campaign

Every member of staff must be made aware of the new thrust and be prepared to be part of the change engine for effective rehabilitation. The method to be used can be a 'top down' and 'bottom up' approach with incentives offered for inputs which can benefit the team. Because of the system of 'seniority' where upward mobility is concerned, some effort will be necessary to convince them of the benefits to be derived from the new thrust.

B. Staff Welfare

A vital issue to be addressed when considering expanding rehabilitation of prisoners is the working conditions of staff. This helps deflect the negative responses of personnel who conclude that the prisoners are being given better chances to have their circumstances in life improved than is in fact the case.

Staff training and welfare have also gained the Minister of Home Affairs' attention and emphasis is directed towards providing solutions in these areas. Moreover, he has initiated collaborative agreements with other Ministries such as Agriculture and Health, to join forces in the tasks at hand, which will benefit the Guyana Prison Service. A number of other alliances are being considered, including one with the Ministry of Education and the Ministry of Youth, Culture and Sport.

VIII. ADVANTAGES OF ALTERNATIVE SENTENCING FOR GUYANA

Many modern studies affirm the need to incorporate new strategies in the care and treatment of offenders, with a priority on rehabilitation. In the highly developed countries, much has been said of 'warehousing' of criminals. Richer countries are able to build bigger and more secure prisons, yet this does not necessarily achieve the rehabilitation of offenders. The use of Community Service Orders for certain categories of offences will reduce overcrowding in the prisons and the risk of criminalizing petty and minor offenders. The additional advantage is that the involvement of the community in the process helps change the mindset of larger segments of the society in respect to the concern for the care and treatment of offenders. It is also a critical tool to assist in expanding efforts of reintegration.

I agree with the concept that certain categories of offences do not merit many being given custodial sentences. Therefore, earnest efforts should be put into the implementation of Alternative Sentencing. I

contend that efforts at community-based alternatives to incarceration cannot achieve their fullest potential unless accompanied by strategized yet synergistic efforts to increase awareness in general society that every person who commits a crime does not have to be incarcerated. The public must be enlightened that the stigma prisoners experience on their release and their inability to obtain and maintain gainful employment, often cause them to reoffend.

Other methods which Guyana can implement include diversion, developing halfway houses and transitional correctional centres, community service and boot camps for youth.

IX. CONCLUSION

I recommend that a forum be considered whereby all the stakeholders may be gathered for consultation on the topic. A proposal I submitted to the Hon. Minister on the execution of a National Symposium, to be titled "Collaborating to Confront the Effects of Crime", has earned the endorsement of the Minister of Home Affairs. The aim is to gather the main stakeholders who can be exposed to presentations and plenary sessions to dissect the problems related to incarceration, overcrowding, rehabilitation, reintegration and the valid position to consider alternative sentencing guidelines.

Since 2008, initial discourse has been undertaken with possible funding agencies, in regards to funding the event. A positive response was garnered from a resident foreign diplomatic agency who indicated their interest in the possible funding of such an event.

I am confident that the opportunity for the execution of such an event will provide a common basis for developing strategies which will cement community involvement in efforts to collaborate in order to confront crime in our nation.

APPENDIX

PRESIDENTIAL RESPONSE TO CRIME PREVENTION

FEATURE ADDRESS OF HIS EXCELLENCY PRESIDENT BHARRAT JAGDEO'S AT THE LAUNCHING OF THE NATIONAL DRUG STRATEGY MASTER PLAN, 2005 - 2009

We are gathered here to launch the Guyana National Drug Strategy Master Plan 2005-2009 and I would like to describe the main components of that Master Plan and speak briefly about our approach to the fight against Crime and Violence in our society.

Our approach is guided by our assessment of the crime statistics in Guyana and in the region, the changing nature of crime, particularly its violent and trans-national features, and by what other countries have done and are doing to fight crime. Above all, we are guided by our economic, social and political realities.

This 2005-2009 Plan was drafted in consultation with key persons in my administration, and included Law Enforcement Agencies, the Military and Non-Governmental Organisations and civilian entities. The Plan foresees the establishment of the National Anti-Narcotics Commission (NANCOM) and its associated Secretariat to implement the Strategy. The Commission will be the focal point in this new counter-narcotics strategy which will lead to the overall improvement in the co-ordination by various agencies.

The actual programmed activities that the Commission will implement and oversee over the next five years are divided into Supply and Demand Reduction categories focused on improving:

- Criminal Justice Administrative system through the sustained training of court officials and the provision of better Court facilities and set the Legal Framework in keeping with the regional legal thrust against the drug trafficking industry.
- Improvement of the Intelligence gathering functions of the Law Enforcement agencies and expanding the Joint Intelligence Coordinating Centre which brings together representatives of the intelligence gathering apparatus of the Joint Services for better intelligence-led counter-narcotic operations.
- The Criminal Investigation Department will be strengthened by expanded application of Information Communication and Technology to create a simple central law enforcement database allowing ready access to records and asset holdings of drug traffickers.
- The counter-narcotic agencies will be strengthened by the provision of additional resources. More equipment for will be procured: secure communication, land and river transportation, better border control facilities and the surveillance of our air and sea spaces.
- The National Forensic Laboratory's capacities will be strengthened by the acquisition of up-to-date technology and recruitment of necessary skills.
- International cooperation will be expanded through the ratification of relevant and important international conventions and treaties including
 - the Inter-American Convention on Mutual Assistance on Criminal Matters; and
 - the Inter-American Convention Against the Illicit Trafficking, Manufacturing of Firearms, Ammunition and Explosives.
- Bilateral cooperation will be strengthened between Guyana, and its neighbours and other countries.

Under the Demand Reduction category of the Plan, the following activities would be implemented:

- Developing and implementing safe lifestyle programmes for our youths, strengthening the current health and family life education programmes that target vulnerable women, children and adolescents

THE 141ST INTERNATIONAL SENIOR SEMINAR
PARTICIPANTS' PAPERS

- Providing continuous statistical surveillance on the prevalence of drug use in selected populations, to enhance policy formulation
- Encouraging increased civil society participation in anti-drug abuse activities including advocacy and the provision of services and increased media involvement
- Providing better clinical and behavioural treatment for drug users and abusers through training of relevant personnel and the establishment of additional rehabilitation centres, either directly or giving support to NGOs. This would improve the availability of rehabilitation and counselling services

The implementation of our anti-drug strategy with its programs and activities would need to be resourced by the combined efforts of Central Government, and our bilateral and multilateral partners. At a minimum the incremental financial costs to implement the Master Plan is projected at G\$650M GYD. This is a significant sum of money for Guyana, but appears paltry when compared to the resources provided elsewhere in this hemisphere to fight Narco-trafficking. Clearly, international support would be critical for the successful implementation of the Master Plan.

I am certain that we are all aware that Guyana and the other countries in the Caribbean and in Latin America have seen an upsurge in criminal activities. Statistics, media reports and research all point to an increases and new trends of violence and transnational crime. I know how shocked we all were a few weeks ago when the Minister of National Security in Trinidad and Tobago disclosed the presence of more than 50 criminal gangs in that territory, and in that same week from Jamaica, there were reports of as many as 157 deaths in one month. More recently, the Prime Minister of Barbados referred to the danger for Barbadian communities as a consequence of increased drug trafficking.

My colleague Heads and I have given considerable attention to this growing threat in the Caribbean. That intense focus led to the creation of the CARICOM Ministerial Committee on Crime and Security. Already that body has proposed initiatives for implementation in CARICOM countries.

However, in spite of the implementation of several of these and other initiatives such as the promulgation of new laws allowing easier criminal prosecutions, maritime interdiction, the provision of additional resources (financial, human and technical), the statistics suggest that we are still to attain a sustained and significant impact on Crime and Violence in our region.

I wish to outline a few areas in which I intend to intensify efforts to make our communities safer places to live. First we must heighten all STAKEHOLDERS INVOLVEMENT in implementing crime prevention and crime fighting measures through:

1. Establishment of a National Commission on Law and Order
2. Creation of Community Policing Ministerial Unit
4. Tougher Action Against Racial Incitement And Violence
5. Greater NGO Involvement In Crime Prevention

FOR CRIME PREVENTION, we also intend to pursue:

Penal Reform with emphasis on correction and reintegration

More attention will be directed to the Prison population and specifically from the perspective of ensuring the return of prisoners especially the young and first offenders, to productive lives on their release. In that regard, the staffing of the Guyana Prison Service would continue to be increased according to the approved four-year plan to increase appointments of training instructors. This would provide more opportunities for prisoners to acquire marketable skills during their period of incarceration. We envisage the introduction of new programmes to develop and enhance life skills that will be beneficial to inmates. This hopefully, would reduce recidivism among young offenders.

Heighten attention to Vulnerable and At-Risk Groups

The Administration will provide more resources that will increase the opportunities for the unemployed, unskilled and out-of-school youth and prevent them falling prey to recruitment by anti-social and criminal

elements. This programme will complement existing ones which target 'out-of-school' young people. Many wished to find a job or to continue studying, but they did not have the basic skills or qualification to realize their ambitions. This program will correct this situation and allow them to lead productive lives. We must ensure that they do not get involved in negative activities.

Waiver of Duty and Taxes on Surveillance Technology for the Private Sector

I am disposed to consider the provision of duty and tax concessions on the importation of electronic surveillance technology and other security related items to registered legitimate businesses to protect their business places and aid crime prevention.

1. Traffic:

We are moving to introduce a modern traffic control system with more stringent laws, harsher punishment and rigid enforcement. These would be supported by greater reliance on advanced technology.

2. White-collar crime:

We will focus more attention and resources to combating white-collar crimes, by strengthening the Fraud Squad in the CID by recruitment, additional training and application of relevant technology.

We will commit more resources to enhance the work of the Financial Investigative Unit. Since becoming a member of Caribbean Financial Action Task Force, we now have greater access to training of staff and the preparation of legislation that would make it easier to prosecute money launderers.

3. Immigration:

Due to the increased trans-national nature of crime involving alien smuggling and trafficking in persons, we will modernise our Immigration and Naturalisation services. Therefore, we are introducing machine-readable Passports using an integrated database and will enact tougher legislation to address Immigration-related offences.

We are examining the feasibility of creating a separate entity to deal with Immigration and Naturalisation services.

4. Gun Control:

Due to increased gun-related crimes, my Administration will introduce tougher penalties for those convicted of illegal possession and use of firearms. We shall also expand the Guyana Revenue Authority's ability to detect smuggled weapons at our sea and airports. Other interventions include plans to increase of our military presence in the border areas for better interdiction and increase international co-operation to combat trafficking in firearms.

Strengthen Law Enforcement Agencies:

In addition to all of the above, there is a need for us to continue the increasing budgetary and policy support provided to the Guyana Police Force and other Law Enforcement agencies. . The focus will be on compiling crime statistics for use in guiding policy and operations.

In conclusion, I wish to thank the citizens who work with us to combat crime, and acknowledge our international partners, for their current and anticipated support.

You are invited to join in - making the entire country safer is a national endeavour.

June 2005

ENHANCING CRIME PREVENTION THROUGH COMMUNITY-BASED ALTERNATIVES TO INCARCERATION

*Leo S. Carrillo**

I. INTRODUCTION

The Philippines, just like many other countries in the world, is actively pursuing its commitment in the international community as set forth in the United Nations Standard Minimum Rules for Non-Custodial Measures (The Tokyo Rules) regarding the treatment of its criminal offenders. It has long been accepted that the search for alternatives to incarceration of offenders should take priority in the sentencing arena if we are to really address the issues of prison effectiveness, overcrowding and the consequential psychological harm resulting from prolonged or unnecessary incarceration.

The Philippines has offered many alternatives to incarceration of its criminal offenders and these alternatives can generally be grouped as interventions in the pre-sentencing or post-sentencing stage of the criminal justice process. In practice however, it is the probation and parole system that is widely used and can be considered as the best alternative for a community-based rehabilitation programme. For these reasons, a more detailed discussion of these systems is presented, including the operational procedure and mandated programmes of the agency, the Parole and Probation Administration, which is tasked by law to administer them.

Other alternatives to incarceration that are practiced in the Philippines are also presented, such as community service, fines, release on recognizance, bail and diversion, which is specifically suited for minors or children in conflict with law and greatly enhanced with the passage of Republic Act 9344.

A brief explanation of the operation of the Philippine Criminal Justice System is also included to show at what stage of the criminal justice process the alternatives to incarceration are offered.

II. UNDERSTANDING THE PHILIPPINE CRIMINAL JUSTICE SYSTEM

The criminal justice system in the Philippines is composed of five components or “pillars” and they are usually referred to as the “Five Pillars of the CJS”. Its components, composition and basic functions are as follows.

A. Law Enforcement

Law enforcement is basically represented by the Philippine National Police (PNP), the National Bureau of Investigation (NBI) and other law enforcement agencies. They have the duty to: (a) investigate crime; (b) arrest suspects; and (c) refer the case and suspects to public prosecutors or courts (if warranted).

B. Prosecution

Prosecution is basically represented by the public prosecutors, the Ombudsman, other prosecuting officers of the different governmental agencies and even private lawyers who act as private prosecutors. They have the duty to: (a) evaluate the police findings; (b) file the corresponding information or criminal complaints in the proper courts; and (c) prosecute the offenders.

C. Judicial

The judiciary is principally represented by the Supreme Court, other regular trial courts and the special courts like Family Courts, Drugs Court, and the *Sandiganbayan*. They have the responsibility of

* Regional Director, Region IX, Parole and Probation Administration, Department of Justice, Philippines.

final determination of the innocence or guilt of the accused after the latter has undergone the hierarchical processes of the Philippine courts.

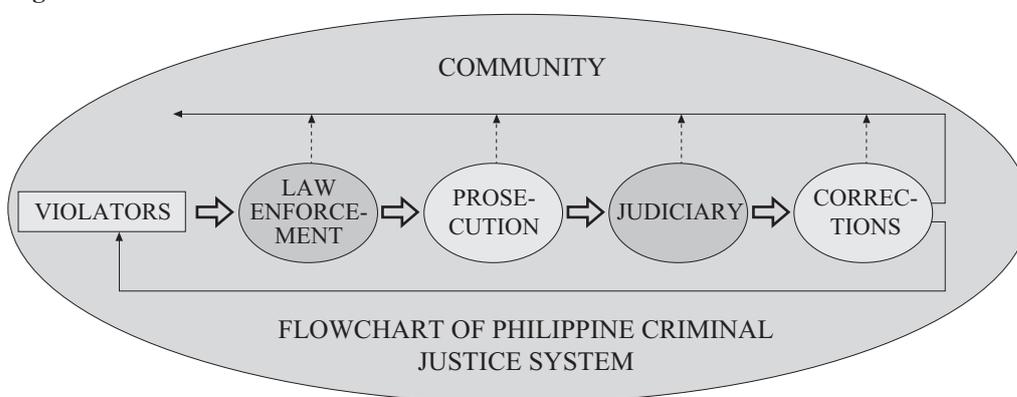
D. Correctional

The correctional aspect is represented by the Bureau of Corrections (BUCOR), the Bureau of Jail Management and Penology, the Provincial Jails for Institutional Corrections, and the Parole and Probation Administration for Non-Institutional Corrections. These agencies have the main function of receiving referrals from courts and other authorized governmental agencies.

E. The Community

The community is composed of the general public and is morally obliged to (a) create the environment for development of civic-spirited and law-abiding citizens; (b) co-operate with duly constituted authorities for effective implementation of criminal justice processes. The interaction and collective efforts of the components of the Philippine criminal justice system is illustrated in Figure 1.

Figure 1



(Note: Just like any other criminal justice model, the choice of alternatives to incarceration is available at the early stage of the criminal justice process.)

III. THE PAROLE AND PROBATION ADMINISTRATION

A. Historical Background

Probation was first introduced in the Philippines during the American colonial period (1898-1945) with the enactment of Act No. 4221 of the Philippine Legislature on 7 August 1935. This law created the Probation Office under the Department of Justice, which provided probation to first-time offenders 18 years of age or over, convicted of certain crimes. On 16 November 1937, after barely two years of existence, the Supreme Court of the Philippines declared the Probation Law unconstitutional because of some defects in the law's procedural framework.

In 1972, House Bill No. 393 was filed in the Congress, intended to establish a probation system in the Philippines. This bill avoided the objectionable features of Act 4221. The bill was passed by the House of the Representatives, and it was pending in the Senate when Martial Law was declared, and the Congress was abolished.

In 1975, the National Police Commission, acting on a report submitted by the Philippine delegation to the Fifth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, created an Inter-disciplinary Committee tasked to formulate a national strategy to reduce crime and to draft a probation law. After 18 technical hearings over a period of six months involving 60 resource persons, including international experts in the field of corrections, the draft decree was presented to a select group of 369 jurists, penologists, civic leaders and social and behavioural scientists and practitioners. The group overwhelmingly endorsed the establishment of an adult probation system in the country.

THE 141ST INTERNATIONAL SENIOR SEMINAR
PARTICIPANTS' PAPERS

On 24 July 1976, Presidential Decree No. 968, also known as the Adult Probation Law of 1976, was signed into law by the President of the Philippines.

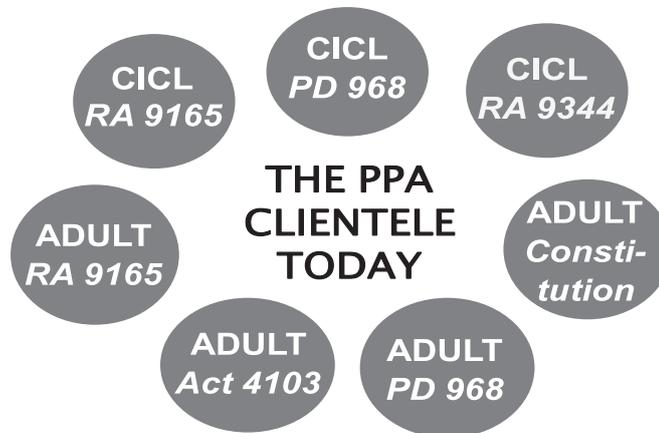
With the enactment of this law, the Probation Administration was created to administer the probation system. Under Executive Order 292, "The Administrative Code of 1987", the Probation Administration was renamed the "Parole and Probation Administration" and given the added function of supervising prisoners who, after serving part of their sentence in jails are released on parole or are granted pardon with parole conditions.

Recently, the investigation and supervision of First Time Minor Drug Offenders placed under suspended sentence (FTMDO) have become another added function of the Administration pursuant to the provisions of Republic Act No. 9165, "The Comprehensive Dangerous Drugs Act of 2002" and per Dangerous Drugs Board Resolution No. 2 dated 19 July 2005 and the Memorandum of Agreement between the Dangerous Drugs Board and the Parole and Probation Administration dated 17 August 2005. As embodied in the said Memorandum of Agreement, the Dangerous Drugs Board tapped the assistance of the Administration through its manpower in the performance of its duties to investigate and supervise minor drug offenders who apply for and/or are granted suspended sentences by the courts. The Dangerous Drugs Board appointed some of the Administration's trained personnel to be its authorized representatives to carry out the former's duty of determining whether a minor drug offender may enjoy a suspended sentence and supervising his or her treatment and rehabilitation.

Further, Executive Order 468, mandating the revitalization of the Volunteer Probation Aide (VPA) programme, places the Administration in the forefront in relation to crime prevention, treatment of offenders in the community-based setting and on the overall administration of criminal justice.

As aforementioned, Presidential Decree 968 was originally envisioned to cover only adult offenders but as practiced today, supervision of clients now covers the following groups of offenders.

Figure 2



B. Major Final Outputs

1. Investigation Services for Petitions for Probation, Parole, Executive Clemency and Suspended Sentence for First Time Minor Drug Offenders

This programme makes certain the suitability of petitioners for probation, parole, conditional pardon and first-time minor drug offenders, who will likely respond to community-based individualized treatment. Those offenders who have no potential to reform are recommended to remain in jail or prison to ensure community safety.

