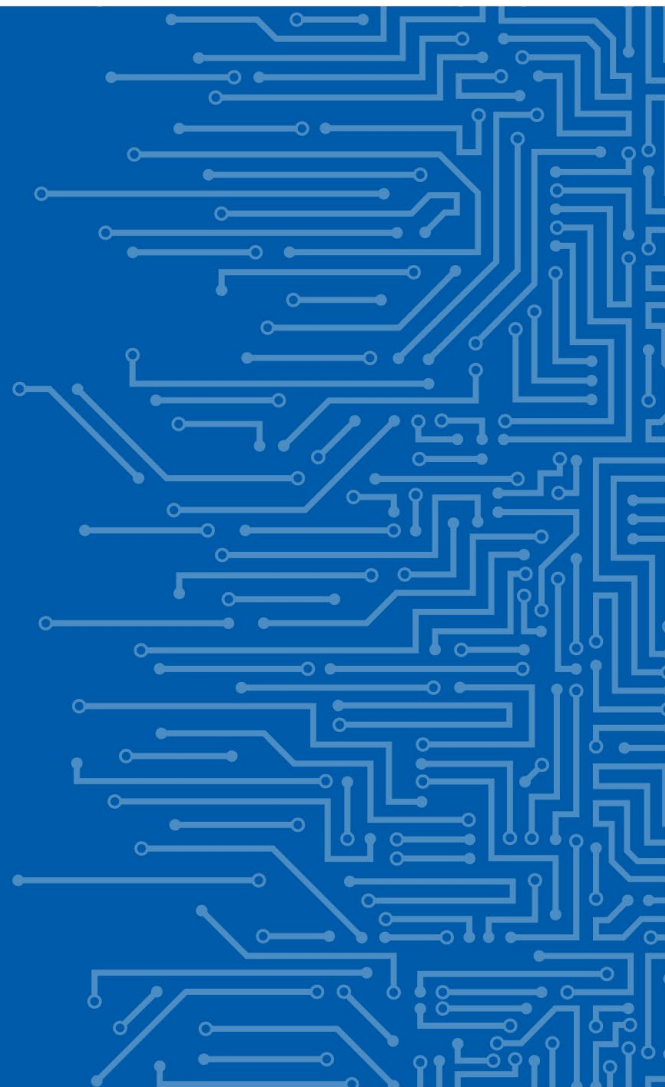# TELECOM SECURITY SUPERVISION AND 5G

7th BEREC Stakeholder Forum, Brussels

Dr. M.A.C. Dekker, ENISA

16 | 10 | 2019

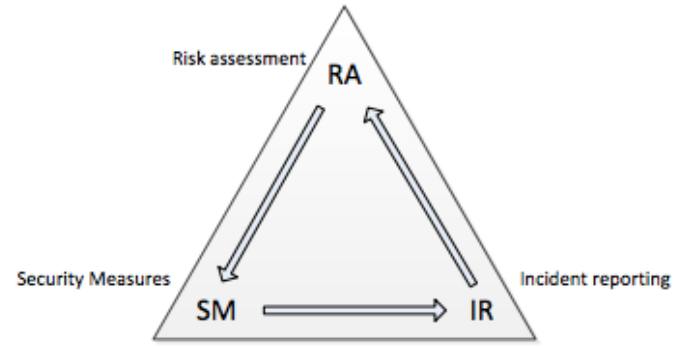# ENISA ACTIVITIES

CAPACITY
- ✓ **Hands on activities**

POLICY
- ✓ **Support MS & COM in Policy implementation**
- ✓ **Harmonisation across EU**

