KU LEUVEN CiTiP

CENTRE FOR IT & IP LAW

imec

The Cybersecurity of airports and ports under the proposed NIS2 and CER Directives

Dr Maja Nišević
Maria Avramidou

Contents

- Introduction
  - EU and Critical infrastructures (CIs)
  - Types and motives for cyberattacks on CIs
  - Airports and ports in context of the CIs
- NIS2 Directive proposal
- CER Directive proposal
- Conclusion

EU and CIs

- ***Cyberspace is "the collection of computing devices connected by networks, in which electronic information is stored and utilized, and communication takes place". Rantapelkonen and Kantola (2013, p.25)***
- CIs: an asset, system or part 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 destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions
- The EU CIs Protection: among others includes ensuring the resilience of transportation infrastructures (e.g., airports, ports)
- The EU legal framework for CIs:
  - Central pillars- Directive 2008/114 (EU CIs Directive) (establishes a procedure for identifying and designating ECIs in the transport and energy sectors with the focus on enhancing the security of physical assets against threats such as terrorism and other intentional and unintentional man-made threats, as well as natural disasters)
  - NIS Directive (focus on the security of network and information systems against cyberthreats)

  Important: Different EU Commission reports on Directive 2008/114 : in 2012 12 (SWD(2012) 190), and in 2017 (SWD(2017) 278)

  Consequence: The Commission presented a new proposal for a Directive on the resilience of critical entities (CER) together with NIS2

Aim: ensuring full coherence; cyber-resilience obligations under NIS2 would apply also to critical entities identified under the new proposal

Types and motives for cyberattacks on CIs

Five basic types of cyberthreats:

- hacktivism
- cyber criminality
- cyberespionage
- cyberterrorism and
- cyberwar
- ***Problem:*** each of them has their individual features relating to actors involved, as well as motivations and objectives behind actions

The diversity of motives:

- excitement
- money
- political agendas (including competition)
- ***Problem:*** possibility to materialize cyber attack (i.e., the number of cyberattacks have shown a year-by-year increase, causing substantial financial losses to society in general and business in particular)
- ***Consequence: cybersecurity a*****s a top-level priority among policymakers, businesses, scholars and individual persons**

Examples of cyberattacks against airports and ports

Airports

- **DDoS attack** on an airline leaves 1,400 passengers stranded at **Warsaw airport** (2015)
- **Boryspil airport** in Kiev, twice victim of attacks against Ukraine (2016 and 2017)
- **A flaw in an Air Canada mobile app** exposes 20,000 customers (2018)
- **British Airways** suffers massive customer data leak by **hijacking the traffic** of thousands of customers who believed they were connecting to the official British Airways website (2018)
- **Cathay Airways security flaws** exploited for malicious purposes (2018)
- **IT supplier in the airport** industry falls victim to a cyberattack - cybercriminals' targets were servers hosting the data of airlines' customers (2021)

Ports

- **Antwerp: malware infiltrates** (2011)
- **Rotterdam: collateral damage from a large-scale contagion** (2017)
- **Long Beach: information system contaminated by ransomware** - the start of a series of international attacks (2018)
- **Barcelona: internal IT systems contaminated** (2018)
- **San Diego: ransomware attack** - a highly sophisticated cyberattack- "temporary impacts on service to the public e.g., park permits, public records requests and business services (2018)
- **Vancouver: DDoS attack** 225,000 user accounts were probed (2018)
- **Langsten: ransomware attack** making system's response slower (2020)
- **Shahid Rajaee**: a cyberattack amidst geopolitical conflict (2020)
- **Kennewick**: ransomware attack – Size is not everything (2020)
- **Houston**: hackers exploit a software flaw (2021)

Airports and ports as CIs

Airports:

- Liberalization of the internal market for aviation in the late 1990s boosted the competitiveness of the aviation sector in the EU

New services, new players, a new organization of air services and broader access to air transport

- ***Commercial aircraft as a Cis: In 2019 number of air passengers was around 1.146,44 million, and in the EU, there are around 2581 active airports across the cities of EU MS (data available at www.statista.com)***

Ports:

- The ports directly impact connectivity across Europe, enabling the connection of islands and isolated areas
- A significant proportion of economic activities are occurred in the ports, mainly through the transfer of goods
- ***Through the EU ports 74% of goods entering or leaving Europe go by sea and around 90% of EU external trade and more than 43% of the internal trade take place via maritime routes, while the gross weight of seaborne goods handled in EU reached in 2014 (data available at https://ec.europa.eu/Eurostat)***

- The ports are considered as vulnerable infrastructure mainly due to their proximity to the sea and the problems faced in controlling the threats coming through it, the number of operations taking place in the ports and their different nature, and the considerable number of people working or involved in several operations in the ports

Airports and ports:

- A part of transportation infrastructures (transport of people and goods)
- A part of transportation infrastructures considered as Critical infrastructure as indicated in the EU Directive 114/2008 since they can be affected by cyberattacks
- Essential for the European economy as a global player and the internal market

Aim of protection of airports and ports: Physical and Cyber security of the network should guarantee Privacy Integration Protocols for the users, transactions and data exchange

NIS2 Directive proposal

- NIS Directive as sector-specific CI protection initiatives (security of network and information systems)
- NIS2 Directive as the new Commission proposal aiming in addressing the deficiencies of the NIS Directive, to adapt it to the current needs and make it future-proof
  - It modernizes the existing legal framework taking account of the increased digitization of the internal market in recent years and an evolving cybersecurity threat landscape.
  - It introduces measures related to cybersecurity and obliges Member States to adopt a national strategy for the security of networks and information systems.