It gathers information on the petitioner's personality, character, antecedents, environment and other relevant information, which includes the internal as well as external resources which shall be tapped in rehabilitating clients.

The investigation of first-time minor drug offenders in the implementation of Section 57 (Probation and Community Service under the Voluntary Submission Program) and Section 70 (Probation or Community Service for a First-Time Minor Drug Offenders in lieu of imprisonment) of Republic Act 9165, "The Comprehensive Dangerous Drugs Act of 2002", was implemented only in 2006 pursuant to a Memorandum of Agreement between the Administration and Dangerous Drugs Board.

2. Supervision and Rehabilitation Services for Probationers, Parolees, Conditional Pardonees and First-Time Minor Drug Offenders Placed on Suspended Sentence or Community Service

This programme seeks to administer and execute existing laws relative to probation and parole systems in order to effect the rehabilitation and integration of probationers, parolees and pardonees as productive, law abiding and socially responsible members of the community.

Supervision is the essence of the probation and parole systems as it is in the area where intervention strategies are effected towards client rehabilitation.

The objective of supervision is the permanent regeneration of the client's attitude towards law observance. Supervision treatment should be concerned with the total configuration of the offender's personality in relation to family, community and society.

3. Administration of Volunteer Probation Aide Program (Volunteer Program Revitalized – Executive Order 468, dated October 11, 2005)

In support of the national policy of maximizing community involvement in the administration of the criminal justice system, it has become imperative for the Parole and Probation Administration to open every opportunity to allow people's participation in the implementation of the parole and probation programmes.

The recruitment and deployment of volunteers who can assist the Administration in the pursuit of its vision, mission and goals will play a pivotal role in strengthening the essence of partnership between government and the private sector in ensuring the success of programmes and activities that derive their existence from public funds.

Volunteer Probation Aides (VPAs) are provided with necessary training and orientation for them to appreciate the knowledge, skills, attitudes and values that will enable them to perform their functions and duties with utmost efficiency, effectiveness and productivity, and at the same time, experience fulfilment and satisfaction from a job that gives them very minimal or no monetary returns at all.

IV. THE PROBATION AND PAROLE SYSTEM

A. Probation

1. Definition

Probation is a disposition under which a person who is convicted of criminal offence is released, subject to the conditions imposed by the sentencing court and to the supervision of a probation officer (Section 3(a), Probation Law of 1976). It is a mere privilege and as such, its grant rests solely upon the discretion of the court. A court may, after it shall have convicted and sentenced a defendant and upon application within 15 days from promulgation of judgment, suspend the execution of said sentence and place the defendant on probation for such period and upon such terms and conditions as it may deem best. It may be granted whether the sentence imposes a term of imprisonment or a fine only. The filing of the application shall be deemed a waiver of the right to appeal. An order granting or denying probation shall not be appealable (Section 4, Probation Law of 1976).

2. Disqualifications

Any person who is not otherwise disqualified under the probation law can apply. The following are disqualified to apply for probation (Section 9, Probation Law of 1976):

- Those sentenced to serve a maximum term of imprisonment of more than six years;
- Those who have previously been convicted by final judgment of an offence punished by imprisonment of not less than one month and one day and/or a fine of not less than two hundred pesos;
- Those who have been placed on probation under the Probation Law;

THE 141ST INTERNATIONAL SENIOR SEMINAR
PARTICIPANTS' PAPERS

- Those who are already serving sentence at the time the Probation Law became applicable or took effect;
- Those whose conviction is on appeal;
- Those convicted of violation of the Omnibus Election Code of the Philippines;
- Those convicted of violation of Wage Rationalization Act (Sec. 12, Republic Act No. 6727).

B. Parole

1. Definition

Parole is the conditional release of a prisoner from a correctional institution after he or she has served the minimum period of his or her indeterminate sentence. A prisoner case shall not be eligible for review by the Board of Pardons and Parole unless: (a) the prisoner is confined in prison or jail to serve an indeterminate sentence, the maximum period of which exceeds one year, pursuant to a final judgment of conviction which has become final and executory, and (b) he or she has served the minimum period of said sentence (Rule 2, Sec. 2.1 of Rules of Parole, 26 June 2003). Act 4103 as enacted in 1933, otherwise known as the Indeterminate Sentence Law, is the basic law governing the administration of the parole system in the country. The Board of Pardons and Parole is the administrative arm of the President of the Philippines in the exercise of the constitutional power to grant parole and other forms of executive clemency after conviction by final judgment.

2. Persons Who are Disqualified from Parole

The following persons are disqualified to be granted parole:

- Those convicted of an offence punished with the death penalty, *reclusion perpetua* or life imprisonment (*reclusion perpetua* has a duration of 20 years and 1 day to 40 years of imprisonment);
- Those convicted of treason, conspiracy or proposal to commit treason or espionage;
- Those convicted of misprision of treason, rebellion, sedition or *coup d'etat*;
- Those convicted of piracy or mutiny on the high seas or Philippine waters;
- Those who are habitual delinquents;
- Those who escaped from confinement or evaded sentence;
- Those who having been granted conditional pardon by the President of the Philippines violated any of the terms thereof;
- Those whose maximum term of imprisonment does not exceed one year or those with definite sentence;
- Those certified as suffering from mental disorder as certified by a government psychiatrist or psychologist;
- Those whose conviction is on appeal or has not yet become final and executory;
- Those who have pending case/cases;
- Those national prisoners serving sentence in a municipal, city, district or provincial jail, unless the confinement in said jails is in good faith or due to circumstances beyond the prisoner's control.

V. ADMINISTRATION OF PAROLE AND PROBATION AS COMMUNITY-BASED ALTERNATIVES TO INCARCERATION

A. Investigation and Supervision

1. Investigation of Court Referrals

The investigation process involves detailed and in-depth study of the applicant's criminal records, family history, educational background, married life, occupational records, interpersonal relationships, spirituality, behavioural history, substance use, economic and social status and other aspects of his or her life.

The investigation procedures as enunciated in the Probation Law of 1976 are as follows: After conviction and sentence, an offender or his or her counsel files a petition for probation with the trial court, which in turn orders the probation officer to conduct a post-sentence investigation to determine whether or not an offender may be placed on probation. The grant of probation is premised upon three conditions: (1) an application for probation by the offender; (2) an investigation conducted by the probation officer; and (3) a determination by the court that the ends of justice and the best interest of the public as well as the offender will be served thereby (*Section 5*). The post-sentence investigation report must be submitted by the probation officer within 60 days from receipt of the order of the court to conduct investigation. The court shall resolve the petition for probation not later than 15 days after receipt of the said report. Pending submission of the investigation report and the resolution of the petition, the defendant may be allowed on temporary liberty under his or her bail filed in the criminal case, provided that, in cases where no bail is

filed or that the defendant is incapable of filing one, the court may allow the release of the defendants on recognizance to the custody of a responsible member of the community who shall guarantee his appearance whenever required by the court (*Section 7*). The grant of probation in effect suspends the execution of the sentence of imprisonment.

2. Investigation of Board of Pardons and Parole/Jail Referrals

The pre-parole/executive clemency investigation is conducted to provide the Board of Pardons and Parole with necessary and relevant information in determining the prisoner's fitness for parole or any form of executive clemency. The investigation and evaluation focus on the physical, mental and moral records of prisoners confined in city jails, the national penitentiary and penal colonies to identify who are eligible for parole or executive clemency.

3. Investigation of Referrals from the Dangerous Drugs Board

The conduct of a Suspended Sentence Investigation which aims to gather substantial data or information about all aspects of the client's life will be a crucial factor in the grant or denial of the petition for suspension of sentence.

B. Administration's Performance Target

In 2007, the national average disposition rate for probation investigation was 94.93, surpassing the Administration target disposition rate of 90% for investigation cases completed within 60 days. For pre-parole/executive clemency investigation, the Administration obtained 97.42% average disposition rate.

It is noteworthy to mention that the courts, the Board of Pardons and Parole and the Dangerous Drugs Board often uphold the findings and recommendation of the field officers as can be measured in terms of sustained recommendation of 99.59% for investigation and 99.91% for supervision.

VI. CORRECTION AND REHABILITATION OF OFFENDERS

Probation once granted to an applicant is accompanied by conditions imposed by the court and which conditions must be followed by the probationer while he or she is under the supervision of a probation officer. There are two types of conditions that the probationer must adhere to. These are the general mandatory conditions and the special or discretionary conditions, both of which are incorporated in every order of probation issued by the court.

- The mandatory conditions require that the probationer shall (a) present him or herself to the probation officer designated to undertake his or her supervision at each place as may be specified in the order within 72 hours from receipt of said order; and (b) report to the probation officer at least once a month at such time and place as may be specified by the officer.
- Special or discretionary conditions are those additional conditions imposed on the probationer which are geared towards his or her correction and rehabilitation outside of prison and in the community to which he or she belongs. The court may require him or her to: (a) co-operate with a programme of supervision; (b) meet his or her family responsibilities; (c) devote him or herself to a specific employment and not to change said employment without the prior written approval of the probation officer; (d) undergo medical, psychological or psychiatric examination and treatment and enter and remain in a specified institution, when required for that purpose; (e) pursue a prescribed secular study or vocational training; (f) attend or reside in a facility established for instruction, recreation or residence of persons on probation; (g) refrain from visiting houses of ill-repute; (h) abstain from drinking intoxicating beverages to excess; (i) permit the probation officer or an authorized social worker to visit his or her home and place of work; (j) reside at premises approved by it and not to change his or her residence without prior written approval; or (k) satisfy any other condition related to the rehabilitation of the defendant and not unduly restrictive of his or her liberty or incompatible with his or her freedom of conscience. The conditions as enumerated are non-exclusive. The court has the discretion to add other conditions or omit some of those already provided.

A violation of any of the conditions may lead either to a more restrictive modification of the same or the revocation of the grant of probation. Consequent to the revocation, the probationer will have to serve the sentence originally imposed.

In order to address the different areas where the client may need assistance or help in pursuing his or her rehabilitation, the Administration through its field officers conducts different rehabilitation activities intended to focus on the needs of the clients. These activities are always conducted in co-ordination with socio-civic, charitable, religious organizations, local government, individuals and our Volunteer Probation Aides. The rehabilitation activities are as follows.

A. Individual and Group Counselling

Individual counselling involves one-on-one interaction between the client and the probation and parole officer. The officer assists the client in trying to sort out his or her problems, identify solutions, reconcile conflicts and help resolve them.

Group counselling has the same objective but it is done with a group, ideally intended for those with similar problems, conflicts or offences. The activity focuses on reminders of compliance to the conditions of their probation and parole, lectures on individual and marital problems, behavioural problems, proper conduct in the community, health issues and social responsibility, as well as environmental awareness.

B. Social-Moral and Values Formation and Spiritual/Religious Activities

These activities are accomplished through seminars, lectures or training offered or arranged by the office, most of the time inviting outside resource person and availing of their services for free. Active Non-Governmental Organizations, local government units, lay ministers and their ministries, school and faculty associations provide much help in facilitating the conduct of these activities.

C. Work and Livelihood

The Administration initiates a self-sustaining livelihood programme to ensure that a client can provide basic necessities for himself and his or her family. Field officers conduct/organize seminars for a home-based, labour intensive economic activity, in co-ordination with local government units, non-government organizations and civic organizations which can assist the clients in the pursuit of feasible livelihood projects.

D. Skills Training

Productivity and economic sufficiency of the clients during the process of reintegration is one of the objectives of the Administration aimed to achieve for the clients, such that clients with inadequate technical know-how are encouraged and referred for skills training to enhance/acquire marketable skills to make them more competitive for employment.

E. Health and Medical Services

To address some of the basic needs of clients and their families, medical missions are organized to provide various forms of medical and health services including physical examination and treatment, free medicines and vitamins, dental examination and treatment, drug dependency test and laboratory examinations. Psychological testing and evaluation as well as psychiatric treatment are likewise provided by the Administration's Clinical Division and if not possible by reason of distance, referrals are made to other government accredited institutions.

F. Literacy Programme

In co-ordination with local government unit programmes, adult education classes are availed of to help clients learn basic writing, reading and arithmetic. Likewise, literacy teach-ins during any sessions conducted for clients become part of the module. This is particularly intended for clients who are "no read, no write" to help them become functionally literate. Likewise, there are regular linkages with educational foundation, other government organizations and non-government organizations for free school supplies, bags and uniform for clients' children and relatives.

G. Community Service

This programme refers to the services in the community rendered by clients for the benefit of society. It includes tree planting, beautification drives, cleaning and greening of surroundings, maintenance of public parks and places, garbage collection, blood donation and similar socio-civic activities.

H. Clients’ Self-Help Organization

This programme takes the form of co-operatives and clients’ associations wherein the clients form co-operatives and associations as an economic group to venture on small-scale projects. Similarly, client associations serve another purpose by providing some structure to the lives of clients where they re-learn the basics of working within a group with hierarchy, authority and responsibility much like in society in general.

I. Payment of Civil Liability

The payment of civil liability or indemnification to victims of offenders is pursued despite the economic status of clients. Payment of obligations to the victims instils in the minds of the clients their responsibility and the consequences of the harm they inflicted on others.

J. Environment and Ecology

To instil awareness of and concern for preserving ecological balance and environmental health, seminars/lectures are conducted wherein clients participate. These seminars/lectures tackle anti-smoke belching campaigns, organic farming, waste management, segregation and disposal and proper care of the environment.

K. Sports and Physical Fitness

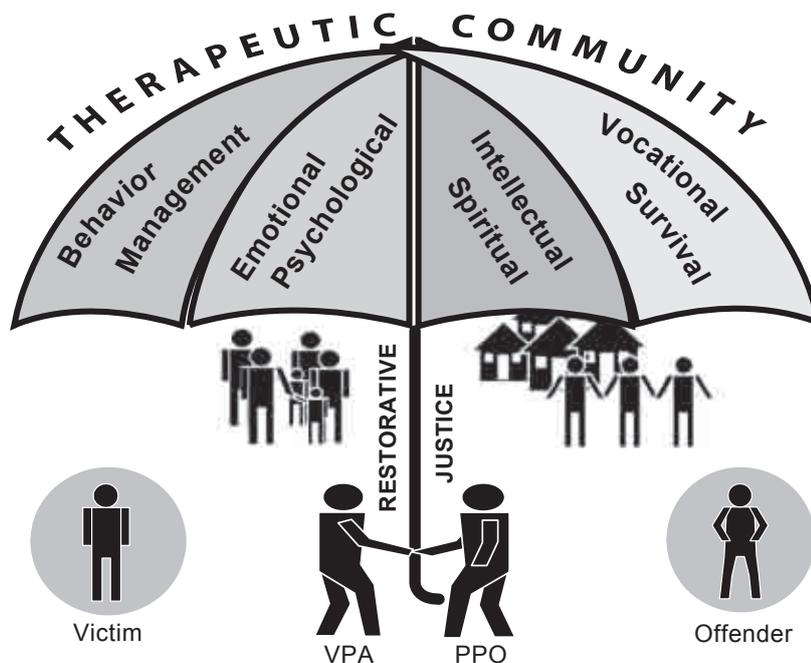
Activities that provide physical exertion like sports, games and group play are conducted to enhance the physical wellbeing of clients. Friendly competitions of clients from the various offices of the sectors, together with the officers, provides an enjoyable and healthful respite.

VII. PROGRAMME FOR THE REHABILITATION OF CLIENTS

It is a community-based, harmonized three-pronged approach to crime prevention and treatment of offenders with restorative justice as its philosophical foundation, therapeutic community its unifying structure and volunteerism its lead community resource.

It can also be described as an individualized, community-based programme using therapeutic community as the treatment modality that integrates restorative justice principles and practices and mobilizes community involvement through volunteerism.

Figure 3: Symbolism of the Umbrella



The integration of the three programmes is depicted by the diagram of the umbrella.

The rod holding up the umbrella represents restorative justice (RJ) which is the philosophical foundation of the agency mission and provides the unifying principle for all rehabilitation activities integrated within the therapeutic community (TC) modality.

The four-panelled canopy represents the TC Modality with its four distinct but overlapping categories of activities, namely: behaviour shaping/behaviour management; emotional and psychological assistance; intellectual and spiritual; and vocational/survival skills categories.

The two figures holding up the umbrella represents the Probation and Parole Officer and the volunteer probation aides (VPA) who work collaboratively in order to bring about the social transformation of offenders, victims and community.

A. Therapeutic Community

Therapeutic Community is based on the Social Learning Model, which utilizes the community as the primary therapeutic vehicle to foster behavioural and attitudinal change. In this model, the client receives the information and the impetus to change from being a part of a community. The expectations that the community places on its individual members reflect not only the needs of the individual, but also the social and support needs of the community. This community model provides social expectations, which are parallel to the social demands that the client will confront upon discharge to their home community. The attitudes, skills and responsibilities learned in the community are not only necessary for survival, but also, essential to surviving in the larger community.

B. Restorative Justice

Restorative Justice is a victim-centred response to crime that provides opportunity of restoring broken relationship caused by crime and putting closure to the hurt feelings and repairing the damage done among those directly affected – the victim, the offender, their families and the community. In the restorative process, parties affected are encouraged to actively participate together in the resolution of matters resulting from the offence with the fair and impartial third party or the Chief Probation and Parole Officer or investigating officer as mediator. During the year 2007, the programme effected the healing process among 1,254 victims and 3,170 clients by way of dialogue, victim-offender mediation, conferencing, restitution, community work service and peacemaking encounter and/or agreement.

C. Volunteer Probation Aide Program

The Volunteerism Program of the Philippines has evolved, being mandated in Section 28 of the Presidential Decree No. 968, otherwise known as Adult Probation Law of 1976, which authorizes the appointment of citizens of good repute and probity to act as Volunteer Probation Aide to assist the probation officer in the supervision of probationers.

Since the Administration recognizes the vital role of the community in the treatment and rehabilitation of clients, probationers, parolees and pardonees, there was a move to revive the Volunteer Probation Aide Program. Hence in 2002, Executive Order No. 468 was issued for the Revitalization of the Volunteer Probation Aide of the Administration which aims to heighten and maximize community involvement and participation in the community-based programme in the prevention of crime, treatment of offenders and administration of criminal justice system. This is also used as a strategy to address the lack of manpower in the Administration.

To implement things in order, the Administration has engaged in aggressive and extensive recruitment and appointment of qualified Volunteer Probation Aides following the prescribed set of criteria with a target that by the end of 2010, the number of Volunteer Probation Aides appointed would reach 5,000. At present, the Administration has already exceeded its initial target set for year 2010.

1. Current Situation

The Philippines has 79 provinces and cities, with 229 Parole and Probation field offices. A total of 704 Probation and Parole Officers are supervising 36,821 clients as of 30 September 2008.

2. Recruitment and Appointment

Only about 259 volunteers were recruited as of 2003. As of 21 November 2008, however, a total of 7,554 Volunteer Probation Aides were already appointed, with 1,704 Volunteer Probation Aides appointed from January to 21 November, 2008.

Figure 4 shows the Cumulative Total of Volunteer Probation Aides Appointed by Region from 2003 to November 21, 2008.

Figure 4

Region	2003	2004	2005	2006	2007	2008
NCR	10	70	107	159	312	521
CAR	0	2	11	39	225	293
I	5	36	191	241	280	323
II	2	12	43	54	168	256
III	6	29	157	652	958	1141
IV	32	154	429	922	1184	1271
V	79	84	90	108	176	225
VI	4	12	348	441	533	764
VII	41	46	203	288	482	709
VIII	2	21	75	121	208	316
IX	27	30	70	147	319	478
X	10	111	112	222	335	416
XI	32	65	115	177	251	332
XII	0	0	43	73	151	214
CARAGA	9	9	36	94	268	295
Total	259	681	2030	3738	5850	7554

2. Volunteer Probation Aide Mobilization

The target ratio for Volunteer Probation Aides supervising clients is 1:2. As of 30 September 2008, of 36,821 total active supervision cases only 7,466 (20.28 percent) are supervised by 2,347 Volunteer Probation Aides. This accounts for only 31% of 7,554 appointed Volunteer Probation Aides.

