# Ontology driven approaches to cybersecurity of 5G networks

*Marina Settembre*

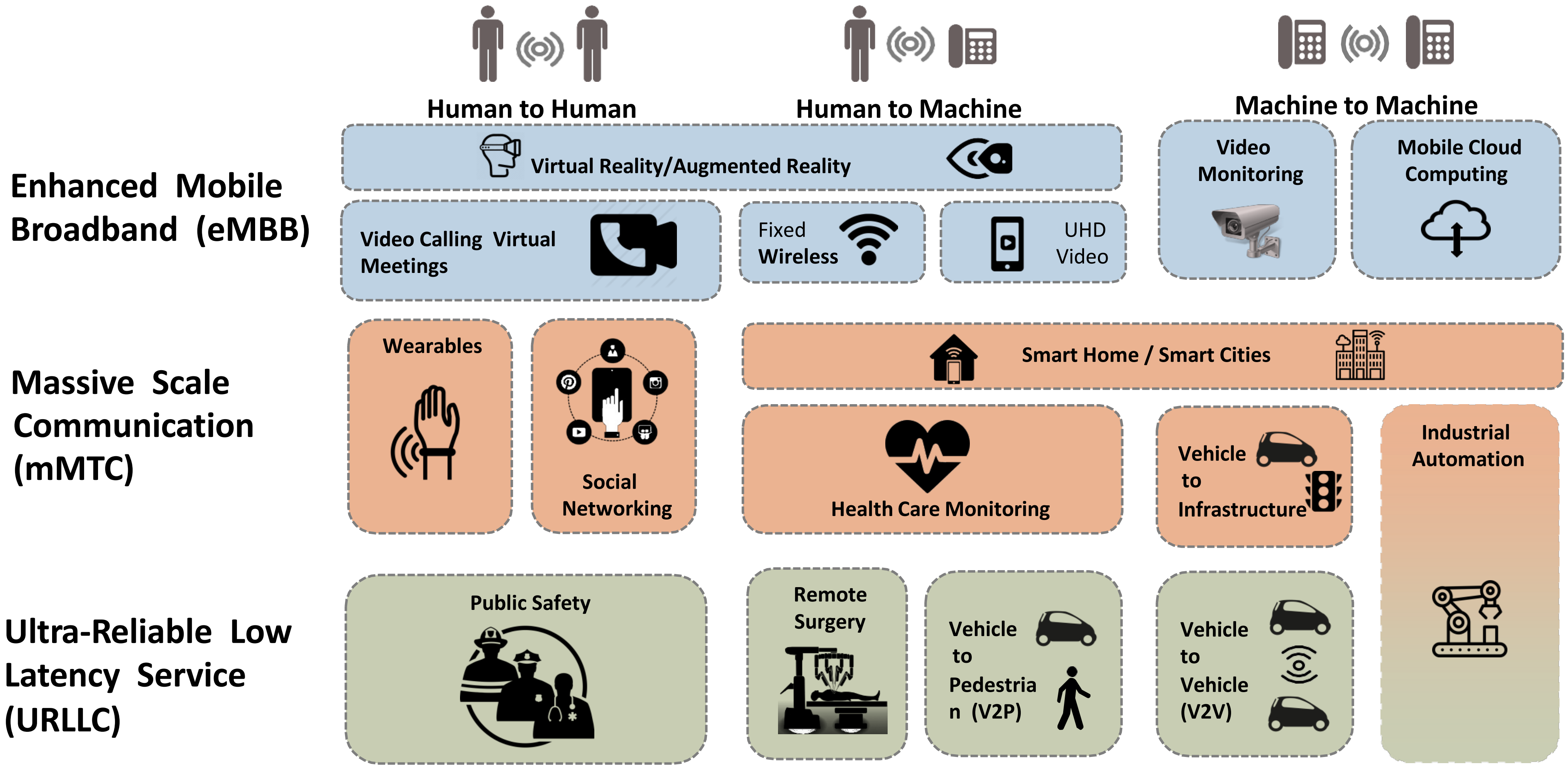
*Fondazione Ugo Bordoni*

ONDM 2023 – 27th International Conference on Optical Network Design and Modelling

08 -11 May 2023, Coimbra (Portugal)

FUB
Fondazione Ugo Bordoni
Ricerca e Innovazione

# 5G PERVASIVENESS ACROSS MOST SECTORS



Human to Human

Human to Machine

Machine to Machine

Enhanced Mobile Broadband (eMBB)

Virtual Reality/Augmented Reality

Video Calling Virtual Meetings

Fixed Wireless

UHD Video

Video Monitoring

Mobile Cloud Computing

Massive Scale Communication (mMTC)

Wearables

Social Networking

Smart Home / Smart Cities

Health Care Monitoring

Vehicle to Infrastructure

Industrial Automation

Ultra-Reliable Low Latency Service (URLLC)

