



THE EU CYBERSECURITY AGENCY

ENISA THREAT LANDSCAPE ON 5G NETWORKS

Louis Marinos

12 | 12 | 2019



TELECOM SECURITY SUPERVISION AND 5G

Dr. M.A.C. Dekker, ENISA

12 | 12 | 2019 Prague cybersecurity meeting



THE EU CYBERSECURITY AGENCY

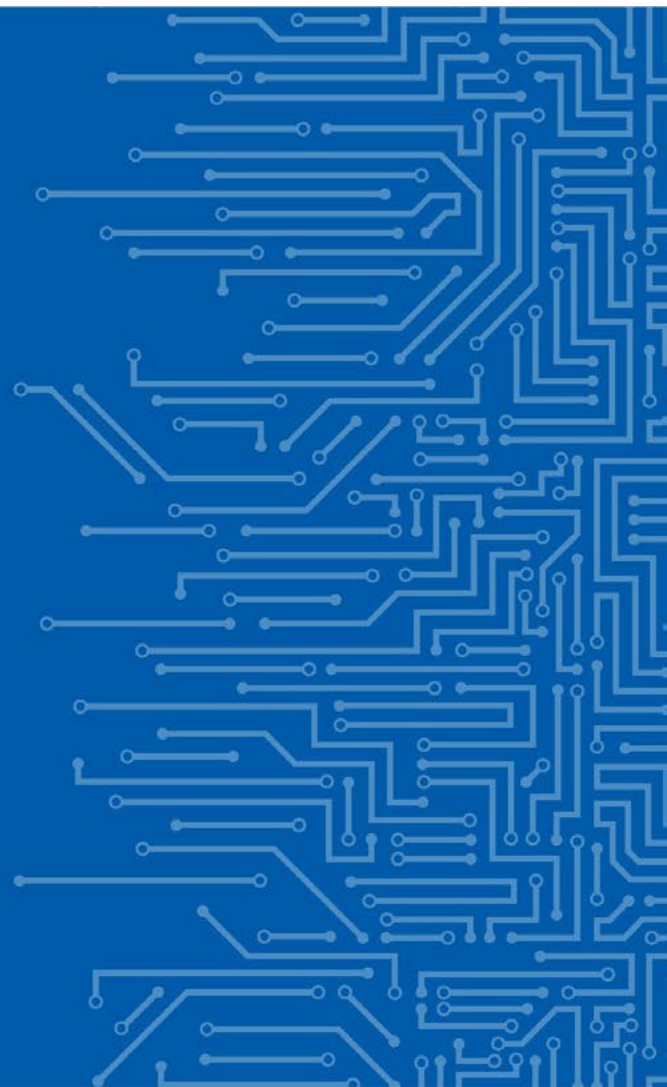


TELECOM SECURITY SUPERVISION AND 5G

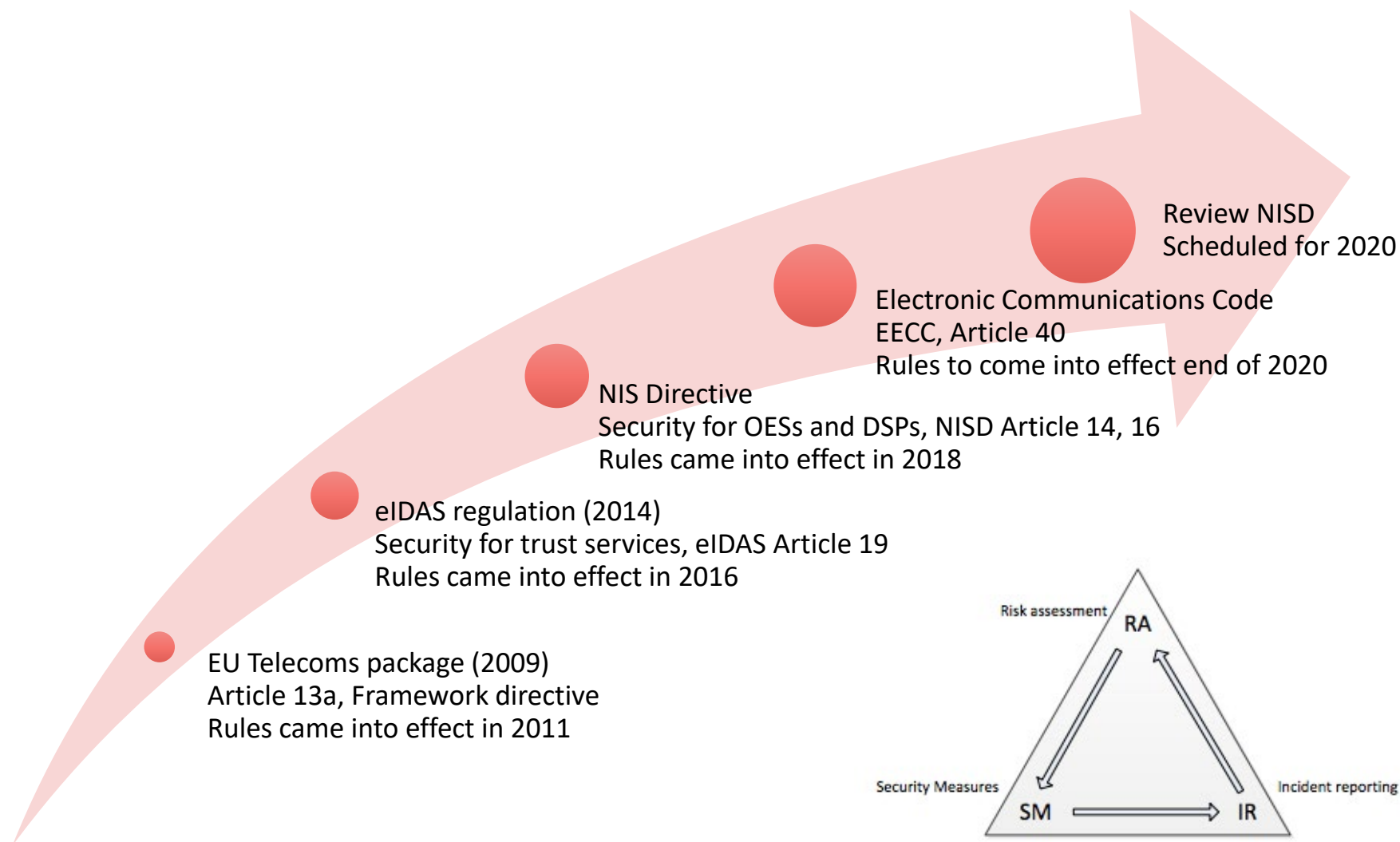
Dr. M.A.C. Dekker, ENISA

12 | 12 | 2019

Prague cybersecurity meeting



TIMELINE EU CYBERSECURITY LEGISLATION



TELECOM SECURITY (ARTICLE 13A)