3. Trainings and Development

For effective implementation of the Volunteer Probation Aide Program and proper utilization of the Volunteer Probation Aides, continuous training and workshops are held to equip the Probation and Parole Officers and Volunteer Probation Aides with adequate knowledge and skills in the implementation of the programme and facilitation of supervision work in the community, with the technical assistance of Japan International Cooperation Agency and the United Nations Asia and Far East Institute for the Prevention of Crime and Treatment of Offenders, since the revitalization of the Administration's programme.

The Basic Training for Volunteer Probation Aides, a 16-hour basic training session, is given to prior to the VPOs' supervision of clients. Other training sessions which are continuously conducted for the Probation and Parole Officers/Volunteer Probation Aides are the following:

- Information Drive
- Orientation
- Basic Training
- Specialized Training on Restorative Justice
- Specialized Training on Therapeutic Community Modality
- Leadership Training
- Capability Building of VPAs on the following:

THE 141ST INTERNATIONAL SENIOR SEMINAR
PARTICIPANTS' PAPERS

- Managing their own organization
- Leadership and Organizational Development
- Team Building
- Counselling and other skills necessary in the conduct of their duties and responsibilities
- In-Country Training Program on the Holistic Approach to Volunteer Resource Development
- Country Training Programme on the Revitalization of the Parole and Probation Administration Volunteer Probation Aide Programme in Japan

4. Organization

At present, out of 229 field offices, 125 ((54.59 percent) have already organized their associations. As to its membership, out of 7,554 appointed Volunteer Probation Aides, 3,870 (or 51.23 percent) are members. Only 104 field offices have not yet organized their association though they have already appointed Volunteer Probation Aides.

There is already a national association of Volunteer Probation Aides – the Association of Volunteer Probation Aides of the Philippines (AVPAP) and registered with the Security and Exchange Commission (SEC).

VIII. OTHER ALTERNATIVES TO INCARCERATION

A. Community Service

This programme refers to the services in the community rendered by clients for the benefit of society. It includes tree planting, beautification drives, cleaning and greening of surroundings, maintenance of public parks and places, garbage collection, blood donation and similar socio-civic activities. The effectiveness of community service is often underestimated or underappreciated and usually imposed only as an add-on requirement in probation and parole supervision. Under RA 9165, The Comprehensive Dangerous Drugs Act of 2002, community service can now be imposed as a separate penalty.

B. Fine

In lieu of imprisonment the court may impose upon the offender the payment of a fine commensurate to the offence he or she committed. Imposition of fines or finical punishment is traditionally used in conjunction with other penalties or for minor offences. Interestingly, the Supreme Court of the Philippines in a circular has discouraged judges from imposing the penalty of imprisonment for violation of Batas Pambansa 22, the Bouncing Check Law, and instead to consider fine as the more appropriate penalty. Prosecution for violation of the Bouncing Check Law is now also covered by the Summary Rules on Criminal Procedure where summons are just issued for the appearance of the accused instead of the usual warrant of arrest.

C. Release on Recognizance

Recognizance is an obligation of record, entered into before some court duly authorized to take it, with condition to do some particular act or acts, the usual condition being the appearance of the accused for trial. The application for release on recognizance may be filed at any time before conviction in the court where the case is pending.

Presently, release on recognizance is available only in the following instances:

1. When the offence charged is for violation of an ordinance, a light felony or a criminal offence, the imposable penalty for which does exceed six months' imprisonment and/or a 2,000 peso fine (Republic Act 6036).
2. When a person is in custody for a period equal to or more than the minimum of the principal penalty prescribed for the offence charged (Rule 114 Section 16, Revised Rules on Criminal Procedure).
3. When the accused has no bail filed or he or she is incapable of filing for bail (Rule 114, Section 24, Revised Rules on Criminal Procedure).
4. When the youthful offender is held for physical and mental examination, trial or appeal (Presidential Decree 603).

A new bill on release on recognizance (Recognizance Act of 2008) is now pending in the Philippine Congress. The Administration strongly supports such proposal. This measure is intended to serve as the enabling law for the full implementation of release on recognizance as an instrument for temporary release. Moreover, this measure is a means to promote the principle of restorative justice especially among poor litigants who have yet to be convicted but are detained due to their inability to post bail or due to a simple lack of an enabling law on recognizance. It would give the members of a community a bigger and more proactive role in reforming suspected offenders and upholding a fair system of justice. This is also a way to address other problems confronting the criminal justice system such as protracted trials, prolonged resolution of cases, lack of legal representation, lack of judges, congestion in jails, and lack of opportunity to reform and rehabilitate offenders. This bill also seeks to expand the coverage of release on recognizance from the present six months up to 20 years' imprisonment.

D. Diversion

Jails and prisons are simply not for children under the new law on juvenile justice. Instead of putting them to jail, children in conflict with the law will be placed in diversion programmes without undergoing court proceedings, subject to the conditions imposed by law. It may be conducted at the *Katarungang Pambarangay*, the police investigation or the inquest or preliminary investigation stage and at all levels and phases of the proceedings, including judicial level (Section 4 (i) of Republic Act No. 9344, or the Juvenile Justice and Welfare Act). The diversion programme includes adequate socio-cultural and psychological responses and services for the child. At the different stages where diversion may be resorted to, the following diversion programmes may be agreed upon, such as, but not limited to:

1. At the Level of the Punong Barangay

- Restitution of property;
- Reparation of the damage caused;
- Indemnification for consequential damages;
- Written or oral apology;
- Care, guidance and supervision orders;
- Counselling for the child in conflict with the law and the child's family;
- Attendance in training, seminars and lectures on anger management skills, problem-solving and/or conflict resolution skills, values formation, and other skills which will aid the child in dealing with situations which can lead to repetition of the offence;
- Participation in available community-based programmes, including community service; or
- Participation in education, vocation and life skills programmes.

2. At the Level of the Law Enforcement Officer and the Prosecutor

- Diversion programmes as specified above; and
- Confiscation and forfeiture of the proceeds or instruments of the crime.

3. At the Level of the Appropriate Court

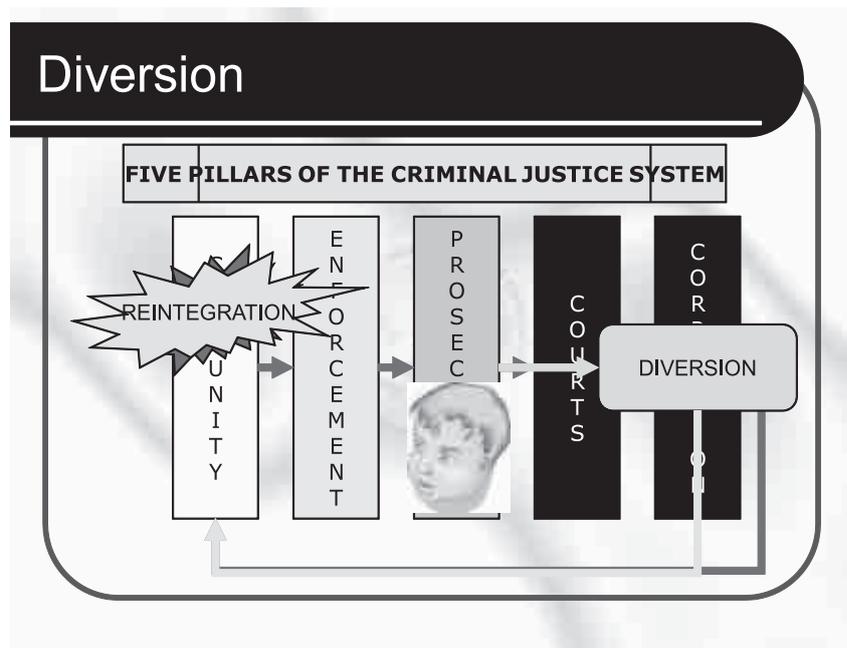
- Diversion programmes as specified above;
- Written or oral reprimand or citation;
- Fine;
- Payment of the cost of the proceedings; or
- Institutional care and custody.

Community-based programmes on juvenile justice and welfare are instituted by the local government units through the Local Councils for the Protection of Children, school, youth organizations and other concerned agencies. The local government units are mandated to provide community-based services which respond to the special needs, problems, interests and concerns of children and which offer appropriate counselling and guidance to them and their families. These programmes shall consist of three levels:

- Primary intervention includes general measures to promote social justice and equal opportunity, which tackle perceived root causes of offending;
- Secondary intervention includes measures to assist children at risk; and
- Tertiary intervention includes measures to avoid unnecessary contact with the formal justice system and other measures to prevent reoffending (Section 19 of Republic Act No. 9344, or the Juvenile Justice and Welfare Act).

To ensure the effective implementation of the new juvenile justice law, a Juvenile Justice and Welfare Council (JJWC) was created, chaired by an Undersecretary of the Department of Social Welfare and Development and attached to the Department of Justice for administrative supervision. Co-ordination with the following agencies is likewise mandated by law: (a) Council for the Welfare of Children (CWC); (b) Department of Education (DepEd); (c) Department of Interior and Local Government (DILG); (d) Public Attorney's Office (PAO); (e) Bureau of Corrections (BUCOR); (f) Parole and Probation Administration (PPA); (g) National Bureau of Investigation (NBI); (h) Philippine National Police (PNP); (i) Bureau of Jail Management and Penology (BJMP); (j) Commission on Human Rights (CHR); (k) Technical Education and Skills Development Authority (TESDA); (l) National Youth Commission (NYC); and (m) other institutions focused on juvenile justice and intervention programmes.

Figure 5



As illustrated above, in the prosecution of minors or children in conflict with law under RA 9344, diversion proceedings are applied at all levels, even up to the judicial level.

E. Bail

As a mode for releasing a person usually under preventive imprisonment, bail can be granted by the court as matter of right or discretion. Release on bail is available as matter of right in the following instances:

1. Before and after conviction in the Municipal Trial Courts;
2. Before conviction in the Regional Trial Courts for offenses not punishable by death, *reclusion perpetua* or life imprisonment;
3. Before conviction in the Regional Trial Court for offences punishable by death, *reclusion perpetua* or life imprisonment where the evidence of guilt is not strong.

After conviction in the Regional Trial Court for offences not punishable by death, *reclusion perpetua* or life imprisonment, release on bail, usually for humanitarian reasons, is already discretionary.

IX. CONCLUSION

With the ever increasing prison population which is prevalent in most jails and prisons locally and internationally, community corrections or alternatives to incarceration are now essential elements of a

modern criminal justice system. While institutional corrections may continue to be practiced alongside other alternatives, it should serve only as a deterrence or remedy of last resort for hardened criminals who may pose a direct or immediate threat to the community. The questionable impact of incarceration as a tool for rehabilitation and treatment has long been seriously challenged. The physical, psychological and dehumanizing effects of unnecessary incarceration have been likewise raised as issues of major concern and identified as a cause for incidence of recidivism. While probation and parole systems may continue to be the traditional community-based alternatives to incarceration, there is still a need to further enhance them or perhaps to develop other alternatives or intermediate sanctions that would provide greater levels of supervision, control and treatment of offenders. If we can have more and more of these community-based alternatives to incarceration then we can be certain that we will have fewer and fewer criminal offenders channelled by our courts to jails and prisons.

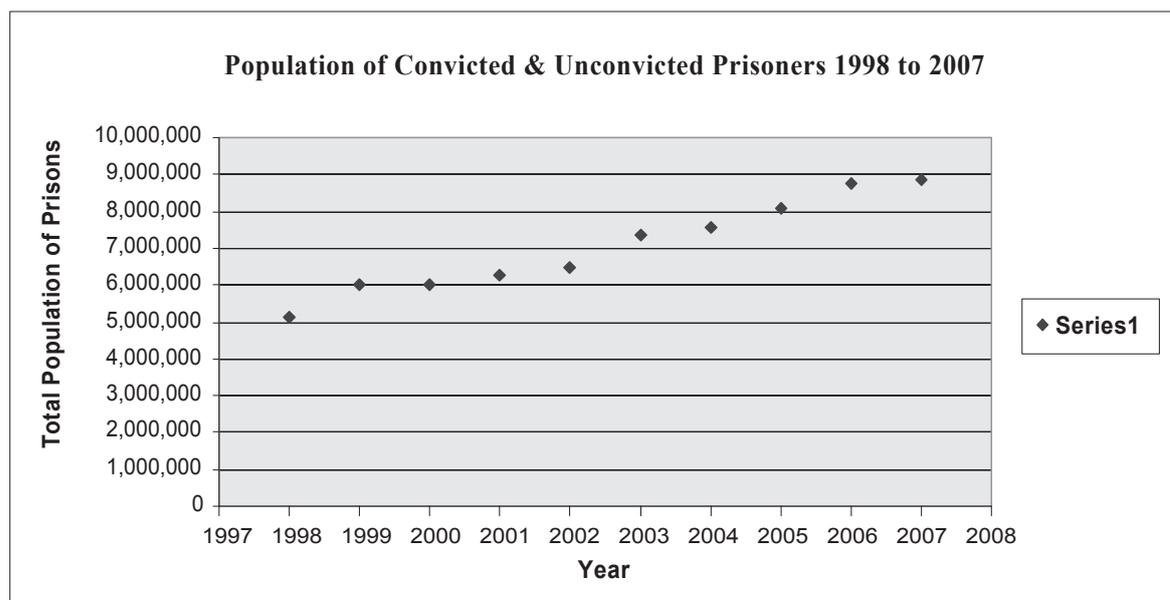
OVERCROWDED PRISONS AND PRESENT PRACTICES AND EXPERIENCE IN RELATION TO COMMUNITY-BASED ALTERNATIVES TO INCARCERATION

*Jagath Abeysirigunawardana**

I. BACKGROUND

A. Overcrowding of Prisons and Non-Institutional Treatment of Offenders

Overcrowding of prisons is a common phenomenon experienced in many countries of the world today. Sri Lanka is one such country. The prison population throughout Sri Lanka is growing rapidly. Facilities such as sleeping accommodation, sanitary and bathing installations, medical and recreational facilities differ between developed and developing countries. Hence, there does not appear to be common criteria on the required accommodation or floor area or other conditions per prisoner.



Source – Department of Prisons in Sri Lanka

B. Causes of Overcrowding in Prisons

There is a close relationship between the population growth of the country and number of crimes committed in the country. Hence, there is a close relationship with overcrowding of prisons and population growth.

The overcrowding of prisons in Sri Lanka is caused by having to accommodate a large number of remand or on-trial prisoners. In Sri Lanka, the ratio of remand to convicted prisoners has been 4:1 or 5:1 for the last 10 years and about 80 percent of prisoners are on remand.

Most of the reasons for overcrowding of remand prisoners in Sri Lanka are the same as in many countries of our region, and are classified below.

* Deputy Director General, Southern Range, Sri Lanka Police.

1. The delay in bringing offenders to trial or legal delays.
2. Trial, along with excessive bail or inadequate use of bail provisions.
3. The legal system of many countries over emphasizes imprisonment as the most powerful weapon against crime and carries imprisonment for far too many offences. As a result, courts resort to imprisonment as the first option (and many cases the only option) instead of it being treated as the last resort. This tendency on the part of the courts may sometimes be seen as reflecting the attitude of the general public who may demand severe punishment as a warning to would-be criminals.
4. Among the convicted prisoners admitted to Sri Lanka prisons, the highest number are sentenced to less than one year. In 2007, these short-timers made up 63% of the convicted prison population. From the very fact that they were given short-term imprisonment, it is clear that most of them could not have been found guilty of serious offences for which alternative punishments to imprisonment could not have been given.
5. Admission of a large number of offenders to prison for non-payments of fines is also contributing to the problem of overcrowding. Out of a total of 31,306 convicted prisoners admitted to prisons in Sri Lanka in 2007, 15,408 or 49.2% were fine defaulters, whom the courts initially thought did not deserve a prison sentence.
6. Admission of persons both as remandees and convicted prisoners for drug-related offences. The percentage of drug offenders (convicted) in Sri Lanka prisons in 1996, which was 41.4, has slightly decreased to 36.7 during the past decade.
7. Use of modern technology and better and widespread policing facilities have increased the rate of detection of crime by police resulting in more convictions and large numbers being admitted to prisons.

Prison overcrowding leads to serious problems for prison authorities. It is related to serious health hazards and disturbs penal rehabilitation and reformation programmes. As a result, security problems, terrorism and subversive actions may occur. If prison is overcrowded hard and soft criminals interact with each other, which may lead to connect mild offenders to hardcore criminals. Overcrowded prisons cause stress for prison officials and further strain prisoners as they live in unacceptable conditions which fail to adhere to the United Nations Standard Minimum Rules for the Treatment of Prisoners.

In Sri Lanka we have very few non-institutional treatment methods, and those methods have not been effective due to administration problems and provisions. Therefore it is time to improve the treatment of offenders through enhancement of community-based alternatives to incarceration.

II. TRADITIONAL ALTERNATIVES TO IMPRISONMENT

Many countries have probation, parole and community service which are commonly known as traditional alternatives to imprisonment. These non-institutional treatment methods are widely used in many developed and developing countries.

The non-institutional measures are mostly community based corrections. The concept has evolved with the thinking that correction, if linked to the community, will be less costly, more humane and more effective than imprisonment in dealing with offenders convicted of minor offences. There is a need in the field of community corrections for a systematic and orderly development having due regard for local conditions and local needs. In developing such a system it is necessary to ensure that no individual who does not require incarceration for the protection of others is confined in an institution and that no individual is subjected to more supervision or control than required. On the other hand creation of community based programmes should ensure that they respond not only to the needs of the offenders but also the interest of the community. If they are not administered properly it will amount to the criminal justice system going soft on crimes and criminals.

In Sri Lanka, we have only a few non-institutional treatment methods and even these few have not been very effective due to lack of administrative provisions and disinclination on the part of the courts to pass such sentences.

A. Parole or Release on Licence

The basic philosophy of parole is that a prisoner shall not be held any longer than necessary as it is detrimental to his or her reformation and also an unnecessary expense to the State. Parole is a procedure whereby a prisoner is released from an institution at a time considered appropriate by Parole Board, prior to the completion of his or her full sentence so that he or she may serve the balance of the sentence at large in society. The offender is also subject to the condition that he or she will be returned to prison if he or she fails to comply with the conditions governing his or her release.

This scheme gained momentum over the years and remains at present one of the very successful non-institutional measures in our country. From 1997 to date 1,199 prisoners have been released. An average of 110 prisoners are released every year. We have had only 89 violations during that period.

1. Practices in Sri Lanka of Treatment of Offenders

(i) Remission

All prisoners are now allowed a normal remission of one third of their sentence for good conduct and industry. Prisoners who have completed one year at an Open Prison Camp are eligible for a special remission of one month of their sentence for each year they serve.

(ii) Special Amnesty

While convicted prisoners who were serving long term sentenced were given special reductions of sentences, some prisoners who were serving short term sentences were released on account of special occasions like Independence Day, Wesak Full Moon Poya Day, etc.

B. Release of Prisoners on Licence Scheme (Social Integration)

The "Licence Scheme", introduced in Order 1969, may be considered a progressive step in dealing with offenders. The system of release of prisoners on licence under para 11 of the Crime Prevention Ordinance was based on a decision by the then Minister of Justice. The members of the first Licence Board were Asst. Secretary, Ministry of Justice, the Senior Prison Medical Officer and the Commissioner of Prisons appointed by the Minister of Justice. The first meeting of the Board was held on 4 October 1969. At the inception, the mode of selection for release under licence scheme depended on the term of imprisonment under which prisoners sentenced to eight or more years of imprisonment who have served half that term were eligible for the scheme sustained by good conduct, character, prison records and rehabilitation susceptibilities. In the first batch they selected seven prisoners who were released on 15 November 1969.

The Licence Scheme underwent several modifications from time to time and now functions under the Commissioner of Prisons Circular no 35/92W/08 of 1 September 1992.