COMMUNITY

Mobilizing EU communities

EXPERTISE
- ✓ **Recommendations**
- ✓ **Independent Advice**
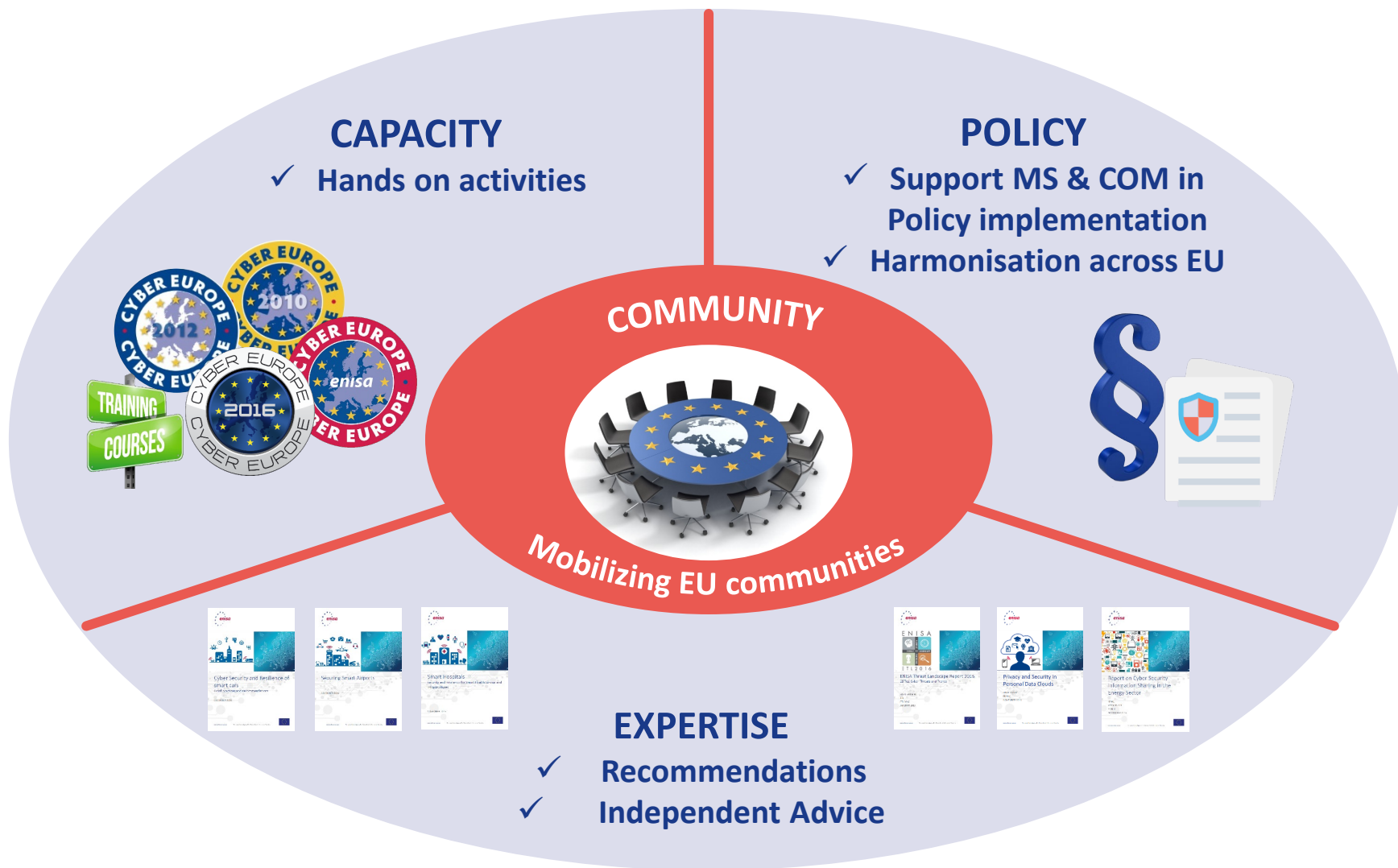
TIMELINE EU CYBERSECURITY LEGISLATION

**Review NISD
Scheduled for 2020**

**Electronic Communications Code
EECC, Article 40
Rules to come into effect end of 2020**

**NIS Directive
Security for OESs and DSPs, NISD Article 14, 16
Rules came into effect in 2018**

**eIDAS regulation (2014)
Security for trust services, eIDAS Article 19
Rules came into effect in 2016**

**EU Telecoms package (2009)
Article 13a, Framework directiveRules
came into effect in 2011**

Risk assessment RA

Security Measures

SM

IR

Incident reporting

enisa

SECURITY UNDER ARTICLE 13A

- Providers have to assess the security risks

- Providers have to take "appropriate" security measures

- Providers have to notify incidents with "significant" impact

- EU member states determine the precise requirements

  - Different requirements, different level of detail,

  - Different reporting thresholds, etc

- Article 13a security framework

  - Harmonization of the security requirements

  - Agreed by experts from EU telecom regulators

  - Standards neutral, but mapping to industry standards

  - Maturity levels (one size does not fit all)

