The NIS 2.0 Directive – Lessons Learnt or Lagging Behind?

A Legal Perspective

Sandra Schmitz

Luxembourg National Research Fund

UNIVERSITY OF LUXEMBOURG

Agenda

1. **Setting the scenario: Flaws of NIS 1.0**

2. **Selected examples of how NIS 2.0 responds to the legal flaws of NIS 1.0:**
   - **Scope of application**
   - **Security measures and incident reporting**
   - **Supervision and enforcement**

3. **Concluding remarks**

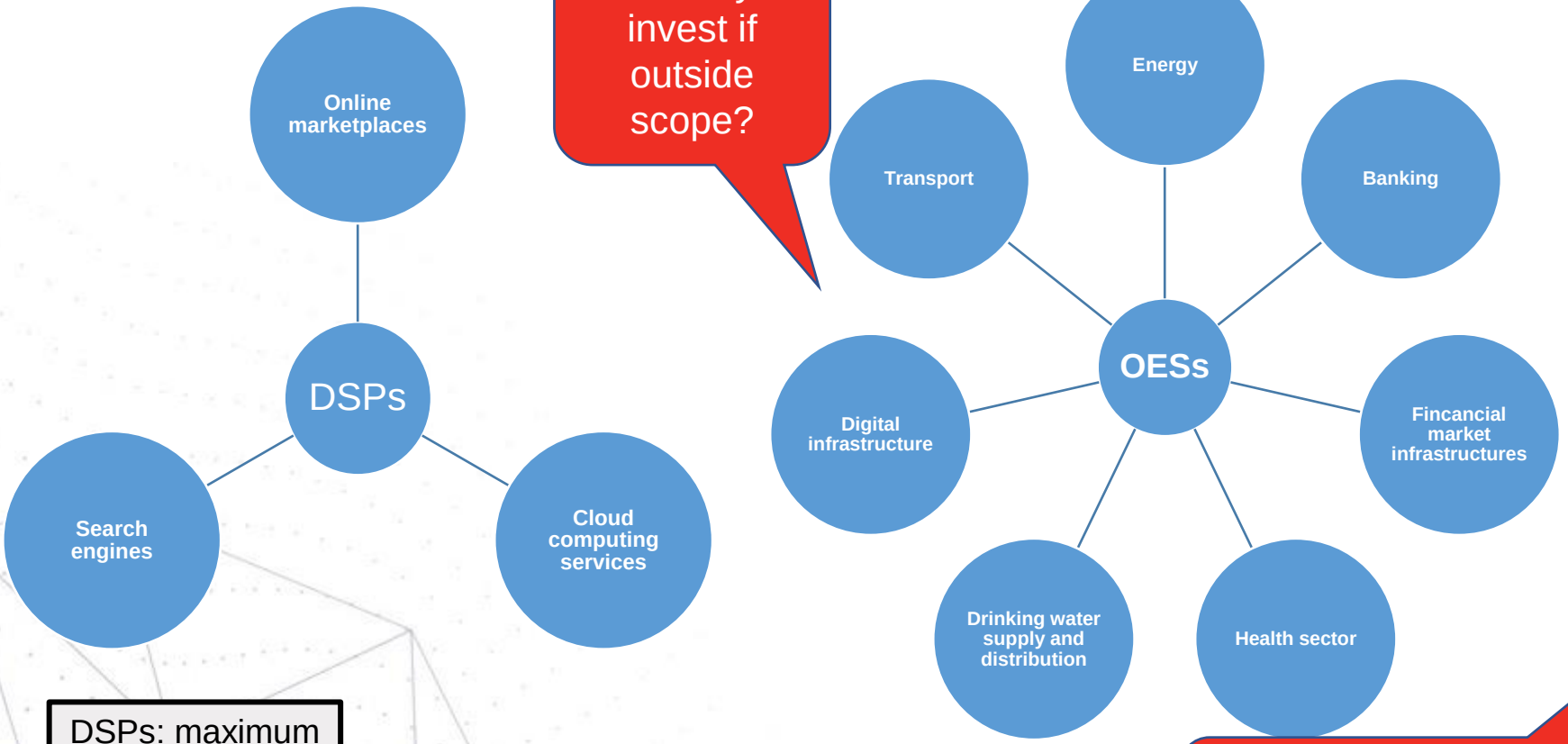
Flaws of NIS 1.0 identified by Commission Review

1. Insufficient level of cyber resilience of businesses operating in the EU
2. **Inconsistent resilience across Member States and sectors**
3. Insufficient common understanding of the main threats and challenges among Member States and lack of joint crisis response

Problems that were considered prominent pre-NISD are still relevant

→ Uneven level of preparedness: fragmented approaches across the Union

Scope of Application: NIS 1.0



Necessity to invest if outside scope?