1. Prisoners serving a sentence of two or more years but less than five years and who have completed a term of one year.
2. Prisoners serving a sentence of five or more years but less than ten years and who have completed a term of two years.
3. Prisoners serving a sentence of ten or more years but less than 15 years and who have completed a term of three years.
4. Prisoners serving a sentence of 15 or more years but less than 20 years and who have completed a term of four years.
5. Prisoners serving a sentence of 20 years or more but less than 25 and who have completed a term of five years.
6. Prisoners serving a sentence of 25 years or more and who have completed a term of six years.

In the case of prisoners who qualify under the above requirements, social reports are compiled by the Welfare Officers and along with recommendations of the Superintendent of Prison(SP) are submitted to the Secretary, Licence Board. The SP (Welfare) is the secretary *ex officio*. Licence Board meetings are held twice

a month at the prisons headquarters and the prisoners according to their qualifications as above are produced to the License Board together with social report files and only those eligible prisoners are recommended to the Hon. Minister by the Licence Board for release on licence. The rest are withheld for reconsideration.

A prisoner released on the licence scheme is conditionally allowed to serve the balance of his or her sentence under the supervision of a Welfare Officer and is reintroduced to society to lead a normal life with his or her spouse and children and parents. A prisoner so released will be guided by the Welfare Officer to live a decent life and he or she will be known as a “Licensee”. The Welfare Officer provides a curative target programme pertaining to the Licensee at the inception which is result-oriented during the licence period. During the licence period the Welfare Officer submits his or her quarterly progress returns, accompanied by the Senior Welfare Officer’s observations, to the Licence Board where they will be discussed and the necessary guidance offered.

If a Licensee transgresses the contracted conditions, attempts are made to admonish him or her through advice and warning by a Welfare Officer and if such attempts fail the Licence Board is consulted for instructions. If that measure too is ineffective the licence granted to him or her will be rescinded and the balance full term of imprisonment from the date of release is reemployed. The case may be referred to a magistrate if necessary and a further term of six months of imprisonment may be imposed. However, transgressions so far have been minimal. This manner of relief is not a right of a prisoner but a privilege.

The member released on license scheme since 1997 to 2007 and the number of licenses revoked for violation of conditions are as follows.

Year	Work Release	Home Leave	License Scheme
1997	200	315	152
1998	199	330	99
1999	212	373	116
2000	171	322	112
2001	249	21	18
2002	230	174	47
2003	210	267	108
2004	559	528	104
2005	320	364	153
2006	553	496	124
2007	1,068	547	208

Source - Department of Prison – Sri Lanka

C. Work Release Scheme

Characterized by the motive of facilitating the penal stage of a prisoner to be spent more fruitfully and with flexibility, the work release scheme was introduced in 1974. The project was approved by the Minister of Justice in terms of Clause 11 of the Crime Prevention Ordinance. The selection of prisoners for the scheme is confined to those serving a sentence of two or more years and those due to serve less than two years of the sentence. The objective of the scheme is to accustom the prisoner to conditions and challenges of the society he or she re-enters once set at liberty from jail. The plentiful bestowal the scheme extends to the inmate after release is the employment opportunity.

The prisoners are engaged in such activities as gardening or clearing under the scheme at state institutions on weekdays from 7.30 AM to 4.00 PM (except public holidays). A retired prison officer is in charge of their security for which service he or she is paid by the institution concerned.

The prisoners so engaged are provided with the midday meal and an allowance of Rest 185/- per day by the institution. The income so earned is credited to their account at the People’s Bank and is gainfully invested after release. This project originated at the one prison has now expanded to the three main prisons.

THE 141ST INTERNATIONAL SENIOR SEMINAR
PARTICIPANTS' PAPERS

The project has benefited nearly 25 state institutions in 2007, the number of prisoners engaged was 230 and their total earnings amounted to Rs.4, 957,205/-.

The current statistics on prisoners engaged in work release from 1997 to 2007 are shown below.

Prisoners Engaged in Work Release scheme 1997 to 2007

Year	No of Prisoners Engaged on Work Release	No Found Unsuitable	Total Amount Earned for the year (Rs)
1997	200	8	1,149,653
1998	199	15	1,365,836
1999	212	12	2,047,301
2000	171	8	1,976,186
2001	249	10	3,387,876
2002	230	15	3,459,993
2003	210	22	2,625,641
2004	559	45	3,280,110
2005	320	44	3,276,166
2006	553	33	3,659,026
2007	1,068	29	4,957,205

Source – Department of Prisons – Sri Lanka

This salutary and successful scheme has served as a catalyst for the reintroduction of inmates to society as useful and reformed citizens.

D. Home Leave

Prisoners who become eligible for release on license and prisoners who have served at least six months at an open prison camp become entitled to visit their homes unescorted for a maximum period of seven days at a time once in six months.

Prisoners Sent on the Home Leave Scheme, 1997 to 2007

Year	No. Sent on Home Leave			No. Violated Law		
	Male	Female	Total	Male	Female	Total
1997	302	13	315	1	-	1
1998	307	23	330	8	-	8
1999	366	7	373	16	-	16
2000	315	7	322	5	-	5
2001	21	-	21	-	-	-
2002	171	3	174	3	-	3
2003	265	2	267	3	-	3
2004	523	5	528	3	-	3
2005	361	3	364	9	-	9
2006	490	6	496	9	-	9
2007	537	10	547	14	-	14

Source - Department of Prison – Sri Lanka

Five hundred and forty seven prisoners were sent on Home Leave during the year bringing the total to 3,584 since the introduction of the scheme in 1974. There were 16 violations of the trust placed in those prisoners.

III. PROBATION SYSTEM

The probation system in Sri Lanka commenced on 12 March 1945, under the Department of Prisons. It was inaugurated with ten Probation Officers who were paid salaries by the Government. However, after 1919 the probation system had been tried in Sri Lanka from time to time through Voluntary Probation Officers. In 1944 the Probation Ordinance was enacted to keep offenders under Probation. Accordingly, by 1960 the probation system had been extended throughout the island by appointing Probation Officers to all Judicial Districts in the Island. Since the probation system was functioning under the Department of Prisons, it was known as the Department of Prisons and Probation with the extension of the probation systems. The Children and Young Persons Ordinance No. 48 of 1952 was enacted and enforced in Sri Lanka. A separate Department, titled the Department of Probation and Child Care Services, was established on 1 October 1956, bringing the probation functions too under its purview. The objectives of the Department as envisaged by the Government are as follows.

With the establishment of Provincial Council system in Sri Lanka, some administrative powers were vested with the Provincial Councils. Hence some of the functions of the Department have been assigned to Provincial Commissioners of Probation.

A. The Objectives of Probation Child Care Services as Envisaged by the Government

1. Limiting the imprisonment of offenders by rehabilitating them using probation strategies with a view to re-integrating them into society as good citizens.
2. Taking very lenient and mitigated judicial actions in respect of children and young persons.
3. Provision of requisite service to needy children and young persons.
4. Offering such children as far as possible the opportunity to live with their parents and provision of due protection.

The following chart shows the number of offenders rehabilitating under the Department of Probation and Child Care.

Probation Offenders - 2005 (Year)

Province	Theft, Looting & Burglaries	Straying	Sale & use of Liquor & Drugs	Sexual Abuse/ Tape/Brothels	Others	Below 15 Years	Between 15 - 19	Between 20 - 24	Over 24 Years
Western Province	142	2	46	4	31	40	122	36	27
Southern Province	35		20	2	9	28	22	4	12
Central Province	45		7	1	9	24	29	3	6
North Western Province	19		1	1	2	19	4		
Sabaragamu Province	63	3	4	8	21	51	41	4	3
Uva Province	17				1	15	1	2	
North Central Province	33		3	4		19	19	2	
North East Province	16		1	14	11	26	16		
Total	370	5	82	34	84	222	254	51	48

Source - Department of Probation & Child Care – Sri Lanka

B. Main Functions of the Probation and Child Care Department

1. Moulding the character and rehabilitation of adults, young persons and juvenile delinquents referred to the Department.
2. Directing children not obedient to their parents, cutting school, stubborn and engaged in anti-social activities even though they have not committed any offence considered a crime under the Penal Code.

THE 141ST INTERNATIONAL SENIOR SEMINAR
PARTICIPANTS' PAPERS

3. Giving protection to and looking after the orphaned, abandoned, destitute and those subject to cruelty and faced with various disasters and subject to abuse.
4. Investigation supervising and providing aids to voluntary organizations and institutions engaged in children's welfare services.
5. Taking resources to lessen and prevent the number of children likely to break down in life due to poverty or other social requirements.
6. Implementation of the Convention of the Rights the Child adopted by the United Nations and taking necessary steps to protect the Rights of the Child.

The chart below describes the offenders investigated during the year under review.

Offenders Investigated During the Year Under Review (Juvenile/Youth/Adults) - 2005

Province	Theft, Looting & Burglaries		Physical Injuries		Seale and use of Drudge		Prostitution & Straying		Psale & Use of Liquor		Attempt to Commit suicide		Acts of terrorism		Others	
	F	M	F	M	F	M	F	M	F	M	F	M	F	M	F	M
Western	9	391	9	18	6	91	41	189	2	50					62	96
Southern	5	44	1	15		9	9	2	7	6					3	18
Central	10	62	12	14	4	28				3		1		1	14	6
Nor/ West	8	33	2	1	2	3	14			2					1	2
Sabaragamu	5	60	4	4	10	45	11		1	22					16	17
Uva	2	34	1	5			2	6			2				16	8
North Central	3	68				3				4	1				1	3
North East	20	24	71	54	6	7	1	9	1	9	30	19	25	29	20	33
Total	62	716	100	111	28	186	78	206	11	96	33	20	25	30	133	183

Source - Department & Probation & Child Care – Sri Lanka

IV. COMMUNITY SERVICE ORDERS

As an alternative to a prison sentence courts may order an offender who has been convicted of an offence punishable with imprisonment to carry out a community task for a number of hours stipulated by the Court within a certain period of time. If the offender fails to carry out his or her work commitments, he or she will be dealt with by the Court by imposing any other appropriate punishment. Community Service by order of the Court is currently practiced in several countries. The Community Service Orders Law was introduced in Sri Lanka by the Administration of Justice Law No. 44 of 1973. However, due to lack of rules regarding the implementation, the courts ceased to impose the sentence. Action has now been taken to establish a separate Department under the Ministry of Justice to supervise carrying out the sentence and legal provisions have been made under Community-Based Correction Act. It is therefore expected that Community Service Orders will be effective in Sri Lanka as a useful non-institutional mechanism in the near future.

V. INTRODUCTION OF NEW LEGISLATION ON GRANTING OF BAIL

In Sri Lanka, attempts also have been made to reduce the pressure of overcrowding in the recent past by introducing new legislation. The introduction of the Release of Remandees Act No. 18 of 1991 was for the dual purpose of reducing prison overcrowding and granting relief to those persons held in custody for their inability to furnish bail. Certain bail regulations made under the Emergency Regulations empowered prison authorities to release some categories of remand prisoners who had failed to furnish bail though ordered by

Courts, upon their signing a bond.

VI. INTRODUCTION OF SUSPENDED SENTENCES

The introduction of suspended prison sentences under the Code of Criminal Procedure Act No. 15 of 1979 for certain categories of offenders helped reduce the admission of a considerable number of convicted prisoners. Presently most of the law level courts have passed this suspended sentences on offenders who committed minor crimes, where there is no grievous impact on society.

VII. REQUIREMENT OF INTEGRATION OF ALL AGENCIES WITHIN THE CRIMINAL JUSTICE SYSTEM

The importance of an integrated approach involving all parts of the criminal justice system, in solving most of the problems of prison including overcrowding, has been accepted by many countries today. However, in practice, each agency works in separated and isolated from each other. In Sri Lanka, police, prisons and probation come under three separate Ministries. The Courts function independently under the Judicial Service Commission. There is very little or no co-ordination existing between the different agencies though they work to achieve interrelated objectives. Therefore, the problems of overcrowding of prisons become the exclusive problem of the correctional institutions. Having realized the roles the other agencies can play in reducing the prison population, such as the police expediting the investigations, and courts expediting the trial process and utilization of non-custodial methods in a greater measure, workshops, Seminars and Conferences have been conducted involving the different agencies through the initiative of the Department of Prisons and Ministry of Justice. Therefore, it is necessary to have a constant dialogue with all agencies within the criminal justice system. When making policies for the country at least policy makers need discuss the matter with each other to reach a consensus.

VIII. CONCLUSION

The problem of prison overcrowding, which has direct links with the increase of population of a country, and the increase of the crime rate resulting from its socio-economic factors, will continue to worry the nations of the world unless some meaningful steps are taken to control it. No country can continue to expand its prison capacity in proportion to the increasing rate of offenders. In this regard it is very important to create a public awareness that imprisonment is not the only effective penal sanction for all types of offence.

On the other hand where corruption within the criminal justice system exists, alternatives to imprisonment amount to additional mechanisms of control and abuses of power such as bribery and denial of justice. Non-custodial measures should be implemented in parallel with pre-trial diversion measures such as caution and mediation mechanisms to ensure that the over-use of arrest and imprisonment are addressed systematically and holistically.

Non-custodial measures include that of discharge (absolute and conditional), suspended sentences, fines, binding over, compensation orders in the mediation process, attendance centre orders, supervision orders (with or without requirements), probation orders, remission of sentences and grant of amnesties, parole of release on licence, work release, and community service orders, etc.

Community service is an order of the court whereby the offender is offered the opportunity of compensating society for the wrong he or she has done by performing work for the benefit of the community instead of going to prison.

In Sri Lanka, the daily average population of convicted and un-convicted prisoners was 24,255. According to Table 1 the number of prisoners will increase day by day according to the prevailing socio-economic situation in the country. As a result, the cost of prisons increases day by day. Hence, there is a social impact prevailing in the country due to a non-effective prison system.

In this circumstance, non-institutional treatment methods for prisoners are urgently required considering the economic and social factors of the country. Therefore, relevant authorities and policy makers should pay serious consideration to reviewing the criminal justice system, focusing on the improvement of the treatment of offenders in community-based alternatives to incarceration.

MEASURES AGAINST OVERCROWDING IN URUGUAY'S JAILS, PRISONS AND REFORM CENTRES

*José Enrique Colman**

I. INTRODUCTION

The difficult situation that has prevailed in the Uruguay penitentiary system for several decades, demonstrating a progressive deterioration and reaching the present the actual numbers of imprisonment (which fall far short of international standards), has determined the generation of different initiatives that today appear with the purpose of contributing to the reduction of the number of inmates and better management of the penitentiary system, trying enhance community-based alternatives to incarceration.

In almost all the countries of Latin America the penitentiary systems are heavily overcrowded and the number of prisoners increases much more quickly than the construction of new jails. In the short term, this could become an untenable situation.

In Uruguay, by 2015, we could expect double the number of prisoners we have today, but the situation is probably similar in all of the countries of the region.

In our country the prison population has grown year by year, leading to overpopulation of the jails as mentioned above. Various factors are suggested as contributors to this phenomenon. We can mention the increase in social violence, due to the deterioration of moral values, and economic, educative and cultural factors. These are only some of most outstanding factors and the discussion of values, mainly morals relating to the causality of the crime and its increase, is a wide discussion as many arguments are subjective.

Our society is immersed in the consumption of an incredible amount and variety of drugs; the worst of them is coca paste. It would seem there are generations that already are lost, for whom it is impossible to establish a moderately coherent conversation. How to rehabilitate these people, and in this way, to contribute to public security, and therefore society?

The difficult reality is that released inmates sometimes spend just a few days enjoying their freedom before backsliding and committing other crimes. They return happily to the prisons, because their friends and relatives are in the jail and they will meet again.

Although it seems cruel, this is the reality, not for all but for the great majority, and we wonder ourselves where are we failing, because according to the statistics of other countries the situation is international, without regard for the budget, status of jails as private or public, or type of government.

Different Uruguayan governments, mainly from the end of the dictatorship in 1985, have voted a series of legal initiatives to avoid the growth of the prison population, gradually choosing alternatives to replace imprisonment as the main social punishment.

In the next pages we will transcribe the main legal norms of our jurisdictional procedures. In some cases we will see conjunctural laws that were passed to clear legal prisons and other decisions that led to the substitution of prison by other alternatives like reduction of punishments, domiciliary arrest, penalty fines, communitarian tasks, fulfillment of only a part of the sentence, enhancement of institutes like the National Patronage of Jailed and Released Inmates in order to reintegrate released offenders, productive activity in

* Executive Co-ordinator, Executive Co-ordination Department, National Bureau of Jails, Penitentiaries and Rehabilitation Centres, Uruguay.

jails, etc., and the last alternative, the Law of Redemption of Penalty, will be outlined below.

Also, because the problem is dynamic and the procedures suggested are not yet sufficient we are designing new alternatives and voting on legal possibilities to continue to develop other types of ideas like the use of electronic bracelets, probation officials, half way houses, etc., which are at present in the study and development stage.

II. RELEVANT LAWS ¹

Uruguayan society has evolved over its two hundred year history and this applies also to the law and legal norms that govern the different aspects of the society, including the penitentiary system.

We must first address the Constitution of the Republic, the fundamental Law of Uruguay, which observes deeply the subject of this paper. Articles 26 and 27 give the primary framework from which the other laws outlined below are derived.

A. Constitutional Dispositions

“Article 26. - Capital punishment will not be applied to any person. In no case it will be allowed that the jails serve to torture; they are just to assure the indicted and condemned, trying for their reeducation, and developing the aptitude for the work and the prophylaxis of the crime.”

“Article 27. - In any stage of the trial which judges preview and from which there can be no imprisonment, the judges will be able to free the inmate for appropriate bail according to the law.”

B. Exceptional and Conjunctural Laws

1. Amnesty Law

In 1985, when Uruguay again became a democracy after a long period of dictatorship, the new government passed laws that tried to fit the national reality and among others, as we said in the Introduction, approved the “Law of Amnesty” where diverse benefits were granted, which, besides correcting illegal situations, led to the humanization of the system. This was so was approved law N° 15,737 of 1985. Included below are only some articles which begin to explain the legal evolution that has occurred from that time to the present time.

“Article 21. - The Supreme Court of Law will be able to give anticipated freedom to the condemned who are private of freedom in the following cases:

- 1º) If the sentence is more than two years of imprisonment and the person has fulfilled half of the imposed punishment.
- 2º) If the sentence imposed was prison or fines.
- 3º) If the convict has fulfilled two thirds of the punishment imposed by the Supreme Court of Law it will achieve the freedom anticipated. It will only be able to deny, by founded resolution, in the cases of manifest absence of signs of rehabilitation of the condemned.”

According to this law more than 800 inmates were freed, and there was a temporary significant decrease in the prison population.

C. Law of Anticipated and Provisional Freedom

With the present government, another law of exceptional type was approved that also allowed the country to clear the different prisons transitorily. This law is Law N° 17,897, “Anticipated and Provisional Freedom. Exceptional Regime.” Article 2 of this law gave powers to the judge to grant anticipated freedom of the inmate where the inmate has fulfilled:

- “a) Two thirds of the imposed punishment, and the same is superior to three years of penitentiary.”
- “b) When they have fulfilled half of the punishment imposed in the case that the imprisonment preview

¹ Please note that all translations are provided by the author.

was of up to three years of penitentiary.”

D. Transitory Exits

This law establishes the possibility of transitory leave for an inmate who conserves his habits of work which will help in his social reintegration.

“Article 62. - For the concession of the transitory leave, it will be required to own good behaviour and it could be granted every time the inmate, personally or through his Defender, present a written request in the Direction of the Jail where the inmate is located.”

In a term that will not exceed 20 days from the presentation of the request, the prison authority will formulate a report to the judge of the cause. If the prison report were opposed to the concession of the transitory leave, because the inmate does not have good behaviour or for another reason, the prison authority will inform the judge of the cause, who will solve, in founded form, the previous opinion of the prosecutor. If the report of the prison authority was favourable, they will have to establish, in precise form, the regime to be followed by the inmate:

- (a) The place or maximum distance to that the inmate will be able to move.
- (b) The norms of conduct that the inmate will have to observe during the leave, as well as the restrictions or prohibitions that are considered advisable.
- (c) The time of duration of the exit, the reason and the degree of security that is adopted.
- (d) Any other requirement or condition if it is considered necessary for the best fulfillment of the regime.

