EU policy on the cybersecurity of 5G networks

ENISA Telecom & Digital Infrastructure Security Forum 2024

Mélanie Scheidt
Unit Cybersecurity Technology and Capacity Building
DG CNECT, European Commission

The EU coordinated approach on 5G cybersecurity - Key milestones

⚠ **1.** Assessing risks

2. Identifying mitigating measures (5G Toolbox)

3. Implementing the 5G Toolbox

4. Complementing and expending the work on 5G cybersecurity

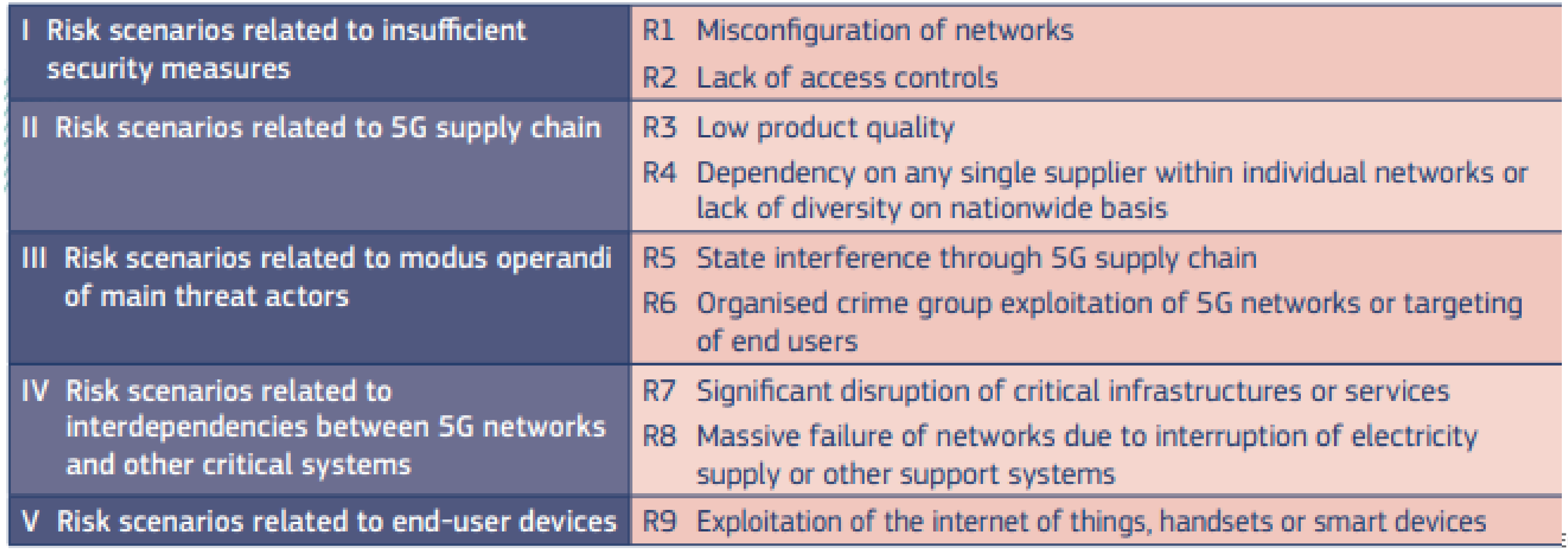
European Commission

1. Assessing risks

European
Commission

Results of 5G coordinated risk assessment (2019)

- Risk assessment carried out by competent national authorities
- Results consolidated in joint European report, supplemented by ENISA report
- Identifies **types of attackers**, **vectors**, **sensitive parts of the network**, **vulnerabilities**, and **major risks**