Broad discretion given to MS to define de facto scope of NISD

OES identification:

- Minimum harmonisation approach
- Designation by national authorities/self-identification
- Variety of approaches (quantitative/qualitative/cross-sectoral thresholds/sector-specific) = inconsistency
- MS also included additional sectors/corresponding sub-sectors
- Number of essential services ranges from 12 to 87 (Ø 35 per MS)

DSPs: maximum harmonisation approach

Distorted competition: companies of same nature may be identified as OES in MS X, as DSP or fall outside scope in MS Y

Negative impact on management of cyberdependencies among MS

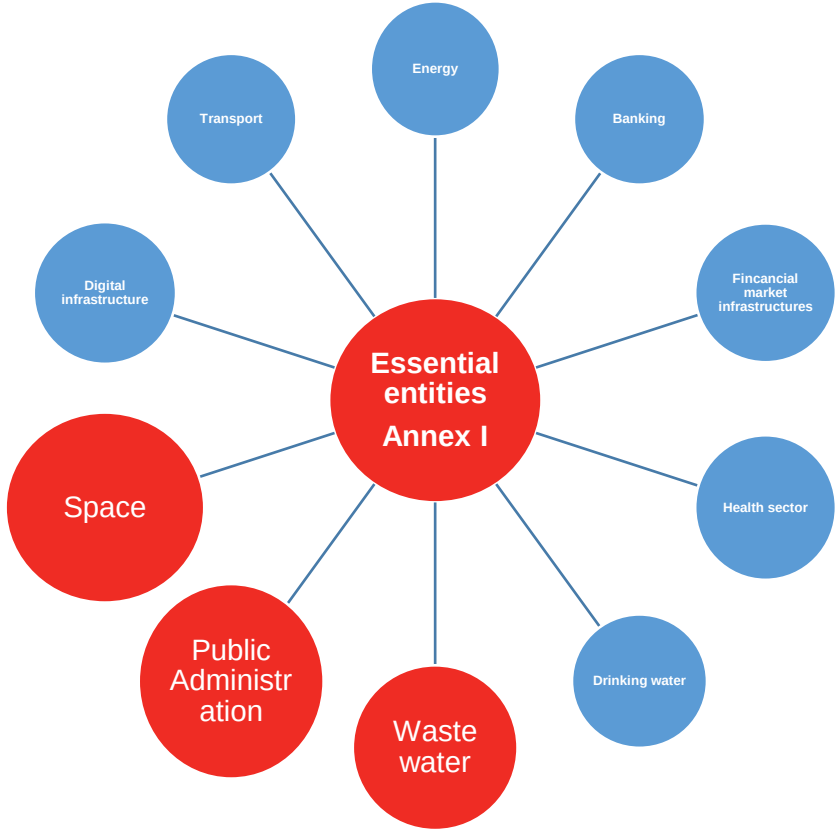
Scope of Application: NIS 2.0

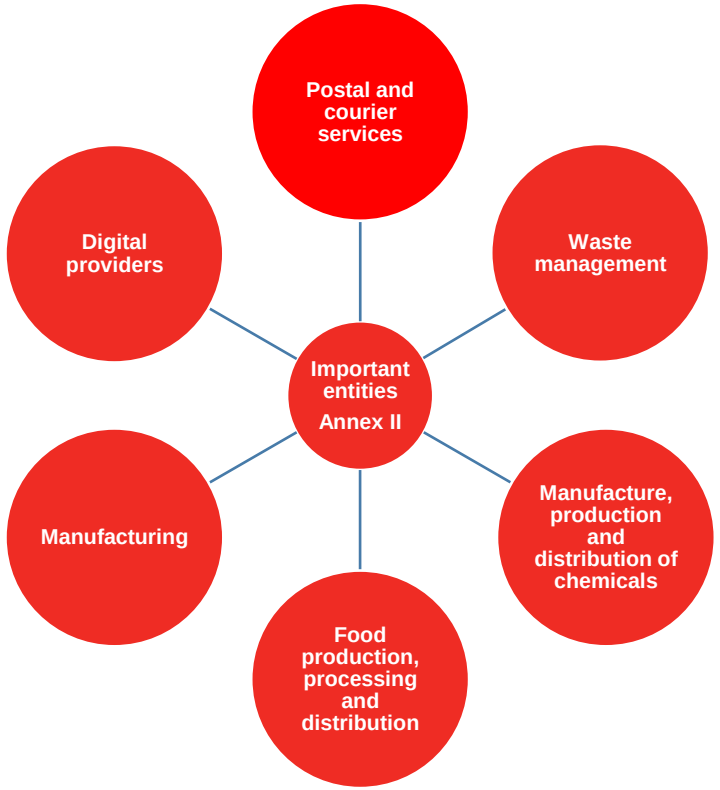
Elimination of distinction between OES and DSP, instead EEs and IEs