The report will be presented by the prison authority to the judge with competency. The copy will be sealed and the day and hour of presentation are noted. The Actuary of the Court, under the most severe responsibility, will have to put the report to the office of the judge in immediate form, who, without further proceeding, will give view to the prosecutor, within a term of five working days. Upon return of the file, the judge, who will have equal term and under his or her more serious responsibility, will be sent notice of the proposed regime or the modifications pertinent to the case.

The decision is not appealable. If transitory leave is denied the inmate cannot present a new request for 90 days.

An inmate granted transitory leave who delays his or her return to the establishment, without justified cause, will receive an increased punishment at the rate of two days for every day of delay. The prison authority will have to inform the judge, within 10 days, of the moment at which the inmate returns the establishment.

To further the aims of the legislation, the prison authority will inform the Directors of the Penitentiary Establishments of the National Direction of Jails, Penitentiary and Departmental Headquarters and Equipment Rehabilitation Centers in its respective jurisdictions of the procedure.

E. Indicting Without Prison

Another law that has had remarkable influence on the present legal regime is “The Law of Indicting without Prison” from 1989. It qualifies judges in certain circumstances not imprison people who satisfy certain requirements and is still effective today. It is law N° 16,058:

“Article 1º. - the preventive imprisonment will not be applicable when concur, simultaneously, the following circumstances:

- (a) If the offence committed will be presumable that will not have to have penitentiary punishment;
- (b) If, according to the Magistrate, the records of the indicted, their personality, the nature of the imputed offense and the circumstances will presume that the person will not avoid the trial;

- (c) If to criterion of the Judge, and the examination of the circumstances mentioned in the literal (b) it will be possible to be inferred that the indicted will not incur in new criminal conduct.

Despite the items (a), (b) and (c), the judge will decree preventive imprisonment, in all the cases, if the person has a background or previous cause in proceeding so requiring.

F. More Severe Sentences for Certain Types of Crimes

1. Law of Citizen Security

In 1995, the Law N° 16,707, "Law of Citizen Security", was passed and relevant articles are included below.

"In the cases of indicting with prison, if the inmate registered one or more pending criminal causes, discharge the freedom of the inmate will have to be founded, including an evaluation on the danger of the agent and his or her possibilities of social reintegration."

This law created new criminal figures, increased the punishment in some cases and diminished it in others, according to the new social reality and criminal typology and began to restrict judges' power to give liberties, which increasing the incarceration rates since many crimes were transformed into non-dischargeable offences and the judges do not have another option than to imprison the offender.

The motivation of the present law, among others, was a situation of social alarm caused by the increase of certain violent crimes and drug trafficking that demonstrated the quick deterioration of the moral basis of Uruguayan society.

G. Domiciliary Arrest

Another important step was the provision of Domiciliary Arrest in certain cases, such as those with serious illnesses or aged people.

"Article 8º. - (Provisional Safety for suspected and convicted offenders who are ill or in other special situations). If the suspect, the indicted, or the condemned during the fulfillment of his or her sentence are presumed to be in some of the states anticipated by Article 30 of the Penal Code (Madness), it will be possible to change the incarceration for his or her internment in a special establishment, subject to expert opinion.

If one person be in serious disease or special circumstances that makes his immediate internment in prison evidently detrimental, the continuity of the deprivation of freedom in a center of imprisonment in which one is, the Judge will be able, previous the expert works that he or she considers pertinent, to prepare the domiciliary prison or other insurer decision.

Equal criterion will be adopted with respect to the situation of the woman in the last three months of pregnancy, as well as during the three first months of maternal lactation. In such case, the judge will previously require an expert report from the Forensic Technical Institute about the convenience or necessity with respect to the adoption of another insurer decision.

The person indicted or punished with domiciliary arrest will be able solely to leave her house to carry out pertinent medical checkups on her state and condition. The breach of this disposition will imply the immediate revocation of the benefit.

Having stopped any one of the hypotheses contemplated in the present article, the processing or punished if so, will have to return to the prison where it fulfilled the measurement or the sentence precautionary."

"Article 9º. - (Domiciliary Prison). The Judge will be able to have the domiciliary prison indicted people or the condemned majors of 70 years, when it does not involve risks, considering especially the circumstances of the committed crime. This last disposition will not be applicable to the accused and the condemned who has committed the following crimes:

The crime of aggravated homicide;
Crimes of violation;

The crimes anticipated in the Statute of Rome of the International Penal Court (Law N° 17.510, of 27 June 2002).”

III. ALTERNATIVES TO IMPRISONMENT

In 2003, social dynamics and the governmental preoccupation with the prison situation motivated a new law, N° 17,726, whereby alternative measures to imprisonment can be imposed as outlined below.

“Article 1°. - Preventive imprisonment will not be applicable in minor crimes or crimes sanctioned with fine, suspension or incapacitation.”

“Article 2°. - A judge cannot decree preventive imprisonment of an indicted person when *prima facie* he or she understands that the behaviour studied is not punishable by imprisonment. In that case some of the measures in the following article will be able to replace preventive imprisonment. The substitution will not be decreed when the gravity of the facts or the damage caused by the crime deserves imprisonment. In all the cases the opinion of the Prosecutor will be required, that to such effect, the alternative measure will not increase the risk to the population.”

A. Substitute for Preventive Prison

“(a) Periodic presentation in the Court or Police Station.

- (b) Prohibition on driving vehicles for a term of up to two years, when found guilty, in occasion of the transit carrying, against the life, physical integrity or would have brought about important damage in the property to criterion of the Judge who will retain the license driver, and he or she will communicate to the local authorities his or her decision.
- (c) Interdiction: the prohibition to concur to certain places, commerce or places, including the own one; or the obligation to remain within certain territorial limits.
- (d) Medical or psychological attention of support or rehabilitation: the obligation to be under certain treatment by a maximum term of six months, if the treatment were ambulatory and of two months if it required internment.
- (e) Voluntarism or communitarian services: the obligation to fulfill the tasks that are assigned to him or her, having in account its aptitude or suitability, public bodies or nongovernmental organizations, whose aims are of evident interest or social utility. These measures will not be able to exceed the two hours per day or twelve hours per week and its maximum term of duration will be of ten months.”

The Supreme Court of Law will establish the general criteria that will have to fulfill the institutions to that it refers this literal one, with the object of determining the remunerations that will be pleased by the work fulfilled by the indicted and that will be deposited in a bank when the person finishes as his or her deal.

The judges will be able to also commit the fulfillment of this measurement to the National Patronage of Jailed and Released or to departmental commissions with similar assignments in the Republic.

- “(f) Domiciliary arrest: the obligation to remain at home, without leaving its limits, for a maximum term of three months or to remain in it during certain days or hours by a maximum term of six months.
- (g) Arrest in hours of rest: the obligation to remain the workable days during the hours of rest under arrest for a maximum term of six months. The arrest will have to be fulfilled in the Home of the Released in the charge of the National Patronage of Jailed and Released, or where it indicates it to the Judge.
- (h) Arrest of weekend or weekly rest: the obligation to remain a continuous day and a half under arrest that will agree with the lapse of weekly rest of the indicted, that will be fulfilled in a Police station, for a maximum term of six months.

- (i) Any other substitute obligation proposed by the indicted and accepted by the Judge, who fulfills the purposes of this law or supposes a suitable repair of the caused damage.

Article 4º. - It will be procured that the substitute measures do not damage or if it do could be as minimum possible in the labor or educative activities of the indicted.

Article 5º. - In case of impossibility of the fulfillment of the measurement by cause non imputable to the indicted, the same will replace or others without increasing its gravity on the other.

Article 6º. - The substitute measures do not come in the cases from recidivism.

Article 7º. - The measures of this law refers the article, will be only revoked in the serious cases of violation of the imposed duties.

Case will be considered burdens the existence of a later processing.

In this case the fulfilled measures will be computed with the object of the preventive one to suffer in the following way:

- (a) Interdiction (literal b) and d)): a day of prison by every five days of the fulfilled measurement.
- (b) In case of ambulatory treatment: a day of prison by the weekly treatment will be computed.
- (c) Communitarian services: a day of prison by every day indeed worked.
- (d) In case of Domiciliary Arrest with absolute prohibition to absent itself: a day of prison by every day of arrest; in case the arrest had been partial: a day of prison by every ten hours of continued arrest.
- (e) Arrest in hours of resting: a day of prison by each day of arrest.
- (f) In case of arrest of weekend or weekly rest: two days of prison by each opportunity of fulfillment of the measurement.”

IV. FINES

“Article 9º (Substitute Punishments). - When the punishment be with prison (not penitentiary punishment-plus two years imprisonment expected) it can be replaced by some of the measures mentioned before.

Article 10 (Application). - When in the sentence was not solved the freedom can be changed by the substitute measure that corresponds whenever the punishment to fall does not surpass the three years of penitentiary. The punishment will not be applied for people with files or habitual. In such cases the Judge, when determining the punishment, will settle down the value of day-fines.

Article 11. - When sentence definitive imposes prison sentence put to the indicted it is possible the conditional suspension of the punishment (article 126 of Code Penal), whenever the person is a primary that has been processed without prison or with the substitute measures anticipated in this law it has fulfilled and them, except for the existence of serious cause properly founded. If the sentence will impose a punishment of up to three years of penitentiary the Judge will be able to grant the suspension conditional of the pain, taking care of the requirements of the previous interjection and previous report of the Forensic Technical Institute, basing its decision. In both cases the term of monitoring by the authority will be of a year.

Article 12 (Determination of day-fines). - The value of day-fines will be determined by the Judge between 0.10 UR (a tenth of a re-adjustable unit) and 5 UR (five re-adjustable units), considering the economic situation of the indicted, the goods that it owns, its income, their aptitude for the familiar work and his personal obligations.

Article 13. - ... the punishment will be eliminated at the rate of day-fines by every day of pain,

discounting the days of prison indeed undergone, or the fulfillment of the computed substitute measure.

Article 14. - ... If the payment of a fine condemns, the indicted will be able to do it effective of the sums that had been deposited in guarantee of payment of day-fines, or to be paid until in eighteen monthly payments, those that will be able to be reduced, in agreement with the economic possibilities of the condemned. The Judge will be able, exceptionally, to reduce his amount when the condemned credits that he or she has gotten worse of fortune...[].

The control of the payment will be of account of the Office Actuary who, without needing the judicial mandate, will come to obligate to the condemned to the payment of the owed thing whenever the payment is late in more than one.

Article 15. - In the cases of conditional freedom, the term of monitoring of the authority will be of three years and could be reduced up to two by the Judge of execution, office or to order of the condemned.

Article 16. - The sums that are collected by the payment of punishment as well as by concept of day-fine, will be deposited for the State.”

V. CAUTIONS (BAILS AND PAROLE)

“203.1. - When the Court has the cease the freedom deprivation, or establishes the cease of other limitations to the physical freedom of the imputed, he will have to require to him that he gives security interest in property or personal of the fulfillment of the imposed obligations.

203.2. - In order to determine the quality and the amount of the bail, the Court will make the estimation so that it constitutes an effective reason and it shows that the indicted abstains to infringe the imposed duties and appears every time it is required of him or her.”

A. Bail

“204.1. - The Bail consists of the affectation of determined, movable or immovable goods that, in guarantee of the sum determined by the Court, it is realized by imputed or the another person. It will be able to constitute in the form of deposit in money or other quotable values or by means of granting of mortgage or pledges or any other form with guarantee that is effective and sufficient to criterion of the Court.

204.2. - When the bail consists of mortgage, the writing document will be granted by notary public proposed by the imputed. In order to authorize it, he will have ten days fixed as of the date of the decree of its designation. Passed this term, the Court will be able to designate to another notary public. The Registries Public will have to issue in urgent form asked for certificates.”

B. Personal Warranty

“205.1. - The personal guaranty consists of the obligation that jointly with the imputed assumes one or more people proposed by the person as warranty with they goods to pay the sum that the Court fixes.

205.2. - It can be constituted in bondsman who has capacity to contract and is, in addition, honest person and with economic solvent, verifying this topic by formal document exhibition, that the secretary or actuary will describe as the Court.”

C. Parole

“Article 206 (Parole). - When the imputed is well-known poor or destitute, instead of the other items the Judge can ask him his Parole, that will consist of its promise to faithfully meet the conditions imposed by the Court.”

VI. PUNISHMENT REDEMPTION

In the same law that established the Regime of Transitory Exits also approved the “Regime of Redemption of Punishment”, which allows inmates to redeem punishment in the following way:

A. Work

A day of imprisonment is equal to two days of Work. They are not computed at more than eight hours daily.

B. Study

A day of imprisonment is equal to two days of study. A day of study is equivalent to six hours weekly.

This area is very important and it is applied widely. An Office has been established with the rank of Direction that exclusively promotes, controls and informs judges of the dispositions above-mentioned. The relevant article from the Law N° 17,897 of 14 September 2005 is outlined below and establishes:

“Article 13 (Redemption of Punishment by work or study). – The Judge will grant the redemption of punishment by work to the inmate without freedom. To the accused and the condemned a day of imprisonment by two days of work will be exchanged to them. For these effects they will not be possible to be computed more than eight hours daily of work.

The prison authority will determine the works that must be organized in each penitentiary center, those that along with the works carried out during the transitory exits authorized by the competent Judge, will be unique the valid ones to redeem punishment.

Also the prison authority will promote the creation of sources of work, industrialists, farming or handicrafts skills according to the budgetary circumstances and possibilities.

For the effects of the evaluation of the work in each center of imprisonment there will be a Advised Council constituted by personnel designated by the prison authority. The Judge will grant the Redemption of punishment by study to the condemned with jail.

To the indicted and the condemned a day of imprisonment by two days of study will be paid to them.

It will be computed as a day of study the dedication to this activity during six hours weekly, thus is in different days. For those effects, they will not be possible to be computed more than six hours daily of study.”

“Article 14 (Labor Insertion of released people). - It would include in all bids on public works and public services. Is mandatory for the contracting industrialists, to register in the work lists a minimum equivalent to 5% (five percent) of the affected personnel to tasks of laborers or similar, to released people who are registered stock-market of Jailed and Released Work of the National Patronage. Also, the Executive authority will be able to establish a system of advantages for those companies that register released registered in stock-market of Work referred, over 5% (five percent) stipulated. The Executive authority, through National Patronage of Jailed and Released, will promote agreements with the Departmental Governments to establish similar regimes with respect to works and services departmental public.”

LABOR AND EDUCATIONAL ACTIVITY IN URUGUAY’S JAILS							
MARCH 2008							
	MEN	WOMEN	TOTAL INMATES OF THE COUNTRY	WORKING	STUDYING	WITHOUT WORK OR STUDYING	TEACHERS
TOTAL	6981	531	7512	1991	1230	4291	122

VII. CREATION OF THE PARLIAMENTARY COMMISSIONER (OMBUDSMAN)

With the battery of measures destined to improve the national prison system in 2003 the parliament approved for the first time a law that instituted the figure of the denominated Parliamentary Commissioner whose main function is to ensure that the human rights of inmates are respected, giving him ample powers to exert that function while at the same time exclusively informing the Legislative Power of his activities

THE 141ST INTERNATIONAL SENIOR SEMINAR
PARTICIPANTS' PAPERS

and the irregularities found.

I think it is better to illustrate the text of the Law:

“Article 1°. - The Parliamentary Commissioner’s main assignment is to advise the Legislative Power in his function of the control of the fulfillment of constitutional, legal and prescribed the norm effective, and of the international treaties ratified by the Republic, referred to the situation of the deprived people of freedom by judicial process. Also the supervision of the activities of the organizations in charge of the administration of the prison establishments and the social of inmate will be incumbent on to him or released reintegration.

Article 2°. - For the fulfillment of his functions, the Parliamentary Commissioner will have the following attributions:

- (a) To promote the respect of the human rights of all the people submissive a judicial procedure that derives its deprivation from freedom.
- (b) To ask for information to the prison authorities in the matter to the conditions of life of the inmates and, in particular, the adopted measures that can affect their rights.
- (c) To formulate recommendations to the prison authorities so that they modify or they lapse measured adopted or incorporate other that tend to the fulfillment of effective the constitutional and legal norms.
- (d) To receive denunciations on violations of the rights of the inmates, in agreement with the procedure that settles down. In such case, it will have to hear the authority explanation before formulating the recommendations that it considers advisable in order to correct the procedures and to restore the limited rights.
- (e) To make inspection of general character to the prison establishments, having to not less than announce its visit to the corresponding authority with twenty-four hours of anticipation. When his control into the jails are for verify a concrete denunciation can do an inspection, to that only effect, without previous warning.
- (f) To prepare and to promote the studies and information that consider advisable for the best performance of their functions.
- (g) To request information to organisms public, offices, defense counsels, organizations of attendance and other analogous ones, with aims of advising and promotion. All report regarding matter or competition of jurisdictional character is excluded from this attribution.
- (h) To annually render a report to the General assembly, in which the management fulfilled express mention of the recommendations and suggestions formulated to the administrative authorities will be analysed. The report will be able to contain, also, recommendations of general character.

When the advises were urgent he will be able to offer an extraordinary report.

The information will not include personal data that allow the identification of the interested in the investigating procedure and will be published in the Official Newspaper.

- (i) To interpose the resources of “habeas corpus” or asylum.
- (j) To do the corresponding penal denunciation when it considers that crimes exist.
- (k) To cooperate with the organisms or National and International Organizations who promote the respect of the human rights and attend and defend the rights of the indicted or condemned.

Article 3°. - The Parliamentary Commissioner will not be able to either annul the acts and resolutions of the Administration, nor to impose penalties nor to grant indemnifications.

It will be able, nevertheless, to suggest the modification of the criteria used for the production of acts and resolutions.

Article 4°. - The recommendations formulated by the Parliamentary Commissioner will not have obligatory character, but the administrative authority to which it goes will have, within the thirty days of notified of them, to give answer in writing, particularly of the reasons that attend to him not to follow them. If the Parliamentary Commissioner will not be satisfied to them or he does not receive acceptable information, he will send backgrounds to the person in top charge of the institution.

If within the next sixty days he does not have a suitable explanation, it will include the subject in his report to the General Assembly, with mention of the authorities or civil servants who have adopted such attitude, the formulated recommendations and the reasons of the Administration, there will be if them.

Article 5°. - The administrative services in charge of the imprisonment establishments are forced to help and to collaborate with the Parliamentary Commissioner in their investigations, inspection or orders of report.

Article 6°. - If in the fulfillment of his functions, the Parliamentary Commissioner reaches the conclusion that a crime has been committed, will have to let know it to the chief corresponding for the purposes of that it he adopt the pertinent measures, notwithstanding had in the literal (I) in article 2°.

Article 7°. - The activities that the Parliamentary Commissioner could make will have reserved character and confidential, as much with respect to the individuals as of the agents, involved offices and organisms.

Article 8°. - All complaint directed to the Parliamentary Commissioner will appear in writing founded, signed by interested or its defender, with indication of the name and address of the signer, within the counted term of six months as of the moment at which anyone of them had knowledge of the facts object of the denunciation. Of all complaint receipt with indication of the date of its presentation will be accused.

The proceeding will be free and it will not require learned attendance.

Article 9°. - It is prohibited the registry, examination, interception or censures of the correspondence, telegraphic or of any other species directed to the Parliamentary Commissioner, including that one sent from any center.

They could not either be object of listening or interference the personals conversation, telephone, radial or any other type, between the Parliamentary Commissioner and the people, including those prisoners, boarding schools or put under safekeeping.

Article 10°. - The Parliamentary Commissioner will have to take to a registry of all the complaints that are formulated to him; those that will be able to transact or to reject. In this last case it will have to do it in writing founded that will notify the interested one, on which will be able to indicate the normal routes or procedures that this one has to its disposition.

