THE EU CYBERSECURITY AGENCY

ENISA THREAT LANDSCAPE ON 5G NETWORKS

Louis Marinos

12 | 12 | 2019

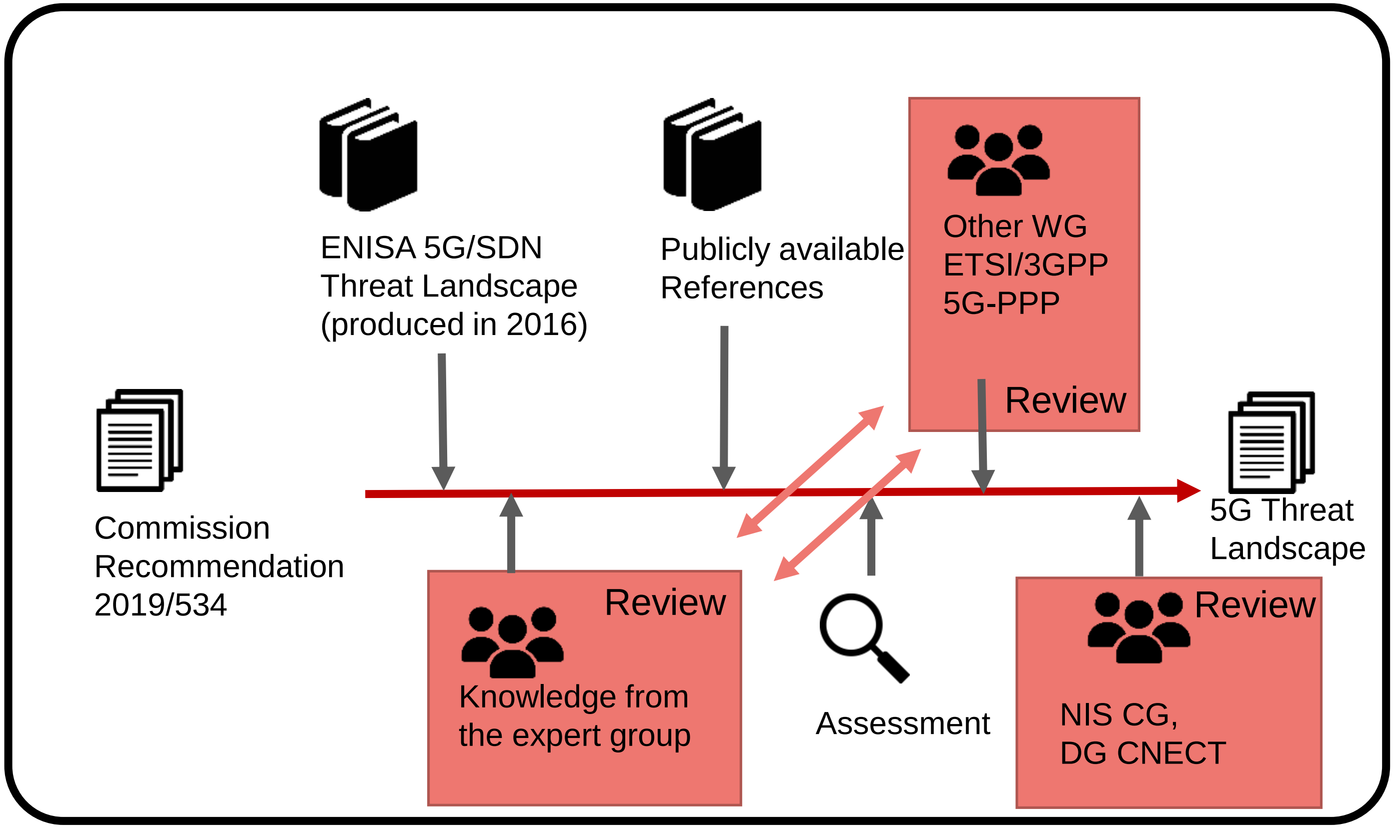
COMMISSION RECOMMENDATION 5G

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



