enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

FROM POLICY TO PRACTICE

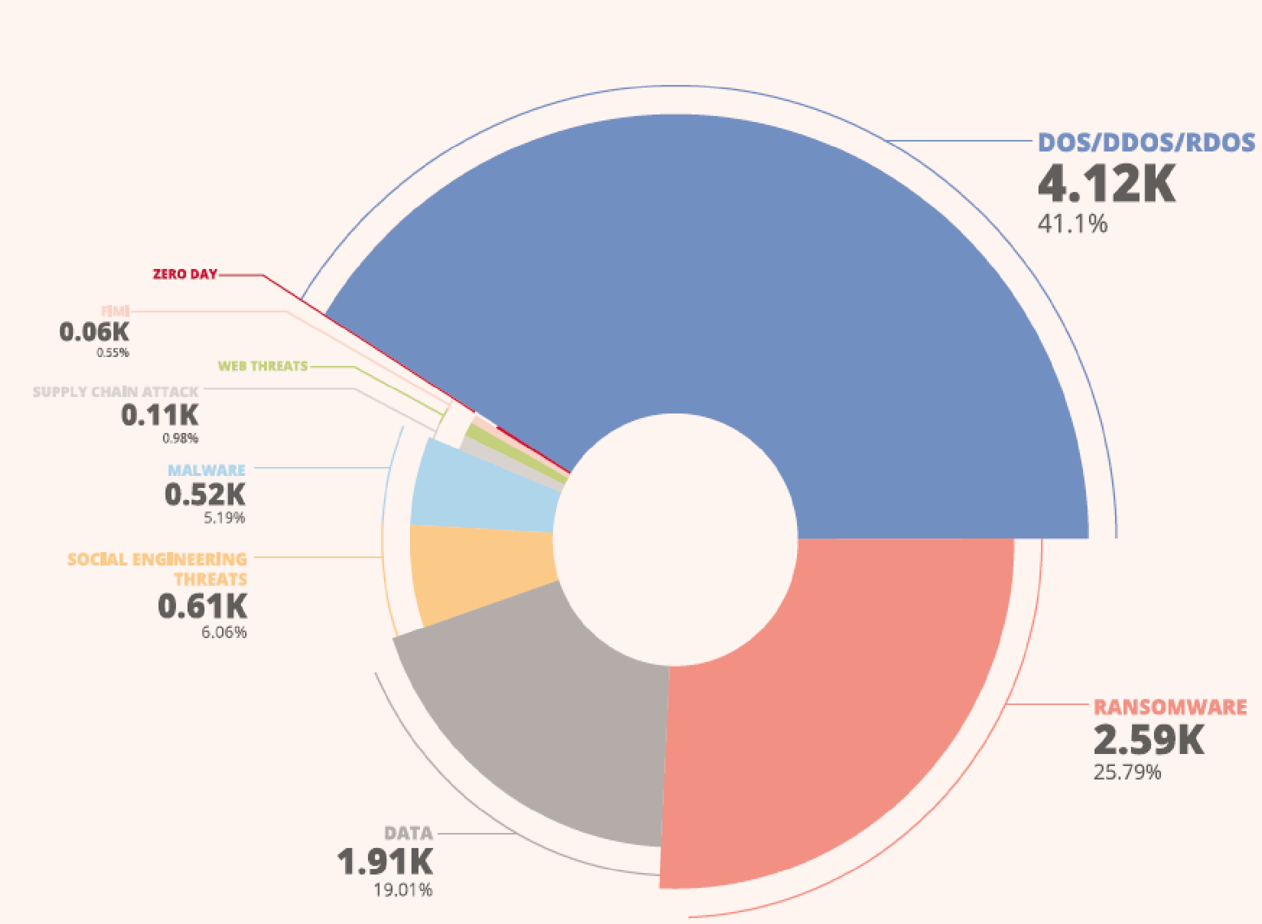
Translating EU policies into practice

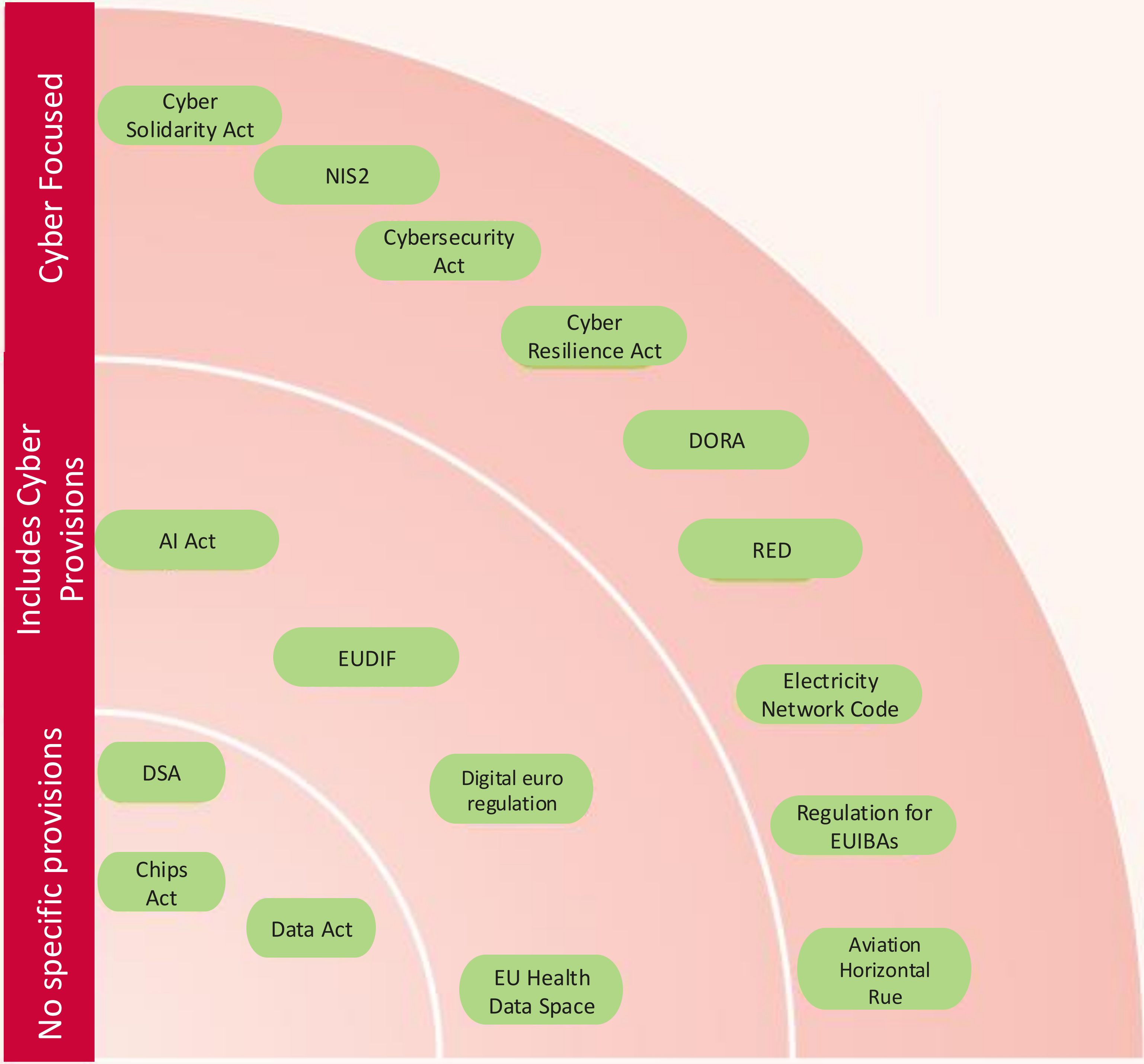
Erika Magonara
Head of Sector – Policy Monitoring and Analysis
ENISA, the EU Agency for Cybersecurity

CYBERSECURITY POLICY-MAKING

Complex and ever-evolving **threat landscape** and **horizontal matter**, requiring a **“Whole-of-Society”** and a **“Whole-of-EU”** approach.