Public Safety

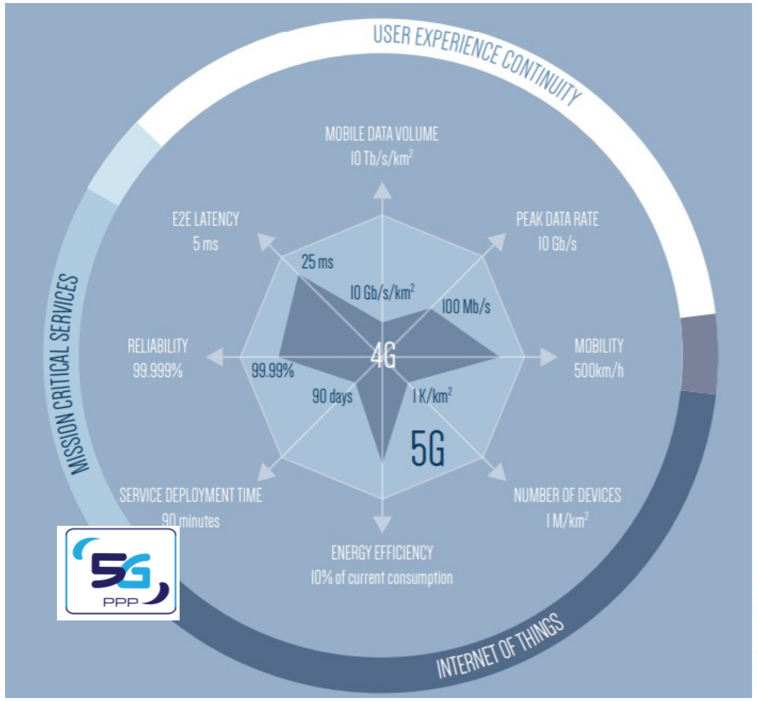
Remote Surgery

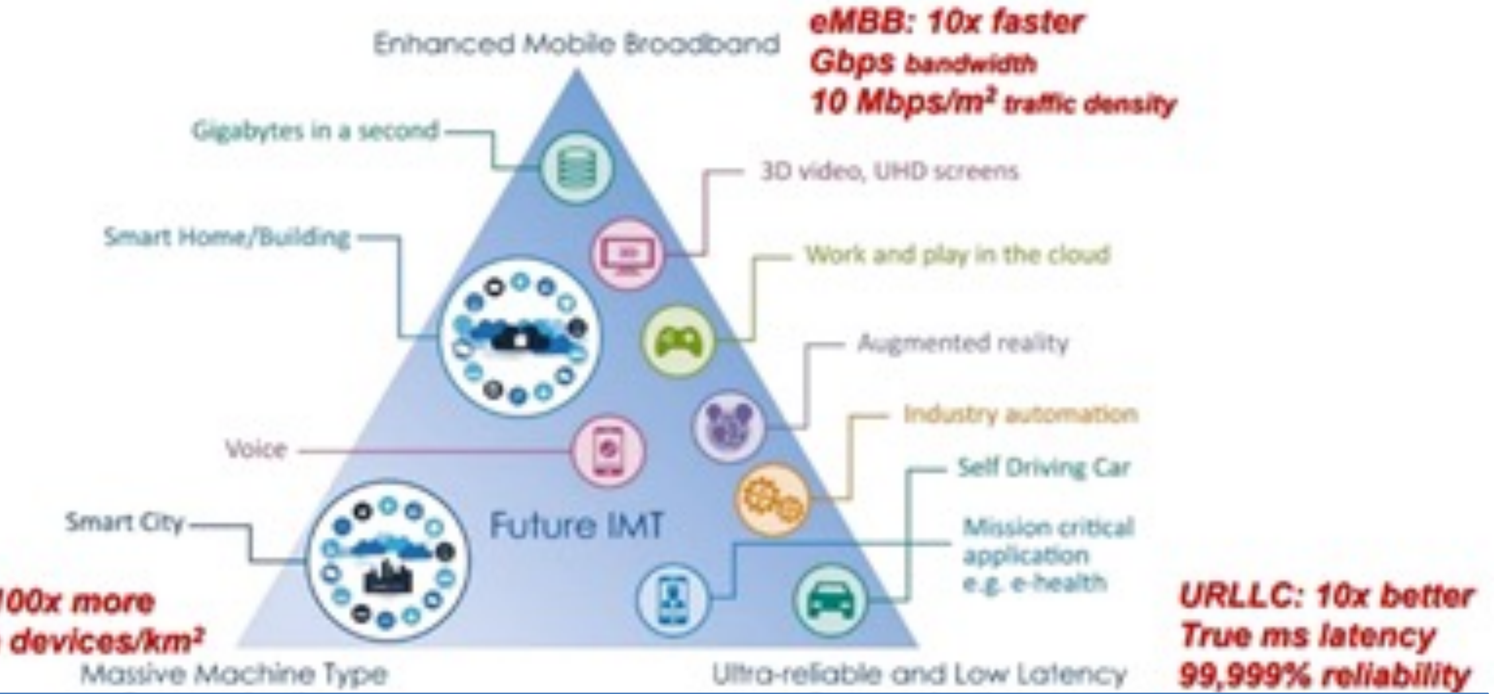
Vehicle to Pedestrian (V2P)