  - https://resilience.enisa.europa.eu/article-13

Article 13a Security framework

D1: Governance and risk management
- SO 1: Information security policy
- SO 2: Governance and risk management
- SO 3: Security roles and responsibilities
- SO 4: Security of third party assets

D2: Human resources security
- SO 5: Background checks
- SO 6: Security knowledge and training
- SO 7: Personnel changes
- SO 8: Handling violations

D3: Security of systems and facilities
- SO 9: Physical and environmental security
- SO 10: Security of supplies
- SO 11: Access control to network and information systems
- SO 12: Integrity of network and information systems

D4: Operations management
- SO 13: Operational procedures
- SO 14: Change management
- SO 15: Asset management

D5: Incident management
- SO 16: Incident management procedures
- SO 17: Incident detection capability
- SO 18: Incident reporting and communication

D6: Business continuity management
- SO 19: Service continuity strategy and contingency plans
- SO 20: Disaster recovery capabilities

D7: Monitoring, auditing and testing
- SO 21: Monitoring and logging policies
- SO 22: Exercise contingency plans
- SO 23: Network and information systems testing
- SO 24: Security assessments
- SO 25: Compliance monitoring

enisa

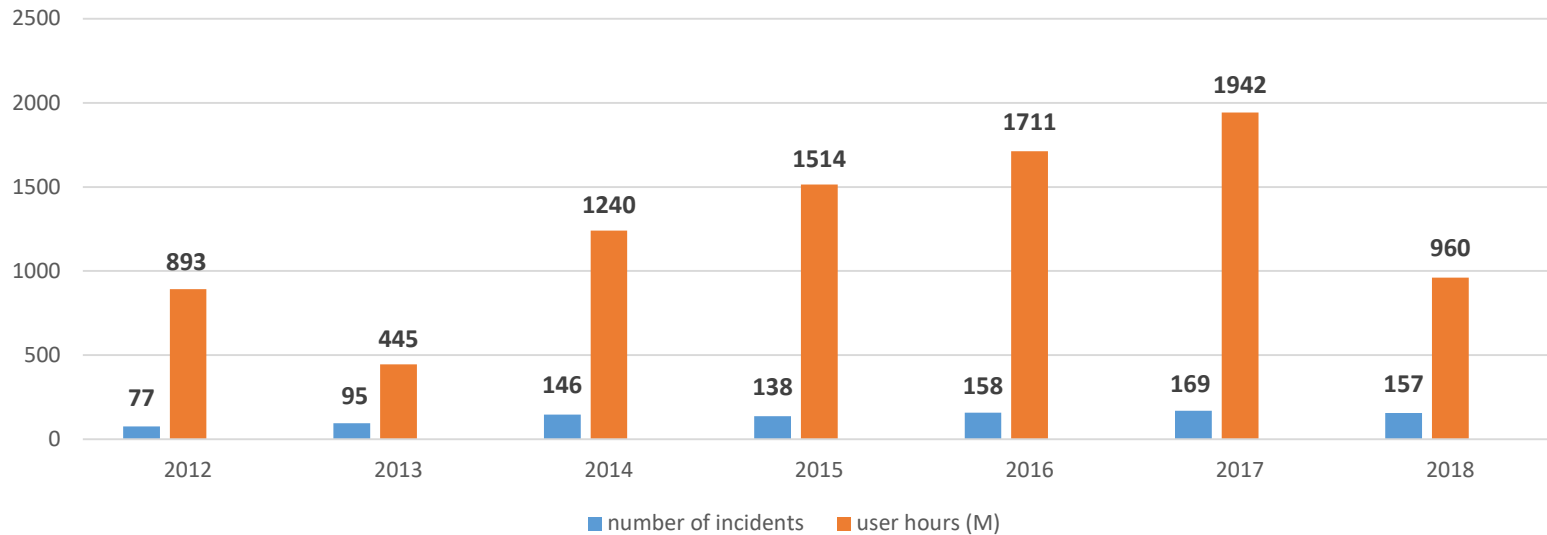# TELECOM SECURITY BREACH REPORTING
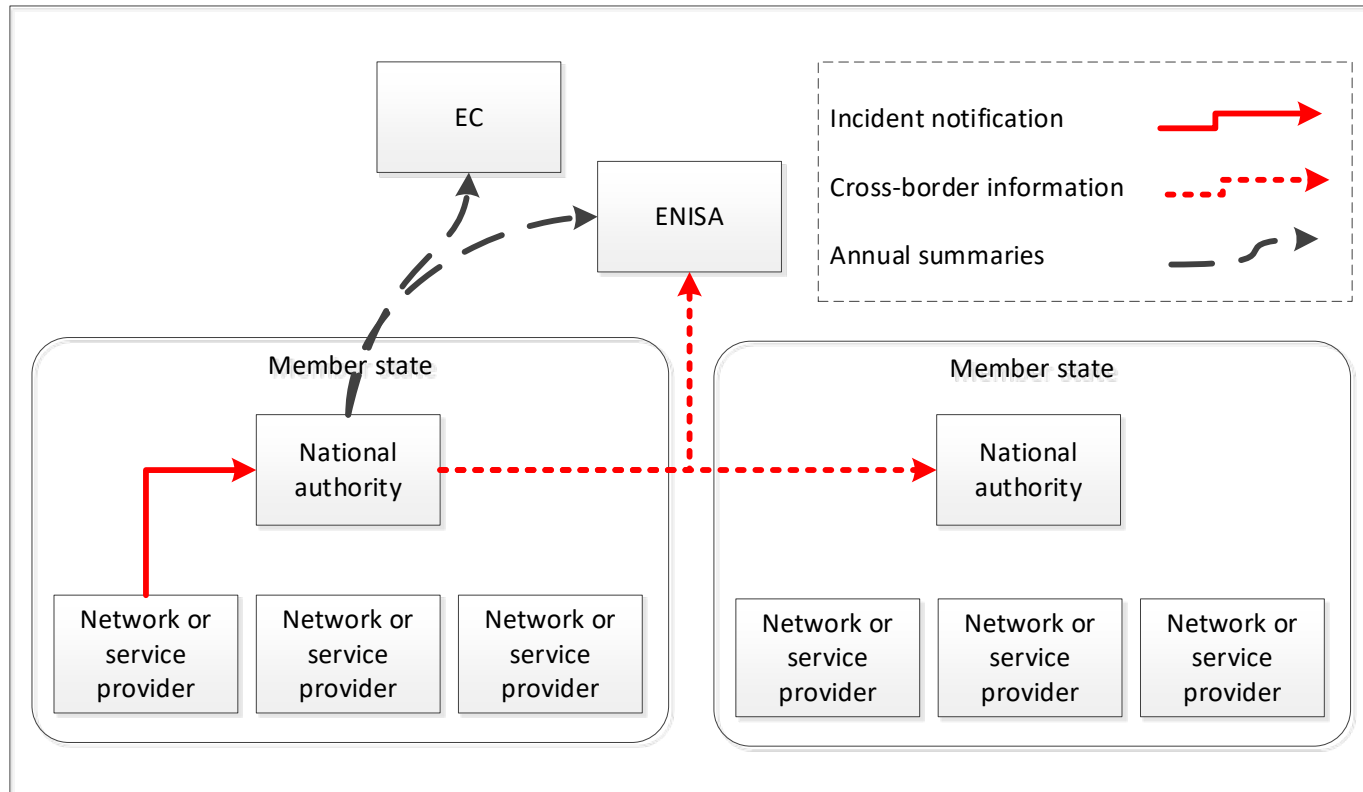
*) note that reporting is mandatory for incidents with significant impact
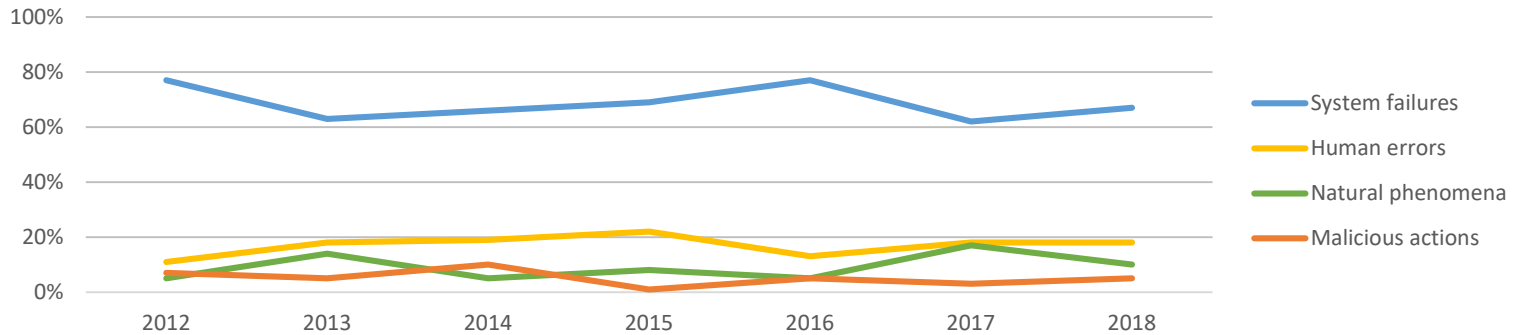   - in most countries the incident needs to impact 100.000s of subscribers