1. Providers have to assess the security risks
 2. Providers have to take “appropriate” security measures
 3. Providers have to notify incidents with “significant” impact
- EU member states determine the precise requirements
 - Different requirements, different level of detail,
 - Different reporting thresholds, timing, 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

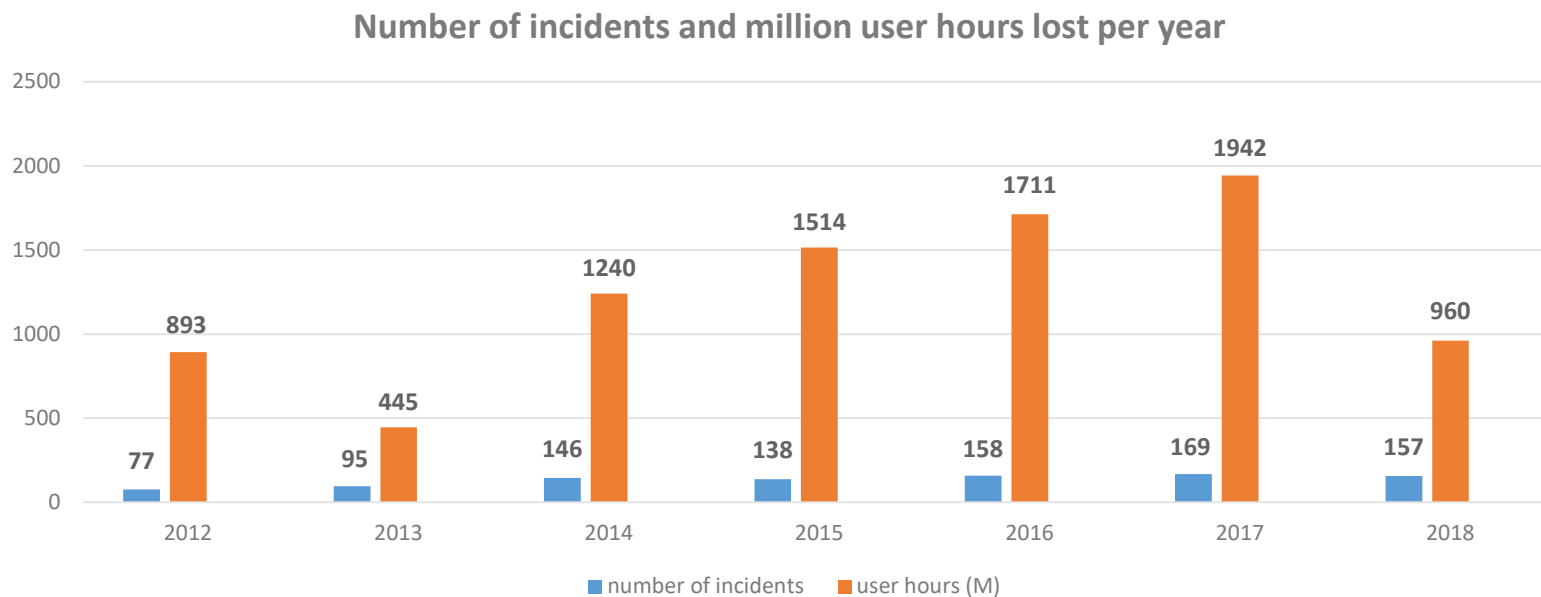
- SO 19: Service continuity strategy and contingency plans
- SO 20: Disaster recovery capabilities