BUT: Leaves flexibility to MS to identify smaller entities with a high security risk profile

NIS 2.0 expands scope of NISD:

- new sectors added based on criticality for economy and society
- Clear size-cap rule: all medium and large companies in selected sectors , i.e.
  50+ staff and annual turnover and/or balance sheet exceeds EUR 10M (self-determination)
- Annex include references to EU legislation containing definitions





Significant increase in entities covered: estimate 7-fold

Security requirements and incident notification: NIS 1.0

- Reporting and security requirements vary significantly:

  burden for companies operating in more than one MS

Also direct result of inconsistent identification process of OES

- Arts. 14(1)/Art. 16(1): take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of NIS;

  having regard to the **state of the art**, those measures shall ensure a level of security of NIS appropriate to the risk posed

- In Practice: Misalignment of security requirements:

  some MS made certain security measures mandatory

  - through a regulation, or
  - a standard,
  - while others recommended measures through guideline documents which are recommended to follow (e.g. Germany)

Security Requirements: NIS 2.0

Recital 11, Article 18 and 20 NIS 2.0: all entities are subject to the same security requirements and reporting obligations

- Minimum list of cybersecurity measures that entities have to take to manage the risks posed to their NIS:
  - (i) risk analysis and information system security policies;
  - (ii) incident handling (prevention, detection, and response to incidents);
  - (iii) business continuity and crisis management;
  - (iv) supply chain security;
  - (v) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
  - (vi) testing and auditing; and
  - (vii) the use of cryptography and encryption
- Security measure must consider state of the art (= NIS 1.0), no reference to industrial standards
- MS may require to have certain ICT products, services and processes certified in accordance with cybersecurity certification schemes adopted pursuant to Art. 49 CSA

Reporting obligations: NIS 1.0

- OESs have to report

  ‘incidents having a **significant impact** on the continuity of the essential service they provide’ (Art. 14(3))
- DSPs have to report

  incidents that have ‘**a substantial impact**’ on the provision of a service ‘that they offer within the Union’ (Art. 16(3))
- Thresholds that trigger obligation unclear
- Voluntary reporting is envisaged and encouraged for those outside scope of Directive

Incident = any event having an actual adverse effect on the security of NIS
(Art. 4(7))

Reporting obligations under NIS 1.0 in Practice

- Modalities in terms of time and authorities to report to is different across MS
  - Reporting time varies: ‘without undue delay’/immediately/24 hours with first report required 5 days after incident to 4 weeks
  - Thresholds vary e.g. by sector
    - ➢ LU: regulatory order for sector to determine ‘significance’
    - ➢ DK: sector defines ‘significance‘
    - ➢ FR & DE: reporting obligation extended to incidents that may result in failure/are likely to have a significant impact
- Reporting statistics:
  - 2019 NIS CG summary report: 432 cybersecurity incidents submitted to competent authorities
  - 2020 BSI Annual Report (DE): 419
  - 2020 ANSSI Press Release (FR): 2,287

Variety of sectoral and national approaches challenges common regulatory approach in the EU

Thresholds set too high? Full picture of threat landscape in light of increased dependency on digital technologies?