Vehicle to Vehicle (V2V)

FUB Fondazione Ugo Bordoni
Ricerca e Innovazione

# 5G: MORE THAN A PROGRESSIVE STEP





**eMBB: 10x faster**
**Gbps bandwidth**
**10 Mbps/m² traffic density**

**mMTC: 100x more**
**1 million devices/km²**

**URLLC: 10x better**
**True ms latency**
**99,999% reliability**

**Cloud native**

**Secure by design**

**New Radio and new spectrum**

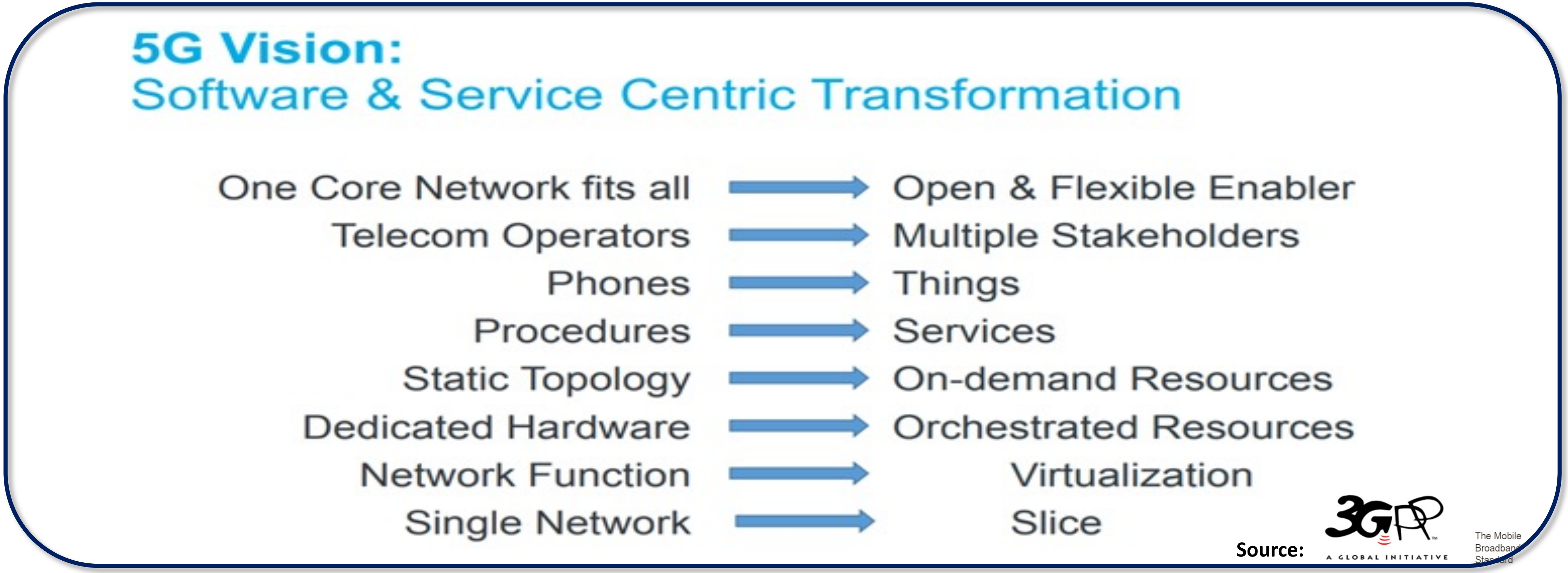
**Programmability**

**Slicing**

**Intelligence**

# 3GPP VISION ON 5G

- 3GPP - 3rd Generation Partnership Project is the reference standard for mobile communications



