enisa 20 years!

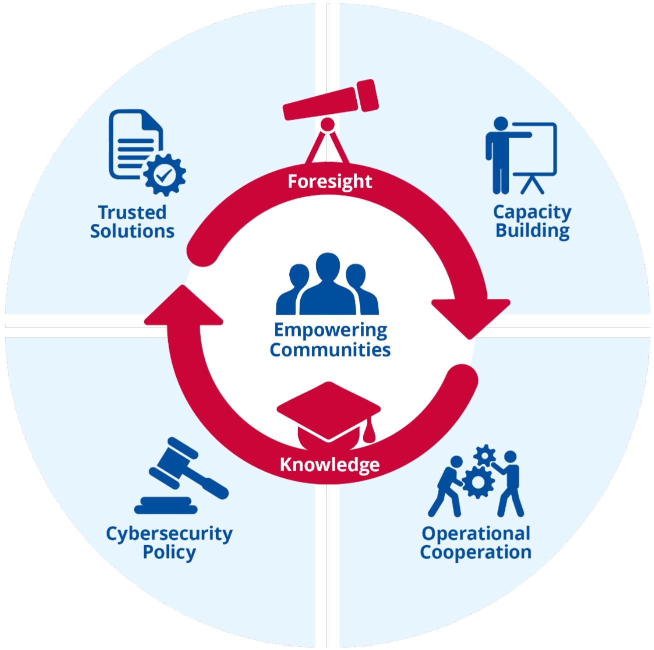
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

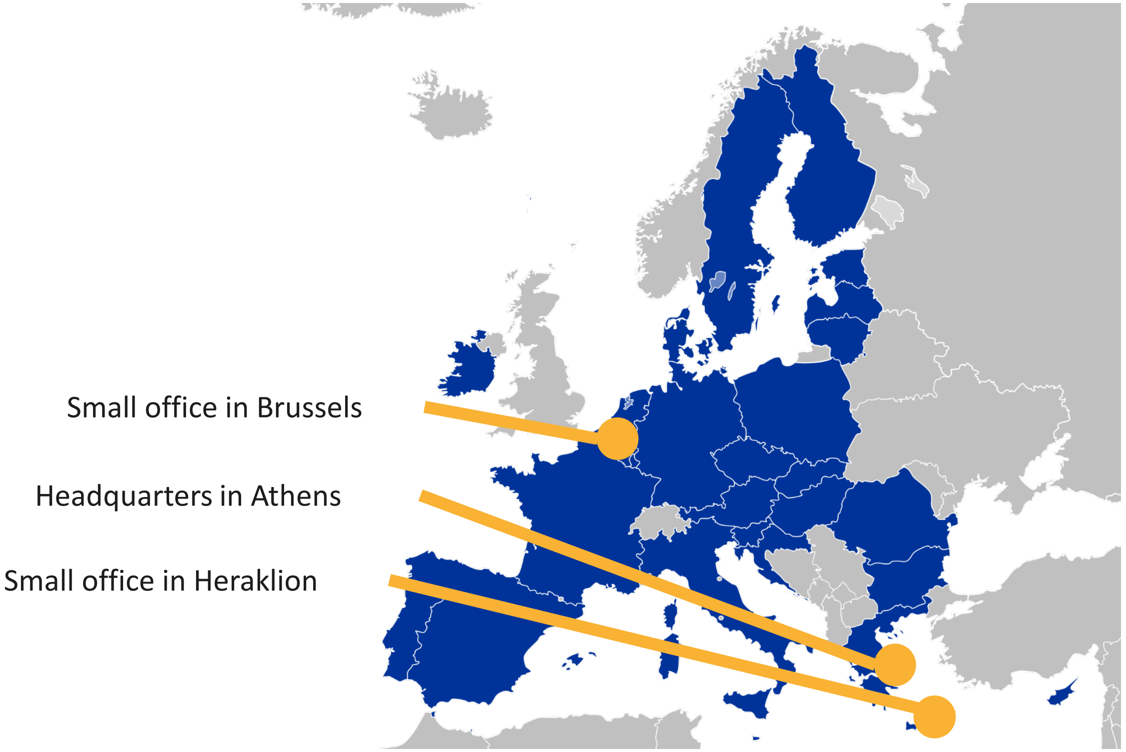
INCREASING RESILIENCE OF CRITICAL SECTORS

Marnix Dekker, Deputy Head of Unit, Resilience of Critical Sectors
Georgia Bafoutsou, Cybersecurity officer – lead for telecom security