The anonymous complaints will be rejected, those that denote bad faith, well-known lack of foundation or trivial being this one or trivial one, having to found the rejection.

When the problem were is the same that is put under judicial decision or of the contentious office staff, it will have to interrupt his action in the tactical mission, but it will not prevent that the investigation continues with a view to solve the involved general problems in the procedure.

Article 11°. - The presentation of a complaint before the Parliamentary Commissioner is notwithstanding the rights that can have the interested to resort by the administrative or judicial route, in agreement with the regime of resources or actions anticipated by the law.

Article 12°. - Admitted the complaint it will be come to make an informal investigation, indicts and reserved, destined to clarify the facts.

THE 141ST INTERNATIONAL SENIOR SEMINAR
PARTICIPANTS' PAPERS

In all the cases they will notify to the organism or involved administrative dependency will occur, through its maximum authority, asking for a report to him in writing within fifteen days. This term can be prorogued if therefore it will be asked for in founded writing and it is considered necessary.

Article 13°. - The refusal of the civil servants or its superiors to send the information that ask for or the lack of collaboration in the attendance or aid to them asked for in form, could be considered obstruct attitudes in the normal operation of the assignments of the Parliamentary Commissioner.

In this case the Parliamentary Commissioner will notify under warning the competent maximum authority that of not acceding itself to the petition within fifteen days will be able to raise the reserve of the activities.

Article 14°. - The civil servant who will prevent the investigation by means of the refusal to answer the information or would not facilitate the access to files or necessary administrative documentation for the investigation, will incur in crime.

Article 15°. - The Parliamentary Commissioner will be designated by the General Assembly, in joint meeting of both Cameras, requiring itself in agreement vote of the three fifth of his components and before the same he will take possession from his position, having rendered oath to carry out to him properly.

Its grant will be determined by the General Assembly to the opportunity to designate to him.

Article 16°. - The duration of the mandate of the Parliamentary Commissioner will be of five years, being able to be re elected by a single time.

Article 17°. - Its position will stop in the following circumstances:

- (a) By death.
- (b) By resignation.
- (c) By destitution by well-known negligence, serious irregularity in the performance of its functions or loss of the demanded conditions of morale, being able to be stopped early in these cases by the General Assembly with the same majorities required for its designation and in public session in which the imputed will be able to exert its defense.

Article 18°. - The Parliamentary Commissioner may choose any person with the following qualities:

- (a) Uruguayan citizen, natural or legal. In this last case he must have a minimum of ten years of citizenship.
- (b) To have reached the age of thirty five years.
- (c) To be a person with recognized specialization in human rights and specifically in the tie rights the people, civil servants and places where they lodge that are private of freedom.

Article 19°. - The General Assembly within the sixty days of promulgating the present law, will integrate a Special Commission of nine members conformed by all the Political Parties to representation in that one, with the assignment to formulate the proposals of candidates, according to the following procedure:

- (a) Within the fifteen days following the constitution of the Commission, the members of the General Assembly will be able to propose in founded form, candidates who adjust to the qualities described in article 18.
- (b) Within the following thirty days, the Commission will be able to invite and to receive to particular citizens or social organizations to listen to proposals or to successfully obtain opinions on the candidates. These sessions and the received information strictly will be reserved.

- (c) In the term of the following thirty days, the Commission will come to elevate to decision of the General Assembly the proposal of the candidate, resolution that in the Commission will have to be adopted by 3/5 (three fifths) of its members.

Article 20°. - The Parliamentary Commissioner will not be subject to imperative mandate, nor will receive instructions of any authority having had to perform his functions with total autonomy, according to his criterion and under its responsibility.

Article 21°. - The activity of the Parliamentary Commissioner will not be interrupted by the inactivity of the Cameras, nor by its dissolution according to the mechanism anticipated in Section VIII of the Constitution of the Republic. In such cases, the relation of the Parliamentary Commissioner with the Legislative Power will be done through the Permanent Commission.

It will not either interrupt his activity in the cases of suspension of the individual security (article 31 of the Constitution of the Republic) or of adoption of quick measures of security (number 17 of article 168 of the same).

Article 22°. - The position of Parliamentary Commissioner is incompatible with another remunerated, public or deprived activity, except for the exercise of teaching.

Article 23°. - The Senate of the Republic, to request of the Parliamentary Commissioner, and in consultation with the House of Representatives will designate, among the civil servants of the organisms of Legislative, advisory and personal the Power necessary for the exercise of the functions that is entrusted to him to the mentioned one.

In no case this personnel could be of more than ten civil servants.

Article 24°. - The advisers will stop automatically at the moment at which he assumes the new Parliamentary Commissioner designated by the General Assembly.”

VIII. NATIONAL PATRONAGE OF JAILED AND RELEASED

The National Patronage of Jailed and Released and the Departmental Patronages are in the fortification process. The government impels a policy of reintegration for people who recover their freedom, and in such sense the Patronage plays a fundamental role in the objective to reduce recidivism.

Created by decree in 1934, their attributions were set down thirty years later in Article 94 of Law 13,318 of 1964. Decree 417/985 regulates each article and establishes the integration of the Patronage, its administrative organization and operation.

In 2005, the new government favoured the institutional fortification of the Patronage with defined measures. The objective was to reinforce its budget, ensure the incorporation of more suitable professionals, and to celebrate new agreements with public institutions like the University of the Republic and City Hall of Montevideo. In addition, Law 17,897, Humanization and Modernization of the Prison System, was approved by the Parliament and allows commissions of government officials with suitable profiles to execute the task.

At present, they are orchestrating details with the Ministry of Social Development and with the Municipality for the entrance of 75 inmates released to the group of “Work by Uruguay”, to fulfill tasks of cutting tree roots and preparing sidewalks in the capital city.

The attention of the Patronage to the released, deprived of freedom and their relationships with their families is fundamental for the rehabilitation and inclusion of those who at some time committed a crime. The mechanisms of social reintegration are for the present administration the key to reducing the rates of violence and criminality.

The Patronage mainly offers social, legal and psychological attention to the people released or soon-to-be released inmates or their families, who so request it.

THE 141ST INTERNATIONAL SENIOR SEMINAR
PARTICIPANTS' PAPERS

Released by the Law of Humanization and the Modernization of the Prison System, they are required to go to the Patronage, and to fulfill an individualized plan of reintegration established in agreement with its referring technicians, according to the capacities or limitations of each released inmate.

In its different areas, the Patronage offers the following attention to attendees.

A. Health

- Free management of the identity card;
- Free management of the membership card of attendance for the services of health publications;
- Co-ordination with centres specialized in cases of drug addiction, alcoholism, AIDS, the handicapped, birth control, etc;
- Free medicine delivery when these are not available in the pharmacies of the different State health centres;
- Psychological attendance and derivation to specialized centers;
- Feeding;
- Delivery of membership cards for the National Institute for Feeding the Population and in special cases, supplies of emergency aid.

B. Houses

- Loans on extremely advantageous grounds for improvement and/or construction of houses (in the cases involving minors and the attendee is a proprietor of land or is properly authorized by the municipality to build a property in a municipal estate or that of a relative).
- Co-ordination with the Ministry of Homes and the Bank of Materials of the Municipality.

C. Education

- Co-ordination with the different educative centres, schools, grammar schools, day-care centres, etc;
- Support for the schooling of minors by means of the subsidized sale of uniforms, sports footwear, equipment, and the donation of scholastic equipment against the presentation of a certainty of inscription at the beginning of the scholastic year;
- Support and stimulus for reintegration in centres of formal education of the young deserters of the same, and support with equipment, footwear, tickets, etc.

D. Work

The labour market takes a registry of attendees that ask for work, and receives requests for personnel on the part of companies.

Weekly, personnel evaluate the candidates and offer help through media ads:

- Loans for the acquisition of tools of work and/or articles for the sale;
- Presentation before companies that ask for personnel through the press;
- Agreements with public organizations for those who lack work sources and psychological support for these people.

E. Training

To increase the possibilities of its use, the Patronage has signed agreements with the Ministry of Education and Culture (CECAP) and the Ministry of Work for the labour training qualification of attendees.

It also has a factory of educative-labour leading to qualifications for the search and obtaining of work.

For the ladies shelter and the sewing factory, informative factories on themes of interest to the attendees are organized (domestic violence, health, HIV/AIDS, etc.).

F. Alternative Punishment

Persons indicted or condemned by the Penal Magistrates with a Personal recognizance are often given an alternative punishment with a measure of communitarian tasks. In order to make possible its fulfillment, the National Patronage of Jailed and Released has signed agreements with the Ministry of Public Health and diverse schools that offer work places. The subject persons receive psycho-social support throughout the

process, support that can extended if they so request, after the fulfillments of the court-mandated treatment.

The statistical results of recidivism in the cases of people indicted without prison and with alternative punishment are noticeably lower than that of persons released from imprisonment centres.

G. Shelters

Board and lodging is provided for released or secluded women with small children who may be vulnerable to homelessness. Psycho-social support is also available, as is multidisciplinary equipment for the sport and recreation of the children of inmates of women's jails who request it.

H. Place for the Expression of Children

Smaller children of the female inmates of women's prisons and shelters, who are experiencing difficulties of a psychological nature, are taken care of by two psychologists.

I. Sewing Factory

Qualifications for women of more than 14 years, with the possibility of obtaining at the end of the course a corresponding diploma.

Production of sheets, uniforms, sets and work clothes.

J. Economic Sale

Sale of beds, mattresses, sheets, blankets, clothes, footwear and clothes for babies; all subsidized elements for which the attended pay a third of the cost.

IX. FUTURE MEASURES TO DIMINISH THE NUMBER OF PEOPLE IN PRISON

As we said at the outset we have seen meticulous laws, regulations, measures, institutions, etc., that during last the decade have been designed to improve the situation of jailed citizens, to facilitate their social reintegration or to diminish their permanence in the jails, but even so the reality and the statistics show that an exponential increase in the amount of incarcerated citizens is continuing. The government, along with the involved organizations, including the National Bureau of Jails, is in the process of measuring efforts to achieve the above-mentioned. It is for that reason that at this moment, besides the importance that it has acquired, the Redemption of Punishment explained above and the other enunciated measures including the following procedures are being implemented.

A. Official of Probation

1. Background

In March 2006, an international nongovernmental organization, Companions of the Americas Uruguay Minnesota, began a project named "Fortification of the System of Justice and Penitentiary System of Uruguay", that was declared of interest by the Supreme Court of Justice and Ministry of Interior.

2. First Stage of the Project

This included a visit of a group of experts of the State of Minnesota, USA for ten days. They met with legislators, members of the Supreme Court of Law, the Association of Magistrates, the Parliamentary Commissioner, the Minister of the Interior, and developed activities of qualification and gave advice regarding the penitentiary system and the justice system.

3. The Second Phase

This allowed the visit of four officials of the penitentiary system of Uruguay to the State of Minnesota, with aims of information interchange and qualification in the general operation of the justice system and the penitentiary system, with special emphasis in the Institute of Probation.

4. The Third Phase

One US expert in the systems of probation and the judiciary visited, concentrating on activities in the diffusion, information and qualification of the systems of probation at all levels. An event of national reach was developed which was attended by more than 120 people involved in the subject.

5. The Fourth Phase

It determined a new visit to the State of Minnesota for a Judge Penal and an official of the penitentiary system, with the purpose of acquiring a deep knowledge in the system of probation, "a pilot experience in probation in Uruguay", since we already counted on the offer of three Penal Courts for its development in the city of Montevideo and the modification of the present legal system not being necessary for its implementation.

6. The Fifth Phase

The fifth stage will:

- Define the institutional insertion of the Office of Probation;
- Define the profile, to select and to enable personnel for the Supervision of Probation;
- Choose the courts that will develop the pilot experience.

Because of this and with the intention to continue searching for solutions that allow us to diminish the number of persons incarcerated, the alternative of supervision in freedom sets out that it controls, it orients, and it guards by the fulfillment of parallel alternative punishment, at the same time as it promotes the communitarian participation of social reintegration.

It is of order to emphasize the importance of advancing in the instrumentation of projects which are generated at present and that try alternative measures to imprisonment which offer a solution for the overcrowding situation in our penitentiary system and we know that this institution is good penitentiary practice in other countries.

B. Electronic Bracelets

1. "System of Electronic Monitoring" Institutional Advantages

The incorporation of technology is a clear advantage of the proposed system:

- It is an innovating product for the prison regime;
- It would contribute reducing overcrowding of our jails;
- It would allow us to try other modalities at different stages of penitentiary treatment, for example, extra-mural work.

2. Advantages for the Inmate

It is another motivating alternative with short term rehabilitation goals, which help to avoid the decline in motivation which occurs over longer periods.

3. Advantages for the Penitentiary Security

It harmonizes with the principle of progressiveness, so that security in this case is a dynamic and flexible concept.

It allows the authorities to rationalize human resources.

It is a fast control response, before the possible transgression of the offender.

It is easy to use, and operators of the equipment have prior qualifications.

In the case of transitory exits, domiciliary and/or labour, it would be easy to control, which at present it is not, because of personnel and logistical deficiencies.

4. Disadvantages

- The operational range is not clear;
- There are no legal norms that rule their use;
- It would be necessary to clearly determine the cost of the equipment;
- Detailed technical information on the operation of the equipment is lacking;
- Further information on the system is required;
- It would be useful to know data on his application and results in compared systems;
- Lack information with respect to service or maintenance of the equipment.

5. Conclusions

- It is necessary to establish the relative cost-benefit, integrating the cost that an inmate generates in detention;
- It would enhance the development of the rehabilitation policy;
- Its implementation harmonizes with the principle of progressiveness;
- It is considered highly beneficial to fulfill labour and educative application programmes;
- It contributes to diminish the tensions of prison life;
- Within the framework of the Progressive Regime of Imprisonment, it would be useful to co-ordinate an offender's application for another alternative, to shorten terms of the granting of the anticipated freedom;
- It could be useful in the application of the Parole and anticipated freedom.

(i) Recommendation

To orchestrate a Pilot Plan, which allows additions to the innovations in execution, a new alternative, which contributes to reinforce the principle of self responsibility, contemplated in Article 60 of Penitentiary Law N° 14,470/75; the Book of Good Penitentiary Practice, published by Penitentiary Reform International (Section K, Literal 3, Page 101); the Minimum Rules for the Treatment of the Inmates (Rule 61, and that is complemented by the Minimum Rules of the United Nations on non-incarceration measures (Tokyo Rules. No. 2).

(ii) Other Advantages

- It is an innovating product for the Prison Regime;
- It would contribute to reducing overcrowding of jails;
- It would allow other modalities at different stages of penitentiary treatment, like for example extra-mural labour;
- It would allow better rationalization of the human and material resources;
- It allows fast responses, before the possible transgression of the covered area, mainly for those released on Transitory Exits, since today it is not counted on any type of control or affected by serious deficiency of resources;
- It is of easy handling, and the operators have previous qualifications;
- It contributes to diminishing the tensions of prison life;
- It allows to the offender the possibility of maintaining relationships and to possibly work, influencing directly his or her recovery and the indices of recidivism of the crime;
- It avoids the contagion produced when jailing minor violators of the Penal Law in the same institution as dangerous delinquents or those jailed for serious crimes;
- It could be integrated into the punitive system as an alternative to prison;
- In similar experiences in other countries (the United States, New Zealand, Australia, Spain, Italy, and Argentina - this one last one in the test stage), the rate of recidivism of offenders subject to electronic monitoring or house arrest as a percentage has been lower than those released under the traditional system.

(iii) Recommendations

Uruguay should increase the use of the measure, especially since the legal framework for its implementation is already in place. We understand that would be a great advance from the penological view to include this type of substitute measure as one more form of social control and not to continue relying on incarceration. The alternatives can be used to fight the complex and many-sided problem of crime, especially when our penitentiary system is facing a humanitarian emergency.

X. HISTORY OF THE NATIONAL BUREAU OF JAILS, PENITENTIARIES AND REHABILITATION CENTERS

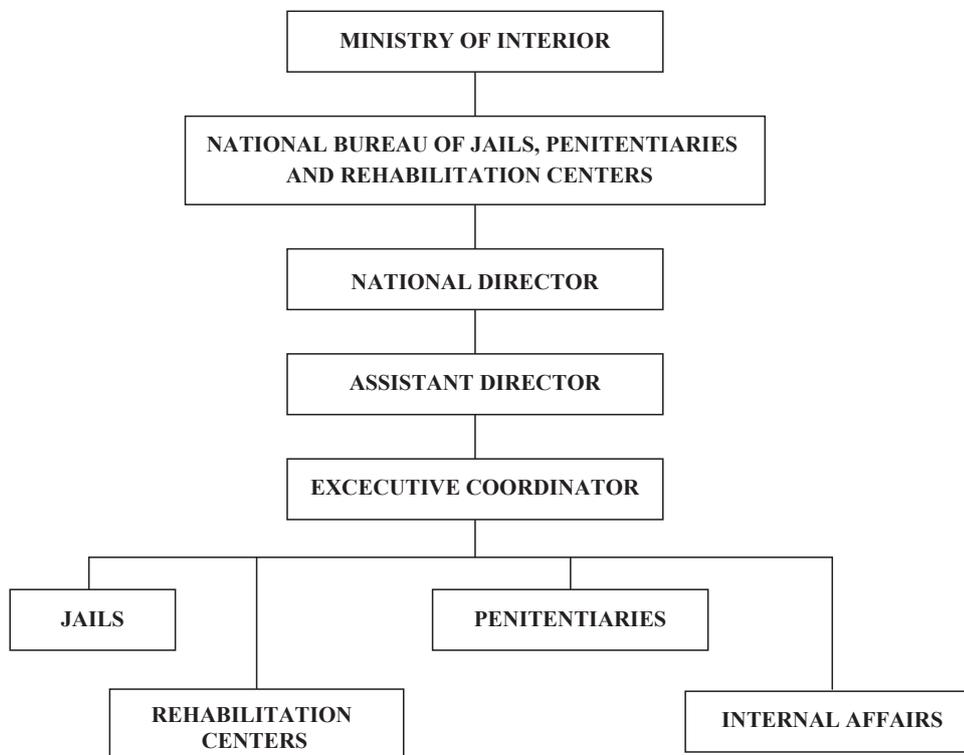
The Council of Patronage of Delinquents and Minors was created by laws of 4 April 1891 and 8 April 1915.

The Main Directorate of Penal Institutes was created on 19 October 1933, and was sanctioned in the statutory law of 16 November 1933, the Ministry of Instruction (today Education and Culture), having jurisdiction.

Through the Decree of the Executive Authority N° 27/971 of 20 January 1971, the Ministry of the

Interior took jurisdiction and the name of the council became the National Bureau of Penal Institutes, acquiring its present denomination in the mid 1980s.

FLOWCHART



XI. PENITENTIARY LAW N° 14,470

The Penitentiary Law N° 14,470/70 consecrates a progressive regime. The progressive system has the main idea of a dynamic interaction between the treatment and the answer, which allows that the inmate is not an object submissive to invariable rules, but a human being who with his or her conduct is conquering new forms of life within the prison.

The start point of the system begins with the criminological opinion (diagnosis and prognosis) of an interdisciplinary team of technicians who consider the personality, age, crime committed, work situation, etc., and consequently pronounce on the danger of the inmate and his or her presumed degree of adaptability, classifying it and assigning him or her to a penitentiary for treatment and a location within the components of the prison complex.

A. Classification

1. Penological Criteria

- 1) Adults of 18 to 25 years;
- 2) Adults of more than 25 years;
- 3) Special, that is, defined as non-adapted to any type of collective programme.

2. Legal Criteria

1. Primary Penological and
2. Relapsing.

We consider a “primary legal” a person who has had contact with justice and minors with file in this category are considered “relapsed”. They are subdivided into

- (i) Indicted; and
- (ii) Condemned.

3. Criterion Type of Offence

- 1. Property;
- 2. People;
- 3. Economic;
- 4. Others, etc.

4. Special Criteria

- 1. Homosexuals;
- 2. Diverse professionals;
- 3. Members of the Army and Police;
- 4. Others.