## 5G Vision:
## Software & Service Centric Transformation

One Core Network fits all → Open & Flexible Enabler

Telecom Operators → Multiple Stakeholders

Phones → Things

Procedures → Services

Static Topology → On-demand Resources

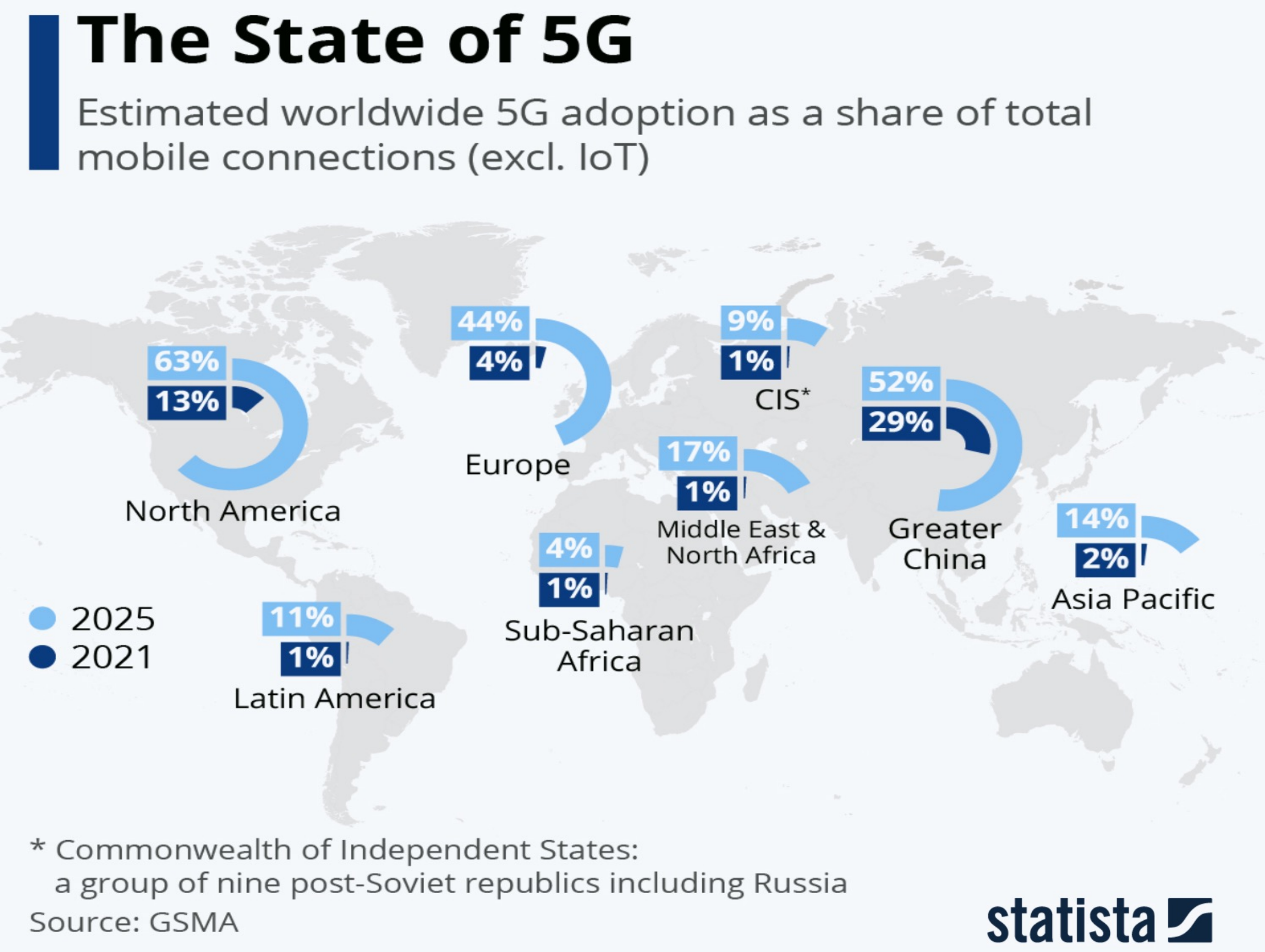
Dedicated Hardware → Orchestrated Resources

Network Function → Virtualization

Single Network → Slice

Source: 3GPP A GLOBAL INITIATIVE The Mobile Broadband Standard

# THE GLOBAL ROLLOUT OF 5G



## The State of 5G

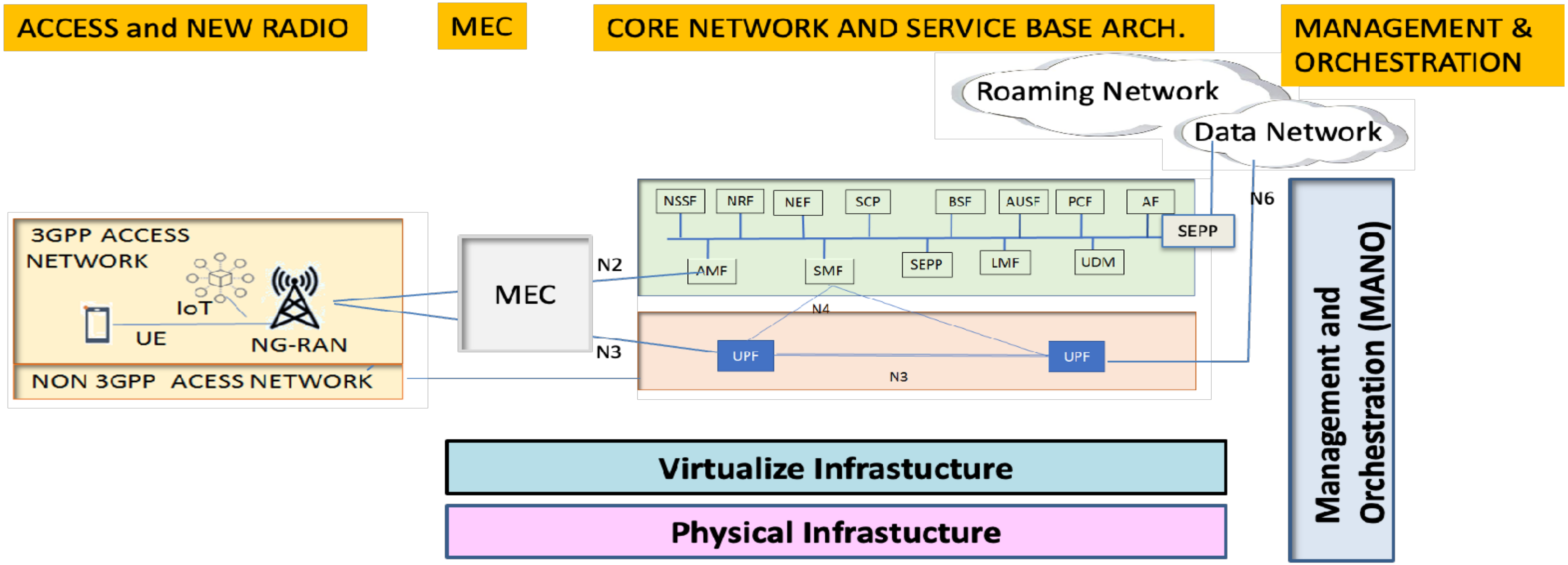
Estimated worldwide 5G adoption as a share of total mobile connections (excl. IoT)

