Cybersecurity

Jakub Harašta

Buzzwords

- Cybersecurity
- Cybercrime
- Cyberterrorism
- Cyberwarfare
- Hacktivism
- Cyber espionage

Wait, there‘s more…

- International incident sharing
- Due diligence for states and individuals
- Cyber as use of force under UN Charter
- Cyber as trigger for Art 5 of NATO treaty
- Cyberdeterrence
- NCW/RMA/6th domain
- Active Cyber Defence
- Standardisation (ISO/NIST)
- Securitization vs. Security

Information Society

- Not new – just better
- Availability – ICT dependency

Information Society II

- Changes
  - Commerce
  - Social life
  - Education
  - Entertainment
  - Government
  - Geography
  - Threats!

Cyber Security

- CIA
  - Confidentiality
  - Integrity
  - Availability
- Alternative concepts
  - Parkerian Hexade
    - confidentiality, possession or control, integrity, authenticity, availability, utility

Confidentiality

- Unauthorized cannot access
  - Authentication – who are you?
    - Knowing, having, being…
  - Authorization – can you do that?

- Perfect situation:
  - Computer minus Internet plus finite list of users plus heavy encryption
    - So…

Integrity

- Preventing change of data
  - Authentication
  - Authorization
  - Nonrepudiation
- Every change has to be listed with possible recovery

Availability

- You need it?
  - Up and running

Or…

- Violation of obligation
  - Non-reporting, updating
  - Private
- Cyber crime
  - Criminal
- Cyber Terrorism
  - Non-state actors
- Cyber Warfare
  - State actors

So far

- Duping the Soviets
  - 80s?
- Estonia 2007
  - DDoS, solely cyberspace
- Georgia 2008
  - DDoS in war, cyberspace within conventional
- Stuxnet
  - APT, sophisticated, air gap
- Red October
  - Espionage
- Anonymous
  - Hacktivism
- Sony 2011
  - More than 75 million accounts stolen

Cyber Security

- Prevention
- Reaction
- Investigation

Prevention

- Standards (ISO, NIST)
- Security policy
- Security proceedings
- Evaluation/re-evaluation

- GET READY!

Reaction

- People and institutions
  - CERTs

- FIX IT and WARN!

Investigation

- Either outside the scope…
  - Police
- …or back to prevention.
  - What happened and how do we prevent it from happening again?

- WHO and HOW?

Legislation

- Act No. 181/2014 Sb. (CZ)
- COM 2013/48 Proposal for a directive concerning measures to ensure a high common level of network and information security across the Union (EU)

But also…

- Discussion
- Education
  - banka123
  - nbu123

CySec != InfoSec

- Information Security
  - China, Russia
  - Content
  - Also offline

But…

- NATO talk
  - Cyber defense
- EU talk
  - Network and information security
    - What did I just say?
  - ICT security

International Cooperation

- Estonia 2007 – CCD COE (NATO)
  - Tallinn Manual (Schmitt et al.)
  - Tallinn Manual 2.0
  - EU reaction?
- ENISA (EU)
- ICRC
- UN: ITU - IMPACT

Czech legislation

- Main issues:
  - What‘s the point of having a legislation constantly challenged?
  - Proportionality
    - Distributive and non-distributive rights

Who is obliged?

- Critical infrastructure operators
  - Critical information infrastructure
  - Critical communication infrastructure
- Significant information systems
- Significant networks
- Provider of electronic communication services

Basic obligations

- Contact information
- Detection of cyber incidents
- Reporting of cyber incidents
- Security documentation
- NSA CZ