

**international co-operation
against cybercrime**

**international co-operation against
cybercrime**

pedro verde/ho

April' 2008

international co-operation between law enforcement agencies – within police or between prosecution services - is crucial to achieve results in criminal investigations

plan

- 2 cases
- 24/7 network
- practical conclusions of the study
- final topics

case study - 1

- not a typical “*cybercrime case*”
- international co-operation tools on cybercrime matters were used

during 2005, a Norwegian citizen attacked a bank in Oslo

he intended to steal money

in the action, a police officer was killed

he ran away and could not be found



- some days later, police found and searched his home and computer

- discovered that he was the owner of an email-account from a provider in the United Kingdom

- international co-operation was required from British authorities

- the email-account was put under surveillance



- one day, he used his email-account to send an email message

- in the United Kingdom, police asked the ISP information about the IP address where the communication came from

- it was found that it came from Spain



case study - 1

- British and Spanish authorities installed an alert system whose objective was to know, each time that he used his email-account, where he was
- each time he used his account, British police obtained the IP address of the computer in the origin of the communication
- provided it immediately to Spanish police
- then, Spanish police asked the Spanish ISPs about the owner or user of the IP address

- all the connexions were made from cybercafés in Madrid

- even proceeding to the area very quickly, during a long period of time it was not possible to arrive at those places before he was gone



- later, he began to use his email-account from a cybercafé by the coast, in Malaga
- it was a smaller town than Madrid



- there, it was possible to put all the cybercafés from a certain area permanently under physical surveillance

case study - 1

- after some days of surveillance, British police announced that he was online, using his email-account, and provided the IP address
- very rapidly, the Spanish ISP informed Spanish police from the concrete location of the cybercafé
- the officers in the street could identify and arrest him in place
- he was extradited to Norway and prosecuted

case study - 2

- a typical “*cybercrime case*”
- international co-operation tools on cybercrime could not be used



Estonia ratified the Convention on Cybercrime in
2003

**Estonia
suffered a
very
important
distributed
denial of
service
(DDoS)
attack in
April and
May of
2007**



case study - 2

- such attacks caused important disturbances to the everyday life of people and to the government
- web pages were defaced, the servers have been saturated and several attacks using *botnets* were executed
- Estonian websites were not available for some days

case study - 2

- a lot of suspect IP addresses were identified
- but only one person was prosecuted and convicted
- he was the only Estonian citizen that could be identified



all the other suspects used foreign IP addresses, from a country that did not sign the Convention – and which law did not allow to provide cooperation

international efforts

- the United Nations General Assembly adopted resolutions on *Combating the Criminal Misuse of Information Technologies*
 - (Resolutions 55/63 and 56/121) which underline the need to ensure that each Member State adapts its law and practice to eliminate “safe heavens” .

international efforts

- Organisation for Economic Co-operation and Development (OECD)
 - since 1983, the OECD studied the existing need for national cybercrime laws
 - made recommendations
 - on international level the same facts should be qualified within similar criminal frameworks

international efforts

- Group of Eight, the G8,
 - Contact Points Network

international efforts

- European Union
 - legal instruments
 - cybercrime
 - International co-operation

international efforts

- Organization for Security and Co-operation in Europe (OSCE)
 - Decision No. 7/06,
 - participating States should consider becoming a party to the Convention on Cybercrime.
 - also encouraged participating States to join the G8 24/7 Computer Crime Network

international instruments

- Convention on Cybercrime
- 1959 European Convention on Mutual Assistance in Criminal Matters
- Schengen and Mutual Legal Assistance Agreement of 2000 (MLA)
 - (Treaty of Lisbon ?)