* Commonwealth of Independent States: a group of nine post-Soviet republics including Russia

Source: GSMA

- Currently, China is leading the race to 5G
- By 2025, 5G is expected to be the predominant standard in China and North America
- 5G will take some years to overtake 4G
- Technology and business evolutions go at a different rate

# 5G Architecture

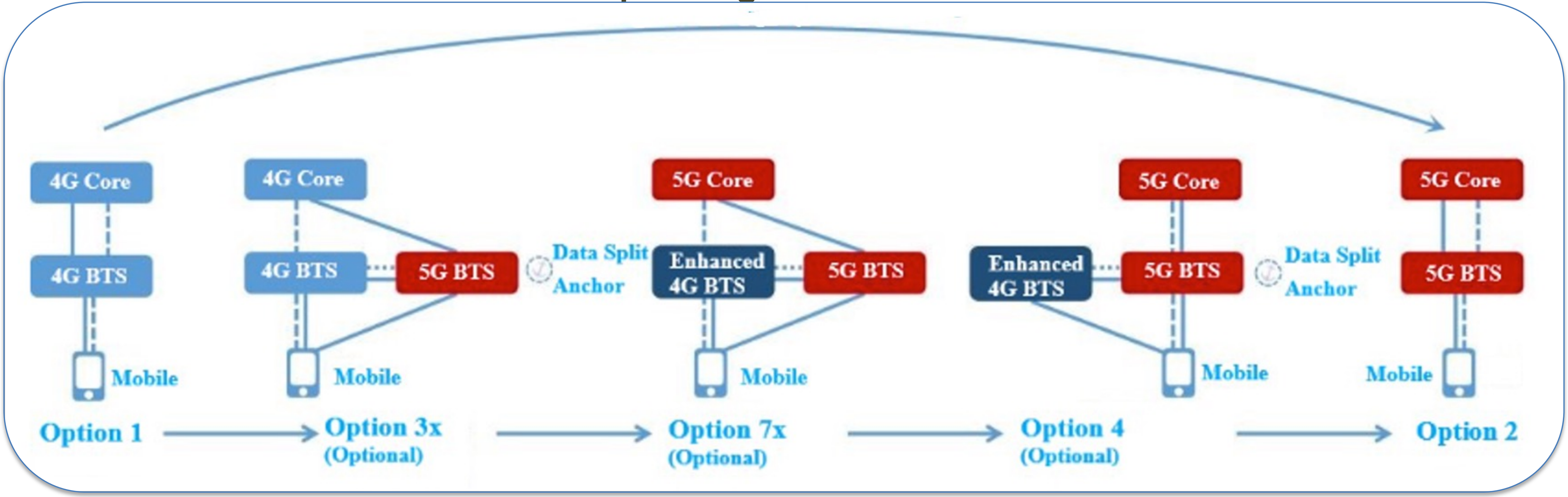


- Integration of multiple and different types of technologies
- Many configuration options

