Cybercrime

Vaclav Stupka

Content

- What is cybercrime?
- Specific attacks/offenses.
- National, EU, international law.
- Convention on Cybercrime
  - Substantive law
  - Procedural law
- Cybercrime vs. cyber security

What is cybercrime?

Cybercrime

- There are many definitions.
- Broadly: Any crime that somehow involves computer(s) or network(s).

Categories of cybercrime

- Stricto sensu: Offenses against confidentiality, integrity and/or availability of computer systems and networks.
- Also: “Traditional” offenses committed using information and communication technologies.
- And: Any offense, in which are these technologies involved.

What is not cybercrime?

- Unwanted activities which are not considered a criminal offense.
- May be punishable in other ways.
- Usually for example:
  - Spam
  - Cyber squatting
  - Etc.

Specifics of cybercrime

- Exploits some properties of information and communication technologies:
  - Global availability
  - Speed
  - Anonymity
  - Availability
  - Asymetry between “attackers” and “defenders”

Specific offenses

Hacking

- Exploiting vulnerabilities of computer systems and networks in order to access the computer system, data or data transfer.
- Cybercrime stricto sensu.
- Usually two conditions:
  - Infringing security measures
  - Illegal access
- These activities may also be done legally: white hats, pentesting

Dissemination of malware

- Many forms of malware:
  - Viruses,
  - Trojan horses,
  - Spyware,
  - Keyloggers,
  - Adware,
  - Etc.
- Qualification depends on specific form.

Botnet creation and control

- Network of zombie computers
- Used for:
  - Mining of data
  - Use of great capacity computing resources – mining
  - DDoS

DDoS

- Denial of service
- Botnet
- Is it criminal offense?
- Difficult investigation.

Sniffing

- Hardware or software used to analyze network traffic in order to get specific data (usually access information)
- Man in the middle attack

Phishing

- masquerading as a trustworthy entity in an electronic communication
- to obtain sensitive information (login information, credit card details)

Content related offenses

- Pornography
- Hate speech
- Racist or xenofobic messages
- Defamation

Copyright infringement

- What is legal, what is offense?
- Sharing is caring
- DRM
- Links, embedding
- Fair use
- P2P

Racketeering

- Malware that encrypts your data
- You are asked to pay in order to receive decryption key

Many others

- Cyber war
- Hacktivism
- Cyber murder
- Etc.

The law

National laws

- Big differences in national legislation
- Some activities are in one country crimes and in other country aren’t
- Cross border nature of cybercrimes
- Need for harmonization

EU

- Directive on attacks against information systems - 2013/40/EU
- Harmonization effort on EU level
- Offenses:
  - Illegal access
  - System and data interference
  - Illegal interception
  - Tools used for commiting offenses
- No procedural provisions

International

- Convention on cybercrime
- Procedural and substantive provisions
- Definition of terms, jurisdiction, international cooperation

Convention on cybercrime

About

- Council of Europe
- 2001
- Signatories: 50
- Ratifications: 47

Offenses (COC)

- Illegal access (accessing of computer system or its part. Optional: infringing security measures, intent of obtaining data, etc.)
- Illegal interception (of non public transmission of computer data, technical means. Recording or using of the data in not required. Optional: dishonest intent, connected systems)
- Data interference (Damaging, deletion, deterioration, alteration or suppression of computer data. Optional: serious harm)
- System interference (Hindering of functioning of computer system)
- Misuse of devices (Possession, production sale, procurement, distribution of a device or password with intent to use it to commit crime. Optional: number of items)

Offenses (COC)

- Computer-related forgery (alteration of data, resulting in inauthentic data with the intent to force someone to think it was authentic. Optional: intent to defraud)
- Computer-related fraud (Causing loss of property by alteration of data, dishonest intent, intent to procure economic benefit)
- Child pornography (production, making available, posession etc. Optional: procuring and possession)
- Copyright infringement (infringement of copyright or related rights. Optional: limited circumstances, damage)