Incidents by threat type (July 2023 to June 2024)





Cyber Focused

Cyber Solidarity Act

NIS2

Cybersecurity Act

Cyber Resilience Act

DORA

RED

Electricity Network Code

Regulation for EUIBAs

Aviation Horizontal Rue

Includes Cyber Provisions

AI Act

EUDIF

Digital euro regulation

EU Health Data Space

No specific provisions

DSA

Chips Act

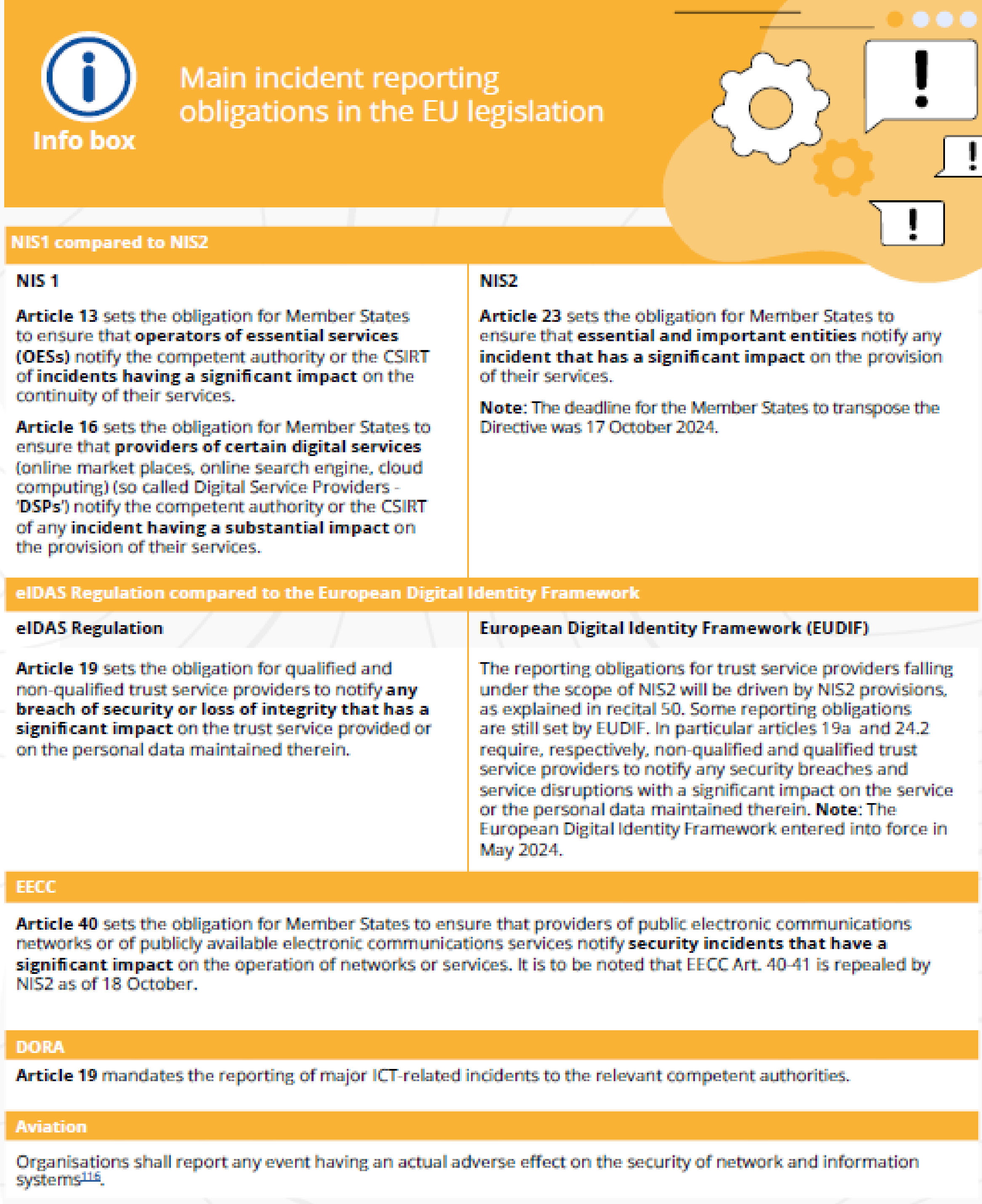
Data Act

EXAMPLE: INCIDENT REPORTING

Reporting obligations: terminology and timelines.

