Cybercrime
Research Institute

CYBERCRIME
ORGANIZED CRIME AND CHALLENGES

ERA Workshop on Cybercrime
11 January 2012, Istanbul, Turkey
Prof. Dr. Marco Gercke

Cybercrime
Research Institute

CYBERCRIME

Cybercrime
Research Institute

CONTENT

- Definition / Phenomena
- Organised Crime
- Regulatory Framework
- Challenges of Fighting Cybercrime

Cybercrime
Research Institute

DEFINITION

- No widely accepted definition
- Suggest to avoid definition of Cybercrime
- Instead using typology (CIA, Computer-related offences, content-related offences, copyright/trademark offences)

DEFINITION

One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity

Cybercrime
Research Institute

CIA-OFFENCES

- Illegal Access
- Data Espionage
- Illegal Interception
- System Interference

Picture removed in print version
Bild zur Druckoptimierung entfernt
WEBSITE

Cybercrime
Research Institute

COMPUTER-RELATED OFFENCES

- Computer-related Fraud (Remaining importance of traditional fraud)
- Computer-related Forgery
- Identity Theft
- Misuse of Devices

Picture removed in print version
Bild zur Druckoptimierung entfernt
WEBSITE

Cybercrime
Research Institute

CONTENT-RELATED OFFENCES

- Erotic and Pornography Material
- Child Pornography
- Hate Speech
- Religious offences
- Illegal Gambling
- Libel
- Spam

Picture removed in print version
Bild zur Druckoptimierung entfernt

ONLINE GAMBLING

Cybercrime
Research Institute

COPYRIGHT/TRADEMARK OFFENCES

- Copyright-related offences
- Trademark-related offences

Picture removed in print version
Bild zur Druckoptimierung entfernt

FILESHARING

Cybercrime
Research Institute

COMBINED OFFENCES

- "Terrorist Use of the Internet"
- "Cyberlaundering"
- "Phishing"
- "Warfare involving network technology"

Picture removed in print version
Bild zur Druckoptimierung entfernt

TERRORIST USE INTERNET

Cybercrime
Research Institute

LEGAL FRAMEWORKS

Cybercrime
Research Institute

Substantive Criminal Law	Illegal Access to a Computer	Illegal Remaining in a Computer	System Interference	Illegal Interception	Illegal Access to Computer Data	Illegal Data Input	Illegal Aquisition of Comp. Data	Illegal Data Interference	Illegal Use of Data	Violation of Data Protection Regul.	Illegal Devices / Misuse of Devices	Computer-related Fraud	Computer-related Forgery	Indecent Material	Pornography	Child Pornography	Solicitation of Children	Dissemination of Racistic Material	Identity-related Crime	SPAM	Threat and Harassment	Disclosure of an Investigation	Copyright Violation	Violation of Secrecy
CoE Cybercrime Convention (2001)	✔		✔	✔				✔			✔	✔	✔			✔							✔	
CoE Convention Protection Children (2007)																✔	✔							
EU FD Non-Cash Payment (2001)											✔	✔												
EU FD Child Pornography (2003)																✔								
EU FD Attacks Information Systems (2005)	✔		✔					✔																
EU DI Child Pornography (2011)																✔	✔							
EU Draft DI Attacks Information S. (2011)	✔		✔	✔				✔			✔													
Draft African Union Convention (2011)	✔	✔	✔	✔		✔		✔	✔	✔	✔	✔	✔		✔	✔		✔				✔		✔
Commonwealth Model Law (2002)	✔		✔	✔				✔			✔					✔								
HIPCAR Cybercrime Model Law (2010)	✔	✔	✔	✔			✔	✔			✔	✔	✔				✔		✔	✔	✔			

Cybercrime
Research Institute

BRINGING LEGISLATION INTO CONTEXT

COMPONENTS

Substantive Criminal Law

Procedural Law

International Cooperation

Convention on Cybercrime

COMPONENTS

National Cybersecurity Strategy

Technology, CERT, ...

