Cyber Defence and Critical Infrastructure Protection

… or …

Why it is vital to include Cyber Defence into education when it comes to Critical Infrastructure Protection

LtCol Téczely Béla
C4I Advisor
NATO Representation
NATO Liasion Office

Critical Infrastructure (CI) or Critical Information Infrastructure (CII)?

- Latest trends and changes initiated by the Internet of Things (IoT)
- Example:
  - Bridges, towers and other constructions with built-in sensors and other devices;
  - Power lines with remote measurement devices;
  - Natural gas, oil and fuel pipelines;
  - Roads/motorways with cameras and sensors (embedded into the asphalt);
  - Air Traffic Control systems and their extensions;
  - Sites, industrial plants, bases, warehouses with remote observation devices and management systems;
  - Etc., etc., etc…
- General CI – nowadays maybe only the internal water routes…
- **Everything else can be considered as CII !!!**

Rationale behind the trend, why it could happen?

- The IT devices getting cheaper and cheaper;
- The IT devices getting more and more sophisticated;
- As distinct from the manpower, the remote sensors and other devices work 24/7, 365 days, all the time, regardless the weather and other conditions;
- The manpower should be saved for those tasks where the human presence is inevitable (typically: for decision making on actions);
- The sensivity and definition/resolution of the IT devices can be much higher than the humans';
- These devices work objectively, no subjective effects exist;
- The newly introduced IPv6 protocol (introduced 6 June 2012) supports this incredible amount of independent devices.

Beneficial effects of IoT to Critical Infrastructure

- A 24/7, 365 day, continuous observation and control can be easily accomplished;
- Some parameters can (and ARE) controlled by automated means;
- The gadgets can provide information from not accessible for humans or highly dangerous places (e.g. high-voltage power lines, inside of a nuclear reactor, etc.);
- Changes can be detected immediately, events and tendencies can be observed and registered automatically.
- Statistics can be made of the measurements to prepare an action or a decision;
- Thanks to mature technological processes, these devices are precise and reliable;
- Thanks to the mass production, they’re cheap.

Dangers caused by IoT to Critical Infrastructure

- Since the vast majority of these devices communicate on public channels, the transmitted information can be intercepted, stolen and the data might be misused;
- For the same reason, the transmitted information can be tampered/faked;
- If the backward (control) channel is hacked, the CI can be damaged or even completely destroyed from a distance;
- Also, some CI elements with overtaken remote control can be used as weapons of mass destruction!!!

Some deterring examples

Some (un)famous cyber attacks …

- 1998-99, Moonlight Maze, USA. Attacker: Russia
- 2003-06, Titan Rain, USA. Attacker: China
- 2007, Estonian government and banks. Attacker: Russia
- 2008, AT&T, USA. Attacker: Philippines

… and some examples when CI was attacked by cyber means …

- 1982, Siberian natural gas pipeline. Attacker: CIA by a „Trojan horse”
- 2003 (14 August) US Northeast, blackout. Caused reportedly by software bug, actually by a cyber attack
- 2005 (7 July), London underground explosion. Attackers: Moslim extremists.
- 2009-10, Iran, sabotage the nuclear power program by Stuxnet virus. Attackers: USA, Israel
- 2015 (23 December), Ivano-Frankivsk, Ukraine. Regional power grid brought down. Attacker: Russia (?) with „Black Energy”.
- 2015, British Railways. At least four times the trains and the infrastructure were attacked during the year.
- 2016-17 (?), USA Power grid – not only possible but likely!!!

Standard measures to protect Critical Infrastructure

EU

Critical Infrastructure Warning Information Network – CIWIN

European Network and Information Security Agency – ENISA

Critical Information Infrastructure Research Coordination – CI2RCO

International organizations in Europe

International Watch and Warning Network – IWWN

Task Force on Computer Security and Incident Response Team – TFCSIRT

Forum of Incident Response Teams – FIRST

European Governmental CERTs – EGC

…

Types of Critical Information Infrastructure

Functional CII

Physically enable the smooth functioning of the information functions of the society. Otherwise, they provide basic information services on infrastructural base.

Supportive CII

They create and continuously provide the necessary material and intellectual base and support background to operate and develop the huge mass of functional information infrastructures.

Security Domains where CI should be protected

- Physical;
- Personal;
- Electronic;
- Administrative;
- **Cyber!!!**

Security Domains to be educated in connection with CIP

- Physical;
- Personal;
- Electronic;
- Administrative;
- **Cyber!!!**

What should be included into the education programme in the cyber domain for CIP?

- **General issues:**
  - The connection between the different security domains;
  - The necessity for cyber protection of CI/CII (why it need to be studied);

What should be included into the education programme in the cyber domain for CIP?

- **Subject-specific and case-specific issues (linked to a certain CI/CII):**
  - Functions of the structure
  - Key (real) IT elements of the structure
  - Specialities of the structure from Cyber perspective
  - Vulnerabilities and the way to exclude them
  - Standard Operational Procedures to accommodate Cyber Security
  - Processing the lessions learned from similar structures
  - Possible/probable cyber attacks and their possible impact to the structure
  - Compulsory and recommended protective measures
  - Catastrophy recovery plan and its rehersal. VITAL!!!

Aims to achieve

- From organizational point of view:
  - Cyber situational awareness
  - Well trained personnel
  - Well known and regularly rehearsed catastrophy plans

- From general point of view (similarly to INFOSEC):
  - CI security
  - CI availability
  - Business continuity
  - Authenticity (of the transmitted information)
  - …

ПИТАННЯ?

KÉRDÉSEK?

FRAGEN?

QUESTIONS?

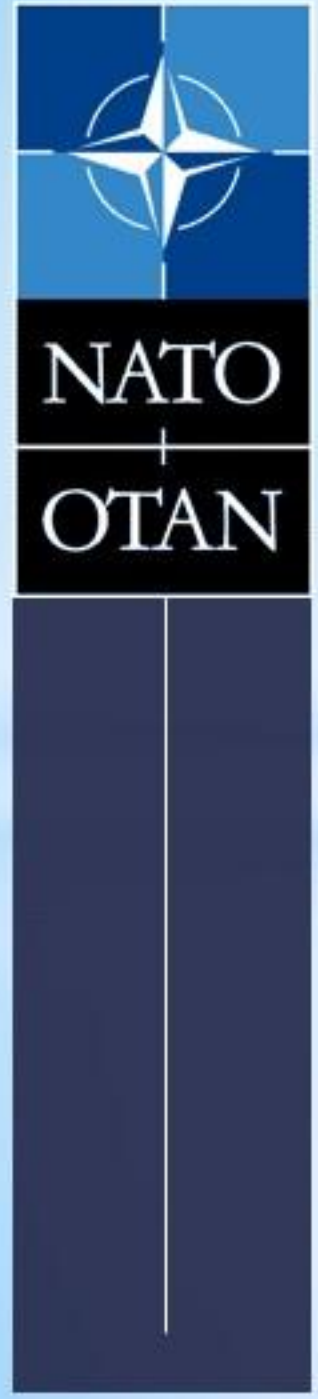
¿PREGUNTAS?

ВОПРОСЫ?

Téczely Béla

Phone: +38 050 317 6166

Email: teczely@nloukraine.org



Thank you for your attention.