Penitentiary treatment can begin in a unit of medium security, or of minimum security if criminological opinion so advises. The Pavilion of Admission is important in this regard.

The technicians who conduct the biosocial study will continue supervising the execution of the treatment, including the personnel of the Complex in charge of the work, education and security of the inmate.

The information will allow the evaluation of the treatment and the change of the same in a positive or negative sense. To such aims, a meeting of treatment in each Unit would work.

APPENDIX A

STATISTICS

PRISON POPULATION PER 100000 INHABITANTS			
Inmates and Population of the Country divided for States in Uruguay.			
Date: 31 July 2008			
STATES	INHABITANTS	INMATES	RATE x 100000 INH.
ARTIGAS	79297	119	150,07
CANELONES	514616	956	185,77
CERRO LARGO	89871	108	120,17
COLONIA	120842	102	84,41
DURAZNO	61321	92	150,03
FLORES	25648	37	144,26
FLORIDA	70235	87	123,87
LAVALLEJA	61910	123	198,68
MALDONADO	149071	409	274,37
MONTEVIDEO	1340273	4593	342,69
PAYSANDÚ	115854	149	128,61
RIO NEGRO	55934	91	162,69
RIVERA	110180	249	225,99
ROCHA	70515	92	130,47
SALTO	127345	165	129,57
SAN JOSÉ	108649	99	91,12
SORIANO	87508	128	146,27
TACUAREMBÓ	95313	120	125,90
TREINTA Y TRES	49670	61	122,81
TOTAL	3334052	7780	233,35

The jails in Uruguay, like those of almost all the Latin American countries, are over-crowded. In Uruguay the incarcerated population (about 7,780 prisoners approximately) represents 0.2% of the total population of the country. This implies a rate of 233 imprisoned people per 100,000 inhabitants, similar to Chile.

REPORTS OF THE SEMINAR

GROUP 1

THE USE OF COMMUNITY-BASED ALTERNATIVES AT THE PRE-TRIAL AND TRIAL STAGES TO REDUCE OVERCROWDING IN PRISONS

Chairperson	Mr. Jagath Abeysirigunawardana	(Sri Lanka)
Co-Chairperson	Ms. Fay Ingrid Clarke	(Guyana)
Rapporteur	Mr. Asghar Ali	(Pakistan)
Co-Rapporteur	Mr. Viet Quoc Nguyen	(Vietnam)
Members	Mr. Joydeb Kumar Bhadra	(Bangladesh)
	Ms. Renny Ariyanny	(Indonesia)
	Ms. Sylvia Reu	(Papua New Guinea)
	Mr. Futoshi Ichikawa	(Japan)
	Mr. Katsuo Higuchi	(Japan)
	Mr. Hiroshi Nakashima	(Japan)
	Mr. Atsushi Ogata	(Japan)
	Mr. Toru Suzuki	(Japan)
	Advisers	Deputy Director Takeshi Seto
Prof. Junichiro Otani		(UNAFEI)
Prof. Tae Sugiyama		(UNAFEI)
Prof. Ryuji Tatsuya		(UNAFEI)

I. INTRODUCTION

On 26 January, Group One held a meeting in the Conference Hall. Ms. Clarke nominated Mr. Jagath for the post of Chairperson and as the participants expressed consensus, he was so elected. Similarly, Ms. Clarke was elected Co-chairperson. Next, Messers. Ali and Nguyen were elected Rapporteur and Co-rapporteur, respectively.

Group One was tasked to discuss and recommend effective measures to improve the treatment of offenders and reduce overcrowding in prisons, through the enhancement of community-based alternatives to imprisonment at the pre-trial and trial stages.

On the first day, the main discussion of the group centered on the subject of bail. The participants who acknowledged that the granting of bail is present in the criminal justice systems of their respective countries, also opined that the number of beneficiaries of the bail system is not very high. It was revealed that in some countries, the conditions for bail are stringent and in other countries the procedure is lengthy. Moreover, in their cases, judges hold very conservative mindsets and are generally reluctant to grant bail to offenders/defendants. Almost all the participants agreed that the granting of bail on a larger scale can avoid over-crowding in prisons.

Following an animated discussion, different types of bail were then discussed. To begin with, the granting of pre-arrest or anticipatory bail was hotly debated. It was argued that pre-arrest bail is of great value to a defendant who may need time to establish his or her innocence. It was expressed that in many developing countries, innocent persons are sometimes falsely implicated in criminal cases. In such cases, being granted pre-arrest bail is welcomed.

Later the discussion was focussed mainly on the power of the police to grant bail. Participants from Bangladesh, Pakistan, Sri Lanka, Guyana and Papua New Guinea said that the police in their countries play an extremely important role in the criminal justice system and they also have the authority to grant bail in cases of minor gravity. However, another participant stated that in Indonesia, the police have the power to release some suspects on the basis of a personal guarantee. In the case of Guyana, this is referred to as being placed on 'Self Bail'. Moreover, the participant from Indonesia further stated that although the Police in that country have the power to grant bail to suspects, they rarely exercise this discretion. Participants from Japan stated that while their police have no power to grant bail, they do have power to release a suspect within 48 hours, and that they frequently exercise that power. Meanwhile, the participant from Vietnam held the firm view that only the Prosecution Office should have the final role in granting bail.

II. POLICE DISCRETION

Discretionary powers and practices of the police were discussed to examine the present status in terms of alternatives to incarceration at the pre-trial stage. Discussions focused on the power of the police to make an arrest, release/bail, close the case and also their role in restorative justice measures, mediation, settlement or alternate dispute resolution.

It was learned that in all the countries representing Group I, excluding Japan, the police can make an arrest in a significant number of cases without a warrant. Usually the police can arrest a person on the grounds of prevention and suspicion, for detention within a stipulated timeframe (which varies from 24-48 hours in most jurisdictions). However in Indonesia after an initial detention period of 20 days, a request must be sent to the prosecutor's office for an extension of further detention. If such extension is granted, the suspect's cumulative detention period cannot exceed 50 days. After an arrest, the police are required to produce the arrestee before either the court or the prosecutor. In Vietnam, it is mandatory that all cases be referred to the prosecutor's office for approval.

In terms of the power of the police to release or bail a person arrested, the police have this authority in all participating countries with the exception of Japan and Vietnam. This means if it is revealed that there is insufficient evidence to detain an arrested person the police can release the person without obtaining permission from the court or prosecutor's office. Furthermore, in Bangladesh, Guyana, Pakistan, Sri Lanka, Indonesia and PNG, the police can release the arrestee on bail with some conditions (such as reporting daily to the police), if the offence committed is minor in nature and there is no substantial evidence against the accused.

During the discussions, it became clear that the police played roles at the pre-trial stage in areas which could be considered facets of restorative justice, mediation, settlement and alternative dispute resolution. This was specifically so in Guyana, Sri Lanka and Papua New Guinea. In some countries, the use of these measures are not in the legal framework but is done unofficially, as in the case of Bangladesh. In Japan where it is also done occasionally by Koban or Community Policing officers, the use of restorative justice, mediation and settlement (among others), will be formalized with the implementation of the *Saiban-in* court system. However, in some countries, there still remains the need for legislative approval for police involvement in such initiatives.

A. Recommendations

- That the police should exercise their powers of arrest with due care and any discretion used should be within clear, legal guidelines;
- That the police should play a facilitating role in mediating settlements and or dispute resolutions, for minor offences, as they are the first point of contact for both parties involved after a crime is committed. Settlements should however be subjected to proper legal supervision;
- That the police should complete investigations without delay, to minimize the detention period at the pre-trial stage.

B. Note

With regard to the use of police discretion at pre-trial stages, the details of the content and procedure of any agreement between two or more disputing parties should be clearly enunciated, and the community and oversight body must be informed accordingly. This measure is to provide a basis for further redress in the event that one or more parties break the agreement.

III. SUMMARY OF DISCUSSION OF PROSECUTORIAL DISCRETION

In Bangladesh, Pakistan, Guyana and Papua New Guinea the prosecution office prosecutes cases in the Judge, High and Supreme Courts. At the Magistrate's Court, the police perform the function of the prosecutor. In the nations of Bangladesh, Guyana and Pakistan, the prosecutor's office starts functioning after receiving a complete investigative report from the police, but they can request the Police to collect more evidence if they still feel there is scope to acquire more evidence. The prosecutor can not close any case nor release any person on bail or guarantee.

The participant from Papua New Guinea stated that the Police Prosecutor prosecutes all Summary cases at the Magistrate's Court. The public prosecutor assists the police during the prosecution of serious crimes at the national court and with cases concerning constitutional office holders who are cited for breaches, either by the Ombudsman's Commission or other relevant authorities. The police, before making an arrest, or the prosecutor, during the trial process, may make a discretionary disposition because of lack of evidence. Serious cases of corruption and fraud are also referred directly to the prosecutors by relevant authorities such as the Fraud and Anti-Corruption Unit. There is a close relationship between the police prosecutor, investigator and public prosecutor.

Participants from Sri Lanka, Vietnam and Indonesia stated that public prosecutors in their countries have discretionary powers to prosecute cases and to supervise the police in the investigative process. Public prosecutors in some countries have power to suspend prosecution because of lack of evidence and can instruct the police to arrest or release people if they feel that the police did not complete a thorough investigation. The participant from Indonesia claimed that formerly in her country, only the public prosecutor could prosecute all cases at all court levels, but since the activation of the Anti Corruption Commission in 2000, prosecutors can also prosecute corruption cases in their own court. Some government departments also have legal authority to investigate cases related to their functions. For example, tax crimes by the Tax Directorate General, illegal fishing by the Department of Fisheries and Seas, Customs, etc. However, after completing their initial investigations, the files must go to the public prosecutor who can conduct any investigation of corruption and human rights violations. They can seize or confiscate assets or bank accounts of a suspect and have discretionary power to prosecute or to withdraw a case and to execute the judges' decisions. There is a close relationship between the police, prosecutor, judge, and other related agencies.

Some participants from Japan stated that the police can arrest and detain a suspect for up to 48 hours, following which the prosecutor will decide whether he or she will apply for a Detention Order from a judge. If there is a reasonable ground to believe that the suspect will leave the jurisdiction or destroy evidence, the judge would issue a detention order. In Japan, after ten days the prosecutor may apply for an extension of the detention order. The prosecutor analyses the case and makes the decision whether or not to prosecute the suspect; even if he or she finds that the suspect is likely guilty, he or she can suspend the prosecution, considering the character, age, environment of the suspect, and gravity, circumstances or situation of the offence. In Japan, there is no mediation or settlement system at the pre-trial stage but if the prosecutor thinks that the case could be dropped on condition that an agreement between the suspect and the victim is reached, he or she suggests to the civil attorney at law, that efforts should be made to reach such an agreement. If an agreement is reached, the prosecutor suspends the prosecution. It was also stated that in several countries, the police and prosecutor have regular meetings.

IV. SUMMARY OF INTERVENTIONS AT THE ADJUDICATION STAGE

Community-based alternatives to incarcerations which some countries apply at the adjudication stage include verbal sanctions, suspension of sentences (suspended sentence), suspension of execution of sentences (conditionally suspended sentences), fines, probation, and community service orders. Appendix One illustrates the results of a "Survey of Participating Countries" and their use of various strategies which contribute to reduced levels of custodial sentencing. Appendix Two describes the various means by which the police may exercise discretionary power at the pre-trial stage. The table in Appendix One shows that fines are used in all the participating countries, while many countries apply the method of suspended sentences. Meanwhile, there are some countries which apply both suspended sentence and suspension of the execution of sentence (conditional sentence). Probation is used in several countries but community service orders are not used frequently, mainly because the society rejects such decisions and their judges therefore rarely use this intervention.

Each country should promote community-based alternatives to incarceration as much as possible under its own legal system, so as to decrease overcrowding in prisons. In addition, we considered that since the pre-trial stage offers the best opportunity to provide a greater impact on possible interventions to reduce overcrowding, increased focus should be directed to that area. One suggestion was that mediation be more extensively considered at the police and community policing levels. While this generated some animated and slightly heated discourse, the consensus was that the guidelines for such use must be clearly outlined in law.

V. RECOMMENDATIONS

1. That stringent efforts be made to use alternative dispute resolution, diversion, settlement and restorative justice practices at pre, mid and adjudication stages;
2. That alternative 'court systems' such as Traffic Courts, Family Courts, Minor Damage Courts, etc. be implemented where applicable, which could free the judiciary to address indictable matters in a speedy manner;
3. That all phases of the process in respect of the investigation, prosecution and trial be executed more efficiently;
4. That the discretionary power for the closing and/or suspension of criminal cases exercised by the police and prosecution should be clearly given oversight by appropriate bodies to ensure accountability and transparency to prevent corruption;
5. That creative public awareness campaigns be undertaken to sensitize the public about the benefits of community-based alternatives to custodial sentencing;
6. That strategies (training, increased sensitization, societal awareness, etc.) be developed to encourage every sphere of the judiciary to make greater use of the legally provided mechanisms permitting the use of community-based alternatives to custodial sentencing in their sentencing practices;
7. That international co-operation for the provision of technical assistance and capacity building to be pursued.

ANNEX I

Survey of Countries' use of Various Strategies to reduce Custodial Sentencing

	SUSPENSION OF SENTENCE (SUSPENDED SENTENCE)	SUSPENSION OF EXECUTION OF SENTENCE (CONDITIONAL SENTENCE)	FINE	PROBATION	COMMUNITY SERVICE ORDER	JURY SYSTEM
Bangladesh	×	○	○	Only for Juveniles	×	×
Guyana	○	○	○	After 1/3 sentence served	×	○
Indonesia	○	○	○	Before and after trial Police and Prosecutor discretion	Community service provided only for juveniles and women	×
Pakistan	○	×	Fine and sentence	○	×	×
P.N.G	○	After sometime spent in jail	○	○	In effect and supervised by Elders of villages and issued by village courts	×
Sri Lanka	○	President can suspend a death sentence but death sentence is rarely used!	Minor offences	○	Although in law, not preferable choice of judges	○
Vietnam	○	In effect, but minimal usage	○	×	×	×
Japan	×	○	○	○	×	×

The meaning of the symbols used in the Table are as follows:

- × Not applicable to that country
- Applicable to that country

ANNEX II

STATUS OF POLICE DISCRETION

COUNTRY	ARREST	RELEASE/BAIL	INITIATE INVESTIGATION	CLOSE A CASE	CHECK & BALANCE	COMMENT
BANGLADESH	√	√	√	√	√	In some cases, the police can arrest, conduct a search without a warrant and initiate investigations. To close cases, they send all documents to the Magistrate to take the final decision.
GUYANA	√	√	√	√	√	In some cases, the police can arrest and conduct searches without warrants. To close some cases, they send all documents to the public prosecutor for advice before making a final decision.
INDONESIA	√	√	√	√	√	For some cases, the police can arrest, conduct searches without warrants and also close cases of less gravity. For cases of higher gravity, the public prosecutor has authority.
JAPAN	×	√	√	×	√	The police need a warrant to arrest a person or to conduct search; they can initiate investigations and release a suspect, but decisions for detention and closing a case are taken by the prosecutor.
PAKISTAN	√	√	√	√	√	For some cases the police can arrest and conduct searches without warrants. To close a case, they send all documents to the magistrate and prosecutor for a final decision. If any arrest is made in connection with a specific case, only the prosecutor can close the case.
PAPUA NEW GUIENA	√	√	√	√	√	For most of cases, the police can arrest but cannot conduct a search without a warrant. To close a case, the police must send all documents to the magistrate for a final decision.
SRI LANKA	√	√	√	√	√	For some cases police can arrest or conduct searches without a warrant; they can initiate investigations and close some cases as mentioned in law and for other cases, the police send all documents to the magistrate for a final decision.
VIETNAM	√	√	√	×	√	For some cases the police can arrest, conduct searches without warrants but the prosecutor's office can ratify such decisions later on. The public prosecutor takes the decision to close a case.

The meaning of the symbols used in the table above are as follows:

- × Not applicable in that country
- √ Applicable in that country

GROUP 2

EFFECTIVE MEASURES TO IMPROVE THE TREATMENT OF OFFENDERS THROUGH THE ENHANCEMENT OF COMMUNITY-BASED ALTERNATIVES TO INCARCERATION AT THE POST SENTENCING STAGE

Chairperson	Ms. Boitumelo Makunga	(Botswana)	
Co-Chairperson	Mr. Akihiro Nosaka	(Japan)	
Rapporteur	Ms. Janet Davey	(Jamaica)	
Co-Rapporteur	Mr. Yasuhiro Date	(Japan)	
Members	Mr. Antonio Carlos Welter	(Brazil)	
	Mr. Sutrisno	(Indonesia)	
	Mr. Jihad H. Majali	(Jordan)	
	Mr. Victor Manuel Esteche Mendez	(Paraguay)	
	Mr. Carlos Vargas Merida	(Peru)	
	Mr. Leo Sarte Carrillo	(Philippines)	
	Mr. Jose Enrique Colman	(Uruguay)	
	Mr. Manabu Nakajima	(Japan)	
	Mr. Shigeru Takenaka	(Japan)	
	Advisers	Prof. Naoyuki Harada	(UNAFEI)
		Prof. Jun Oshino	(UNAFEI)
		Prof. Tetsuya Sugano	(UNAFEI)
		Prof. Koji Yamada	(UNAFEI)

I. INTRODUCTION

The group convened on 26 January 2009 and concluded discussions on 3 February 2009. The group was chaired by Ms. Makunga, with Mr. Nosaka as the co-chairperson, Ms. Davey as the rapporteur and Mr. Date as the co-rapporteur. The group consisted of 13 participants from ten countries; who had diverse professional experience ranging from legal expertise to policing as well as probation work to working with convicted inmates. The group was assisted by four UNAFEI professors.

The members of Group 2 were required to examine: “Effective measures to improve the treatment of offenders through the enhancement of community-based alternatives to incarceration at the post sentence stage.”

Sub- topics included:

- a) The mechanism of community-based alternative measures to incarceration undertaken by each country;
- b) Current situations and problems facing existing legal systems and/or practice of the above mentioned mechanisms;
- c) Countermeasures under current legal systems and/or practice of the above mentioned mechanisms;
- d) Identification of other effective intervention models;
- e) Measures to monitor and evaluate all mechanisms discussed.

II. SUMMARY OF THE DISCUSSIONS

A. Mechanism of Community-Based Alternatives to Incarceration in Each Country

The group first reviewed the current systems of community-based alternatives to incarceration employed in each participant’s country. These are listed in Table 1 below. There were slight variations in the administration of some of the alternatives, the general agreement was: even if the term is the same; there is a difference in the use for each country. With this in mind there were differences in some of the non-custodial options - included in the differences were: parole, probation and suspension of execution.

THE 141ST INTERNATIONAL SENIOR SEMINAR
REPORTS OF THE SEMINAR

These variations are outlined below.

TABLE 1: A SUMMARY OF NON-CUSTODIAL ALTERNATIVE MEASURES TO INCARCERATION UNDERTAKEN BY EACH COUNTRY

	Brazil	Indonesia	Jamaica	Japan	Jordan	Paraguay	Peru	Philippines	Uruguay
	Parole	Parole	Parole	Parole		Parole	Parole	Parole	Parole
Probation	Probation	Probation	Probation	Probation			Probation	Probation	
		Suspended Sentence Supervision Order							
Fines	Fines	Fines	Fines	Fines	Fines	Charity Help		Fines	Fines
Extramural labour		Community Services Order				Community work	Community Labour	Community Service	Community Labour
Suspended Sentence		Suspended Sentences		Suspension of Execution	Suspended Sentences				
Dismissal with warning		Conditional release					Remission	Commutation of Sentence	Reduced Sentences
	Domiciliary Arrest	Remission				House Sentences - for people over seventy and pregnant women	Domiciliary Arrest		Domiciliary Arrest
	Halfway house			Halfway house				Halfway house	Halfway house
Presidential Pardon		Amnesty Pardon		Amnesty Pardon	Amnesty Pardon	Pardon	Amnesty Pardon	Amnesty Pardon	Amnesty
Corporal Punishment	Rights Restricted	Bound over to keep the peace						Good conduct time allowance	Indictment without prison
	Redemption/- (for person who study or work in prison)	Electronic monitoring (currently piloting)							Patronage
	Reprieve	Admonished and Discharged							Extra wall leave
		Combination Orders							Family leave
									Redemption for prisoners who work or study in or out of prison.