D7: Monitoring, auditing and testing

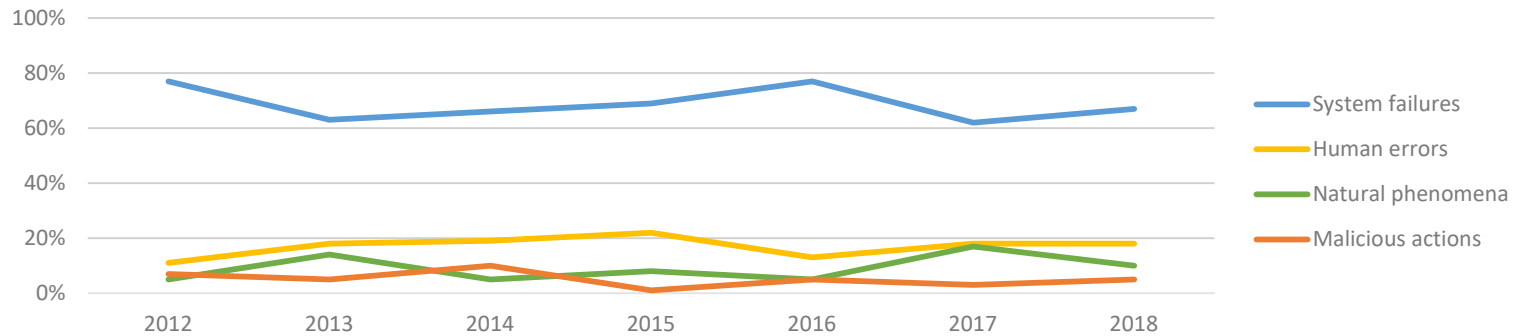
- SO 21: Monitoring and logging policies
- SO 22: Exercise contingency plans
- SO 23: Network and information systems testing
- SO 24: Security assessments
- SO 25: Compliance monitoring



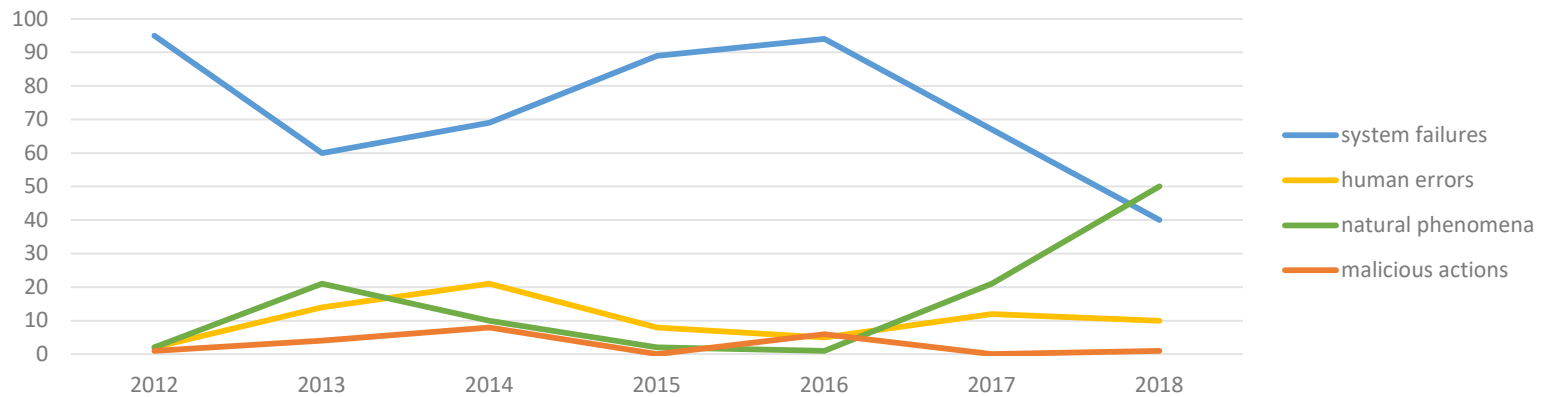
EU TELECOM SECURITY BREACH REPORTING OVER THE YEARS



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



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



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
 - Draft was reviewed by BEREC
 - to be published very soon
- Ongoing work on 5G security, within the NIS Cooperation Group
 - BEREC is part of the 5G work stream (the BEREC adhoc working group on 5G)

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)

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)

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

WS on 5G
cybersecurity

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

Part 1: National 5G risk assessments (NIS CG document)

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 (ENISA paper)

Detailed overview of technical assets and threats

<https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks>

Published 21 November

Part 3: 5G Toolbox (NIS CG document)