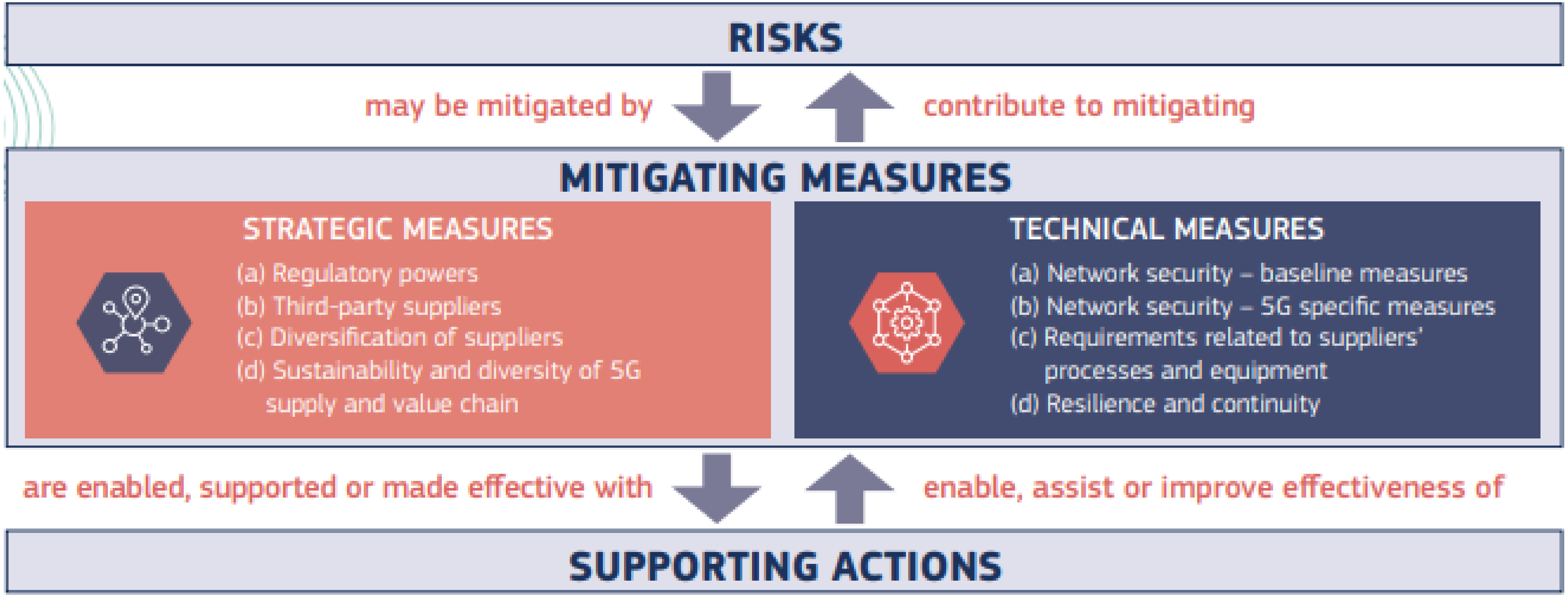


I Risk scenarios related to insufficient security measures	R1 Misconfiguration of networks
	R2 Lack of access controls
II Risk scenarios related to 5G supply chain	R3 Low product quality
	R4 Dependency on any single supplier within individual networks or lack of diversity on nationwide basis
III Risk scenarios related to modus operandi of main threat actors	R5 State interference through 5G supply chain
	R6 Organised crime group exploitation of 5G networks or targeting of end users
IV Risk scenarios related to interdependencies between 5G networks and other critical systems	R7 Significant disruption of critical infrastructures or services
	R8 Massive failure of networks due to interruption of electricity supply or other support systems
V Risk scenarios related to end-user devices	R9 Exploitation of the internet of things, handsets or smart devices

2. Identifying mitigating measures (5G Toolbox)

European Commission

5G Toolbox: Overview of measures (2020)



RISKS

may be mitigated by ↓ ↑ contribute to mitigating

MITIGATING MEASURES

STRATEGIC MEASURES

(a) Regulatory powers
(b) Third-party suppliers
(c) Diversification of suppliers
(d) Sustainability and diversity of 5G supply and value chain

TECHNICAL MEASURES

(a) Network security – baseline measures
(b) Network security – 5G specific measures
(c) Requirements related to suppliers' processes and equipment
(d) Resilience and continuity

are enabled, supported or made effective with ↓ ↑ enable, assist or improve effectiveness of