Cybercrime Policy

Crime Prevention, Technology

Criminal Law

Substantive Criminal Law

Procedural Law

International Cooperation

Electronic Evidence

Liability of ISPs

Trained Investigators

Equiptment Training

Cybercrime
Research Institute

POLICY AND LAW	Policy	Substantive Criminal Law	Procedural Law	International Cooperation	Electronic Evidence	Liability of ISPs
CoE Cybercrime Convention (2001)		✔	✔	✔		
EU Frameworks	✔	✔	✔	✔		✔
Commonwealth Model Laws		✔	✔		✔	
HIPCAR Model Laws	✔	✔	✔	✔	✔	✔

Cybercrime
Research Institute

ALWAYS REVIEW

Cybercrime
Research Institute

EXAMPLE: CHILD PORNOGRAPHY

- As cooperation requires legislation gaps can have significant impact
- In the early discussion about legal response to an online distribution of child pornography the drafter of regulations focused on digital images
- Today not only images and videos but also audio recordings of the sexual abuse of children are distributed online
- Older approaches often use language (such as "visually" or "image") that excludes such material

Convention on Cybercrime

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.

EU Directive Child Pornography 2011

(c) 'child pornography' means:
(i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct;

Cybercrime
Research Institute

EXAMPLE: CHILD PORNOGRAPHY

- As cooperation requires legislation gaps can have significant impact
- In the early discussion about legal response to an online distribution of child pornography the drafter of regulations focused on digital images
- Today not only images and videos but also audio recordings of the sexual abuse of children are distributed online
- Older approaches often use language (such as "visually" or "image") that excludes such material

Picture removed in print version
Bild zur Druckoptimierung entfernt

IOL News 2011

Picture removed in print version
Bild zur Druckoptimierung entfernt

US Training Manual

Cybercrime
Research Institute

EXAMPLE: CHILD PORNOGRAPHY

- HIPCAR Model Law consequently avoids the term "visually"
- In addition the definition of the model legislative text contains a clarification that audio material is included

HIPCAR MODEL LAW (2010)

(4) Child pornography means pornographic material that depicts presents or represents:
a child engaged in sexually explicit conduct;
a person appearing to be a child engaged in sexually explicit conduct; or
images representing a child engaged in sexually explicit conduct;
this includes, but is not limited to, any audio, visual or text pornographic material.

