CYBERCRIME

NEW THREATS RELATED TO THE FIGHT AGAINST CYBERCRIME
-Part 2: Investigation -

Plovdiv, 17th December 2007

Dr. Marco Gercke

POSSIBILITIES

- There are no doubts that the ongoing improvement of information technology enables the law enforcement agencies to carry out investigations that were not possible previously
- Automated search for key-words / hash-values
- Great chance for public private partnership (Microsofts CETS)

EXAMPLE CHILD PORNOGRAPHY

Picture removed in print version

POSSIBILITIES

- Apart from new instruments the ongoing technical development is going along with a number of challenges for law enforcement agencies.
- Investigations can be more difficult or even impossible if the offender is just using some basic technical means
- Challenges of fighting Cybercrime go way beyond that

EXAMPLE CHILD PORNOGRAPHY

Picture removed in print version

INTERNATIONAL DIMENSION

- Network Protocol contains an automatic search procedure for the fastest connection
- This leads in an nearly uncontrollable way to international dimensions within data exchange processes

TRACING ROUTE

Picture removed in print version

TCP-IP contains of two elements:
TCP (Transfer Control Protocol) and IP (Internet Protocol)

Real Routes of data exchanges can be traced back using tracing software such as "TraceRoute"

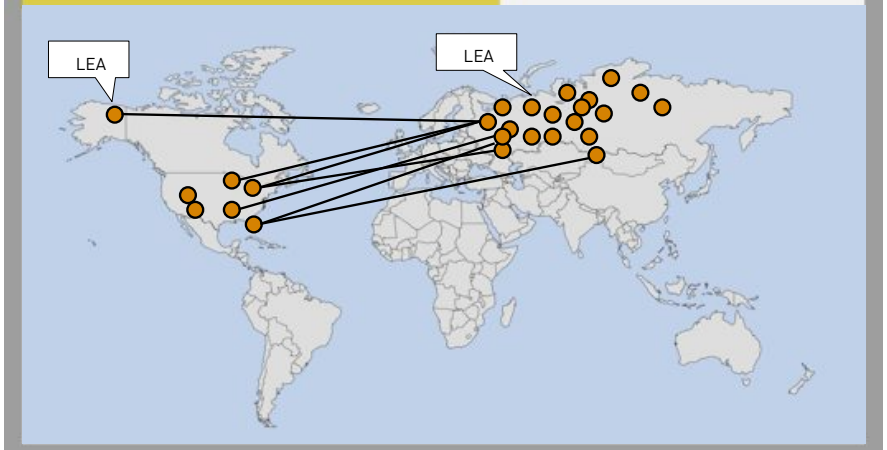
24/7 NETWORK

Art. 35 24/7 NETWORK

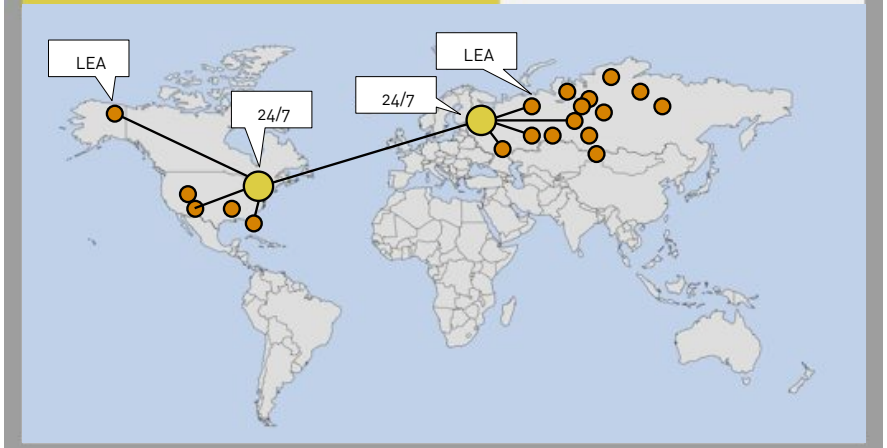
1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a) the provision of technical advice
b) the preservation of data pursuant to Articles 29 and 30;
c) the collection of evidence, the provision of legal information, and locating of suspects.

24/7 NETWORK



24/7 NETWORK

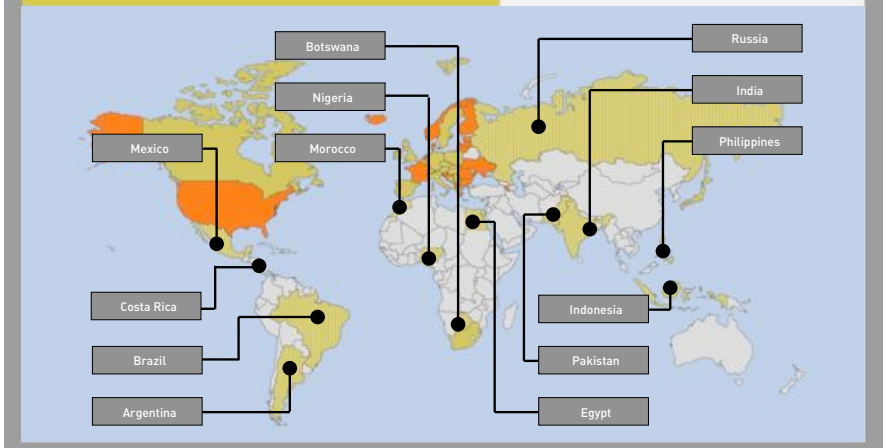


SIGNATURES UNTIL 2007

DETAILS ABOUT SIGNATURES

43 States signed the Convention 185 ("Convention on Cybercrime") until March 2006, among them are 4 Non-Members. Details are available unter www.coe.int