Reporting obligations: NIS 2.0

- More precise definition of incident: '**any event compromising the availability, authenticity, integrity or confidentiality** of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems'
- Reporting threshold: '**significant impact** on the provision of their services'
  - Art. 20 (3): incident shall be considered significant if

    '(a) the incident **has caused or has the potential** to cause **substantial operational disruption or financial losses** for the entity concerned,

    (b) the incident **has affected or has the potential to affect** other natural or legal persons by **causing considerable** material or non-material **losses**' = potential to cause harm sufficient
- Mandatory reporting of significant 'cyber threats' that 'those entities identify that could have potentially resulted in a significant incident'
  - cyber threat means 'any potential circumstance, event or action that **could** damage, disrupt or otherwise **adversely** impact NIS, the users of such systems and other persons' (Article 2(8) CSA)
- Entities *falling outside* the scope of NIS 2.0: legal basis for voluntary submission
- Detailed tiered plan with initial notification, intermediate report (upon request) and final report
- BUT: still room for fragmentation with different competent authorities, no standardised online reporting tool, no requirement as to machine-readable format, no alignment with additional legislative proposals

Increase awareness on cyber threats by information sharingand enhance entities capacities to prevent threats from materialising

Reporting Obligations: NIS 2.0

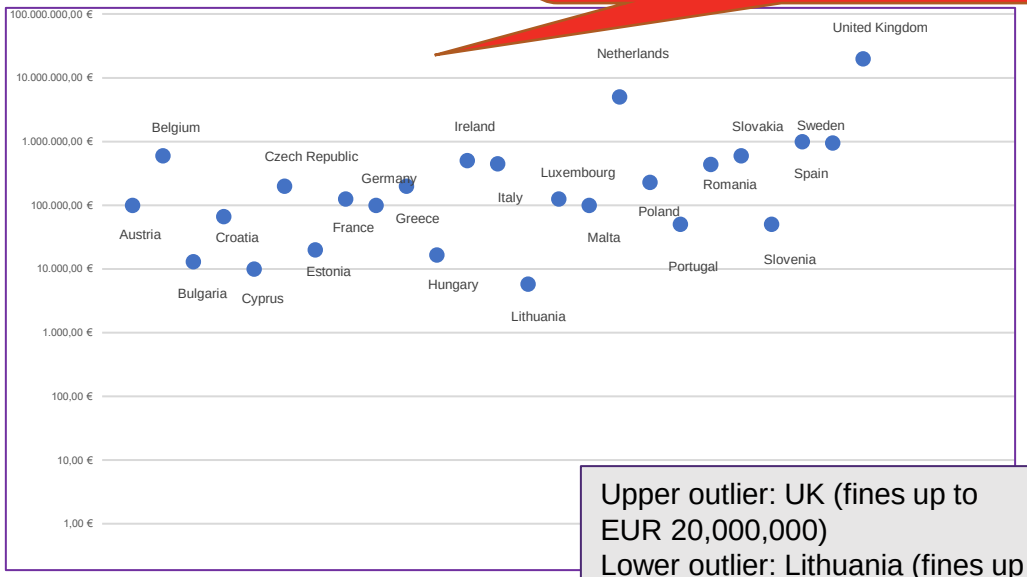
	EC NIS 2.0	EP Draft Resolution	Council General Approach
Reporting of incidents: significant impact	Significant impact = has caused or has the **potential** to cause **substantial harm**/has affected or has the **potential** to cause **considerable loss**	Parameters to consider: • number of recipients of the services; • incident duration; • geographical spread of affected area; • extent to which the functioning and continuity of the service is affected; • extent of the impact on economic and societal activities'	Significant impact = has caused or has the **potential** to cause **substantial harm**/has affected or has the **potential** to cause **considerable loss**
Reporting of significant cyber threats	Yes	No	No
Alternative		Voluntary information sharing on potential incidents and 'near misses'	Voluntary information sharing on potential incidents and 'near misses'
Reason for departure from EC NIS 2.0 Proposal		'unrealistic'/risk of over-reporting/ risk of inhibiting effectiveness of concerned entity's response/ challenges report handling by NCAs	Entities fear to be overburdened

Extended scope: x7!

Evidence?