**) note that what is an incident for a subscriber is not always an incident for the telecom provider,
            - telecom providers do not (and cannot) check everything that passes over their wires

EU TELECOM SECURITY BREACH REPORTING OVER THE YEARS

Number of incidents and million user hours lost per year

Bar chart showing number of incidents and user hours (M) per year:

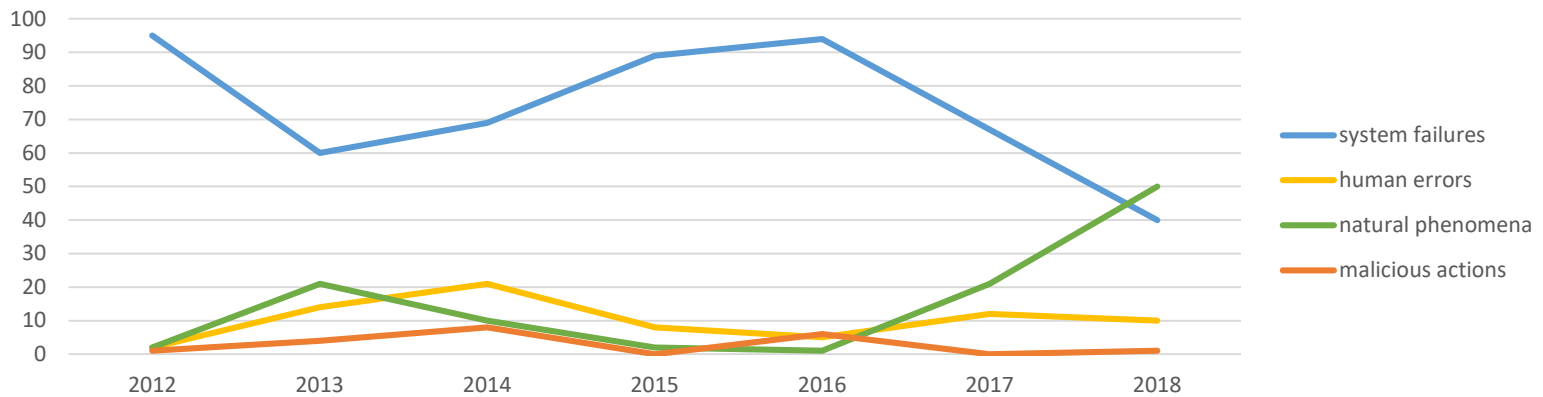| Year	number of incidents	user hours (M)
2012	77	893
2013	95	445
2014	146	1240
2015	138	1514
2016	158	1711
2017	169	1942
2018	157	960

■ number of incidents   ■ user hours (M)

enisa

Root cause categories Telecom security incidents in the EU - reported over 2012-2018

Legend:
- System failures
- Human errors
- Natural phenomena
- Malicious actions

User hours lost per root cause category - multiannual 2012-2018 (percentage of total user hours lost)

Legend:
- system failures
- human errors
- natural phenomena
- malicious actions

See also the online visual tool for analysing the incidents and diving into the ~1000 reports
https://www.enisa.europa.eu/topics/incident-reporting/for-telcos/visual-tool

OTHER ENISA TELECOM SECURITY WORK

- 2018 paper on the security issues with the SS7 interconnection protocol

- 2018 paper on the security exceptions to the EU net-neutrality rules
  - In collaboration with BEREC

- 2019 paper on BGP security (7 steps to shore up BGP)