Modes of reporting: governance and tools.

Practical aspects: cross-border dimension, incentives, data aggregation.



Info box

Main incident reporting obligations in the EU legislation

NIS1 compared to NIS2

NIS 1	NIS2
Article 13 sets the obligation for Member States to ensure that **operators of essential services (OESs)** notify the competent authority or the CSIRT of **incidents having a significant impact** on the continuity of their services. **Article 16** sets the obligation for Member States to ensure that **providers of certain digital services** (online market places, online search engine, cloud computing) (so called Digital Service Providers - 'DSPs') notify the competent authority or the CSIRT of any **incident having a substantial impact** on the provision of their services.	**Article 23** sets the obligation for Member States to ensure that **essential and important entities** notify any **incident that has a significant impact** on the provision of their services. **Note**: The deadline for the Member States to transpose the Directive was 17 October 2024.

eIDAS Regulation compared to the European Digital Identity Framework

eIDAS Regulation	European Digital Identity Framework (EUDIF)
Article 19 sets the obligation for qualified and non-qualified trust service providers to notify **any breach of security or loss of integrity that has a significant impact** on the trust service provided or on the personal data maintained therein.	The reporting obligations for trust service providers falling under the scope of NIS2 will be driven by NIS2 provisions, as explained in recital 50. Some reporting obligations are still set by EUDIF. In particular articles 19a and 24.2 require, respectively, non-qualified and qualified trust service providers to notify any security breaches and service disruptions with a significant impact on the service or the personal data maintained therein. **Note**: The European Digital Identity Framework entered into force in May 2024.

EECC

Article 40 sets the obligation for Member States to ensure that providers of public electronic communications networks or of publicly available electronic communications services notify **security incidents that have a significant impact** on the operation of networks or services. It is to be noted that EECC Art. 40-41 is repealed by NIS2 as of 18 October.

DORA

Article 19 mandates the reporting of major ICT-related incidents to the relevant competent authorities.

