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 is 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 sub-paragraph (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 sub-paragraph (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.