Jurisdiction

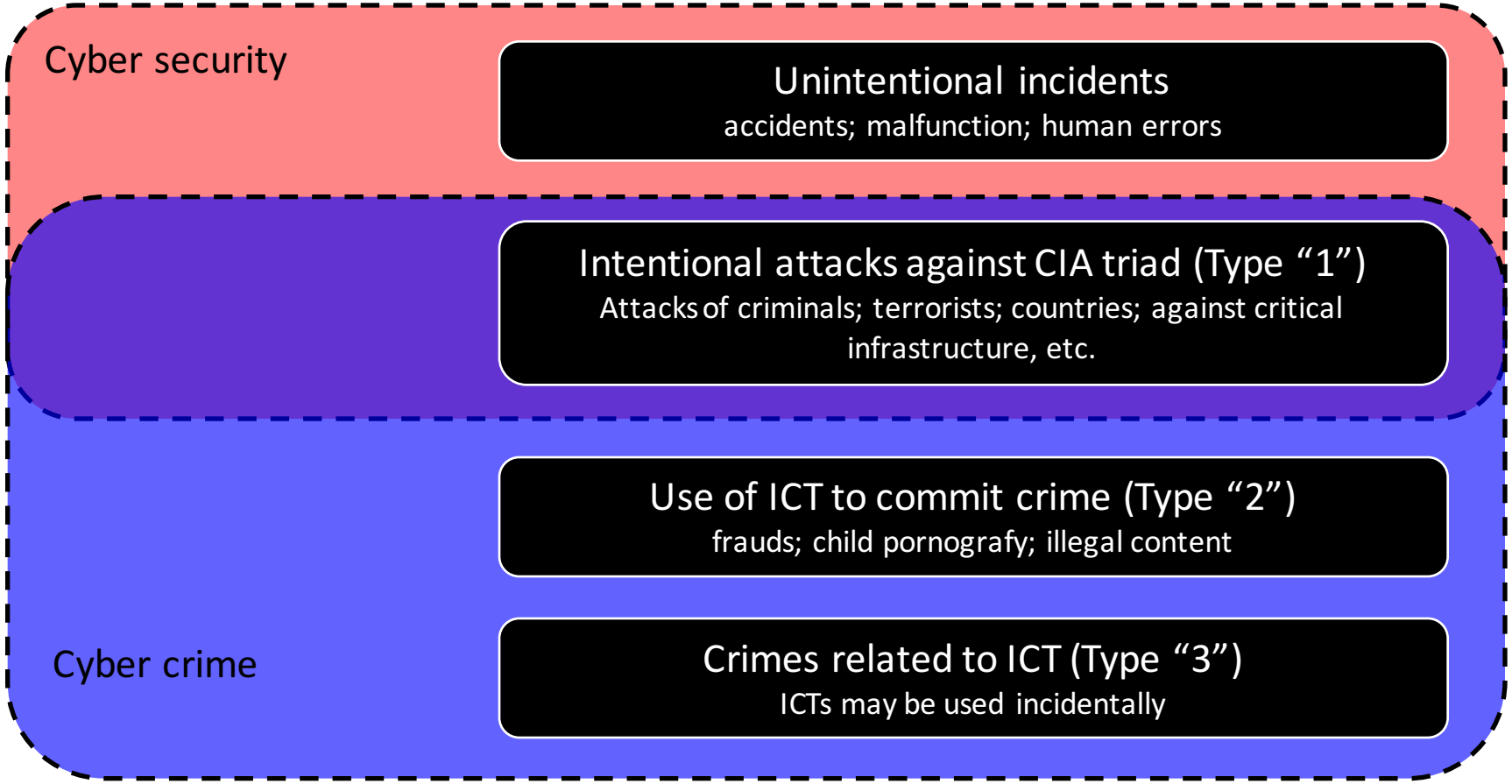
- Where the offence was committed
- By whom
- Location of offence
- Location of result
- Consultations – 24/7 network

Procedural measures (COC)

- Production order (to get data, subscriber info. Limit: allready existing data)
- Search and seisure (search systems and data, seisure of data, ordering operator to cooperate)
- Interception (collection of traffic data, content data)

Cybercrime vs. cyber security

What they focus on



The goal

- Cybercrime: to catch the offender, to punish him
- Cyber security: to protect the system, to make sure it is working safely

Thank you for your attention

vaclav.stupka@law.muni.cz