Due end of 2020

Work almost done, final drafting stages



we are here

CONTACT US, WORK WITH US

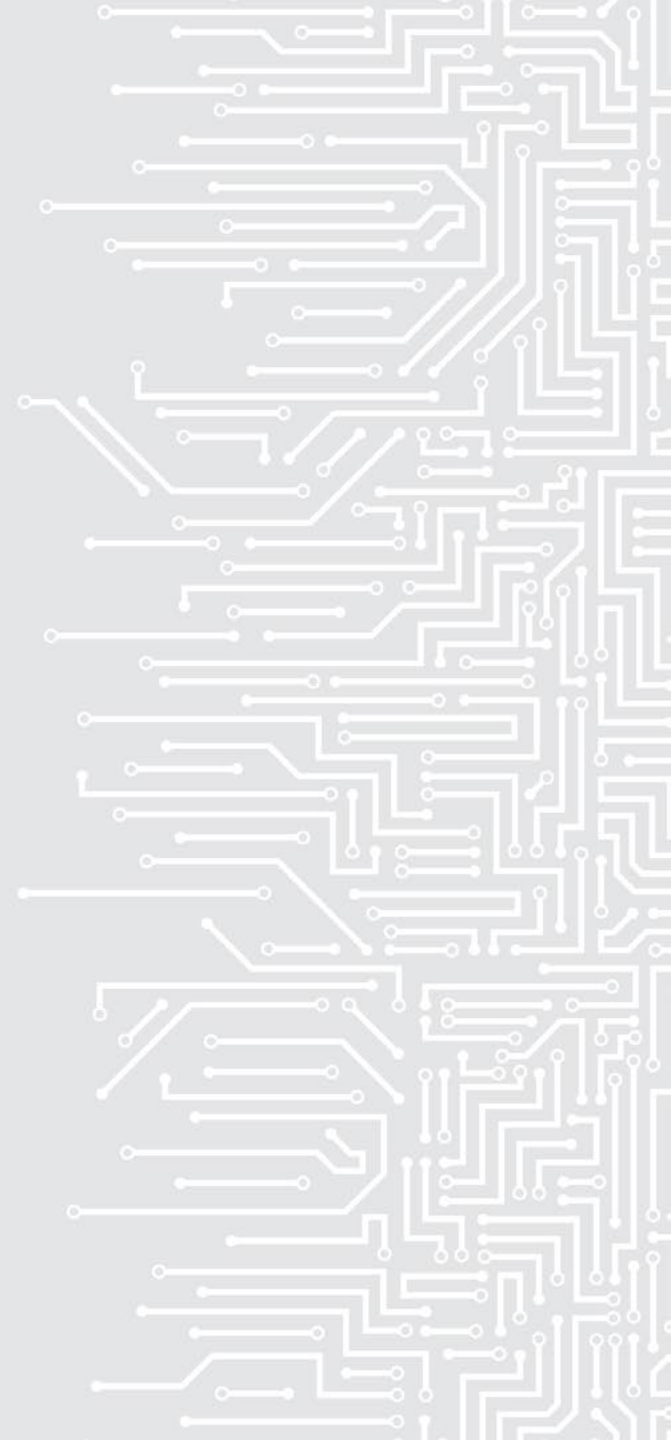
marnix.dekker@enisa.europa.eu

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



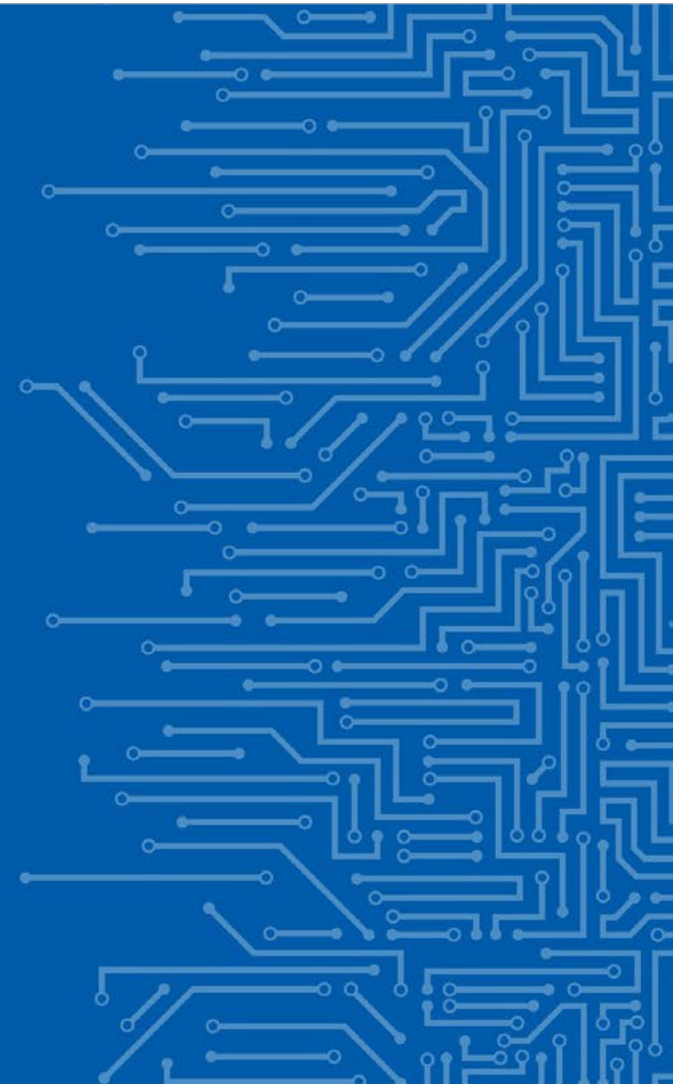


THE EU CYBERSECURITY AGENCY

ENISA THREAT LANDSCAPE ON 5G NETWORKS

Louis Marinos

12 | 12 | 2019





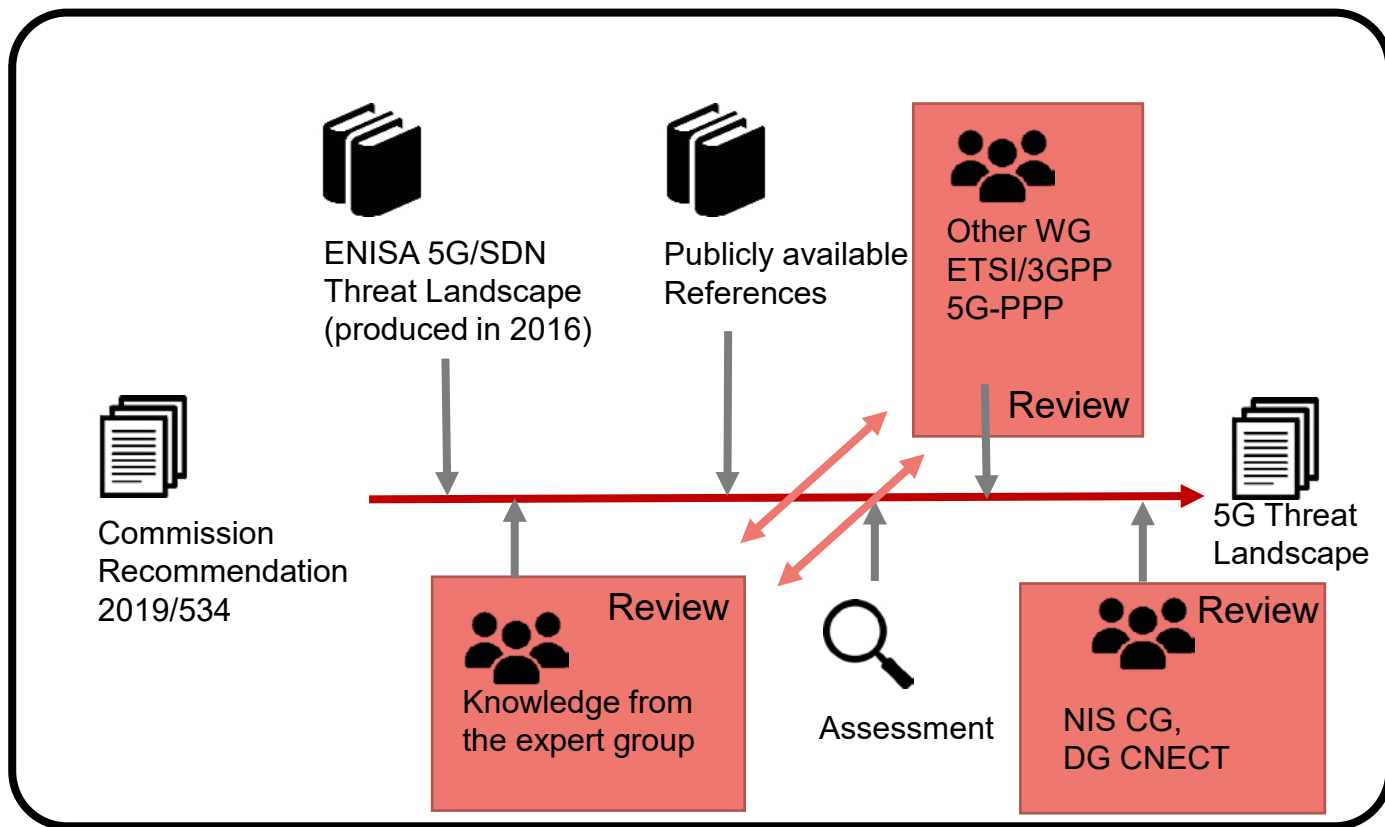
COMMISSION RECOMMENDATION 5G

The Commission Recommendation “EC(2019) 2335 final” states:

“Member States should transmit their national risk assessments to the Commission and to the European Agency for Cybersecurity (ENISA) by 15 July 2019...”

