Securing Critical Infrastructure

MVV60K Cybersecurity Law

Jakub HARAŠTA

Introduction

- Complex issue on the intersection of policy, politics, technology, law, culture etc.
- Objects vs. processes
- Procedure

Definitions

Infrastructure

- Roads, bridges, water supply, sewers, oil supply, energy grid

- Take time to watch *„Infrastructure: Last Week Tonight with John Oliver (HBO)“* on YouTube

Critical Infrastructure

- *„[a]ssets that are essential for the functioning of a society and economy.“* (Wiki)

- Critical infrastructure vs. Infrastructure?
  - Time / circumstances

Critical Infrastructure (law) - US

- Patriot Act of 2001 – 42 USC 5195c(e):

  „Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.“

(**consequence-oriented** definition of criticality)

Critical Infrastructure (policy) - US

- Critical Infrastructure is essential to *„economy, security, and way of life“* (The White House, The National Strategy to Secure Cyberspace, 2003)

Critical Infrastructure (policy) - EU

- Proposal for a Council Framework Decision on Combatting Terrorism, COM2001 521 final (EC, 2001):

  Attack on critical infrastructure is „*causing extensive destruction of a Government of public facility, a transport system, an infrastructure facility, including information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or results in major economic loss.*“

  (note the distinction between **income-generating** and **non-income-generating** objects)

Critical Infrastructure (policy) - EU II

- Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the fight against terrorism, COM2004 702 final (EC, 2004)

  Critical Infrastructure is defined as „*those physical resource services, and information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or effective functioning of governments.*“

Critical Infrastructure (law) - EU

- Directive 2008/114/EC:
  - Distinction between Critical Infrastructure and EU Critical Infrastructure
  - Critical Infrastructure „*means an asset, system or part of thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or descturction of which would have a significant impact in a Member States as a results of the failure to maintain those functions.*“
  - EU Critical Infrastructure is „*critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effect resulting from cross-sector dependencies on other types of infrastructure.*“
  - Per principles of the EU Law, national CI is out of the scope

Criticality

Why ‚critical‘?

- What is labelled as critical matters, because of:
  - Resources
  - Attention
  - Oversight
  - Procurement

Resources

- Not enough money
  - Gaps between what is needed and what is provided in billions of USD in virtually every single country
- Policy-setting, legal definitions, critical infrastructure – allocation of resources
- What kind of resources?
  - Money, personnel, intelligence agencies (threat monitoring) …

Attention

- What is ‚critical‘ is ‚important‘.
- If ‚important‘ does not work, it is an issue.

- Media coverage, opposition parties, mobilisation potential for voters etc.

- Exercises / preparation

Oversight

- Often private owners
- Originally public monopols, then liberalisation
  - Tragedy of ‚commons' (UK railway system)
- If CI, then requirements!
- Proportionality issue

Procurement

- Easy procurement procedure in case of disaster/emergency response

- Difficult procurement procedure in case of technology acquisition
  - E.g. Huawei/ZTE

Broad (Strategic) and Narrow (Operative)

Broad Definition

- Anything can be critical infrastructure, if it is important etc.

- In the past, CI often physical, clearly delineated and entrenched – physical security
- Shift to holistic approach after 9/11 (Pursiainen, 2009)

- Function, consequence – critical proces?

Operative procedures

- From broad norm (what is critical infrastru
  application (is this critical infrastructure?)

- New definitions, but old mindset.

- Critical procedures symbolised by critical assets.

- What is critical infrastructure in delivery of drinking water?
- What is the difference between CZ and Israel?

Operative Guidelines (CZ)

- Framed by 432/2010 Sb.
- Some sectors are critical
  - Energy, Water management, food industry and agriculture, health services, transport, communication and information systems, financial market and currency, emergency services and public administration
- Something in sectors is critical (sector criteria)
- If something happens to an asset, and consequences reach certain gravity, it is critical (cross-cutting criteria)
- Fun fact: hospitals are critical if they have at least 2500 beds

Interdependence

- Broad definition – accounts for interdependencies

- Operative guidelines – not so much…
  - Assets represent processes that we would like to maintain, therefore assets are critical

Types of interdependencies (Rinaldi 2001)

- Physical Connection
  - Power plants require coal, therefore coal mines may be critical in terms of technology and/or policy, but power plants might be critical in terms of technoloy and/or policy and/or law
- Cyber connection
  - Status depends on information transmitted through information infrastructure
- Geographic connection
  - Proximity (environmental event can lead to state changes in all of them)
- Logical Proximity
  - Human decision-making; variable in one infrastructure affects different infrastructure

Cyber interdependence

- Czech legislation:
  - If cyber affects critical infrastructure asset, it is critical (law)

- Why did we choose to regulate this interdependency?
  - Prioritization etc.

Conclusion

- Infrastructure
- Critical Infrastructure

- Criticality in law/policy/technology (simulations)
  - Hypes and issues

- Highly Complex

- Who should decide on what is critical? Policy-makers, politicians, lawyers or computer/system scientists?

References

- C. Pursiainen, The challenges for European critical infrastructure protection, *Journal of European Integration,* vol. 316, pp. 721–739, 2009.
- S. Rinaldi, J. Peerenboom and T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems* vol. 216, pp. 11–25, 2001.

Thank you for your attention.

Feel free to contact me at

jakub.harasta@law.muni.cz