Article 29

expedited preservation of stored computer data

- 1 - A Party may request another Party to **order or otherwise obtain the expeditious preservation of data stored by means of a computer system**, which is located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

Article 29

expedited preservation of stored computer data

- 3 - Upon receiving the request from another Party, the requested Party shall **take all appropriate measures to preserve expeditiously** the specified data in **accordance with its domestic law**. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

Article 30

expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made under Article 29 to preserve traffic data concerning a specific communication, **the requested Party discovers that a service provider in another State was involved in the transmission of the communication**, the requested Party **shall expeditiously disclose to the requesting Party a sufficient amount of traffic data in order to identify that service provider and the path** through which the communication was transmitted.

Article 31

mutual assistance regarding accessing of stored computer data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29
2. (...)
3. The request shall be responded to on an expedited basis where:
 - (a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
 - (b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32

trans-border access to stored computer data with consent or where publicly available

A Party may, **without obtaining the authorisation** of another Party:

- (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- (b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33

mutual assistance regarding the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other with respect to the real-time collection of traffic data associated with specified communications in its territory transmitted by means of a computer system. Subject to paragraph 2, assistance shall be governed **by the conditions and procedures provided for under domestic law.**
2. Each Party shall **provide such assistance** at least with respect to criminal offences for which real-time collection of traffic data would be available **in a similar domestic case.**

Article 34

mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other with respect to the **real-time collection or recording of content data** of specified communications transmitted by means of a computer system **to the extent permitted by their applicable treaties and domestic laws.**

24/7 Contact Points (G8/CoE)

- the existing 24/7 contact points network idea, in the context of Article 35 from the Cybercrime Convention, was born from the “G8 High-Tech Crime Subgroup”

24/7 Contact Points (G8/CoE)

- operational network of experts on high-tech criminality
- provide help and co-operation very quickly even if a formal co-operation request must follow this informal way
- one single point of contact for each country, available 24 hours a day, 7 days a week
- direct communications between the points
- mainly planned to provide the possibility to immediately preserve traffic data and other stored data worldwide

24/7 Contact Points (G8/CoE)

general overview

- most of the contact points are police contact points
- only four countries (“the former Yugoslav Republic of Macedonia”, Romania, the Netherlands and the United States of America) designed Prosecution Services as contact points
- only three states have not yet designated a 24/7 contact point

24/7 Contact Points (G8/CoE)

- G8 welcomed countries from outside the G8 to join the network.
- Since the beginning, it was expected that this network could expand to other countries, building a global network
- in concrete and real investigations, only a widely expanded network could provide the expectancy of efficiently obtaining sufficient evidence to be used to investigate and prosecute suspects

24/7 Contact Points (G8/CoE)

- no coincidence countries party on the Convention / countries listed in G8 24/7 contact points network
- in the G8 network, only 12 of them ratified the Convention on Cybercrime
- 24 countries of them have not signed or ratified the Convention
- eight of the 27 European Union Member States have not yet joined the network

24/7 Contact Points (G8/CoE)

The G8 network and the Council of Europe network

- the merge between the G8 network and the Convention network can clarify the role of the previous informal structure
- it can give confidence to non G8 members to become new members of the network
- on the other hand, the association with the network described on Article 35 of the Convention gives a legal framework to the G8 network

conclusions of the study

- Convention on Cybercrime is seen as a useful tool in Romania and in France
- effectively used for international co-operation in order to rapidly preserve computer data
 - and to forward countries information obtained within the framework of its own investigations to other
- until now, the framework of the Convention has not been used by France and Romania to ask for co-operation regarding the interception of communications
 - these countries have not yet received such requests from any other Party of the Convention

conclusions of the study

- in Estonia, the Convention framework is not very much used yet, and other channels are preferred
- generally, the common framework that the Convention creates is considered an advantage
- however, the small number of countries that have so far ratified the Convention is seen as a problem

final topics

- cybercrime is the most transnational of all crimes
- investigating cybercrime means efficient international co-operation
- without such co-operation, investigations are unlikely to succeed

final topics

- Convention on Cybercrime
 - provides many useful tools regarding international co-operation, including in particular the network of 24/7 contact points under Article 35 of the Convention