The European Agency for Cybersecurity (ENISA) should complete a specific 5G networks threat landscape mapping.”

PROCESS OF ENISA 5G ETL





SCOPE/OBJECTIVES

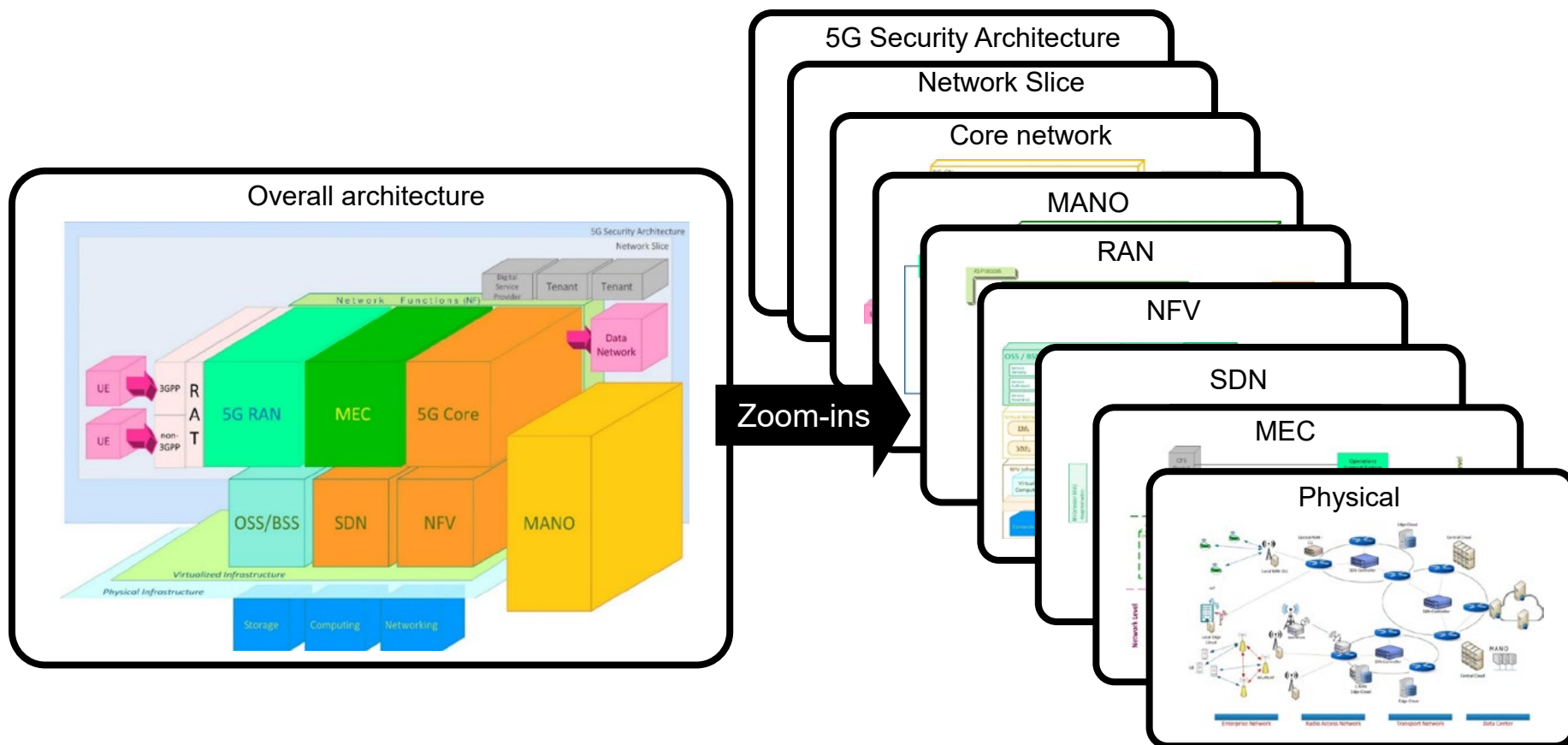
- Review the 5G/SDN Threat Landscape produced by ENISA in 2016.
- Involve members from the **community of experts**.
- Define a general **5G architecture** for the purpose of the assessment.
- Focus on 5G **network functions** specification.
- Assess the most **relevant assets** based on the general 5G architecture and information available from open sources.
- Identify the **known threats** targeting the assets.
- Identify the trends associated with **threat agent groups** that are likely to target 5G Networks.
- Prepare **recommendations** for future assessments.