MODEL LAW



AVAILABILITY OF INFORMATION

- Secret Information are available in the Internet
- Available especially through search engines
- "Google hacking"

Example (Sat. Picture)

Picture removed in print version

AVAILABILITY OF INFORMATION

Services like Google Earth were reported to be used in several attacks:

- In attacks against British troops in Afghanistan
- In the planning of attacks against an airport in the US
- In attacks against British troops in Iraq
- In attacks against Israel

Telegraph.co.uk (13.01.2007)

Terrorists attacking British bases in Basra are using aerial footage displayed by the Google Earth internet tool to pinpoint their attacks, say Army intelligence sources.Documents seized during raids on the homes of insurgents last week uncovered print-outs from photographs taken from Google.

Guardian (25.10.2007)

Palestinian militants are using Google Earth to help plan their attacks on the Israeli military and other targets, the Guardian has learned. Members of the al-Aqsa Martyrs Brigade, a group aligned with the Fatah political party, say they use the popular internet mapping tool to help determine their targets for rocket strikes.

AVAILABILITY OF INFORMATION

- Robots used by Search-engines can lead the disclose of secret information
- Handbooks on how to build explosives and construct chemical and even nuclear devices are available
- Internet sources have been used by the offenders in a number of recent attacks

TERRORIST HANDBOOK

Picture removed in print version

MUJAHIDIN MAGAZINE

Picture removed in print version

AVAILABILITY OF INFORMATION

RAGNAR'S ENCYCLOPEDIA

Picture removed in print version

- Information regarding the construction of weapons were available long time before the Internet was developed
- Ragnar's Action Encyclopaedia of Practical Knowledge and Proven Techniques
- Approaches to criminalise the publication of information that can be used to

AVAILABILITY OF INFORMATION

Example (http:wslabi.com)

Picture removed in print version

- Information about system vulnerabilities are published on websites
- In addition these information are offered for sale by some businesses
- Information can be used to increase security as well as to commit computer-related offences

SOLUTION

EU FRAMEWORK. TERRORISM

Picture removed in print version

- EU approach to criminalise the publication of certain information
- Regional approach
- Difficult with regard to the international dimension of the network
- Regional approach would require filtering
- Potential conflict with "Freedom of Speech" principle
- Cybercrime Committee would be the right venue to discuss this issue

ANONYMOUS COMMUNICATION

Anonymizer (www.anonymizer.com)

Picture removed in print version

- "Felt Anonymity"
- Key motivation especially with regard to crimes connected pornography
- Technology available that can hinder law enforcement to trace back the route of an offender (eg. www.anon.de)
- Benefit of Anonymous Communication vs. Effective Law Enforcement
- Possibility to pretend to be some else (Remote Software)

Similar problem with regard to the use of encryption software. Benefits for the Society vs. Effective Law Enforcement

ANONYMOUS COMMUNICATION

Example (Public Internet terminal)

Anonymous communication can be reached by:

- Use of public terminals
- Use of open wireless networks
- Hacked (closed) networks

ENCRYPTION

PGP

- Encryption is the process of obscuring information to make it unreadable without special knowledge
- Encryption can be used to ensure secrecy
- Encryption can be used to hide the fact that encrypted messages are exchanged
- Encryption used by criminals can lead to difficulties collecting the necessary evidence

BREAKING A KEY

How long it takes to break a key

- Brute Force Attack: Method of defeating a cryptographic scheme by trying a large number of possibilities; for example, exhaustively working through all possible keys n order to decrypt a message
- Gaps in the encryption software
- Dictionary-based attack
- Social Engineering
- Classic search for hints
- Need for legislative approaches?

GLOBAL PHENOMENON

MICROSOFT BITLOCKER

- Availability of encryption technology is a global challenge
- Powerful software tool that enable are available on a large scale in the Internet
- Some of the latest versions of operating systems contain encryption technology

SOLUTION

MAGIC LANTERN

Picture removed in print version

Technical solutions (with legal component)

- Magic Lantern (US)
- Remote Forensic Software (Germany)

Legal solution

- Various restrictions on import/export and use of encryption technology
- UK: Obligation to disclose password (Sec. 49 of the UK Investigatory Powers Act 2000)

STEGANOGRAPHY

Steganography

Picture removed in print version

- Steganography is a technique used to hide information in some other information
- Example: Hiding a message in picture
-
- Technique can be used to keep the fact that the exchange of encrypted messages is taking place secret

THANK YOU FOR YOUR ATTENTION

gercke@cybercrime.de