FUB Fondazione Ugo Bordoni Ricerca e Innovazione

# …MANY IMPLEMENTATION OPTIONS (not exhaustive)

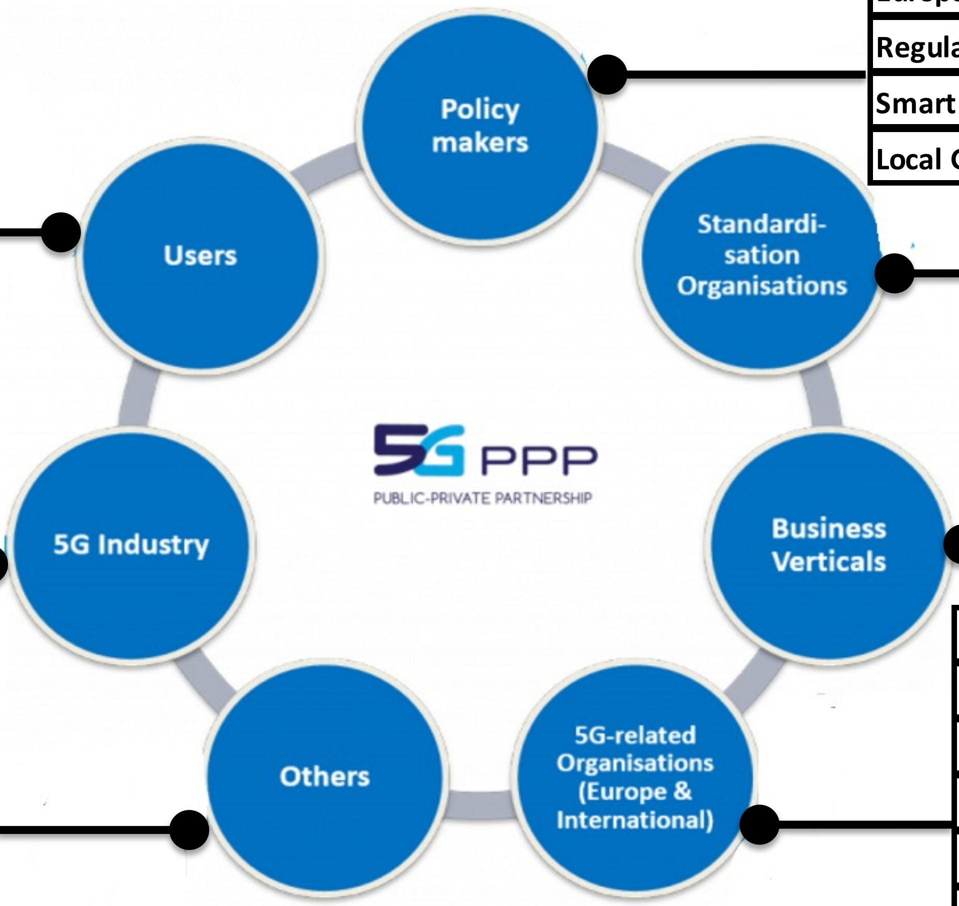
**Stand Alone (SA) path**
**One step to target architecture**



**Non Stand Alone (NSA) Networking**
**Gradual Investment, smaller Risk**

Source: Hocell

# ...MANY 5G STAKEHOLDERS


Policy makers
Users
Standardi-sation Organisations
5G PPP
PUBLIC-PRIVATE PARTNERSHIP
5G Industry
Business Verticals
Others
5G-related Organisations (Europe & International)

- End Users
- Smart cities
- SMEs
- Research Institutiions/Organizations
- Application Service Providers
- Content Providers

- European Commission
- Regulators
- Smart Cities
- Local Governements

- 3GPP
- ETSI
- ITU
- IETF/IRTF
- IEEE

- Connettivity providers
- Technology providers
- SMEs

- 5GIA
- Automotive
- eHealth
- Factory
- Media & Entertainment

- Other International projects
- Open Source projects
- Other national projects
- Investors

- 5G Forum
- IMT 2020
- NGMN
- 5GMF
- 5G Americas
- FSAN
- AIOTI

# …NEW SECURITY CHALLENGES

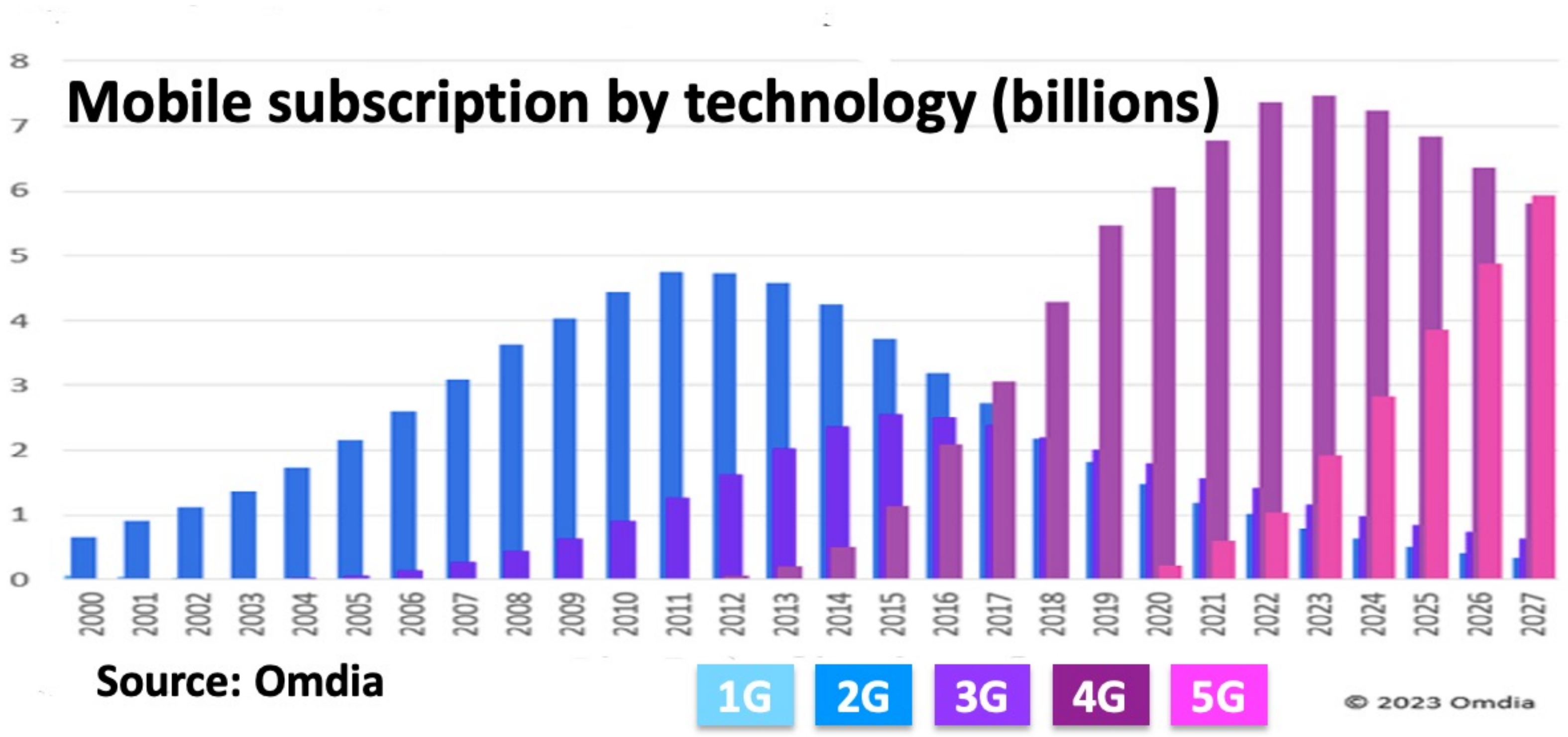
5G introduces stronger security preventive measures respect to 4G, but new security challenges arise:

- *More* ***openess and interconnections***
- ***Diversified service offerings*** *complicate assurance of continuous level of security*
- ***Network slicing, virtualizaztion and disaggregation*** *brings new risks*
- ***Heavy use of web protocols*** *lowers barriers against attackers*
- ***Coexistence of 4G and 5G***
- ***High fragmentation*** *of security standards bodies*
- *Standard is not sufficient,* ***security assurance testing is needed***
- ***Growing numbers of digital threats and attacks***

FUB
Fondazione Ugo Bordoni
Ricerca e Innovazione

# 5G COMPLEXITY

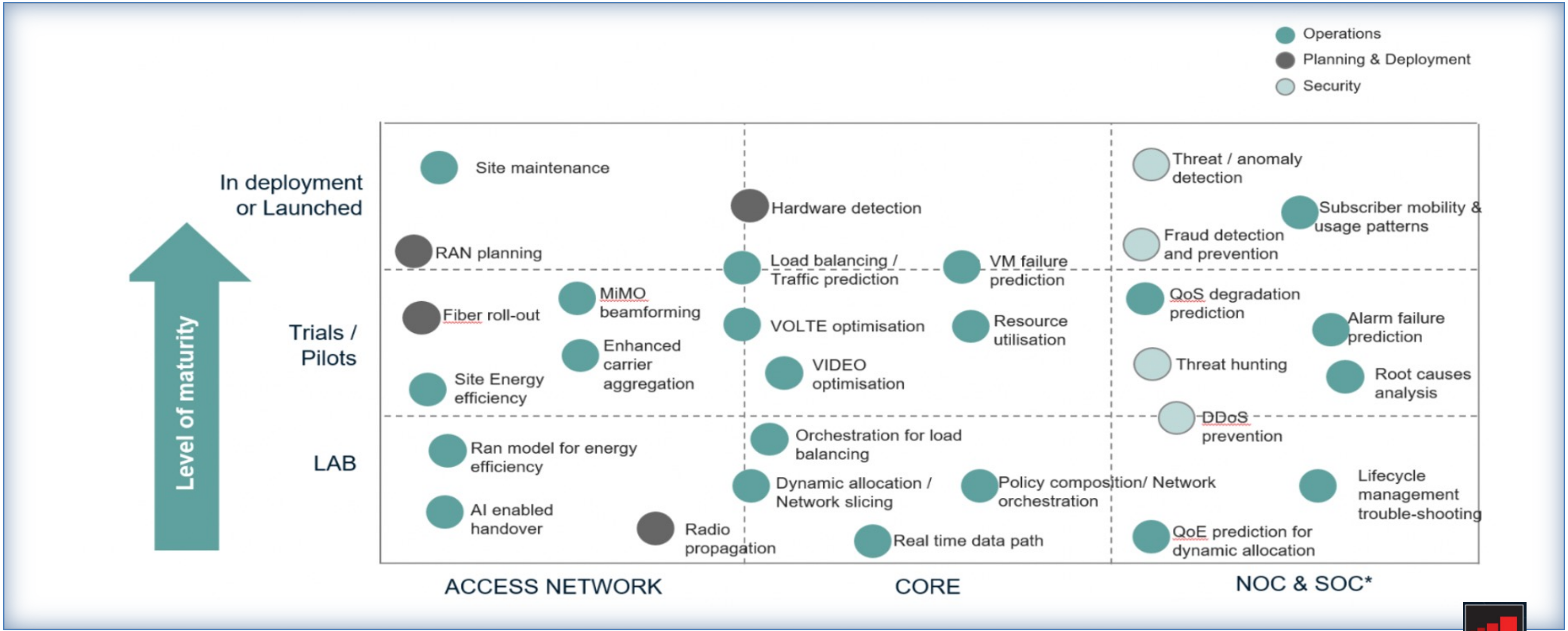
- Integration of multiple and different type of technologies
- Increasing number of sub-systems with high dinamicity and variability
- Many deployments options
- Many configuration options
- Many stakeholders
- New threat landscape