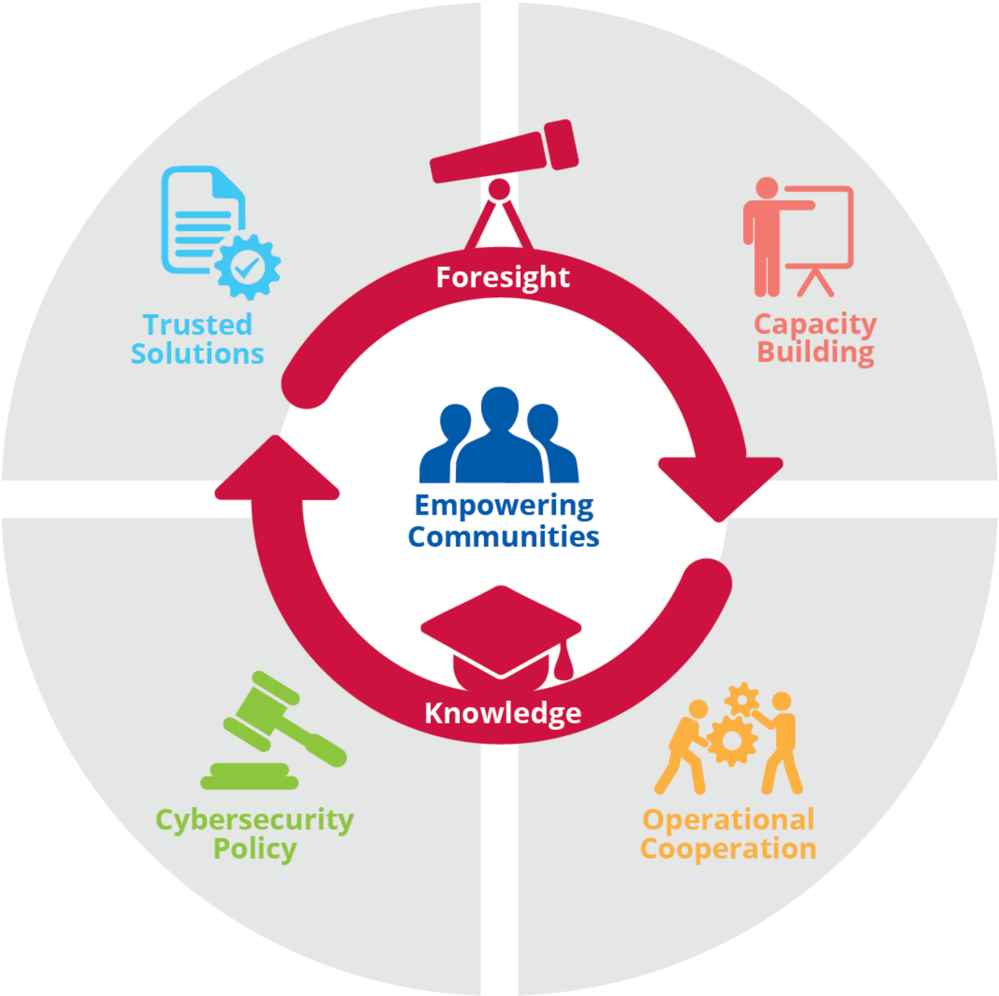
Aviation

Organisations shall report any event having an actual adverse effect on the security of network and information systems[116].

ENISA'S ROLE

ENISA is the European Union Agency for Cybersecurity, working towards a **trusted and cybersecure Europe.**

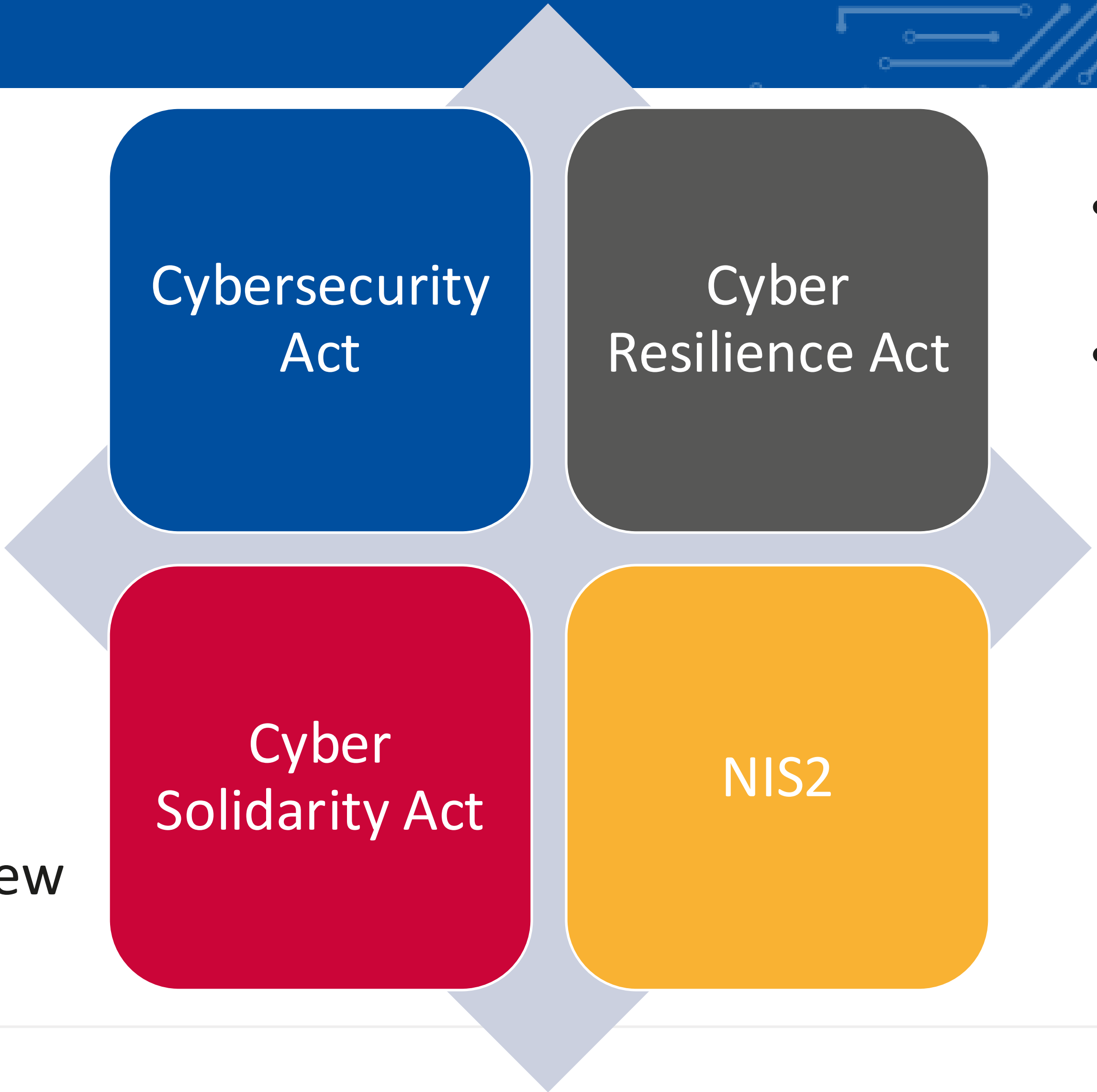
We support the implementation of EU policies in Member States (among others).