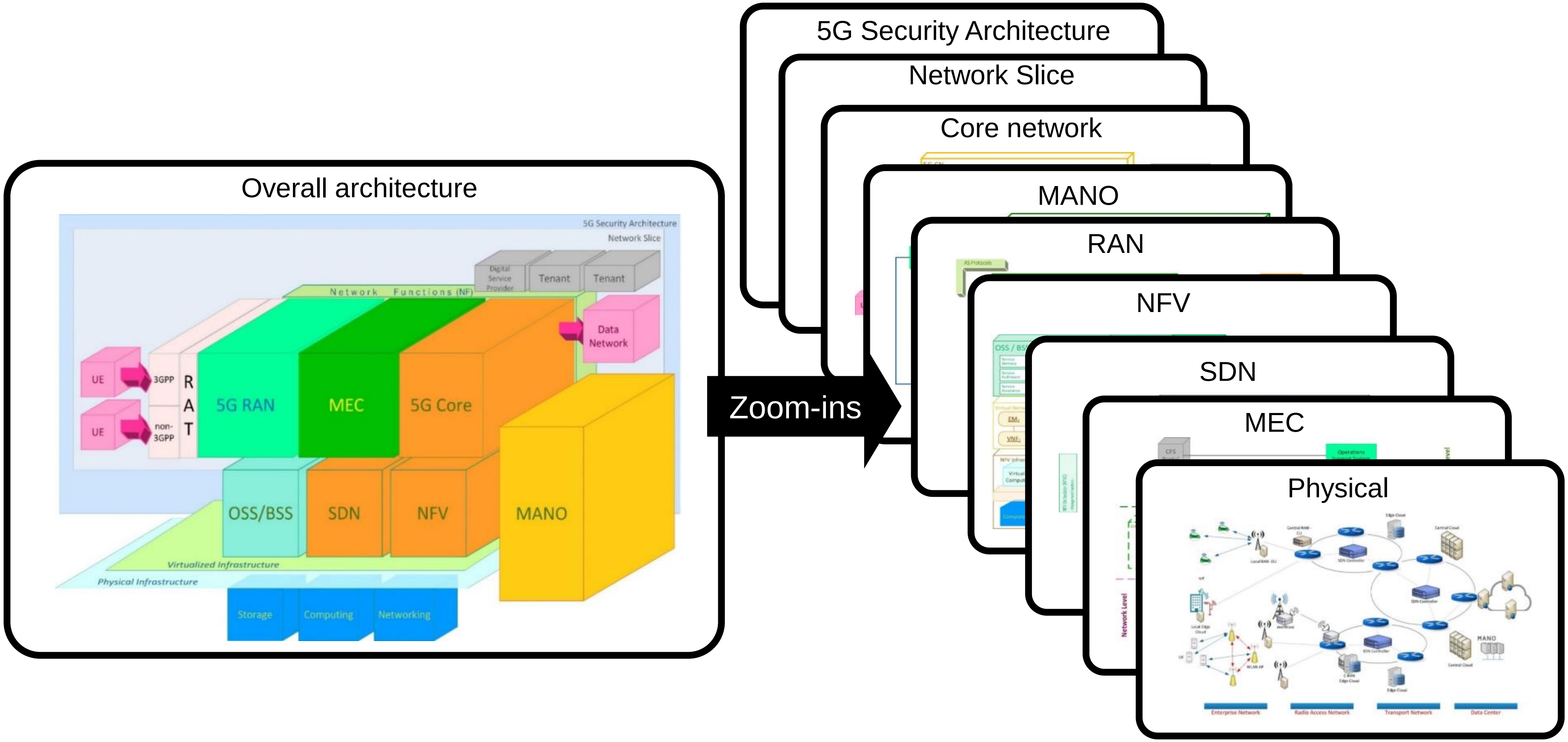
SCOPE/OBJECTIVES

- 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



Overall architecture

Zoom-ins

5G Security Architecture

Network Slice

Core network