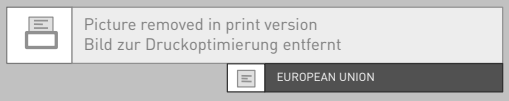
Cybercrime
Research Institute

EU INSTRUMENTS

Cybercrime
Research Institute

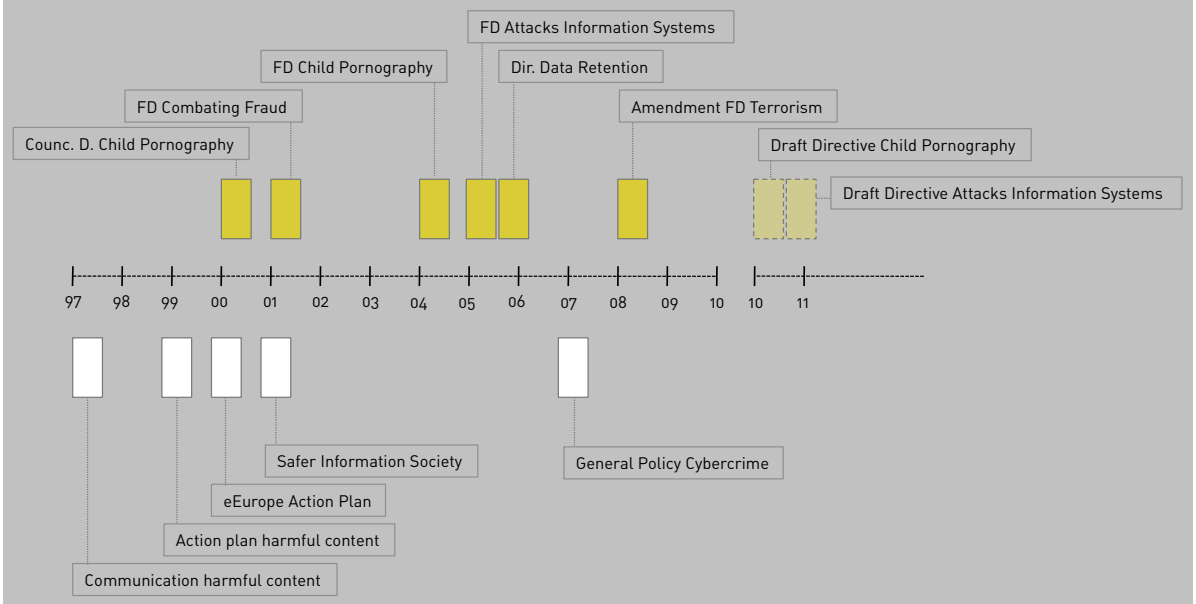
EUROPEAN UNION

- The European Union is a political Union of 27 member states
- One of the mandate of the EU is to harmonise legislation in selected areas
- It has adopted several Framework Decision and Directives to harmonise the legislation with regard to Cybercrime
- The 27 member states are obliged to implement the legislation within the given time period



Cybercrime
Research Institute

EUROPEAN COMMUNITY / UNION



NON-CASH MEANS OF PAYMENT

- Framework Decision on combating fraud and counterfeiting of non-cash means of payment (2001)
- Interesting approach as it contains a provision (Art. 4) that criminalises the production as well as possession of tools particularly adopted for the commission of committing computer fraud
- Not covered by the 2001 Council of Europe Convention (Art. 6 only refers to offences described by Art. 2 – 5)

FD on Combating Fraud

Art. 4 - Offences related to specifically adapted devices
Each Member State shall take the necessary measures to ensure that the following conduct is established as a criminal offence when committed intentionally:
the fraudulent making, receiving, obtaining, sale or transfer to another person or possession of:
— instruments, articles, computer programmes and any other means peculiarly adapted for the commission of any of the offences described under Article 2(b);
— computer programmes the purpose of which is the commission of any of the offences described under Article 3.

SEXUAL EXPLOITATION

- Framework Decision on combating sexual exploitation of children and child pornography (2004)
- Unlike the Convention on Cybercrime not focusing on Internet-related offences
- Similar approach with regard to the acts covered

FD on Combating Sexual Exploitation

Art. 3 - Offences concerning child pornography
1. Each Member State shall take the necessary measures to ensure that the following intentional conduct whether undertaken by means of a computer system or not, when committed without right is punishable:
(a) production of child pornography;
(b) distribution, dissemination or transmission of child pornography;
(c) supplying or making available child pornography;
(d) acquisition or possession of child pornography.

Cybercrime
Research Institute

SEXUAL EXPLOITATION

- Framework Decision like the Convention on Cybercrime contains options for restrictions that enable Member States to adjust the criminalisation to the national demands and in accordance with legal traditions

FD on Combating Sexual Exploitation

2. A Member State may exclude from criminal liability conduct relating to child pornography:
(a) referred to in Article 1(b)(ii) where a real person appearing to be a child was in fact 18 years of age or older at the time of the depiction;
[...]
(c) referred to in Article 1(b)(iii), where it is established that the pornographic material is produced and possessed by the producer solely for his or her own private use, as far as no pornographic material as referred to in Article 1(b)(i) and (ii) has been used for the purpose of its production, and provided that the act involves no risk for the dissemination of the material.

Cybercrime
Research Institute

DATA RETENTION

- Directive on Data Retention (2005)
- Adopted after a controversial discussion
- Unique with regard to the limited time for discussion between the introduction and adoption
- Ongoing debate about a violation of fundamental human rights
- Recent decision from the Romanian Constitutional Court

Data Retention Directive

Article 1 - Subject matter and scope
1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

Cybercrime
Research Institute

ATTACKS INFORMATION SYSTEMS

- Framework Decision on attacks against information system (2005)
- Focusing on harmonisation of substantive criminal law provisions related to computer crime (illegal access, system interference and data interference)
- In addition it contains a regulation dealing with jurisdiction as well as exchange of information

FD Attacks against Information Systems

Article 11 - Exchange of information

1. For the purpose of exchange of information relating to the offences referred to in Articles 2, 3, 4 and 5, and in accordance with data protection rules, Member States shall ensure that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week.
2. Each Member State shall inform the General Secretariat of the Council and the Commission of its appointed point of contact for the purpose of exchanging information on offences relating to attacks against information systems. The General Secretariat shall forward that information to the other Member States.