THE ENTIRE MATERIAL PROCESSED IS BASED ON 5G SPECIFICATIONS

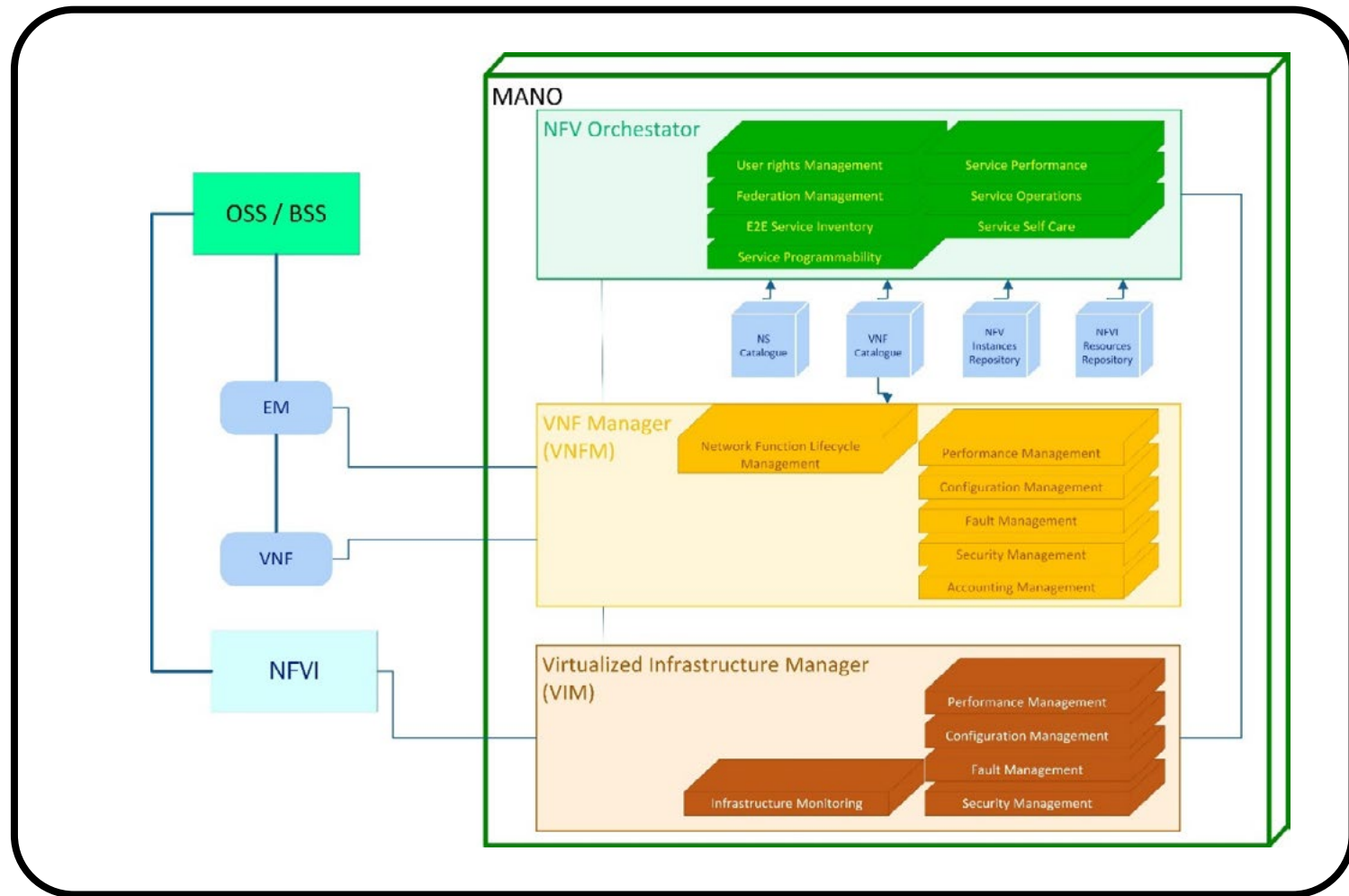


KEY FINDINGS