ENISA, the EU Agency for Cybersecurity

ABOUT ENISA – THE EU AGENCY FOR CYBERSECURITY





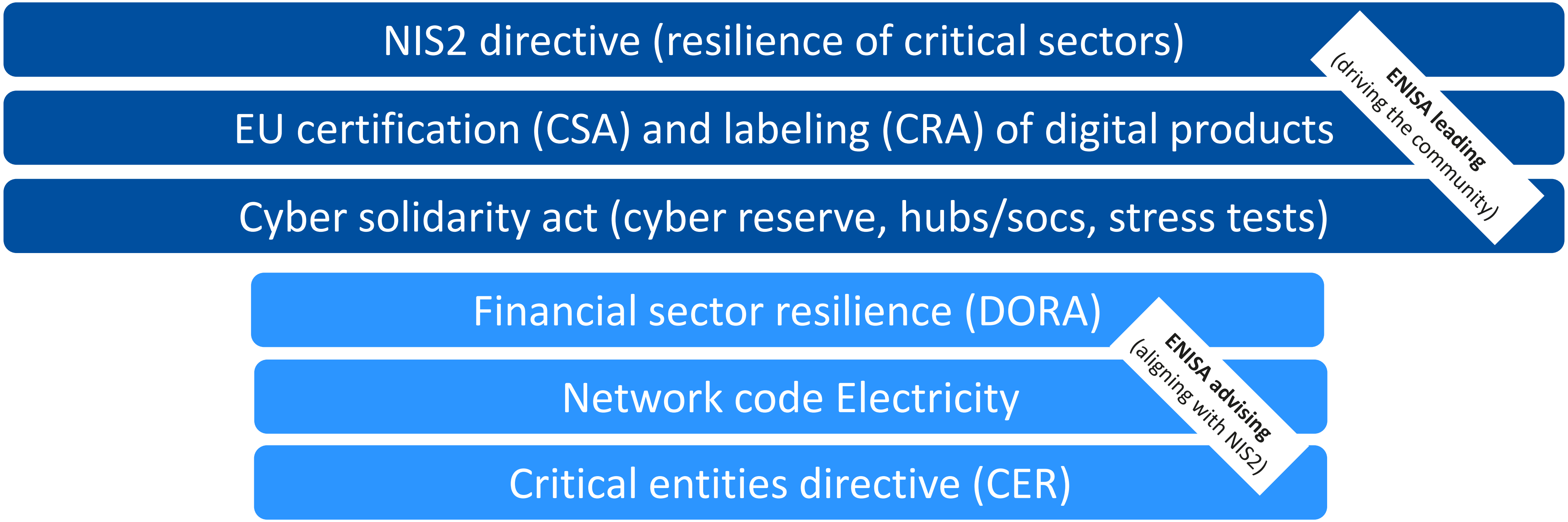
About 100 staff

- **Operational collaboration:** EU CSIRTs network, EU Cyclone, EU situational awareness
- **Resilience of critical sectors:** NIS2, 5G toolbox, DORA, Network code electricity, etc.
- **Capacity building:** Cyber exercises, challenges, trainings, EU support action, EU cyber reserve, etc.
- **Certification and labeling:** EU cybersecurity certification (CSA, EUCC, EUCS) and EU cybersecurity labeling (CRA)

EU POLICIES FOR CYBER RESILIENCE

Many EU policies coming into force – NIS2, DORA, AI act, Digital Services Act, Digital Markets act, etc.