- Ongoing work on security supervision under the EECC
  - ENISA paper on security supervision under the new EECC, to be published very soon
  - Draft was reviewed by BEREC

- Ongoing work on 5G security, within the NIS Cooperation Group
  - BEREC is part of the 5G work stream

enisa

NIS DIRECTIVE IN A NUTSHELL

- **Chapter I: General provisions**
  - Boost overall level of cybersecurity
  - Minimum harmonization approach (go beyond)

- **Chapter II: National cybersecurity capabilities**
  - Designate national competent authorities and SPOC
  - Establish a national CSIRT
  - Adopt a national cybersecurity strategy

- **Chapter III: Cooperation**
  - EU-wide NIS Cooperation group
  - EU-wide CSIRT Network

- **Chapter IV: Security of essential services**
  - Includes IXPs, DNS, TLDs
  - National approach, ex-ante supervision

- **Chapter V: Security of digital services**
  - Includes cloud services, marketplaces, search engines
  - EU approach, light touch, ex-post supervision

- **Chapter VI: Standardisation and voluntary notification**

Policy	Sector	Subsectors
NISD OES – Article 14	**Energy**	Electricity
		Oil
		Gas
	Transport	Aviation
		Rail
		Maritime
		Road
	Finance	Financial market infra
		Banking
	Health	
	Drinking water	
	Digital infrastructure	IXP, TLDs, DNS providers
NISD DSP – Article 16	**Digital service providers**	Online marketplaces, online search engines, cloud computing providers
Article 19	**Electronic trust services**	Electronic trust service providers (TSPs) like certificate authorities
Article 13a	**Electronic communications**	Electronic communication providers, telcos and OTT service providers (EECC)

enisa

NIS Cooperation group

NIS Cooperation group
Chair: Rotating with EU presidency
Secretariat: European Commission

Biannual Work program
2018-2020

| WS1: OES Identification criteria (led by DE) | WS2: OES Security measures (led by FR) | WS3: Incident reporting (led by RO) (previously NL/PL) | WS4: Cross-border dependencies (led by EE) | WS5: Digital service providers (NL previously IE) |

| WS6: Cybersecurity of EP elections (led by EE/CZ) | WS7: Large scale incidents (blueprint) (led by FR/ES) | WS8: Energy sector (led by AT) | WS9: National Cyber capabilities (led by AT/UK) | WS10: Digital infrastructure (led by PL) |

WS on 5G cybersecurity

ENISA supports all work streams with drafting, research, analysis, surveys, exercises, etc.

Article 13a group
eComms security
(chaired by NL)

Article 19 group
eTrust security
(chaired by AT)

5G CYBERSECURITY ACTIVITIES

NIS Cooperation group work stream on 5G

    BEREC representatives are member of this work stream

Part 1: National 5G risk assessments

    Output: EU coordinated risk assessment of 5G networks security

    Published 9 October https://europa.eu/rapid/press-release_IP-19-6049_en.htm

Part 2: ENISA Threat landscape
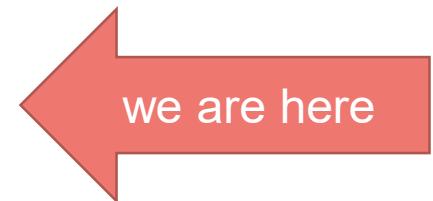
    Detailed overview of technical assets and threats