Supervision and enforcement: NIS 1.0

There is great variation in the magnitude of penalties across Member States



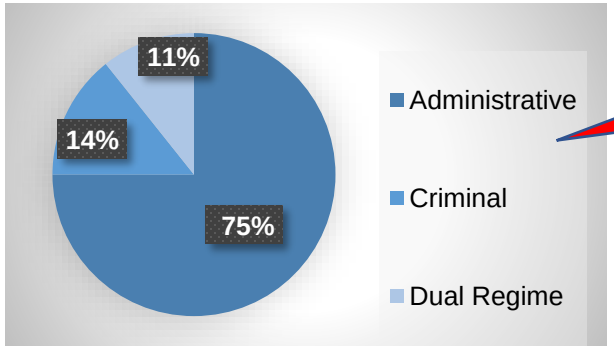
Upper outlier: UK (fines up to EUR 20,000,000)
Lower outlier: Lithuania (fines up to EUR 6,000)

Supervision:

- NCAs/SPOC/CSIRT
- Designation of competent SPOCs and NCAs: centralised/de-centralised
- NCAs 'shall monitor the application of the Directive at national level' and 'shall have the necessary powers and means to assess compliance of OES with their obligations under Art. 14' (Art. 15); ex post supervision of DSPs in terms of requirements laid down in Art. 16 (Art. 17)

Penalties:

- Art. 21: penalties provided for shall be effective, proportionate and dissuasive



Variation in characteristics of penalties

Supervision and enforcement: NIS 2.0

IEs only ex post

Supervision:

- Supervisory powers strengthened via minimum list of ex post and ex ante actions/means
  - Incl. regular audits (EEs)

Enforcement:

- Greater harmonisation of penalties:

  Penalties up to EUR 10,000,000 or 2 % of the entity's total worldwide annual turnover

- Additional sanctions other than fines:

  Suspension of authorization, temporary ban from exercise of managerial functions, etc

New: Responsibility and accountability of management bodies and their members for the compliance with cybersecurity requirements

NIS DIRECTIVE: JURISDICTION

JURISDICTIONAL RULES APPLICABLE TO CROSS-BORDER ACTORS UNDER NIS 1.0 AND NIS 2.0

uni.lu | SNT

EnCaViBS
Enhancing Cybersecurity Across Vital Business Sectors

www.encavibs.uni.lu

NIS 1.0

Operators of Essential Services (OES)

Separate/Concurrent Jurisdictional Rule

- States identify OES with an establishment in their territory
- OES are subject to the jurisdiction of the Member State where they provide essential services
- Cross-border OES are subject to the jurisdiction of each of the Member States where they provide essential services in parallel
- Minimum harmonisation approach

Digital Services Providers (DSPs)

Exclusive Jurisdictional Rule

- DSPs are only subject to the jurisdiction of the Member State where they have their main establishment (one-stop-shop approach)
- DSPs not established in the EU need to designate a representative and will be subject to the jurisdiction of the Member State where the representative is established
- Light-touch regime and maximum harmonisation approach

Main Problems

OES — Multi-level fragmentation

- Identification
- Supervision and enforcement
- Security and reporting requirements

DSPs — Regulatory shopping and delays

- Pro-business or less-expensive regulator.
- Bottleneck scheme
- Cloud Services and its clients OES will often be under the jurisdiction of different regulators

NIS 2.0

Essential and Important Entities

Rule

- Both categories are subject to the jurisdiction of the Member State where they provide their services.
- Cross-Border Entities: concurrent jurisdiction rule.

Exception

- Certain types of entities in the digital infrastructure and digital services provider sectors are subject to the jurisdiction of the Member State where they have their main establishment (exclusive jurisdiction rule)

Highlights

- Both categories are subject to the same security and reporting requirements.
- Broader applicability of the one-stop-shop mechanism.
- More guidance to identify the main establishment
  - The number of employees as a criterion to determine the main establishment is problematic.

uni.lu | SNT

Take-Aways

NIS 1.0 weaknesses:

- Lack of harmonisation leading to fragmentation
- Uneven level of cyber resilience

NIS 2.0

Responds to the deficits of NIS 1.0 with regard to the exemplary subject matters:

- Expands scope of Directive paying regard to increased interconnectedness and based on criticality of sectors
- Strengthens and streamlines security and reporting requirements
- Provides for extended mandatory incident reporting to increase awareness and preparedness
- More stringent supervisory measures for national authorities
- Stricter enforcement requirements and harmonisation of sanctions

Interdisciplinary Centre for Security, Reliability and Trust

Contact: sandra.schmitz@uni.lu

This research was funded by the Luxembourg National Research Fund (FNR) C18/IS/12639666/EnCaViBS/Cole, https://www.fnr.lu/projects/the-eu-nis-directive-enhancingcybersecurity-across-vital-business-sectors-encavibs/.

Connect with us

@SnT_uni_lu

SnT, Interdisciplinary Centre for Security, Reliability and Trust