MAIN EU POLICIES FOR CYBER RESILIENCE

- ENISA mandate
- EU Cybersecurity Certification

- Embedding security into digital products
- “security by design”



Cybersecurity Act

Cyber Resilience Act

Cyber Solidarity Act

NIS2

- EU CS alert system
- CS Emergency Mechanism
- EU CS incident review mechanism

- Unified framework for critical sectors
- Cross-border cooperation
- National Strategies

NIS2 IN A NUTSHELL

To achieve a high common level of cybersecurity across the EU

Network & Information
Systems Directive

1. National capabilities

- National authority
- National strategy
- National CSIRT
- National crisis management framework (new)
- National vulnerability disclosure framework (new)

2. EU collaboration

- NIS Cooperation group
- EU CSIRT network
- EU Cyclone (new)

New mechanisms under the NIS2

- Cybersecurity state of the union report
- EU Vulnerability database (EUVD)
- EU Digital infrastructure registry (EUDIR)
- WHOIS requirements
- Union evaluations of ICT supply chain risks

3. Supervision of critical sectors

- Management responsibility (new)
- Security measures
- Incident reporting

- Twice as many sectors
- More companies within a sector
- Management responsibility entities
- All hazard, including cyber-physical
- Supply chain security
- Cloud and datacenters essential under NIS2
- Managed service providers new under NIS2
- Telecoms and trust integrated into NIS2

SUPPORTING NIS2 IMPLEMENTATION

Knowledge

Outreach and awareness material
Map of national strategies
Specific reports e.g. Crisis management