    Close to publication, review by Member States of the final draft
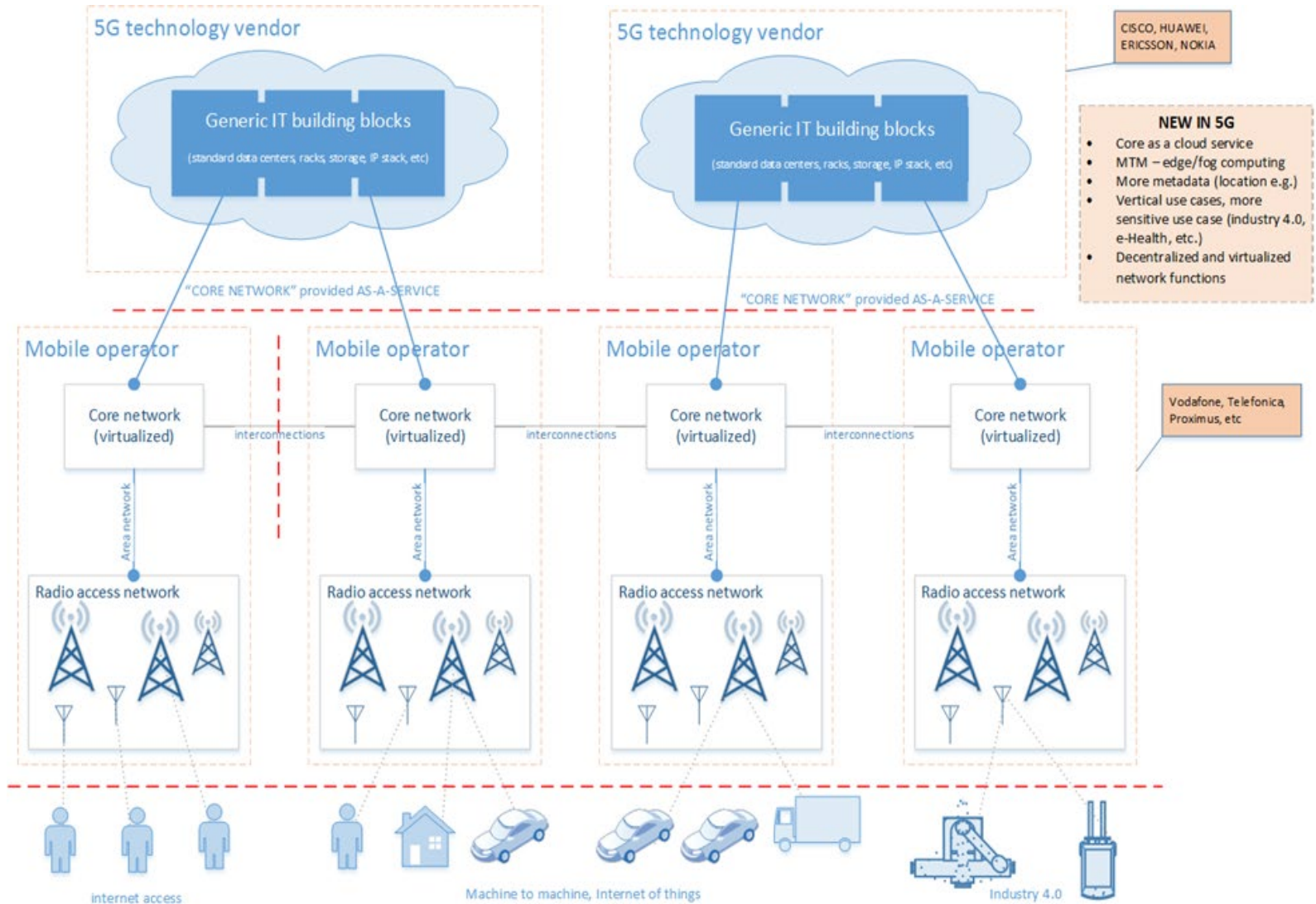
Part 3: 5G Toolbox

we are here

    Work just started, due to be finalized end of 2019

    We are using also the input from the BEREC 5G survey

5G FUTURE SETUP

5G technology vendor

Generic IT building blocks

(standard data centers, racks, storage, IP stack, etc)

5G technology vendor

Generic IT building blocks

(standard data centers, racks, storage, IP stack, etc)

CISCO, HUAWEI, ERICSSON, NOKIA

NEW IN 5G
- Core as a cloud service
- MTM – edge/fog computing
- More metadata (location e.g.)
- Vertical use cases, more sensitive use case (industry 4.0, e-Health, etc.)
- Decentralized and virtualized network functions

"CORE NETWORK" provided AS-A-SERVICE

"CORE NETWORK" provided AS-A-SERVICE

Mobile operator

Core network (virtualized)

Mobile operator

Core network (virtualized)

Mobile operator

Core network (virtualized)

Mobile operator

Core network (virtualized)

interconnections

interconnections

interconnections

Vodafone, Telefonica, Proximus, etc

Area network

Area network

Area network

Area network

Radio access network

Radio access network

Radio access network

Radio access network

internet access

Machine to machine, Internet of things

Industry 4.0

enisa

CONTACT US,
WORK WITH US

marnix.dekker@enisa.europa.eu

ENISA, the EU Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu