Overview of cybersecurity policies in the EU

Domenico Ferrara, Policy Officer
European Commission, DG CNECT.H.1
Cybersecurity Technology and Capacity Building

1 June 2021
Continuous policy response to the evolving threat landscape:
- **2013** EU Cybersecurity Strategy: 'An Open, Safe and Secure Cyberspace'
- **2016** Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry; NIS Directive
- **2017** Cybersecurity package, proposal for a Cybersecurity Act (CSA)
- **2018** Proposal for the European competence centre and network
- **2019** Entry into force of CSA
- **2020** Cybersecurity Strategy, Review of NIS Directive

Building EU Resilience to cyber attacks

**Capacity Building**
- Enhanced national capabilities & Risk management requirements (NIS)
- Financial Support from the EU
- Industrial capabilities

**Prevention & Response Coordination**
- ENISA operational support & Cooperation between national CSIRTs
- Coordinated response to large-scale cybersecurity incidents and crises & exercises
- Single Market for certified ICT products and services (CSA)
EU in action about cybersecurity
The Cybersecurity Strategy
Why a new Strategy?

- **Critical services** have gone digital
- **IoT** proliferating: 25 bn connected objects
- **Cyberattacks** increasing 241% (DDoS)
- **Dependency** accelerated by pandemic - also expanding **attack surface** (hospitals, vaccine distribution)
- **Geopolitical** contest over cyberspace; authoritarian regimes damage open global Internet & try dominate international bodies/norm setting
- **Digital transformation can only succeed with cybersecurity**
Overview of tools and actions

- Smart digital investment: up to €4.5bn for cybersecurity 2021-27 (MFF+RRF+MS+Industry)
- New regulatory tools
- New policy instruments
- Comprehensive
  - internal market
  - law enforcement
  - diplomacy
  - defence
## Resilience and leadership

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Adopt NIS 2.0 [CID]</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cyber Shield</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Develop Network of Security Operations Centres</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ultra secure connectivity</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Quantum enabled encryption</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5G networks</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Complete implementation of Toolbox</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internet security</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Develop DNS4EU</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supply chain autonomy</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Encourage EUR 4.5 bn investment across digital supply chain through Competence Centre and Network</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Skills</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Eg investment in business resilience against cyber-enabled IP theft</td>
<td></td>
</tr>
</tbody>
</table>
Operational capacity: prevent deter, respond

- Joint Cyber Unit
  - Milestones and process to be set out in 2021

- Cybercrime
  - Complete Security Union agenda

- Cyberdiplomacy toolbox
  - Embed Member State cyber intel in INTCEN
  - Deterrence posture

- Cyber Defence
  - Vision and strategy for CSDP military missions
Global and open cyberspace

EU leadership on international norms and standards

Cooperation with partners

Global resilience and capacity
The NIS Directive
NIS Directive: Main Features

**Greater Capabilities**
Member States have to improve their cybersecurity capabilities.

**Cooperation**
Increased EU-level cooperation

**Risk Management**
Operators of essential services and Digital Service Providers have to adopt risk management practices and notify significant incidents to their national authorities.
Main challenges of existing NIS 1

| Not all sectors that may be considered critical are in scope | Great inconsistencies and gaps due to the NIS scope being *de facto* defined by MS (case by case OES identification) |
| Diverging incident notification requirements | Ineffective supervision and limited enforcement |
| Diverging security requirements across MS | Voluntary and ad-hoc cooperation and info sharing between MS and between operators |
Main challenges of existing NIS 1

Example: Discrepancies in the identification of operators of essential services (OES)

Identified OES in the five biggest Member States (per 100 000 inhabitants)
The NIS 2 vision - main objectives

1. Cover a larger portion of economy and society (more sectors)

2. Within sectors: systematically focus on bigger and critical players (replace current identification process)

3. Align security requirements (incentivize investments and awareness including by mandating board-level accountability), expand supply chain and supplier relationships risk management

4. Streamline incident reporting obligations

5. Align provisions on national supervision and enforcement

6. More operational cooperation approach including on crisis management

7. Align with proposed Resilience of Critical Entities Directive
### Two regulatory regimes

<table>
<thead>
<tr>
<th>Essential entities</th>
<th>Important entities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
<td>Scope of NIS1 + certain new sectors</td>
</tr>
<tr>
<td><strong>Security requirements</strong></td>
<td>Risk-based security obligations, including accountability of top management</td>
</tr>
<tr>
<td><strong>Reporting obligations</strong></td>
<td>Significant incidents and significant cyber-threats</td>
</tr>
<tr>
<td><strong>Supervision</strong></td>
<td>Ex-ante + ex post</td>
</tr>
<tr>
<td><strong>Sanctions</strong></td>
<td>Minimum list of administrative sanctions, including fines. Only for essential entities: <em>ultima ratio</em> possibility to suspend authorisation or impose temporary ban on managerial duties</td>
</tr>
</tbody>
</table>
| **Jurisdiction**   | General rule: MS where the service is provided  
Exception: Main establishment + ENISA registry for certain digital infrastructures and digital providers | |
• **Identification** has proven **inefficient** → difficulty in identifying consistent thresholds

• **Size** as a clear-cut benchmark (all companies, which are medium-sized or larger) and a proxy for importance. **Exceptions:** electronic communications, trust services, TLD registries and public administration.

• **MS** will be in a position to add operators **below the size threshold** in the following cases:

  • **Sole providers** of a service
  • Potential disruption of a service provided by an entity could have an impact on **public safety, public security or public health**
  • Potential disruption of a service provided by an entity could induce **systemic risks**
  • Entities with specific **importance at regional or national level** for a particular sector or type of service, or for other interdependent sectors in a Member State
  • Entities considered as **critical under the proposed Resilience of Critical Entities Directive**
### Which sectors are covered?