Cybercrime
Research Institute

TERRORISM

- In 2008 the Framework Decision on Combating Terrorism was amended
- Framework Decision is referring to terrorist use of the Internet
- Specifically mentioning recruitment and training
- It is one of the first regional approaches specifically addressing Internet related acts

FD Combating Terrorism

(4) The Internet is used to inspire and mobilise local terrorist networks and individuals in Europe and also serves as a source of information on terrorist means and methods, thus functioning as a 'virtual training camp'. Activities of public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism have multiplied at very low cost and risk.

Cybercrime
Research Institute

LISBON TREATY

- Lisbon Treaty fundamentally changed the structure and instruments of the European Union
- Main instrument is now the directive
- In addition the mandates was clarified
- Since the ratification of the Lisbon Treaty the EU has a strong mandate with regard to Cybercrime legislation (Art. 83)

Treaty on Functioning of the EU

Art. 83
1. The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis.
These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, **computer crime** and organised crime.
[...]

Cybercrime
Research Institute

DIRECTIVE CHILD PORNOGRAPHY

- In 2011 the EU adopted a Directive repealing the existing Framework Decision on combating sexual exploitation was published
- First draft contained a provision related to the blocking of child pornography websites

Draft Directive Child Pornography

Article 21 - Blocking access to websites containing child pornography
Member States shall take the necessary measures to obtain the blocking of access by Internet users in their territory to Internet pages containing or disseminating child pornography. [...]

Adopted Directive Child Pornography

Article 25 - Measures against websites containing or disseminating child pornography
1. Member States shall take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory.
[...]

Cybercrime
Research Institute

DIRECTIVE CHILD PORNOGRAPHY

- The draft directive is taking regarding to changing international standards
- New approaches on an international level - criminalisation of obtaining access to child pornography
- Necessary to cover new technical solutions to watch movies ("streaming video")

Directive Child Pornography

Article 5 – **Offences concerning child pornography**
[...]
3. Knowingly obtaining access, by means of information and communication technology, to child pornography shall be punishable by a maximum term of imprisonment of at least one year.

Cybercrime
Research Institute

DIRECTIVE CHILD PORNOGRAPHY

- The criminalisation is going beyond child pornography
- The directive for example includes a provision criminalising "grooming"
- In addition the provision is dealing with sexual exploitation of children

Directive Child Pornography

Art. 6 – Solicitation of children for sexual purposes
1. Member States shall take the necessary measures to ensure that the following intentional conduct is punishable:
the proposal, by means of information and communication technology, by an adult to meet a child who has not reached the age of sexual consent, for the purpose of committing any of the offences referred to in Article 3(4) and Article 5(6), where that proposal was followed by material acts leading to such a meeting, shall be punishable by a maximum term of imprisonment of at least 1 year.

Cybercrime
Research Institute

DIRECTIVE ATTACK INFORMATION S.

- In September 2010 the EU published a draft directive on attacks against information systems
- Update of the 2005 framework decision on attacks against information systems
- The draft directive also contains fundamental policy options

Directive Child Pornography

Article 6 – **Solicitation of children for sexual purposes**
The proposal, by means of information and communication technology, by an adult to meet a child who has not reached the age of sexual consent under national law, for the purpose of committing any of the offences referred to in Articles 3 (3) and Article 5 (6), where this proposal has been followed by material acts leading to such a meeting, shall be punishable by a maximum term of imprisonment of at least two years.

Cybercrime
Research Institute

COUNCIL OF EUROPE CONVENTION ON CYBERCRIME

Cybercrime
Research Institute

COUNCIL OF EUROPE

- Council of Europe is an international organisation focusing on the European integration
- 47 member states
- Convention on Cybercrime (2001)
- First addition protocol to the Convention on Cybercrime (2003)
- Convention on the protection of children against sexual exploitation and sexual abuse (2007)

Picture removed in print version
Bild zur Druckoptimierung entfernt

COUNCIL OF EUROPE

Cybercrime
Research Institute

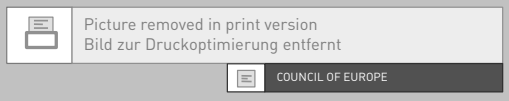
RATIFICATION PROCESS

- 32 countries ratified the Convention on Cybercrime
- Just one country (United States) is not member of the Council of Europe
- No mandatory evaluation of the ratification
- 16 countries have not ratified it in the last 9 years