SUPPORTING ACTIONS

- ➢2 types of measures: strategic and technical
- ➢Identifies 8 strategic measures and 11 technical measures to mitigate risks

Measures concerning equipment and service suppliers

Assessment of risk profile of suppliers

- **Objective criteria**
- Importance of **non-technical risk factors**: legal obligations, judicial constraints, corporate governance of the supplier

Restrictions/exclusions for high-risk suppliers

- Restrictions to apply to **critical and sensitive parts of the network** → core network, network management and orchestration, access network functions
- **Transition periods** for replacement

European Commission

3. Implementing the 5G Toolbox

State of play on the implementation of the 5G Toolbox (15 June 2023)

1)
Member States report on implementation of Toolbox

2)
Commission Communication

1) Member States' report

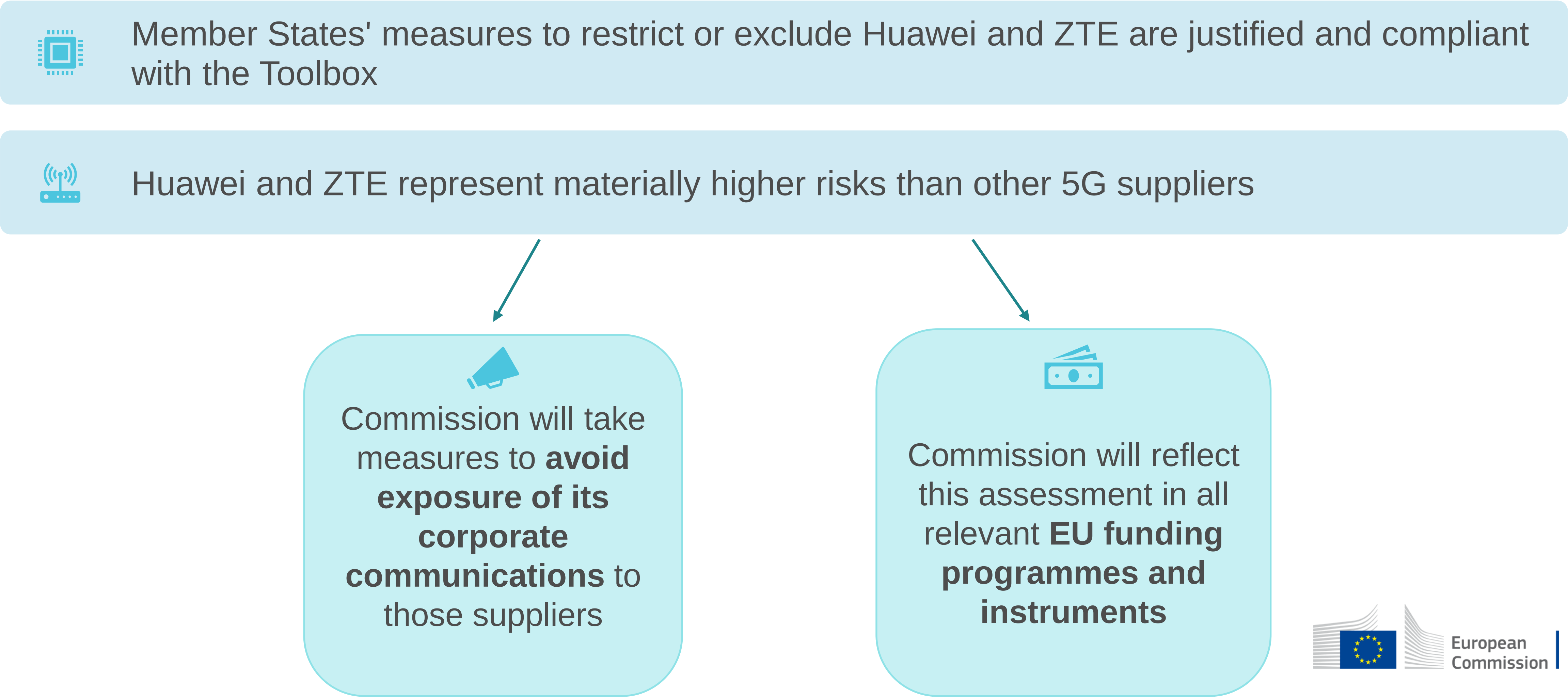
Significant progress with some shortcomings