ENISA's main focus is on:



NIS2 directive (resilience of critical sectors)

EU certification (CSA) and labeling (CRA) of digital products

Cyber solidarity act (cyber reserve, hubs/socs, stress tests)

ENISA leading
(driving the community)

Financial sector resilience (DORA)

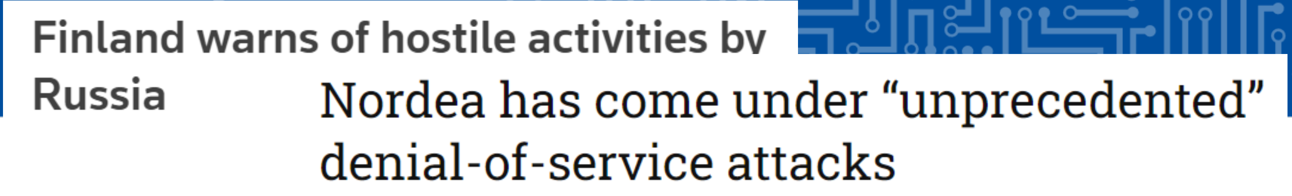
Network code Electricity

Critical entities directive (CER)

ENISA advising
(aligning with NIS2)

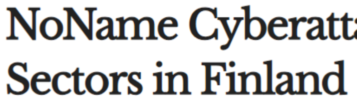
MAIN CYBER THREATS FOR THE UNION

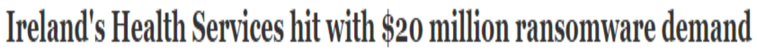
DDoS attacks


Finland warns of hostile activities by Russia

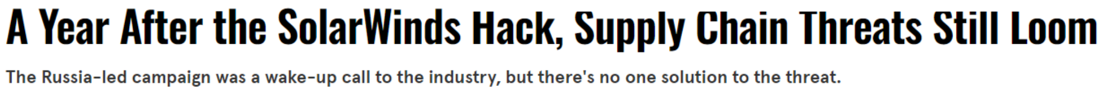
Nordea has come under “unprecedented” denial-of-service attacks

Ransomware


NoName Cyberattacks Escalate, Targeting Diverse Sectors in Finland

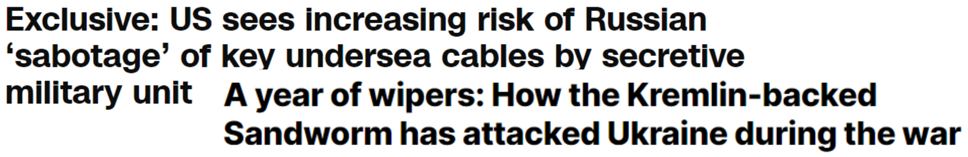

Ireland's Health Services hit with $20 million ransomware demand

Supply chain attacks


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

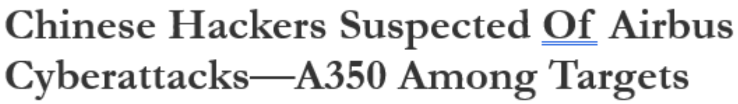
The Russia-led campaign was a wake-up call to the industry, but there's no one solution to the threat.

Russia’s war of aggression against Ukraine

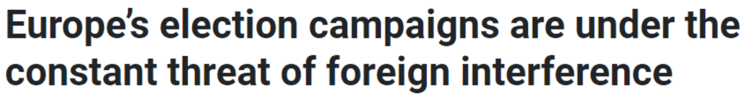

Exclusive: US sees increasing risk of Russian ‘sabotage’ of key undersea cables by secretive military unit

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

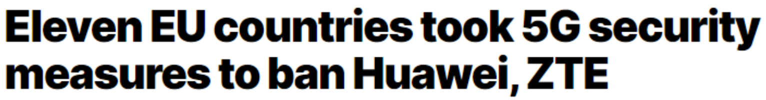
Industrial and state espionage


Chinese Hackers Suspected Of Airbus Cyberattacks—A350 Among Targets

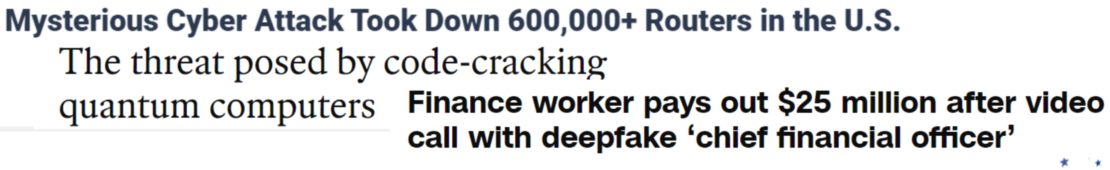
Foreign interference


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

Supply chain risks


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

Emerging threats (IoT, AI), future issues (PQC)