Cybercrime
Research Institute

USE OF THE CONVENTION

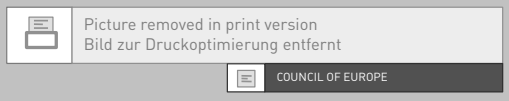
- Convention on Cybercrime was signed by 46 states
- The Council of Europe recently published in two official documents that more than 100 jurisdictions around the world have either acceded/sought accession to, or have based their national legislation on this Convention
- However, the Council of Europe neither specifies the number nor provides a list of the countries. This hinders a verification as well as a debate with the scientific community



Cybercrime
Research Institute

USE OF THE CONVENTION

- In addition the Council of Europe does not verify if the countries reported to have used the Convention did only implement single provisions as guideline or drafted major part of their legislation in accordance with the instrument
- Finally the Council of Europe does not specify on which scientific basis it determines if a country used the Convention (similar legislation, reference to the Convention in an official document, expert statement, ...)



Cybercrime
Research Institute

USE OF THE CONVENTION

- Publication of information in official documents without verification is surprising as the Council of Europe is strongly supporting the idea of Freedom of Information and Access to Information
- Scientific debate can prevent misquotation like in the 2005 Council of Europe Organized Crime Report

Picture removed in print version
Bild zur Druckoptimierung entfernt

2005 COE Organized Crime Report

Cybercrime
Research Institute

REVIEW

- Despite the technological developments and the changing criminal environment the Convention was not changed in the last 10 years
- This is especially relevant with regard to procedural law as law enforcement agencies need sophisticated investigation instruments to address recent challenges that are not contained in the Convention

2007 Convention Protection Children

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

Cybercrime
Research Institute

ORGANISED CRIME

Cybercrime
Research Institute

ORGANISED CRIME

- Definition of organized crime group in Art. 2 United Nations Convention against Transnational Organized Crime (UNTOC)

Several conditions:
- Group of three or more persons
- Structured
- Existing for a period of time
- Acting in concert with the aim of committing one or more serious crimes
- Financial or other material benefit

UNTOC

Article 2.Use of terms
For the purposes of this Convention:(a)"Organized criminal group" shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit;

Cybercrime
Research Institute

ORGANISED CRIME

- Several studies, surveys and publication closely link Cybercrime to organized crime. Some studies even see a growing importance of organised crime
- Relevant especially with regard the applicability of the UN TOC Convention
- With regard to all areas of Cybercrime there is an involvement of organised crime
- Main challenge is the determination of the extend of an involvement of organised crime
- IWF Report from 2008 for example indicates that the number of commercial website decreases.

SOURCE: IWF REPORT 2006-2009

Cybercrime
Research Institute

EXAMPLE ORGANISED CRIME R.

- An example for quotations without verifiable reference was discovered by the Wall Street Journal in 2006.
- While investigating a quotation that "child pornography is a multibillion business – 20 billion USD a year - the journalist reported that two main documents containing information about revenues from 3 billion to 20 billion – a publication from NCMEC and one from the Council of Europe - did refer to Institutions that did not confirm the numbers.

2005 CoE Organised Crime Situation R.

Cybercrime
Research Institute

OPPORTUNITIES

Cybercrime
Research Institute

OPPORTUNITIES

- Availability of computer technology improved the ability of law enforcement to carry out investigations
- DNA sequence analysis and finger print databases are examples for an emerging use of information technology in traditional criminal investigation

Picture removed in print version
Bild zur Druckoptimierung entfernt

FINGERPRINT DATABASE

Cybercrime
Research Institute

AUTOMATE

- Software tools are available to automate investigations
- Significant reduction of time for an investigation
- One example is the Software PERKEO that detects child pornography pictures on the basis of hash values

Picture removed in print version
Bild zur Druckoptimierung entfernt

PERKEO

Cybercrime
Research Institute

AUTOMATE

- Automation techniques can also be used to identify copyright violations
- One example is file-sharing monitoring where software tools can automatically detect copies of copyright-protected art-work made available
- Another example is the automatic scanning of scientific work (like PhD)

Picture removed in print version
Bild zur Druckoptimierung entfernt

GUTTENPLAG

Cybercrime
Research Institute

OPPORTUNITIES

- Case example 1: Within an investigation of a murder case law enforcement was unable to identify a murder based on search engine history. They were able to use search engine logs on the suspects computer to identify places he was interested in.