All Member States to complete implementation of measures urgently

Risk of critical EU dependence on high-risk suppliers

- Take into account designations of HRS by other MS
- Impose restrictions without delay
- Restrictions must also apply to radio equipment (RAN)
- For equipment covered by restrictions, no installation of new equipment. Transition periods within the shortest possible timeframe

2) Commission Communication



Member States' measures to restrict or exclude Huawei and ZTE are justified and compliant with the Toolbox

Huawei and ZTE represent materially higher risks than other 5G suppliers

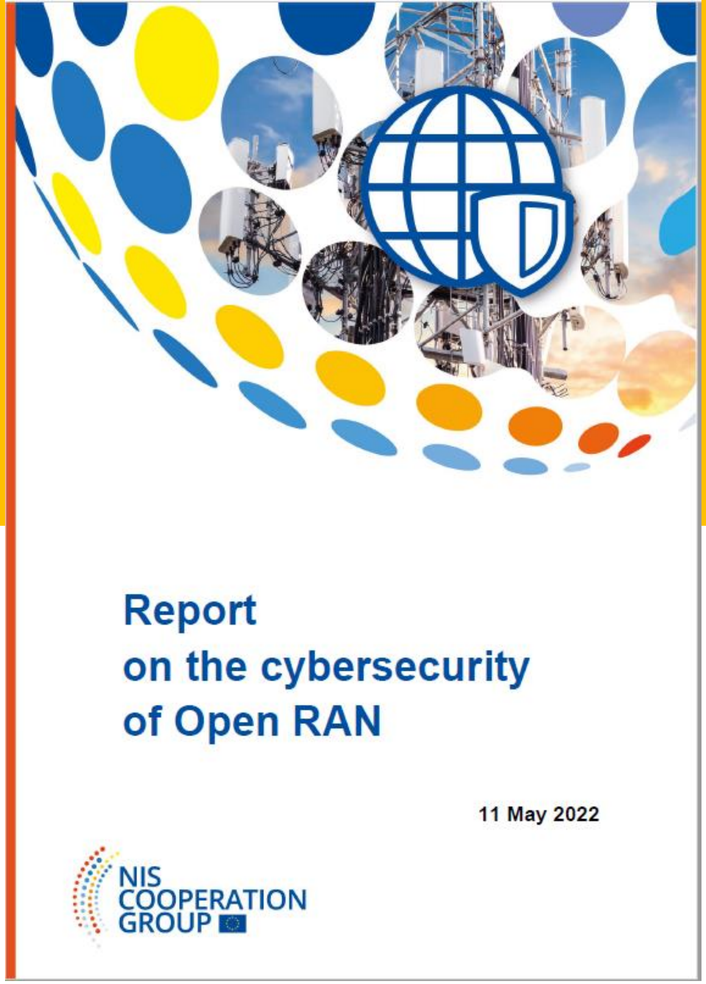
Commission will take measures to **avoid exposure of its corporate communications** to those suppliers

Commission will reflect this assessment in all relevant **EU funding programmes and instruments**

4. Complementing and expending the work on 5G cybersecurity

- Risk assessment on **Open RAN**
- Risk assessment on **connectivity networks and infrastructures**

4.1. Cybersecurity of Open RAN



Report
on the cybersecurity
of Open RAN

11 May 2022

NIS COOPERATION GROUP

Report on the cybersecurity of Open RAN (2022)

Security assessment of Open RAN

- Impact of Open RAN on identified security risks (from 5G risk assessment)
- New security risks of Open RAN
- Security opportunities of Open RAN