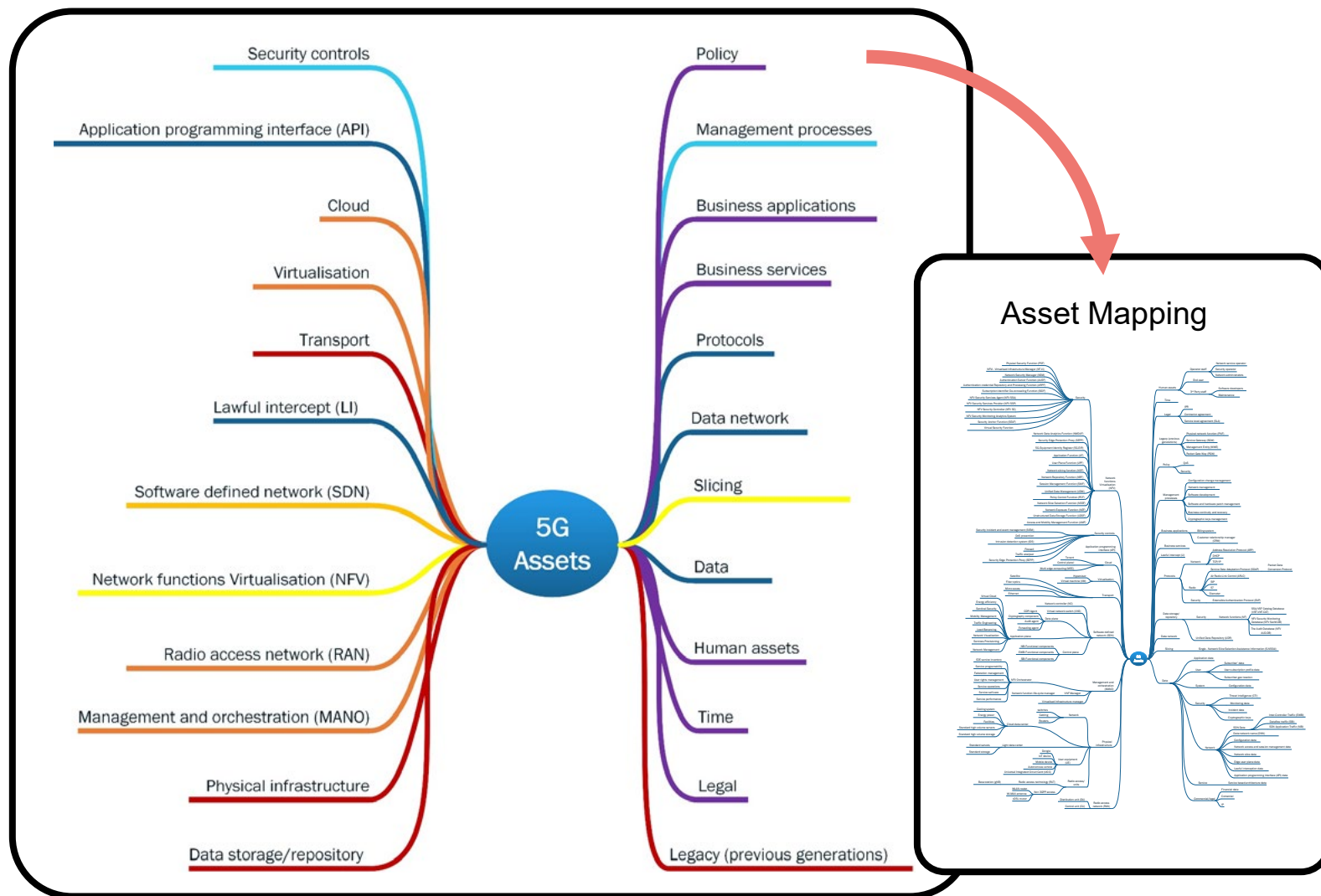
GENERAL 5G ARCHITECTURE



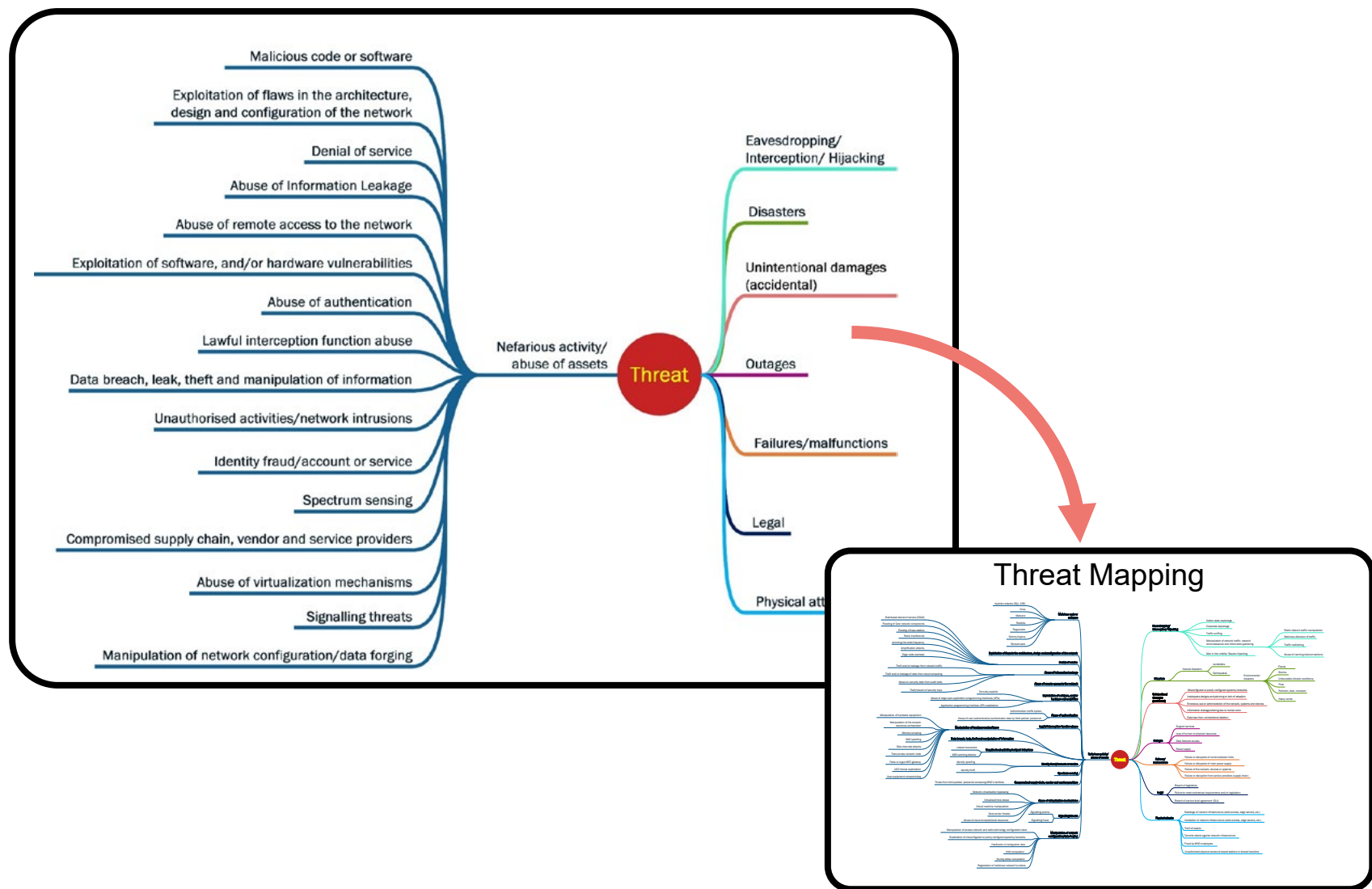
MANO ZOOM-IN (EXAMPLE)