Picture removed in print version
Bild zur Druckoptimierung entfernt

Informationliberation.com

Cybercrime
Research Institute

OPPORTUNITIES

- Case example 2: Investigator were able to discover that the suspect was searching for specific terms such as ““undetectable poisons,” “fatal digoxin levels,” “instant poisons,” “toxic insulin levels,” “how to purchase guns illegally,” how to find chloroform,” “fatal insulin doses,” “poisoning deaths,” “where to purchase guns illegally,” “gun laws in PA,” “how to purchase guns in PA,”

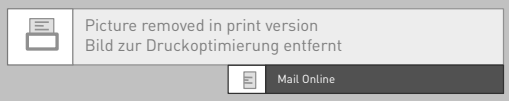
Picture removed in print version
Bild zur Druckoptimierung entfernt

PCWORLD

Cybercrime
Research Institute

OPPORTUNITIES

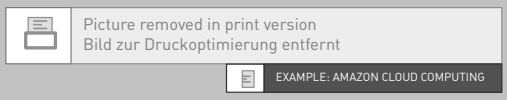
- Google searches including '1,000 ways to die', 'how to kill someone' and 'ten easy ways to kill someone with no trace', 'can you kill someone with a punch?', 'dangerous drugs for the elderly', 'if you hit someone across the back of the head with a brick will they die or just get a bruise?' and 'easiest way to kill an old person', 'delayed symptoms of concussion', 'sugar in petrol tank', 'poisonous salts', 'suffocation symptoms', 'heart attack symptoms' and 'dying in your sleep'.



Cybercrime
Research Institute

DEVICES PROCESSING DATA

- Devices do often store information that are valuable for traditional investigation
- The user do not necessary have knowledge about such operation
- One example is the iPhone that stored the geo-location of the user and thereby enabled the reconstruction of movements/travel



Cybercrime
Research Institute

OPPORTUNITIES

- New forensic technology can be very useful in computer crime and Cybercrime investigation as well
- Software tools that automatically search for key-words in text documents on the suspects computer or check the hash-values of pictures to identity child pornography are examples for highly effective forensic tools
- Internet can in addition be used to inform public about the search for suspects

Picture removed in print version
Bild zur Druckoptimierung entfernt

INTERPOL INVESTIGATION

Cybercrime
Research Institute

POSSIBILITIES

- But by using just very basic techniques offenders can delay investigations
- Using more sophisticated technology such as encryption or anonymous communication can increase the challenges and in the worst case even hinder investigation

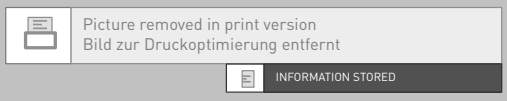
Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE CIRCUMVENTION

Cybercrime
Research Institute

TRACES

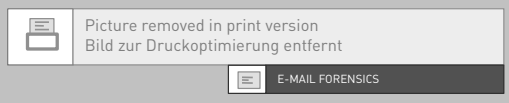
- "Nobody knows you are a dog" ?
- Internet users leave traces
- Access-Provider for example often for a certain period of time keep records to whom a dynamic IP-address was assigned
- Data retention obligations even increase the volume of data stored (but go along with questions related to the legality of this investigation instrument)



Cybercrime
Research Institute

E-MAIL FORENSICS

- Uses of Internet-services such as e-mail leave various traces
- Information contained in an e-mail go way beyond sender, recipient, subject and content
- Header information can help law enforcement to identify the sender of threatening mails



Cybercrime
Research Institute

CHALLENGES INVESTIGATION

Cybercrime
Research Institute

DEPENDANCE

- Threats of internet based attacks against critical infrastructure
- Energy, Communication, Transportation, Health, Food supply, Finance, Government services, Essential manufacturing, ...
- Even military infrastructure is depending critical technology