Community engagement

Support to NIS CG, CSIRTs Network and Cyclone
Working with the private sector

Tools

EU Vulnerability Database
EU Digital infrastructure registry
Technical guidance

Capacity Building

National Capabilities Assessment Framework
Knowledge-exchange
Peer-reviews

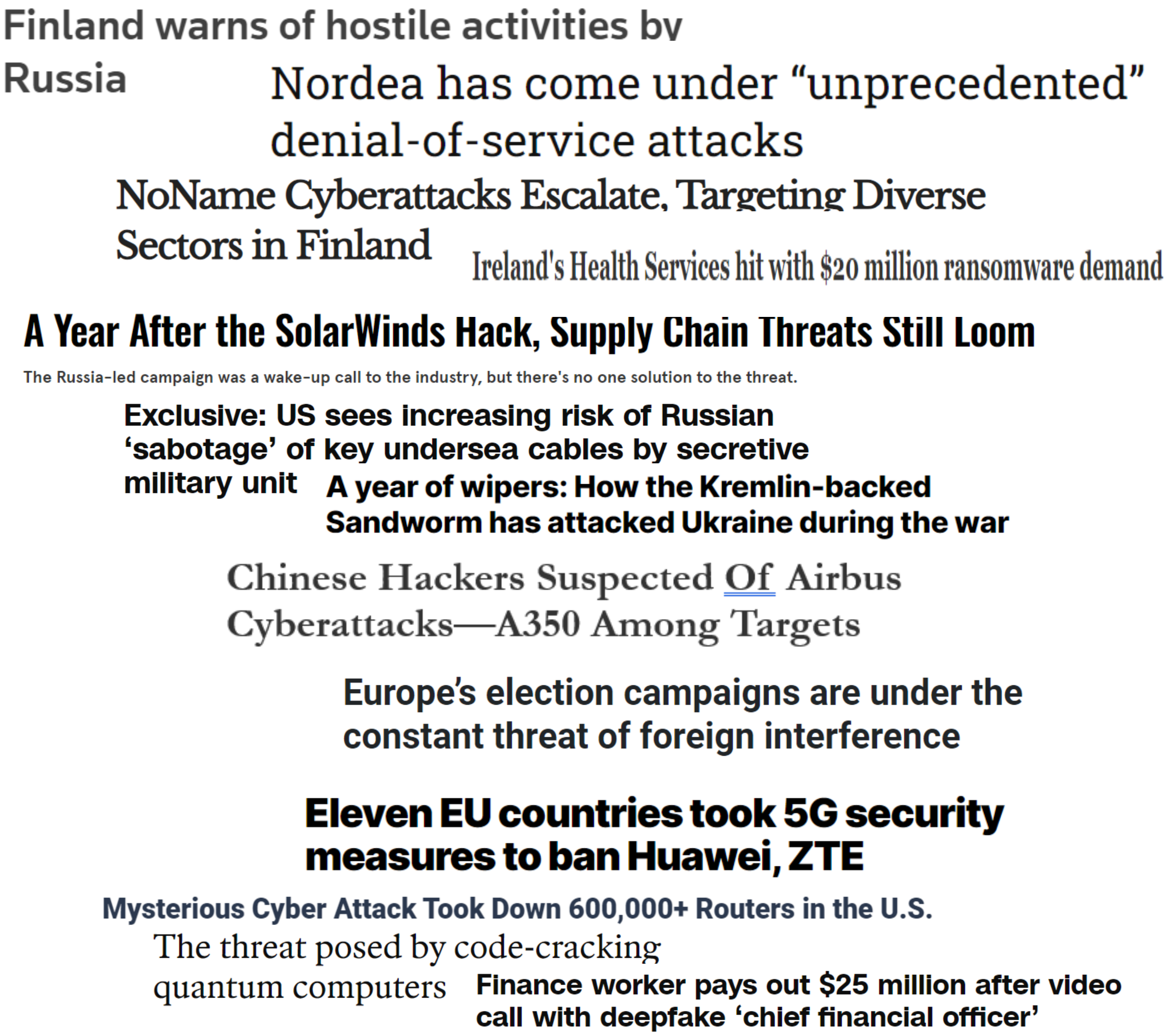
SOME OBSERVATIONS

*Making the most of **existing** structures…*

*Strengthening **technical** and **financial** support to authorities and entities…*

*Enhancing the **understanding** of **sectorial specificities and needs…***

*Balancing Member State **flexibility**, with **uniform** EU implementation…*



Finland warns of hostile activities by Russia

Nordea has come under "unprecedented" denial-of-service attacks

NoName Cyberattacks Escalate, Targeting Diverse Sectors in Finland

Ireland's Health Services hit with $20 million ransomware demand

A Year After the SolarWinds Hack, Supply Chain Threats Still Loom

The Russia-led campaign was a wake-up call to the industry, but there's no one solution to the threat.

Exclusive: US sees increasing risk of Russian 'sabotage' of key undersea cables by secretive military unit

A year of wipers: How the Kremlin-backed Sandworm has attacked Ukraine during the war

Chinese Hackers Suspected Of Airbus Cyberattacks—A350 Among Targets

Europe's election campaigns are under the constant threat of foreign interference

Eleven EU countries took 5G security measures to ban Huawei, ZTE

Mysterious Cyber Attack Took Down 600,000+ Routers in the U.S.

The threat posed by code-cracking quantum computers

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

It's about the threats, not the rules.

THANK YOU

YOUR INPUT, IDEAS, AND SUGGESTIONS ARE VERY WELCOME

📱 Email or connect on Linkedin

✉ Erika.Magonara@enisa.europa.eu

🌐