MANO

RAN

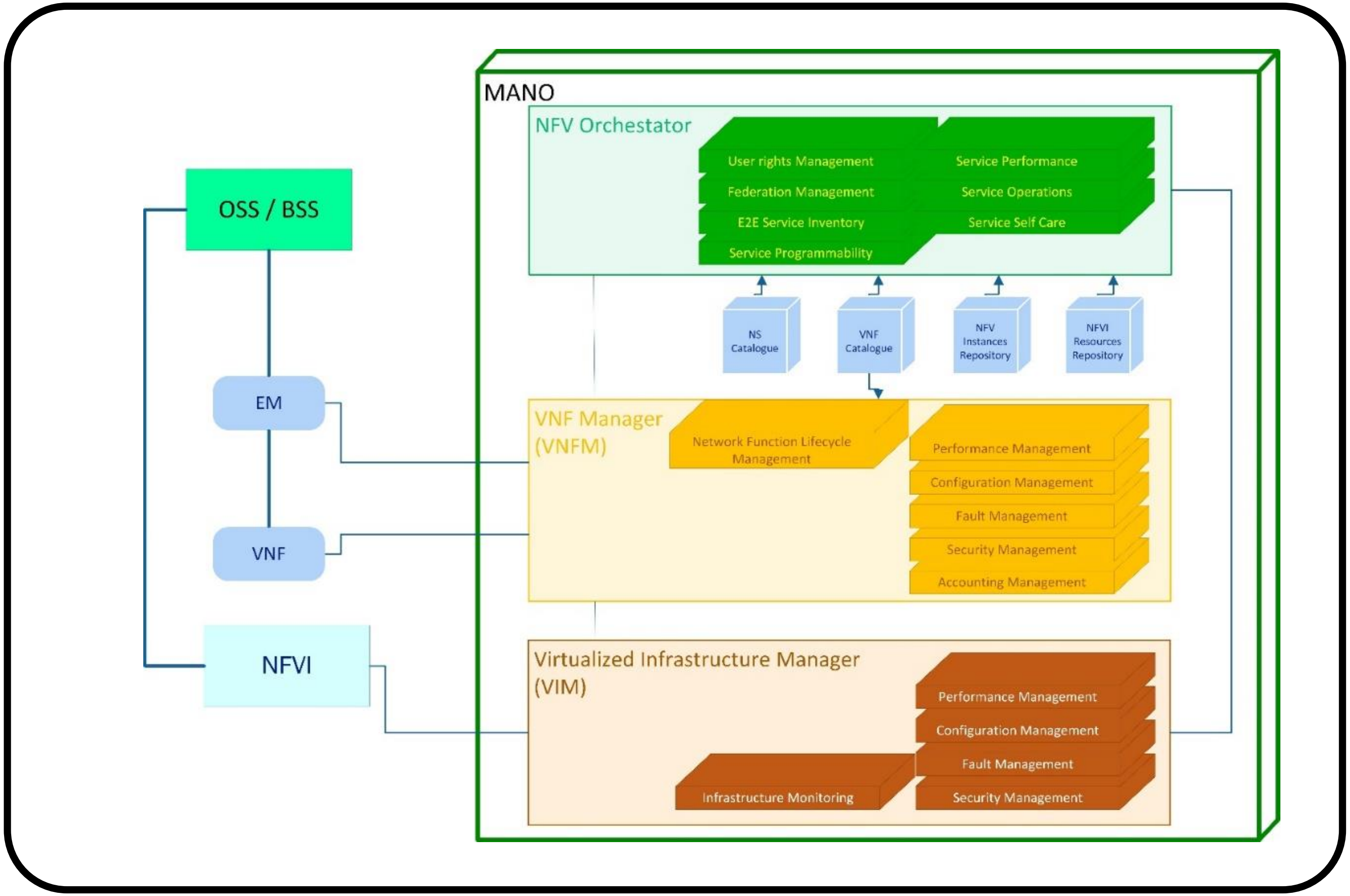
NFV

SDN

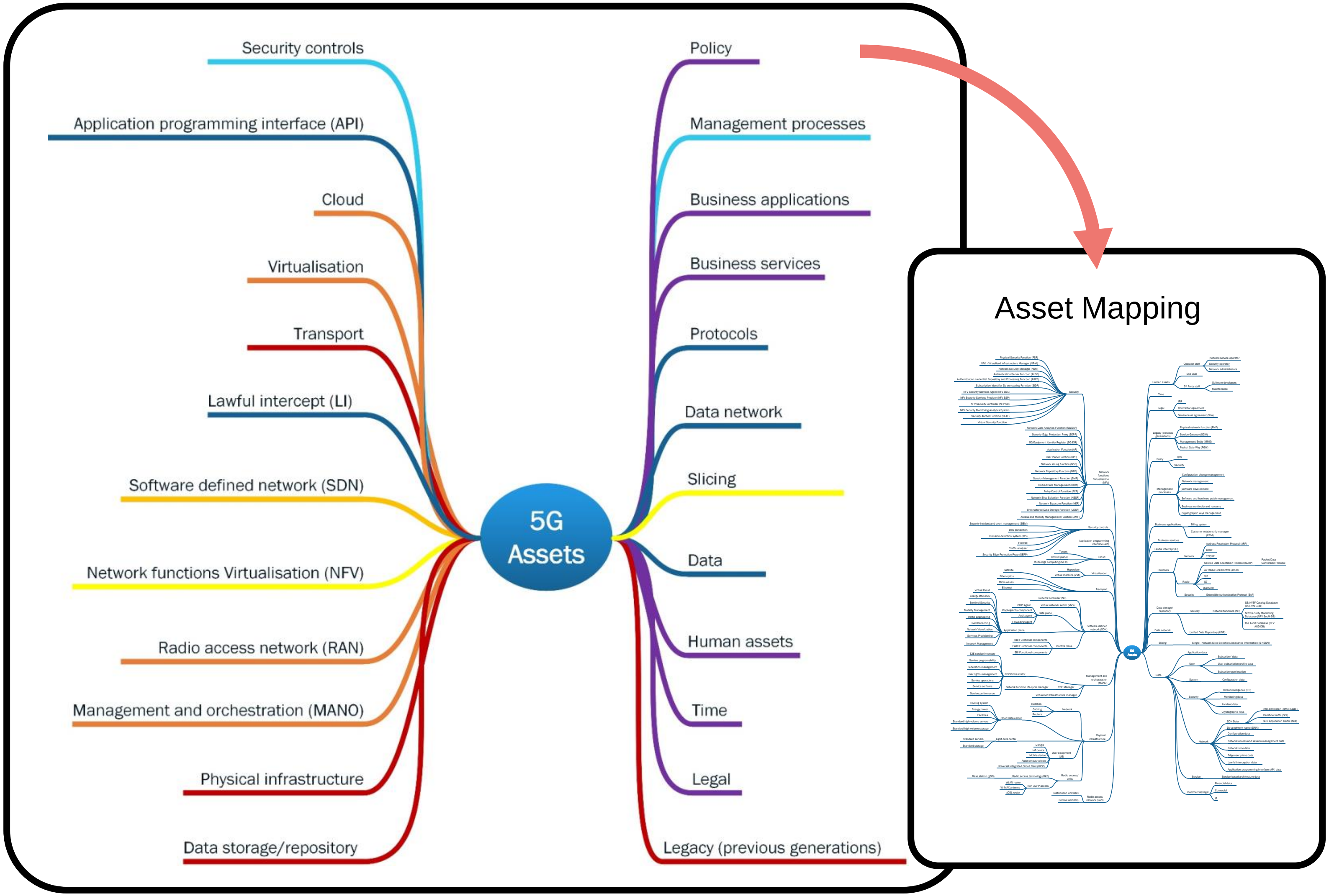
MEC

Physical

MANO ZOOM-IN (EXAMPLE)



ASSET GROUPS



5G Assets

Security controls

Application programming interface (API)

Cloud

Virtualisation

Transport

Lawful intercept (LI)

Software defined network (SDN)

Network functions Virtualisation (NFV)

Radio access network (RAN)

Management and orchestration (MANO)