Picture removed in print version
Bild zur Druckoptimierung entfernt

CRITICAL INFRASTRUCTURE

Cybercrime
Research Institute

DEPENDANCE

- Alternative Communication Systems that could be used in cases of emergency are not able to cover the necessary resources
- Monoculture with regard to major technical components of computer systems, software and network technology

Picture removed in print version
Bild zur Druckoptimierung entfernt

SASSER COMPUTER WORM

Cybercrime
Research Institute

STUXNET

- Malicious software targeting Windows operating system
- Discovered in June 2010
- Specifically focussing on Supervisory Control And Data Acquisition (SCADA)
- SCADA is for example used in Siemens S7 systems that are used to control critical infrastructure such as power plants

Picture removed in print version
Bild zur Druckoptimierung entfernt

Siemens S7-300

Cybercrime
Research Institute

PAYLOAD

- Researches indicate that the software was capable of manipulating the frequency of the centrifuges at Iran's enrichment plant
- Regular speed is between 807 Hz and 1210 Hz
- The virus might have changed the frequency down to 2Hz and up to 1410Hz
- High speed and "shaking-effect" has the potential to physical damage the centrifuges

Picture removed in print version
Bild zur Druckoptimierung entfernt

APA Website

Cybercrime
Research Institute

PHYSICAL DAMAGE VIA NETWORKS

- Stuxnet underlined again that the impact of a network attacks does not need to limited to hindering data transmissions
- Various possible threat scenarios of attacks against targets that are more difficult to protect than critical infrastructure
- Recovery of hardware failure of hard drives can go along significant costs

Picture removed in print version
Bild zur Druckoptimierung entfernt

Hard Drive

Average cost of logical recover is $400 to $600, average cost of physical recovery is $1,200 - $2,000 and up to $15,000 for complex systems.

Technology News

Cybercrime
Research Institute

AUTOMATE

- Computer and Networks enable offenders to automate attacks
- Within minutes millions of spam mails can be send out without generating high costs - sending out one million regular letters would be very expensive and take days
- The fact that millions of approaches to illegally enter a computer system are detected every day is not a result of the high number of offenders but the ability to automate attacks

Picture removed in print version
Bild zur Druckoptimierung entfernt

WWW.HACKERWATCH.COM

Cybercrime
Research Institute

AUTOMATE

- Another example for the use of automation is SPAM
- Currently between 60% and 90% of all e-mails are SPAM
- Several billion SPAM e-mails are sent every single day
- Can only work on the basis of automation

Picture removed in print version
Bild zur Druckoptimierung entfernt

NORTON CYBERCRIME INDEX

Cybercrime
Research Institute

AUTOMATE

- Automation enables offenders to generate high profit by committing various offences with rather small amounts each
- Background: Victims that have just lost rather small amounts tend not to report the crime

Picture removed in print version
Bild zur Druckoptimierung entfernt

Reporting

Cybercrime
Research Institute

UNCERTAINTY REGARDING EXTENT

- Lack of reporting leads to uncertainty with regard to the extent of crime
- This is especially relevant with regard to the involvement of organized crime
- Available information from the crime statistics therefore not necessary reflect the real extent of crime

The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform 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.

HEISE NEWS 27.10.2007

Cybercrime
Research Institute

RESOURCES

- Current analysis indicate that up to a quarter of all private computer connected to the internet could be used by criminals as they belong to “botnets”

  Souce: BBC report “Criminals 'may overwhelm the web“

- Despite the fact that the estimation is not based on a scientifically reliable basis the growing size of detected botnets highlight the challenge

- Debate about legal response just started

Picture removed in print version
Bild zur Druckoptimierung entfernt

WWW.SHADOWSERVER.ORG

Cybercrime
Research Institute

RESOURCES

- Critical mass is already reached

- Attacks in the context of the Wikileaks discussion highlight that a relatively small number of people can affect large businesses

- This underlines the threat level

Cybercrime
Research Institute

CONSIDERATION

- With regard to Internet-related attacks the most powerful resources are not necessary under control of state, military and law enforcement
- Debate about continuing attacks against government computer systems and the inability of states to control secret information published online underlines this