Challenges that arise for ports and airports from the NIS2

Challenge 1: Incident notification – Unclarity of the term of "at least equivalent"

Challenge 2: Unclear how the medium and large companies' size-cap for entities that should be subjected to the NIS2 **will be translated to port and airport managing bodies**, and which port and airport managing bodies would be considered smaller entities with a high security risk profile

Some recommendations:

- Development of Guidelines indicating which elements are important to determine which obligations are "at least equivalent" to the ones enshrined in NIS2
- Development of Guidelines facilitating the designation/translation of the size cap of the NIS2 to the port and airport context

CER Directive proposal

- This proposal reflects the priorities of the Commission's EU Security Union Strategy for:
  - a revised approach to critical infrastructure resilience that better reflects the current and anticipated future risk landscape
  - the increasingly tight interdependencies between different sectors, and also
  - the increasingly interdependent relationships between physical and digital infrastructures.

EU Commission impact assessment → replacement of the ECI Directive with a new instrument (i.e., CER) aimed at enhancing the resilience of critical entities in the sectors considered as essential by the proposed NIS2 Directive

- The CER will have a **much wider sectoral scope** (compared to its predecessor) covering ten sectors:

Energy	Transport	Banking	Financial Market Infrastructure	Health
Drinking water	Waste water	Digital Infrastructure	Public Administration	Space

Core elements of the CER Directive proposal

- provides a **procedure for EU countries to identify critical entities based on a national risk assessment**

- **lays down obligations for Member States to take certain measures** aimed at **ensuring the provision in the internal market of services essential for the maintenance of vital societal functions** or economic activities, in particular to **identify critical entities and entities to be treated as equivalent in certain respects**, and to **enable them to meet their obligations**

- establishes **obligations** for critical entities aimed at **enhancing their resilience and improving their ability to provide those services in the internal market**

- establishes **rules on supervision and enforcement of critical entities**, and specific **oversight of critical entities** considered to be of particular European significance

NIS2	CER
Identified based on the size of the operators	Operators designated by member states
Essential entities	Critical entities
Energy	Energy
Health	Health
Transport: including airports and ports	Transport: including airports and ports
Banks	Banks
Financial market infrastructure	Financial market infrastructure
Drinking water	Drinking water
Waste water	Wastewater
Digital infrastructure	Digital infrastructure
Space	Space
Public administration	Public administration
Important entities	-
Postal and courier services	
Waste management	
Chemicals	
Food	
Manufacturing	
Digital providers	

Conclusion

- Open issue: protection of CIs in the EU
  - To effectively protect the CIs the reduction of vulnerabilities of CIs in the European Union is essential
  - Entities providing essential services must be able to resist, absorb, accommodate to and recover from incidents that can lead to serious disruptions

Conclusion: The current framework on CIs protection is not sufficient to address the challenges we are facing (i.e., the risk landscape is becoming more and more complex, operators are confronted with challenges in integrating new technologies and become increasingly reliant on one another)

Consequence: need for fundamental switch from the current approach of protecting **specific assets** towards reinforcing the resilience of the **critical entities that operate them**

✓The CER and NIS2 constitute a considerable change as compared to the EU ECI Directive and NIS

Conclusion

- NIS2 Directive provides for a **more comprehensive coverage of sectors and services:**
  - In addition to the sectors already covered under the NIS Directive (i.e., energy, transport, banking and financial market infrastructure, health, drinking water, digital infrastructure and certain digital service providers), NIS2 adds **new sectors** (i.e., telecoms, chemicals, food, postal and courier services, certain manufacturing, public administration, social-networking platforms, space, waste management and wastewater management)
  - Instead of the current identification of individual operators at a national level, the proposed rules introduce a **size-cap** to cover, within the selected sectors, all medium and large enterprises as defined under EU law
  - No longer distinguishes between operators of essential services and digital service providers but, instead, NIS 2 classifies entities between **essential and important categories**
  - Broadening the **extra-territorial effect** (in place under the current regime) (i.e., selected providers of digital infrastructure or digital services who do not have a European establishment, but offer services in the EU, will also fall under the scope of the proposed NIS2 Directive)
  - Higher penalties: EU Member States would be required to provide for **administrative fines** up to at least **EUR10 million** or **2% of the total worldwide turnover**
- The CER will have a **much wider sectoral scope** (compared to ECI)**:**
  - Cover ten sectors (i.e., energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, and space)
  - Provides a procedure for EU countries to identify critical entities on the basis of a national risk assessment
  - Sets out obligations on EU countries and the critical entities that they identify that are subject to specific oversight

KU LEUVEN CiTiP

CENTRE FOR IT & IP LAW

imec

Thank you for your attention!
Questions?

Maja, Nišević, maja.nisevic@kuleuven.be
Maria, Avramidou, maria.avramidou@kuleuven.be