Physical infrastructure

Data storage/repository

Policy

Management processes

Business applications

Business services

Protocols

Data network

Slicing

Data

Human assets

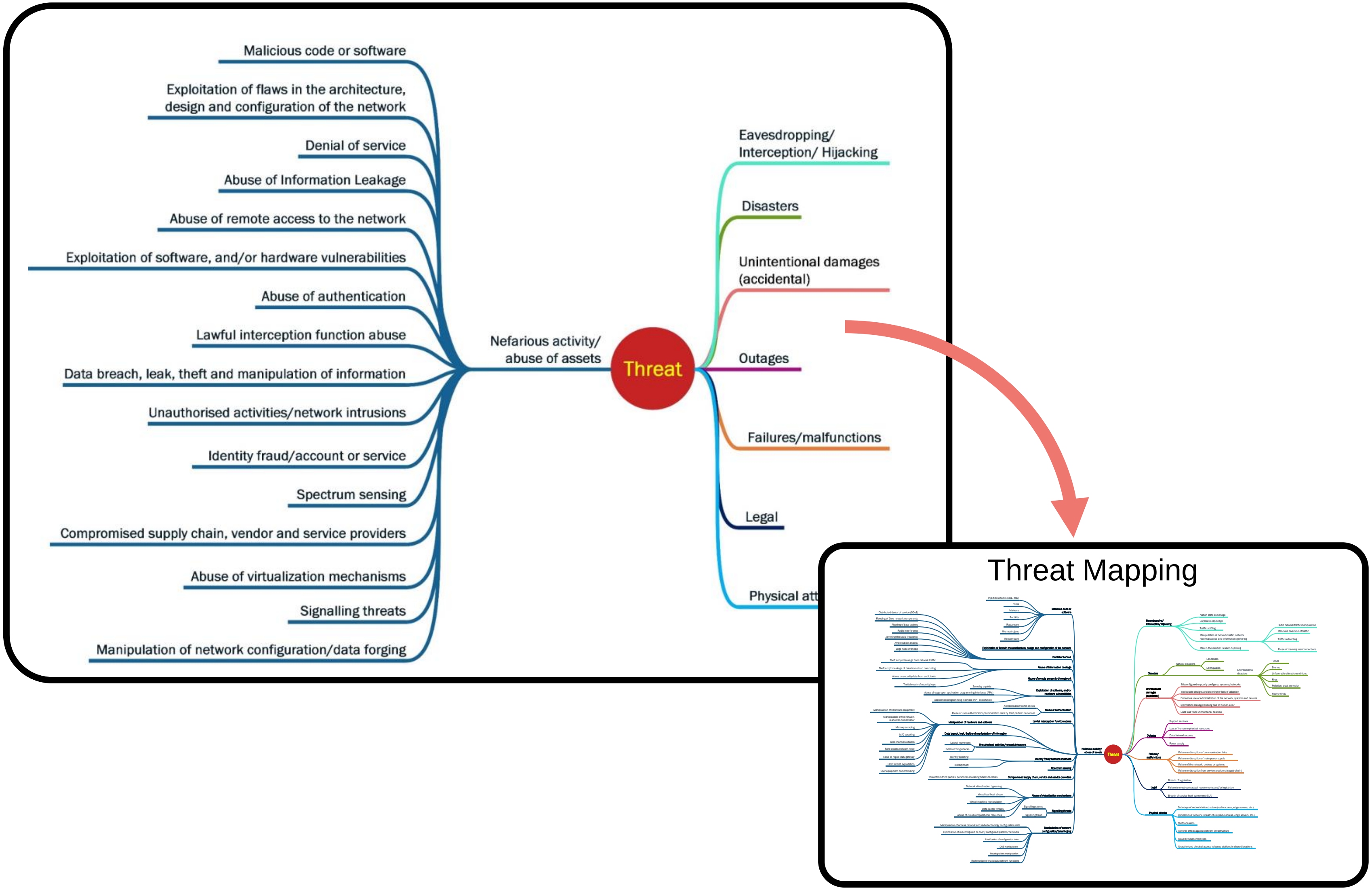
Time

Legal

Legacy (previous generations)

Asset Mapping

HIGH LEVEL THREAT TAXONOMY



Malicious code or software

Exploitation of flaws in the architecture, design and configuration of the network

Denial of service

Abuse of Information Leakage

Abuse of remote access to the network

Exploitation of software, and/or hardware vulnerabilities

Abuse of authentication

Lawful interception function abuse

Data breach, leak, theft and manipulation of information

Unauthorised activities/network intrusions

Identity fraud/account or service

Spectrum sensing

Compromised supply chain, vendor and service providers

Abuse of virtualization mechanisms

Signalling threats

Manipulation of network configuration/data forging

Nefarious activity/ abuse of assets

Threat

Eavesdropping/ Interception/ Hijacking

Disasters

Unintentional damages (accidental)