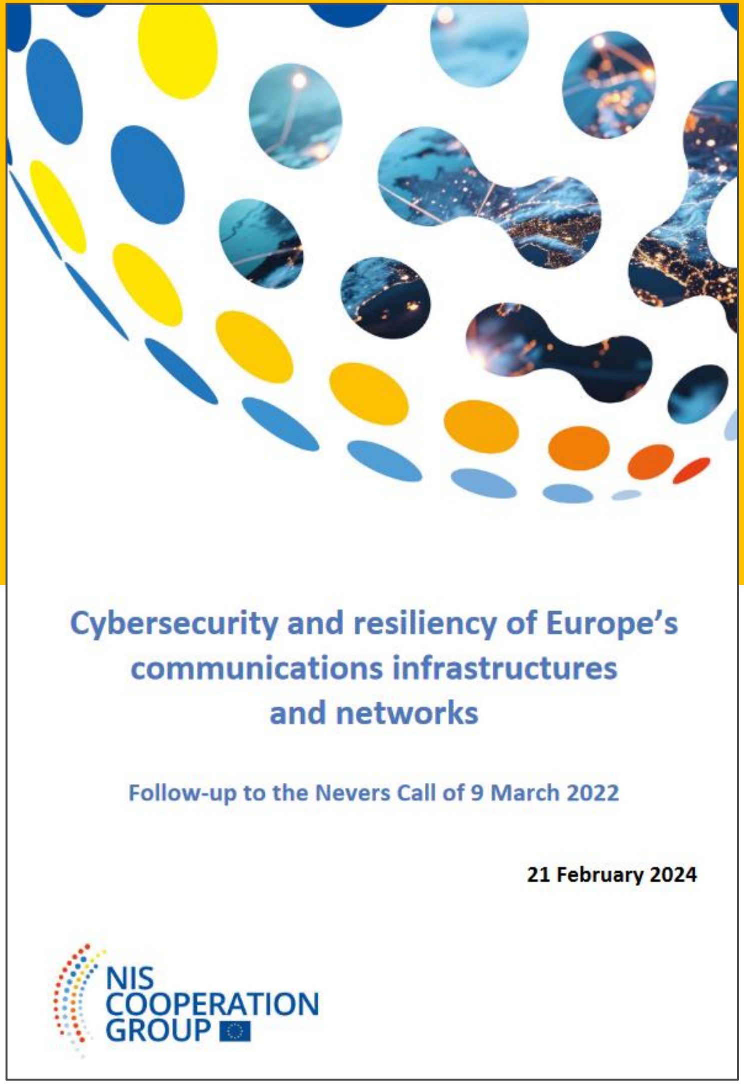
Guidance on Toolbox implementation for Open RAN deployments

- Certain 5G Toolbox measures need to be reinforced or adjusted, e.g.:
  - ➢ National authorities to scrutinise any large-scale Open RAN deployment
  - ➢ Look at dependencies from a broader perspective and not just the RAN

Main conclusions

- Cautious approach to moving towards this new architecture is recommended

4.2. Risk assessment on connectivity networks and infrastructures (2024)



Cybersecurity and resiliency of Europe's communications infrastructures and networks

Follow-up to the Nevers Call of 9 March 2022

21 February 2024

NIS COOPERATION GROUP

Scope

Risk scope:

- NIS2 **all-hazard approach**
- Risks of **cyber-attack**s on the **EU's communications networks and infrastructures**, by a hostile third country, i.e. nation state actors, but also organised crime groups and hacktivists acting in support of nation states
- Findings of **5G risk assessment and Toolbox** remain valid and relevant

Assets:

Public electronic communications networks:

- Mobile networks, including the signalling networks;
- Fixed networks;
- Satellite networks;

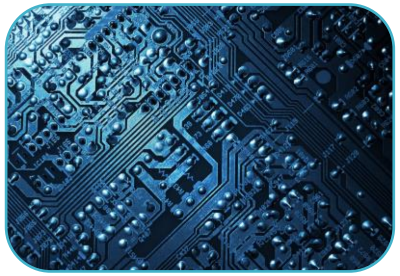
Core Internet infrastructure:

- Routing of Internet traffic;
- Submarine and underground cables;
- Internet exchange points (IXPs) and data centres;
- Networks and systems used for the provision of Top-level domain registries (TLDs) and Domain Name System (DNS) services.