B. Current Situations and Problems

Participants deliberated on the major problems impacting on the administration of the various alternatives to incarceration processes. The main problems were lack of financial resources to maintain community-based programmes as well as lack of adequate human resources to monitor and guide offenders. Also stated were numerous problems which were unique to each system in each country. These were itemized as follows:

1. Lack of community understanding and societal support: communities deem offenders to be dangerous and do not appreciate them being released into their environment; believing that this type of practice can endanger the populace as a whole;
2. Lack of collaboration between agencies: results in the fragmentation or duplication of services by agencies that work with offenders in the community; causing the agencies services to be overstretched. Furthermore, this in turn could result in lack of support systems for some candidates;
3. Slow legal procedures: this was believed to be related to the lack of adequate risk assessment procedures. For example, what criterion was to be used to select offenders suitable for parole?
4. A highly centralized processing system: the end result of a centralized system is a backlog of cases resulting in the impediment of carrying out the prescribed sentence;
5. Too many high-risk offenders: making the option of community-based alternatives to incarceration risky for the community;
6. Inadequate monitoring due to lack of human resources.

The problems outlined by participants from countries using parole as an alternative to incarceration are as stated above. However, some of the participants listed a short parole period (resulting in a high recidivism rates) and a highly centralized processing system (resulting in a backlog of cases and the ensuing impediment of carrying out the prescribed sentence) as major problems.

Of the ten legal systems, six had probation as an alternative to incarceration. In the case of Jamaica this is a separate order and not pinned to any other order as is evident in the systems that have it pinned to parole or suspension of execution. The major problems affecting probation are similar to the ones stated above.

Regarding the alternative of monetary penalties/economic sanctions, most of the participants stated that there are no major problems with this option; however, the participant from Botswana stated that offenders may have a tendency to believe they can buy the criminal justice system because they have the means to do so. Another participant indicated by that the major problem with the administration of this option was the non-payment of fines. The participant from Indonesia pointed out that fines are only granted for special cases i.e. traffic accident offences and limited corruption cases.

Most of the participating countries utilized some form of suspended sentence. Concerning the option of suspended sentence without supervision, participants indicated that the major problems encountered with the administration of this alternative are a high recidivism rate and lack of recognizance on the part of the offender.

On the subject of a suspended sentence with supervision order, most participants indicated that the major problems encountered in the administration of this alternative are similar to the former. In addition, the participant from Jamaica pointed out that lack of human and financial resources hampered the implementation of programmes and projects for offenders who are subjects of this option.

Participants from Indonesia, Japan, Jordan, Uruguay, Peru, and the Philippines stated that amnesty was used in their countries as an alternative to incarceration. However, they pointed out that the problems with this option include increased recidivism rates due to poor evaluation of recipients, limited use of the option by the judiciary and the lack of clear procedures in some jurisdictions.

One legal system is piloting electronic monitoring and this will be used as a measure to enhance other options. Problems include a high cost, a lack of clear legislation and lack public sensitization.

THE 141ST INTERNATIONAL SENIOR SEMINAR
REPORTS OF THE SEMINAR

Community Service Orders, Combination Orders, Charity, and Extramural Labour all punish offenders in the community. These forms of alternatives to incarceration were defined in a similar manner - unpaid public work or service conducted outside the prison. However, participants agreed that the major problem with this option is a high risk factor for penal institutions, where offenders could/would bring in contraband into the prison, as well as a high recidivism rate.

Brazil was the only country which has Rights Restricted as an alternative to incarceration and the problems encountered in relation to that option are similar to the problems mentioned in the introduction of this section above.

Brazil, Uruguay and Paraguay are the only represented countries which have house sentence/domiciliary arrest as an alternative to incarceration. This option requires an offender to remain in his/her own abode with certain restrictions. The problem encountered in relation to this option is a lack of human resources. Similarly Uruguay's patronage for released people and extra-mural leave had problems with lack of financial resources and carried a risk factor of the importation of contraband for penal institutions. Extra-mural leave also encountered the same problems in Brazil. Family visits existed as an alternative in some countries and the problems cited were similar in nature to those encountered in the use of patronage for released people and extra-mural leave as alternatives to incarceration.

Reduced Sentences/remission were outlined as alternatives to incarceration in some countries and the major problems with were cited as a lack of comprehensible legislation: inadequacies in the selection process of suitable offenders, a lack of adequate human resource and slow legal processes.

Corporal punishment was used as an alternative in one jurisdiction. One of the participants stated that it was an inhumane and degrading punishment; another stated that it was a violation of human rights; however, corporal punishment should be viewed in its cultural context.

Verbal sanctions i.e. admonition and discharge or dismissal with warning are used in Jamaica and Botswana respectively. The main disadvantage of these options were identified as a lack of human resources.

Redemption is used in Brazil and Uruguay as an alternative to incarceration and as a measure of rehabilitation and social reintegration. However the major problem is inadequate support services i.e. lack of employment opportunities and educational facilities.

C. Countermeasures and/or Practice of the Above Mentioned Mechanisms

The participants went on to deliberate upon the problems that were encountered by, and possible solutions for, the relevant agencies responsible for offenders.

Table 2-A. Collaboration among related agencies- e.g. Parole, Probation, Suspension of Execution

PROBLEMS	SOLUTIONS
<ul style="list-style-type: none"> • Lack of financial resources • Inadequacies regarding information sharing • Lack of capacity building • Lack of human resources • Lack of support systems for victims of crime • Fragmentation of the availability of services; e.g. health services for drug users and offenders with mental illness • Limited employment opportunities • Police confidentiality of criminal records tends to be lax 	<ul style="list-style-type: none"> • Enhancement of NGOs & CBOs by: <ul style="list-style-type: none"> - Information Sharing - Capacity Building - Sensitization • Secondment of officers to other related agencies • Sensitization and regular consultation meetings among related agencies • Creation of a multi-sectoral board to assist in the search for solutions • Victim compensation and assistance programmes • Offender education regarding recognizance and restitution • Skills-development for parolees and probationers • Keep criminal records valid for a set period of time • Enhancement of the PPP (Public-Private Partnerships) • Tax incentives for companies/agencies that employ ex-offenders • Change of legislation to prevent access of passed criminal records that will disadvantage the parolee or probationers regarding their reintegration into society • Developing a policy of anonymity for certain categories of parolees and probationers; i.e. keeping their IDs anonymous in order to enable them to reintegrate into society with minimal stigma and discrimination, but this should not be afforded to sex offenders and those who have committed violent crimes

Table 2-B. Improvement of Staff Skills

PROBLEMS	SOLUTIONS
<ul style="list-style-type: none"> • Lack of capacity building • Lack of financial resources • Lack of screening of potential personnel • Poor motivation and incentive work packages • Closed/guarded incarceration systems • Lack of periodic evaluation of prison personnel • Lack of specialized training 	<ul style="list-style-type: none"> • Holistic training done by qualified persons and experts • Work in collaboration with skilled professionals from other sectors in order to gain much needed knowledge and skills • Regular refresher courses especially for senior personnel in order to keep them informed of current trends • Work–study programmes to further staff development • Development of efficient VPO systems • Encouraging school-leavers and university graduates to take up employment in the sectors that work with offenders • Develop in-country/national networks whose sole focus would be developing community-based alternatives to incarceration • Develop biannual international collaboration forums. • Develop skills banks nationally and internationally to exchange best practices • Develop efficient selection procedures for personnel • Develop attractive career development processes

THE 141ST INTERNATIONAL SENIOR SEMINAR
REPORTS OF THE SEMINAR

**Table 2-C. Improvement of Treatment Programmes offered while the Offender serves his/her Sentence
(in an institution and/or the community, etc.)**

PROBLEMS	SOLUTIONS
<ul style="list-style-type: none"> • Problems with prison officer/offender ratio • Lack of financial resources • Lack of Capacity Building • Lack of human resources to monitor and assist offenders • Lack of support systems; i.e. drug rehab; sex offender rehab and health care for the offenders • Lack of facilities; i.e. with regard to employment and education opportunities for the offenders • “Proper” sentencing of offenders e.g. some drug traffickers are given probation which is not practical • HIV/AIDS and related problems as a critical health problem • Lack of sustainability of VPO programme • Lack of committed staff • Poor training of prison officers • Increased aged & disabled prison populations 	<ul style="list-style-type: none"> • Provision of funding for prison systems and prison programmes • Capacity building of prison personnel • Robust community programme to help communities understand community-based alternatives to incarceration • Post-release control of offenders • Improve infrastructure to afford employment and education opportunities for offenders • Availability of formal educational facilities and vocational training opportunities within prisons that afford inmates qualifications to use in the community • Have newly qualified professionals in psychology, sociology, criminology, medicine etc offer a year’s service on completion of programme (mandatory national service) • Decentralization of mental healthcare for those in need of relevant care • Affordable; accessible healthcare for offenders • Collaboration with health sector and drug rehab sector to conduct drug-testing • Intensive HIV/AIDS prevention and treatment programmes; including TB treatment in order to prevent or reduce the possibility MDR TB or XDR TB • Sex offender-treatment that is evidence-based • Small group therapeutic communities where offenders support each other: this is cost effective • Therapeutic community modality with a restorative justice as a conceptual framework and utilization of volunteers as a strategy • Creation of field training labs to enhance recruitment of VPOs • NGOs train offenders in various skills • Supervision and support of NGOs that work with offenders • NGOs that assist offenders families until children are 18 • Collaboration with private sector; including private sector administration of prisons • Collaboration of universities’ health faculties (or relevant institutions) with agencies that assist offenders • Review of treatment programmes in order to make them all evidence-based • Employment of professional experts from outside the offender rehabilitation sector • Establishment of national prison hospitals to care for inmates with health problems • Provide psychological treatment for all inmates/offenders

D. Identification of Other Effective Intervention Models

The group participants went on to identify a number of practical intervention models, as follows:

- The relevant ministries should work in collaboration to provide additional community support services and halfway houses that meet the needs of aged and disabled offenders;
- Domiciliary (house) arrest should only be considered for aged, chronically ill and disabled people;
- Establishment of a workable probation officer/offender ratio;
- Establishment of an effective risk assessment system to determine suitable candidates for house arrest and other community-based alternatives to incarceration;
- Electronic monitoring;
- Identify and adopt specific and effective drug treatment programmes for offenders with drug abuse problems; e.g. the Therapeutic Community Model;
- Establishment of comprehensive community crime prevention forums.

E. Measures to Monitor and Evaluate all Mechanisms Discussed

The importance of monitoring and evaluation were considered; and critical areas were highlighted as follows:

- Monitor recidivism rates in order to evaluate the success of the prescribed programmes;
- Monitor effectiveness of treatment models used to rehabilitate offenders;
- Employ qualified staff to monitor effectively;
- Establish an effective offender management system;
- Develop short-term and long-term monitoring systems;
- Monitor the mortality and morbidity of offenders to evaluate the level of healthcare provided for them;
- Establish a national crime statistics register that includes community crime statistics;
- Conduct a cost/benefit analysis of treatment programmes;
- Develop risk assessment tools to assist with analyses;
- Involve offenders in the choice of alternative sentencing;
- Establish neighbourhood commissions/committees that can help with the monitoring of offenders;
- Establish effective VPO systems;
- Conduct public surveys to establish public opinion of alternative sentencing methods and involve the public in the planning of releasing offenders into their respective communities;
- Establish international networks that focus on monitoring and evaluation of alternatives to incarceration.

III. RECOMMENDATIONS AND CONCLUSION

Using incarceration as the only method of punishment will only lead to high recidivism rates, and furthermore it will be a violation of human rights. Although we need to reduce the number of inmates in our prisons, the most important of our goals should be the rehabilitation of inmates. Therefore, to be effective

THE 141ST INTERNATIONAL SENIOR SEMINAR
REPORTS OF THE SEMINAR

and to improve the treatment of offenders, the alternatives to incarceration that we propose should:

1. reduce stigmatization;
2. promote the social reintegration of offenders;
3. prevent recidivism.

In order to succeed in this objective we believe that by matching the right offenders with the right sentencing options and ensuring that community-based programmes are adequately resourced and administered with integrity, community-based alternatives to incarceration can become a reality for productive and prosperous societies that aspire to reduced rates of crime.

The following are the recommendations proposed by the group members:

1. Non-custodial options be considered as effective rehabilitation strategy;
2. Sentencing officers who utilize alternative sentencing options should be cognizant of the human rights of offenders;
3. Recidivism rates be continuously monitored;
4. Risk assessments be used as an efficient supervision/monitoring system for community-based non-custodial options;
5. Inmates be evaluated during incarceration and as follow-up post release;
6. Effective measures for evaluation of social measures be established;
7. Effective public education programmes be implemented in order to sensitize and inform the public about community-based alternatives to incarceration;
8. Human and financial resources be increased to enhance the administration of community-based alternatives to incarceration;
9. Continuous research in these areas through public education forums, conferences, seminars and networking, at national, regional and international levels.

Finally, as societies we must understand that inmates are human beings who belong to our respective societies and communities. We have discussed many community-based alternatives to incarceration and we have arrived at the conclusion that the only way to reinstate offenders into society and into communities is by developing rehabilitation programmes in order to avoid recidivism - especially in this era where violence is emerging due to deterioration in moral values, the current economic recession, influence on cultural values and other related factors.

GLOSSARY

- * AIDS –Acquired Immuno-deficiency Syndrome
- * CBO – Community Based Organizations
- * HIV – Human Immune Virus
- * M & E – Monitoring and Evaluation
- * MDR – TB - Multi-drug resistant tuberculosis
- * NGO – Non-governmental Organization
- * TB – Tuberculosis
- * VPO – Volunteer Probation Officers
- * XDR – TB – Extreme multi-drug resistant tuberculosis

APPENDIX

COMMEMORATIVE PHOTOGRAPHS

- *140th International Training Course*
 - *Eleventh International Training Course on the Criminal Justice Response to Corruption*
 - *141st International Senior Seminar on the Improvement of the Treatment of Offenders through the Enhancement of Community-Based Alternatives to Incarceration*
-
-

The 140th International Training Course



Left to Right:

Above:

Mr. Jung, Prof. Higuchi, Prof. Yamada, Prof. Sugano

4th Row:

Ms. Ono (Staff), Mr. Iwakami (Staff), Mr. Matsumoto (Chef), Mr. Takagi (Staff), Mr. Kosaka (Staff), Mr. Shirakawa (Staff), Mr. Koiwa (Staff), Ms. Uenishi (Staff), Ms. Ota (Staff), Ms. Usuki (Staff)

3rd Row:

Mr. Kitada (Staff), Mr. Kojitani (Staff), Ms. Tomita (Staff), Mr. Sakamoto (Japan), Mr. Matsunaga (Japan), Mr. Omura (Japan), Mr. Naploeon (Indonesia), Mr. Ito (Japan), Ms. Ono (JICA)

2nd Row:

Mr. Suiama (Brazil), Ms. Lam (Hong Kong), Mr. Mirza (Bangladesh), Mr. Suzuki (Japan), Mr. Prommajul (Thailand), Mr. Sosa (Philippines), Mr. Malagoda (Sri Lanka), Mr. Saleh (Jordan), Mr. Ahsan (Pakistan), Mr. Carvalho (Brazil), Mr. Rodriguez (Mexico), Mr. Nlanda (Botswana)

1st Row:

Mr. Fujiwara (Staff), Mr. Fujii (Staff), Prof. Naito, Prof. Tatsuya, Deputy Director Seto, Dr. Gercke (Germany), Director Aizawa, Mr. Schwarz (USA), Prof. Oshino, Prof. Sugiyama, Prof. Otani, Mr. Nakasuga (Staff), Ms. Lord (LA)

The Eleventh International Training Course on the Criminal Justice Response to Corruption



Left to Right:

Above:

Prof. Higuchi, Prof. Sugano

4th Row:

Mr. Kosaka (Staff), Ms. Ono (Staff), Ms. Tomita (Staff), Mr. Matsumoto (Chef), Mr. Takagi (Staff), Mr. Iwakami (Staff), Mr. Nakayasu (Staff), Mr. Kojitani (Staff), Mr. Koiwa (Staff), Mr. Kitada (Staff), Ms. Usuki (Staff), Ms. Ota (Staff), Mr. Shirakawa (Staff)

3rd Row:

Mr. Poudel (Nepal), Mr. Bhattarai (Nepal), Mr. Yamada (Japan), Mr. Sorayuth (Thailand), Mr. Mongkol (Thailand), Ms. Jayasinghe (Sri Lanka), Ms. Uthaiwan (Thailand), Ms. Martinez Lagarde (Mexico), Mr. Khittkhun (Thailand), Mr. Tshering (Bhutan), Mr. Abeysuriya (Sri Lanka), Ms. Kita (JICA), Ms. Uenishi (Staff)

2nd Row:

Ms. Tosaporn (Thailand), Mr. Seksan (Thailand), Mr. Ishiwatari (Japan), Mr. Virote (Thailand), Mr. Al-Suhaiqi (Yemen), Mr. Obayashi (Japan), Mr. Vannak (Cambodia), Mr. Azeez (Iraq), Mr. Yasunaga (Japan), Mr. Somido (Philippines), Mr. Sy (Philippines), Mr. Moustafa (Egypt), Ms. Pervin (Bangladesh)

1st Row:

Mr. Fujiwara (Staff), Prof. Tatsuya, Prof. Yamada, Prof. Oshino, Deputy Director Seto, Mr. Kwok (Hong Kong), Director Aizawa, Mr. Gallo (Italy), Prof. Otani, Prof. Sugiyama, Prof. Naito, Mr. Fujii (Staff), Ms. Lord (LA)

The 141st International Senior Seminar



Left to Right:

Above:

Mr. Herradura (Philippines), Mr. Reddy (Singapore), Prof. Higuchi

4th Row:

Mr. Kosaka (Staff), Mr. Shirakawa (Staff), Ms. Ono (Staff), Mr. Matsumoto (Chef), Mr. Iwakami (Staff), Mr. Nakayasu (Staff), Mr. Takagi (Staff), Mr. Kojitani (Staff), Mr. Kitada (Staff), Ms. Usuki (Staff), Ms. Ota (Staff),

3rd Row:

Ms. Tomita (Staff), Mr. Nosaka (Japan), Mr. Welter (Brazil), Mr. Joydeb (Bangladesh), Mr. Ichikawa (Japan), Mr. Jagath (Sri Lanka), Mr. Ali (Pakistan), Mr. Nakajima (Japan), Mr. Date (Japan), Ms. Yamamoto (JICA), Ms. Uenishi (Staff)

2nd Row:

Mr. Takenaka (Japan), Mr. Ogata (Japan), Mr. Sutrisno (Indonesia), Ms. Clarke (Guyana), Ms. Makunga (Botswana), Mr. Nakashima (Japan), Mr. Suzuki (Japan), Mr. Carrillo (Philippines), Mr. Colman (Uruguay), Mr. Esteche (Paraguay), Mr. Vargas (Peru), Mr. Nguyen (Viet Nam), Mr. Majali (Jordan), Ms. Davey (Jamaica), Ms. Renny (Indonesia), Ms. Reu (Papua New Guinea), Mr. Higuchi (Japan)

1st Row:

Mr. Fujiwara (Staff), Mr. Fujii (Staff), Prof. Sugano, Prof. Sugiyama, Prof. Yamada, Deputy Director Seto, Ms. Sariya (Thailand), Dr. Kittipong (Thailand), Director Aizawa, Ms. Glenn (U.K.), Prof. Oshino, Prof. Otani, Prof. Tatsuya, Prof. Harada, Mr. Nakasuga (Staff), Ms. Lord (LA)