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’

NIS2 DIRECTIVE 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 frameworks (new)

2. EU collaboration

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

New ENISA tasks under the NIS2

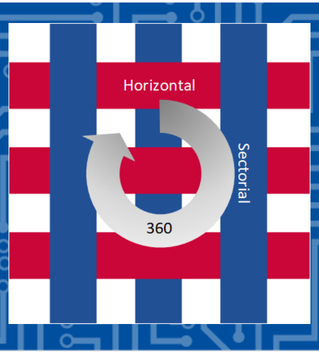
- EU Vulnerability database (EUVD)
- EU Digital infrastructure registry (EUDIR)
- WHOIS requirements
- Union evaluations of supply chain risks
- Cybersecurity state of the union report

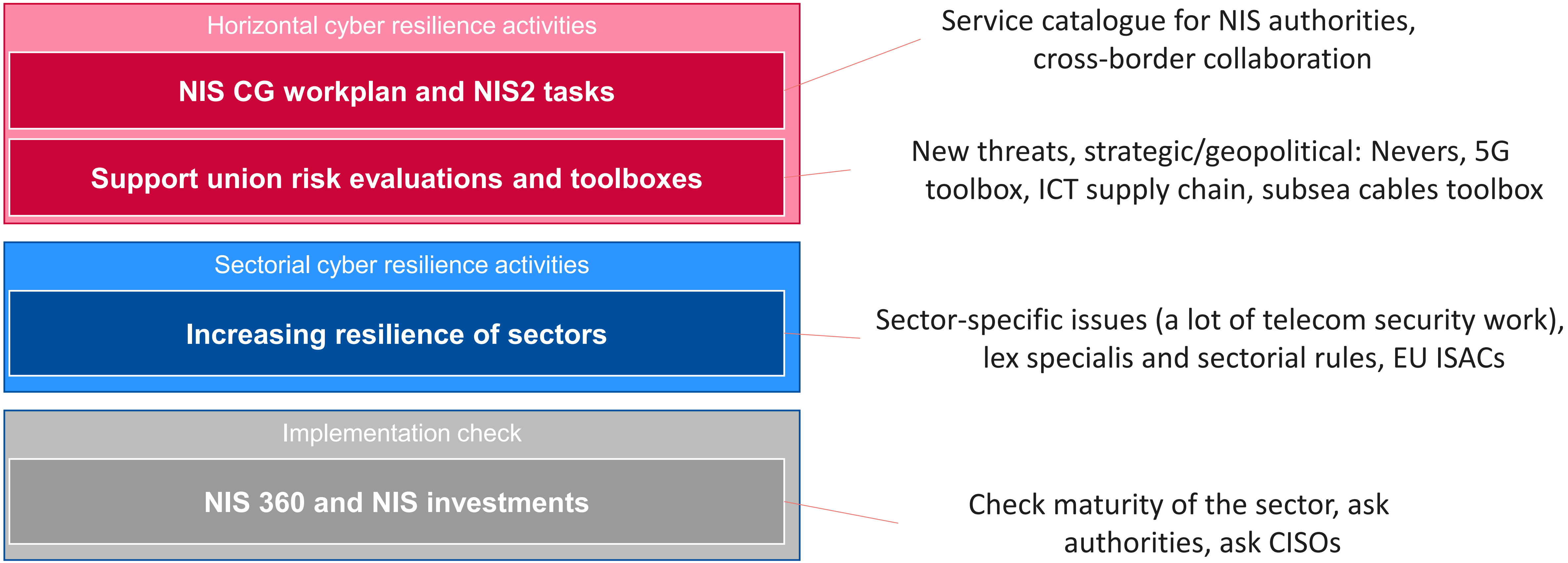
3. Supervision of critical sectors

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

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

ENISA RESILIENCE WORK - PREPAREDNESS





Horizontal cyber resilience activities

NIS CG workplan and NIS2 tasks

Support union risk evaluations and toolboxes

Sectorial cyber resilience activities

Increasing resilience of sectors

Implementation check

NIS 360 and NIS investments

Service catalogue for NIS authorities, cross-border collaboration

New threats, strategic/geopolitical: Nevers, 5G toolbox, ICT supply chain, subsea cables toolbox

Sector-specific issues (a lot of telecom security work), lex specialis and sectorial rules, EU ISACs

Check maturity of the sector, ask authorities, ask CISOs

ENISA SUPPORTING THE NIS SECTORS

ENISA NIS sector strategy

- We **focus on 6 main sectors**, and are involved with 3 other sectors
- **Services:** Knowledge building, Threat landscapes, Cyber Europe, Awareness raising campaigns
- Supporting **sectorial groups of EU national authorities**
  - Telecom security (ECASEC), Energy cybersecurity (WS8), Health cybersecurity (WS12)
- Sectorial groups **support also the horizontal NIS2 work**
  - NIS2 taskforces in sectorial groups
  - Bringing technical/sectorial expertise in NIS2 horizontal tasks
- We facilitate public-private **dialogue between NIS authorities and industry**
  - Examples: Yearly ENISA Telecom security forum (Q1 2025), ENISA eHealth conference, …
- **We promote alignment and consistency** between NIS2 and sectorial initiatives and lex specialis

ENISA focus in 2024

Sustain	**Energy-electricity** **Telecoms** **Core internet and cloud** **Trust**
Build	**Health** **Rail**
Involve	**Finance** **Space** **Aviation**
Prepare	Public administrations

GROUPS OF TELECOM AUTHORITIES WE WORK WITH

NIS COOPERATION GROUP

NISCG Workstream on 5G/telecoms cybersecurity

ECASEC

European Competent Authorities for Secure Electronic Communications

powered by ENISA

Formed in 2010, as Article 13a expert group – this telecom collaboration was the model for the NIS Directive!

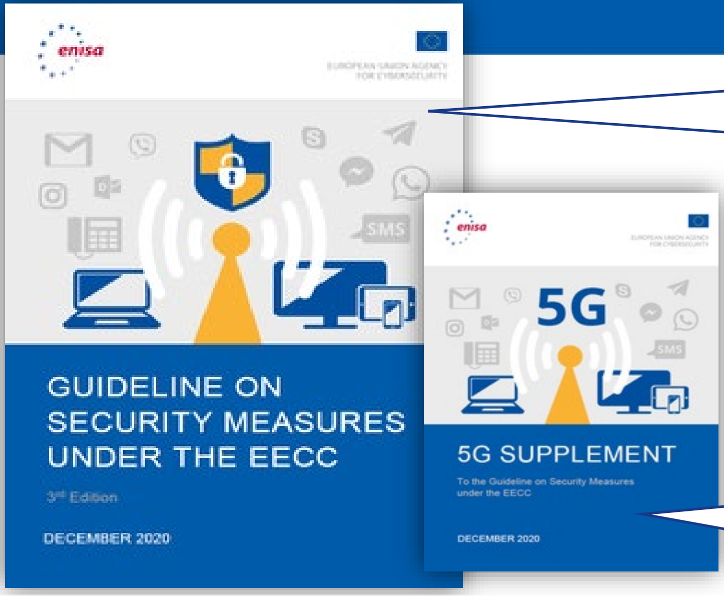
BEREC Expert group on resilience

Subsea cable expert group

Formed in 2024

Note: Usually, consultation with telecom industry takes place at national level – between authorities and its sector.
We do welcome input and feedback! By email, linkedin or at an event.
Annually we organize the ENISA telecom security forum – for public-private discussions – NRAs-Telcos. Next in Q1 2025.

ENISA TELECOM FRAMEWORK AND DEEPDIVES



enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

GUIDELINE ON SECURITY MEASURES UNDER THE EECC

3rd Edition

DECEMBER 2020

enisa

5G SUPPLEMENT

To the Guideline on Security Measures under the EECC

DECEMBER 2020

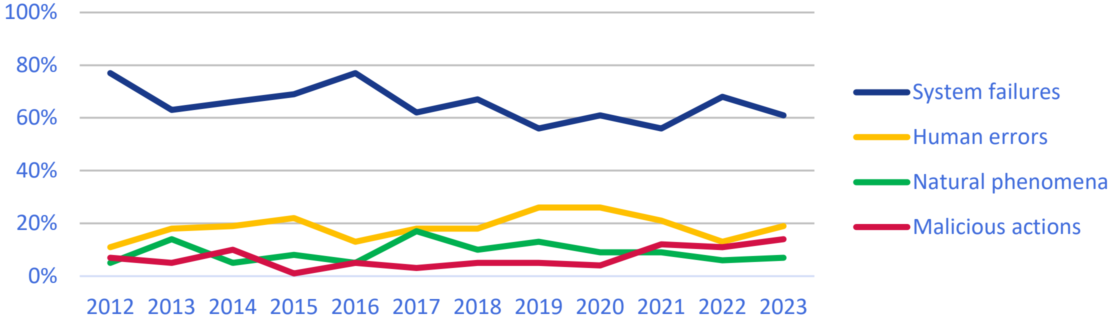
NIS2 Update now ongoing in ECASEC led by Malta

5G Security Controls Matrix

powered by ENISA

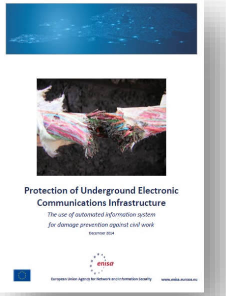
Implementing the EU 5G toolbox

Root causes EU Telecom security incidents



Examples of ENISA deep dives:

- Protection of underground cables
- Power supply dependencies
- National roaming for resilience
- Signaling security (SS7 4G, Diameter 5G)
- Security in 5G network slicing
- Security exceptions to net-neutrality rules
- 7 steps to shore up BGP
- 2020: Telecom security in a pandemic
- 2021: SIM Swapping
- 2021: EECC Consumer outreach by telcos about threats
- 2022: SS7 checklist
- 2022: eSIM security
- 2023: Subsea cables ecosystem
- 2024: CPE security (Home/SOHO internet modems/routers)
- 2025: Smishing



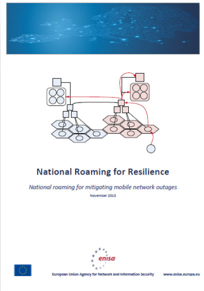
Protection of Underground Electronic Communications Infrastructure

The use of automated information system for damage prevention against civil work

December 2014

enisa

European Union Agency for Network and Information Security www.enisa.europa.eu



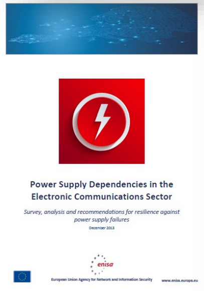
National Roaming for Resilience

National roaming for mitigating mobile network outages

November 2013

enisa

European Union Agency for Network and Information Security www.enisa.europa.eu



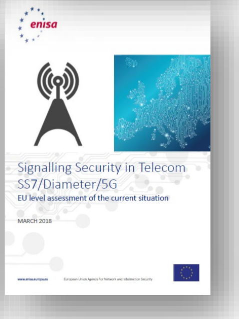
Power Supply Dependencies in the Electronic Communications Sector

Survey, analysis and recommendations for resilience against power supply failures

December 2013

enisa

European Union Agency for Network and Information Security www.enisa.europa.eu



enisa

Signalling Security in Telecom SS7/Diameter/5G

EU level assessment of the current situation

MARCH 2018

www.enisa.europa.eu European Union Agency For Network and Information Security

enisa

Guideline on assessing security measures in the context of Article 3(3) of the Open Internet regulation

VERSION 1.0 - DECEMBER 2018

www.enisa.europa.eu European Union Agency For Network and Information Security

enisa

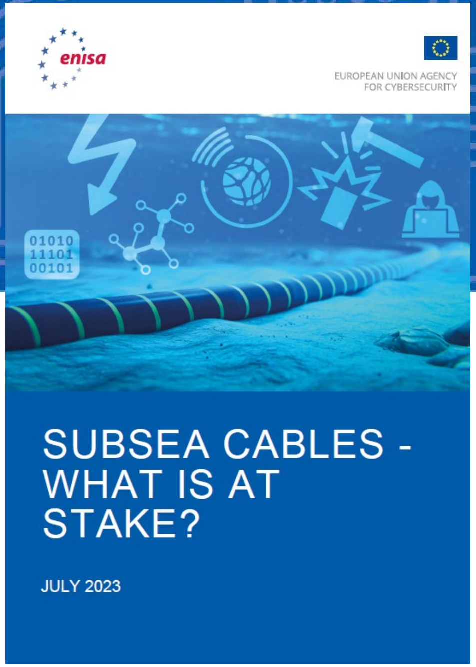
THE EU CYBERSECURITY AGENCY

7 STEPS TO SHORE UP BGP

MAY 2019

https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

ENISA PAPER ON SUBSEA CABLES



enisa

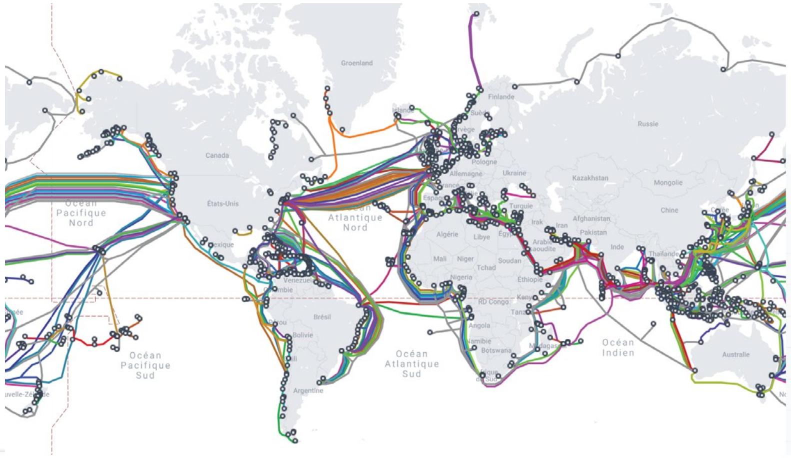
EUROPEAN UNION AGENCY FOR CYBERSECURITY

SUBSEA CABLES - WHAT IS AT STAKE?

JULY 2023

- Submarine fiber-optic cables, carry 90~95% of the international internet traffic.
  - Globally around 400 undersea cables in service.
- Complex ecosystem (cable owners, cable vessels, repair vessels)
- Mostly in international waters, hard to protect
- Highly strategic, geopolitics play a big role

- Concerns about **coordinated sabotage attack** on multiple cables, or an incident in a cable concentration point
- Cable laying and cable repair vessels highly specialized and there are only a few
- Landing points also need protection, for instance from sabotage
- Lead authority and mandate not always clear
- International interconnections are a grey area, need to be put in scope explicitly
- Paper at https://www.enisa.europa.eu/publications/undersea-cables



WHAT’S NEXT – AND WHAT ARE CHALLENGES

Have your say on the NIS2 technical guideline (deadline 9 December): www.enisa.europa.eu

Main activities in the coming months

- Nevers action plan (our ambition is to address all recommendations in 2024-2025)
  - Security of SOHO modems/routers aka CPE security, smishing prevention by operators
  - Subsea cable security (supporting the EU collaboration)
  - Survey to check telecom security maturity wrt other technical issues (SS7, BGP)
- NIS2 for telecoms: Update ENISA telecom security framework to align with NIS2
  - Further harmonization, security rules for telecoms, cloud, etc.
- Resilience stress tests, for instance on subsea cables

Challenges

- How to create a culture of trust, better reporting about non-outages and incidents at suppliers, 3rd party service providers?
- How to protect the larger most critical operators, especially in a crisis, disaster or black swan event.
- How to support the smaller companies in the sector or supply chain, with more basic security?

Q&A

YOUR INPUT, IDEAS, SUGGESTIONS VERY VERY WELCOME

GEORGIA BAFOUTSOU - FOR TELECOMS AND ECASEC GEORGIA.BAFOUTSOU@ENISA.EUROPA.EU

MARNIX DEKKER - FOR NIS2 MARNIX.DEKKER@ENISA.EUROPA.EU

☎ Email us or connect with us on Linkedin

✉ ENISA-NIS-Directive@enisa.europa.eu

🌐