Threats

T1. Wiper/ransomware attacks

T2. Supply chain attacks

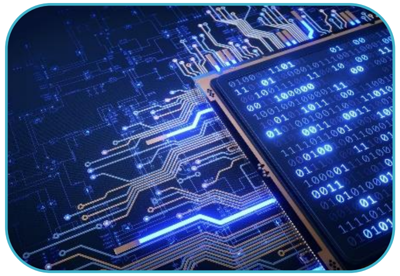


T3. Attacks on M(S)SP, or other third-party service provider

T4. Network intrusions

T5. DDoS attacks

T6. Physical attack/sabotage



T7. Nation State interference on supplier

T8. Interconnection attacks

T9. Power cuts affecting communications networks and infrastructures

T10. Insider threats

Vulnerabilities

V1. Vulnerable network equipment

V2. Vulnerable routing and interconnection protocols

V3. Vulnerable network management and operation

V4. Vulnerable end-user devices

V5. Vulnerable physical infrastructure

V6. Dependencies on suppliers and M(S)SPs

V7. Power supply dependencies

V8. Dependency on technical expertise

Spill-over effects

Disruption of access to **emergency services and numbers**, public warning systems

Disruption of emergency services if their communications and systems depend on the public mobile networks

Disruption of **digital payments**

Disruption of **secure communication** with potential consequences on national security

Disruption of other critical sectors such as the **health sector**

Recovery of the **energy** grid and energy supply would be more difficult

Potential impact on the **safety** of individuals, the security of systems or networks used in other critical sectors, and/or on the confidentiality of intellectual property, trade secrets, etc.

Risk scenarios

Risk level	Risk scenarios
High	**R1.** Wiper attack to cause a large-scale network outage
	R2. Supply chain attack to gain access to the infrastructure of operators
	R3. Network intrusion as a preparation for future cyber-attacks
	R4. Third-country interference on a supplier, M(S)SP or submarine cable
	R5. DDoS attack to cause a large-scale network outage
	R6. Coordinated physical sabotage/attack on digital infrastructure
	R7. SS7 signalling attack to intercept communications and geolocation of target persons
High to moderate	**R8.** Smishing attack to gain access to systems in other sectors
Moderate	**R9.** Power cut to cause a regional network outage
Low	**R10.** Interconnection attack to cause a large-scale network outage

Strategic recommendations

Resilience of international interconnections	• Assess resilience of international interconnections and clarify mandate • Assess criticality, resilience and redundancy of core Internet infrastructure, such as submarine cables
Supply chain risks	• Create transparency on the landscape of suppliers and M(S)SPs used for fixed networks, fibre technology, submarine cables, satellite networks and other important ICT suppliers
Situational awareness and operational collaboration	• Involve the sector in cyber exercises and operational collaboration • Foster information sharing and improve situational awareness about threats for the operators
Support operators with technical measures	• Provide funding support through relevant funding programmes to operators for technical measures against cyber-attacks in their networks
Physical attacks on digital infrastructure	• Exchange good practices among national authorities about physical attacks on digital infrastructure • Extend physical stress testing of critical infrastructure to include digital infrastructure

Technical recommendations

Mobile and fixed networks	• Exchange good practices to support the detection and prevention of signalling attacks • Exchange good practices to mitigate smishing attacks • Exchange good practices and develop technical guidelines on the security of home routers
Network traffic routing security (Telecoms-as-a-shield)	• Exchange good practices and develop technical guidelines about blocking of cyber-attacks by operators • Facilitate sharing of good practices on mitigating very large DDoS attacks
Submarine cables	• Exchange good practices and develop technical guidelines on the resilience of submarine cables
Satellite communication networks	• Develop good practices in the area of securing satellite networks
Core Internet infrastructure	• Raise awareness of BGP security and promote good practices for the security of global Internet routing • Develop guidelines to support Member States with cybersecurity supervision of IXPs and CDN