Cybercrime
Research Institute

BOTNET

- Short term for Robot-Network
- Botnets are very powerful instruments
- Main use: SPAM, DoS
- Computers are in most cases infected by malicious software
- Software is taking over part of the control

Picture removed in print version
Bild zur Druckoptimierung entfernt
BACKGROUND: BOTNET

Cybercrime
Research Institute

ANONYMOUS COMMUNICATION

- People using Internet tend to feel unobserved ("felt anonymity") which – due to the storage of user and traffic data is often not the case
- But there is technology available that can hinder law enforcement to trace back the route of an offender
- Ongoing debate about the benefit of anonymous communication vs. effective law enforcement

Picture removed in print version
Bild zur Druckoptimierung entfernt

WWW.ANONYMIZER.COM

Cybercrime
Research Institute

ANONYMOUS COMMUNICATION

- Another possibility to enable anonymous communication is the use of specialised services
- Example: Remailer, that enable the sender to submit e-mails without appearing as sender
- Anonymous communication services that enable the user to access websites without leaving traces

Picture removed in print version
Bild zur Druckoptimierung entfernt

WWW.TORPROJECT.ORG

Cybercrime
Research Institute

ENCRYPTION

- 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

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE PGP

Cybercrime
Research Institute

GLOBAL PHENOMENON

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

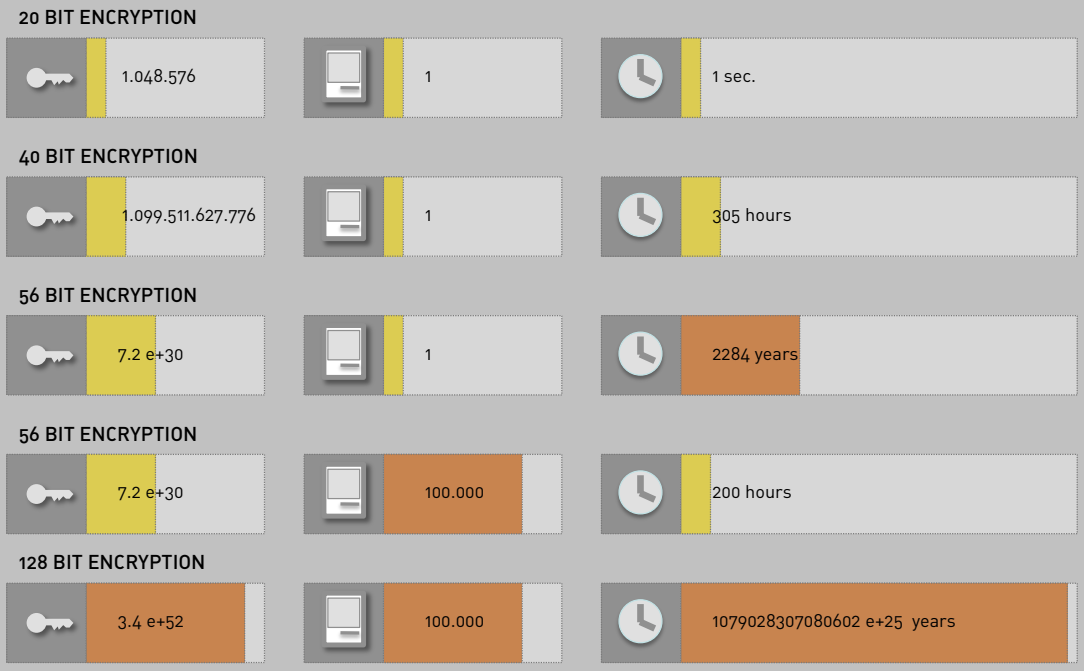
Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE BITLOCKER

BREAKING 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 in order to decrypt a message
- Gaps in the encryption software
- Dictionary-based attack
- Social Engineering
- Classic search for hints

- Need for legislative approaches?



FURTHER INFORMATION

- Further information about EU legislation on Cybercrime can be found in the 225-page publication "Understanding Cybercrime: A Guide for Developing Countries" that is available free of charge in all UN languages:

  http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html

- 3rd Edition (520 pages) will be available shortly

Cybercrime Research Institute
Prof. Dr. Marco Gercke

Niehler Str. 35
D-50733 Cologne, Germany
gercke@cybercrime.de
www.cybercrime-institute.com