ASSET GROUPS



HIGH LEVEL THREAT TAXONOMY



THREAT ASSESSMENT

Threat Type	Threats	Potential Effect	Affected Assets	
Nefarious Activity/ Abuse of assets (NAA)	Manipulation of network configuration/data forging <ul style="list-style-type: none"> - Routing tables manipulation - Falsification of configuration data - DNS manipulation - Manipulation of access network and radio technology configuration data - Exploitation of misconfigured or poorly configured systems/networks - Registration of malicious network functions 	<ul style="list-style-type: none"> - Information integrity - Information destruction - Service unavailability 	<ul style="list-style-type: none"> - SDN, NFV, MANO - RAN, RAT 	<ul style="list-style-type: none"> - System configuration data - Network configuration data - Security configuration data - Business services
	Exploitation of software, hardware vulnerabilities <ul style="list-style-type: none"> - Zero-day exploits - Abuse of edge open application programming interfaces (APIs) - Application programming interface (API) exploitation 	<ul style="list-style-type: none"> - Information integrity - Information destruction - Service unavailability 	<ul style="list-style-type: none"> - SDN, NFV, MANO - RAN, RAT - MEC - API - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation 	<ul style="list-style-type: none"> - Subscribers' data - Application data - Security data - Network data - Business services
	Denial of service (DoS) <ul style="list-style-type: none"> - Distributed denial of service (DDoS) - Flooding of core network components - Flooding of base stations - Amplification attacks - MAC layer attacks - Jamming of the network radio - Edge node overload 	<ul style="list-style-type: none"> - Service unavailability - Outage 	<ul style="list-style-type: none"> - SDN, NFV - RAN, RAT - MEC - CLOUD 	<ul style="list-style-type: none"> - Network services - Business services
	Remote access exploitation	<ul style="list-style-type: none"> - System integrity 	<ul style="list-style-type: none"> - SDN, NFV, MANO - CLOUD 	<ul style="list-style-type: none"> - Network services
	Malicious code/software <ul style="list-style-type: none"> - Injection attacks (SQL, XSS) - Virus - Malware - Rootkits - Rogueware - Worms/trojan 	<ul style="list-style-type: none"> - Service unavailability - Information integrity - Information destruction - Other software asset integrity - Other software asset destruction 	<ul style="list-style-type: none"> - Data network - Business applications - Security controls - Cloud, virtualisation 	<ul style="list-style-type: none"> - Subscribers' data - Application data - Security data - Network data - Business services - Network services



THREAT AGENT GROUPS

- Cyber criminals
- Insider (own, third parties)
- Nation states
- Hacktivists
- Cyber-fighters
- Cyber-terrorists
- Corporations
- Script kiddies



RECOMMENDATIONS (1/2)

Recommended courses of action for ENISA

- Disseminate current details of 5G assets and 5G threat landscape to all kinds of stakeholders
- Refine/amend existing material according to the pace of 5G developments
- Establish hooks to enroll and mobilize strategic stakeholders

Recommended courses of action at EU-Level

- Inject existing 5G knowledge to stakeholder communities
- Create /mandate bridges between all stakeholders
- Enable iterations necessary to develop current material on cyber threat



RECOMMENDATIONS (2/2)

Recommendations for 5G market players

- Engage in EU-wide discussions on 5G matters
- Contribute to the knowledge collection/dissemination
- Bring in knowledge on economic/investment/market penetration dimensions

Recommendations for EU competent bodies in the area of 5G cybersecurity:

- Disseminate existing 5G material
- Inform about 5G activities held in the scope of responsibilities
- Provide available expertise and human resources

THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

 +30 28 14 40 9711

 info@enisa.europa.eu

 www.enisa.europa.eu