Outages

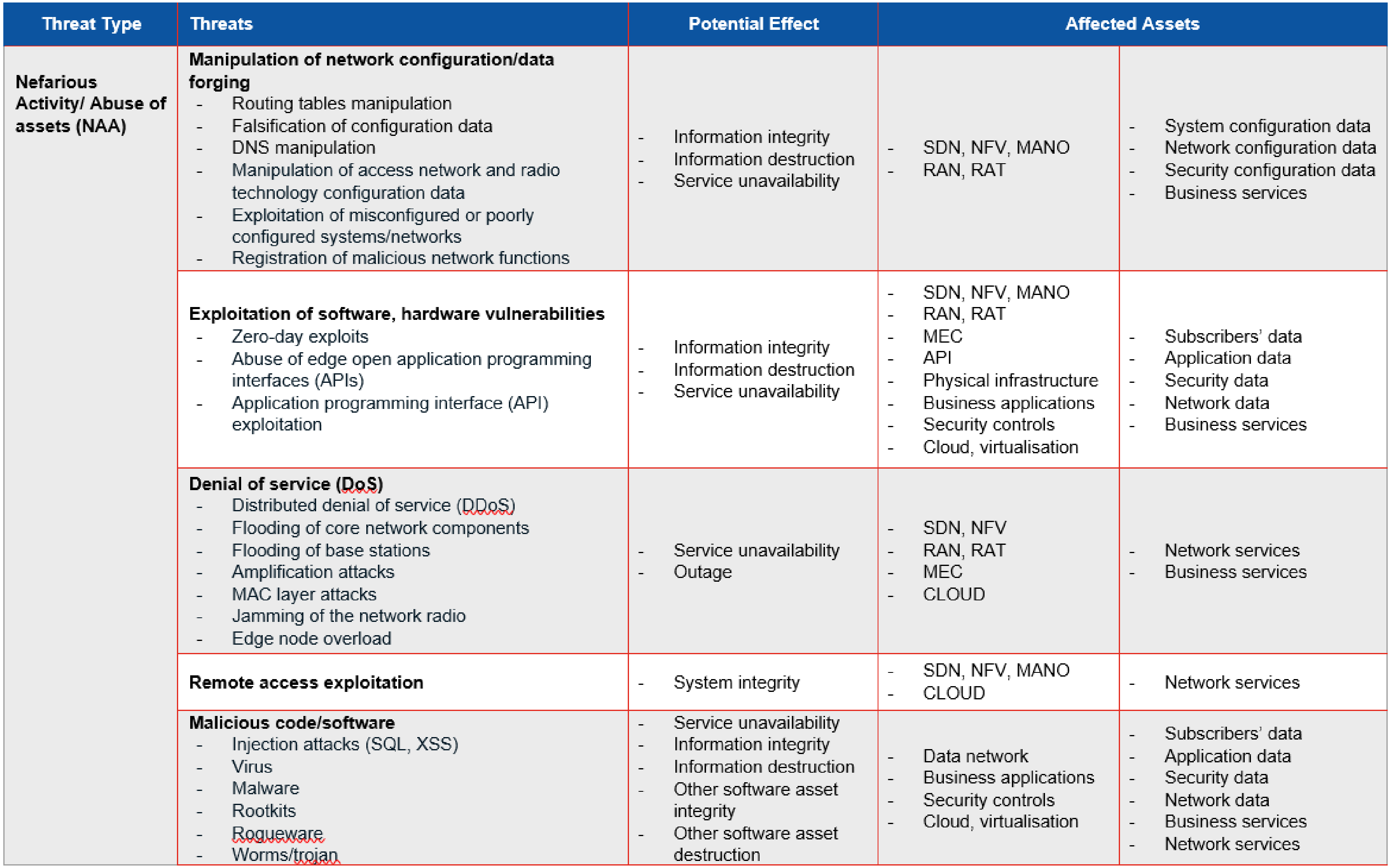
Failures/malfunctions

Legal

Physical att

Threat Mapping

THREAT ASSESSMENT



Threat Type	Threats	Potential Effect	Affected Assets	
Nefarious Activity/ Abuse of assets (NAA)	**Manipulation of network configuration/data forging** - 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	- Information integrity - Information destruction - Service unavailability	- SDN, NFV, MANO - RAN, RAT	- System configuration data - Network configuration data - Security configuration data - Business services
	Exploitation of software, hardware vulnerabilities - Zero-day exploits - Abuse of edge open application programming interfaces (APIs) - Application programming interface (API) exploitation	- Information integrity - Information destruction - Service unavailability	- SDN, NFV, MANO - RAN, RAT - MEC - API - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation	- Subscribers' data - Application data - Security data - Network data - Business services
	Denial of service (DoS) - 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	- Service unavailability - Outage	- SDN, NFV - RAN, RAT - MEC - CLOUD	- Network services - Business services
	Remote access exploitation	- System integrity	- SDN, NFV, MANO - CLOUD	- Network services
	Malicious code/software - Injection attacks (SQL, XSS) - Virus - Malware - Rootkits - Rogueware - Worms/trojan	- Service unavailability - Information integrity - Information destruction - Other software asset integrity - Other software asset destruction	- Data network - Business applications - Security controls - Cloud, virtualisation	- 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