<table>
<thead>
<tr>
<th>Essential entities</th>
<th>Important entities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Energy</strong> (electricity*, district heating, oil, gas and hydrogen)</td>
<td>Postal and courier services</td>
</tr>
<tr>
<td><strong>Transport</strong> (air, rail, water, road)</td>
<td>Waste management</td>
</tr>
<tr>
<td><strong>Banking</strong></td>
<td>Chemicals (manufacture, production, distribution)</td>
</tr>
<tr>
<td><strong>Financial market infrastructures</strong></td>
<td>Food (production, processing, distribution)</td>
</tr>
<tr>
<td><strong>Health</strong> (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)</td>
<td>Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)</td>
</tr>
<tr>
<td><strong>Drinking water</strong></td>
<td>Digital providers (search engines, online market places and social networks)</td>
</tr>
<tr>
<td><strong>Waste water</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Digital Infrastructure</strong> (IXP, DNS, TLD, cloud, data centres, CDN, electronic communications and trust service providers)</td>
<td></td>
</tr>
<tr>
<td><strong>Public administrations</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Space</strong></td>
<td></td>
</tr>
</tbody>
</table>

*New types of entities in electricity*: electricity markets, production, aggregation, demand response and energy storage
More harmonised security requirements

- Accountability for top management for non-compliance with cybersecurity risk management measures
- Risk based approach: appropriate and proportionate technical and organisational measures
- Measures to at least include:
  - risk analysis and information system security policies
  - incident handling
  - business continuity and crisis management
  - supply chain security
  - security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
  - policies and procedures to assess the effectiveness of cybersecurity risk management measures
  - the use of cryptography and encryption
  - Cybersecurity certification
More harmonised reporting requirements

- Entities to report both significant incidents and cyber threats
- Entities to inform recipients of their services
- Incident notification in **three stages**:
  - Initial notification
  - Intermediate report upon request of CA or CSIRT
  - Final report within one month

- MS to inform each other and ENISA of incidents with cross-border nature
Coordinated vulnerability disclosure

• As part of the national cybersecurity strategy, Member States will be required to develop a policy framework on coordinated vulnerability disclosure.

• Each Member State shall be required to designate one national CSIRT as a coordinator and facilitator of the coordinated vulnerability disclosure process at national level.

• In cases where the reported vulnerability affects multiple vendors across the Union, the designated CSIRT shall cooperate with the CSIRT network to facilitate multi-vendor coordinated vulnerability disclosure.

• European vulnerability registry run by ENISA
Timeline of the NIS Directive

- **2013**: Legislative proposal for the NIS Directive
- **2014**: Political agreement
- **2015**: First meeting of the Cooperation Group and creation of work streams
- **2016**: Entry into force of NIS 1
- **2017**: MS submit information about OES identification
- **2018**: Transposition deadline
- **2019**: Commission OES report
- **2020**: Start of negotiations between the co-legislators
- **2021**: Impact assessment and evaluation
- **2020**: Start of the country visits
- **2021**: Legislative proposal for a revised NIS Directive
The Cybersecurity Act
What's new with the regulation?

- Focused Mandate
- Adequate Resources
- Permanent Status

enisa

European Network and Information Security Agency
ENISA's growing role in prevention & response

In case of significant incidents and crises
- Provides support to or carry out an **ex-post technical enquiry**
- Contribute to develop a cooperative response to large-scale cross-border incidents or crises (**Blueprint**)

Regular EU Cybersecurity Technical Situation Report

Organise an upgraded pan-European cybersecurity exercise (**Cyber Europe**) to an annual event

Prominent Role in the Certification Framework
Cybersecurity Certification

A voluntary European cybersecurity certification framework...

...to enable the creation of tailored EU cybersecurity certification schemes for ICT products and services...

...that are valid across the EU
The European Cybersecurity Certification Framework - features

- One Framework, many schemes
- Voluntary nature: unless specified in future EU/national rules.
- Scope: Products, services, or processes
- Inclusive and transparent governance processes.
- Union Rolling Work Programme for priorities
- Each scheme can contain specific provisions on: re-certification, vulnerability handling and disclosure, provision of updates, surveillance, peer review
- Three levels of assurance to be defined on basis of risk of intended use
Establishment of an EU Cybersecurity Certification Scheme

1. **European Cybersecurity Certification Group (MSs)**
   - Advises ENISA and may propose the preparation of a candidate scheme to ENISA

2. **Union Rolling Work Programme on Cybersecurity Certification**
   - Requests ENISA to prepare Candidate Scheme

3. **Commission**
   - Requests ENISA to prepare Candidate Scheme

4. **ENISA**
   - Ad hoc Working Group for each scheme
   - Prepares candidate scheme

5. **ENISA**
   - Consults Industry, Standardisation Bodies, other stakeholders

6. **European Commission**
   - Adopts Candidate Scheme
Union Rolling Work Programme for European cybersecurity certification

- Identifies strategic priorities for future European cybersecurity certification schemes;
- Multi-annual document to be drafted by the Commission with inputs from SCCG and ECCG and other stakeholders;
- Cybersecurity Strategy stated that the URWP should be adopted in 2021;
- It shall be updated at least once every three years and more often if necessary.
European cybersecurity certification framework – state of play

Cybersecurity Act
• Entry into force June ‘19

Candidate Schemes
• “SOG-IS MRA” – (Common Criteria)
• Cloud services
• 5G networks

Union Rolling Work Programme for European cybersecurity certification
• Publication 2021

Advisory groups
• ECCG - established
• SCCG - established
Thank you for your attention!

Trust in a Digital Society

Connected mobility
Cybersecurity
Health
Electronic identity
Connected cities
Online privacy
Public services
Electronic transactions