Mobile subscription by technology (billions)

Source: Omdia

# Complexity of 5G networks calls for the use of automation and artificial intelligence

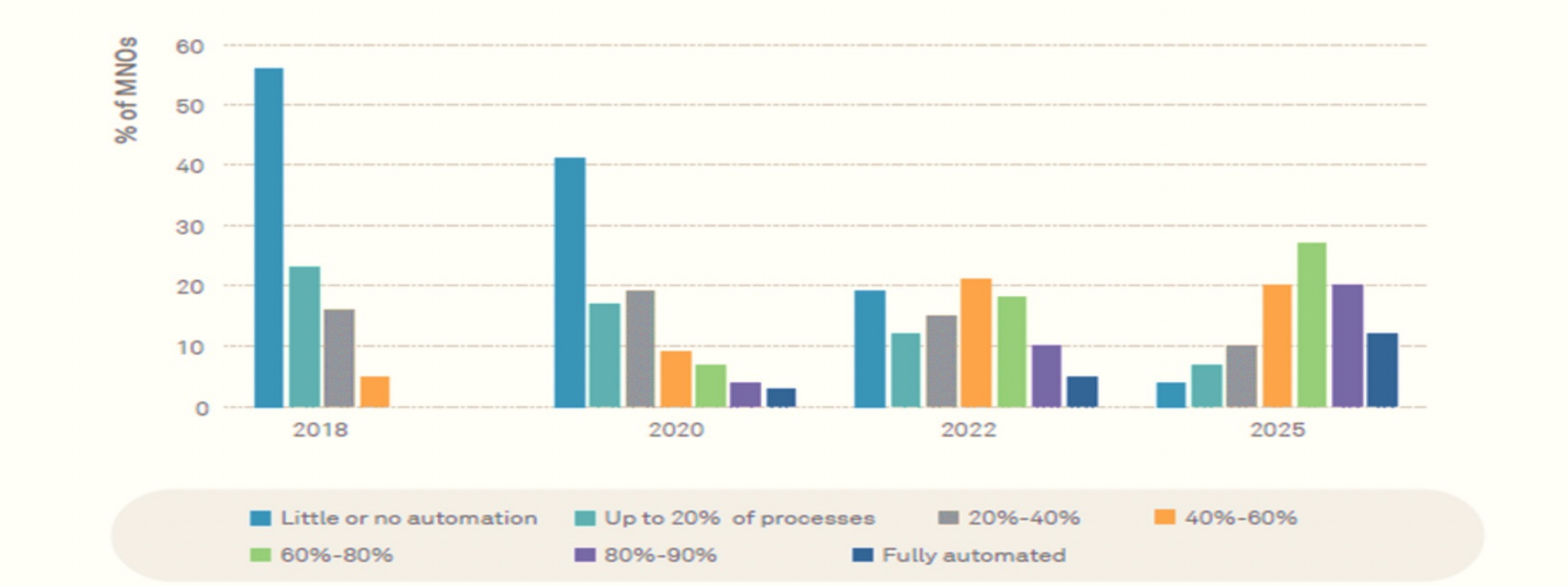
# AI IN TLC NETWORKS



| | ACCESS NETWORK | CORE | NOC & SOC* |
|---|---|---|---|
| In deployment or Launched | 🟢 Site maintenance<br>⚫ RAN planning | ⚫ Hardware detection<br>🟢 Load balancing / Traffic prediction<br>🟢 VM failure prediction | ⚪ Threat / anomaly detection<br>🟢 Subscriber mobility & usage patterns<br>⚪ Fraud detection and prevention |
| Trials / Pilots | ⚫ Fiber roll-out<br>🟢 MiMO beamforming<br>🟢 Enhanced carrier aggregation<br>🟢 Site Energy efficiency | 🟢 VOLTE optimisation<br>🟢 Resource utilisation<br>🟢 VIDEO optimisation | 🟢 QoS degradation prediction<br>🟢 Alarm failure prediction<br>⚪ Threat hunting<br>🟢 Root causes analysis |
| LAB | 🟢 Ran model for energy efficiency<br>🟢 AI enabled handover<br>⚫ Radio propagation | 🟢 Orchestration for load balancing<br>🟢 Dynamic allocation / Network slicing<br>🟢 Policy composition/ Network orchestration<br>🟢 Real time data path | ⚪ DDoS prevention<br>🟢 Lifecycle management trouble-shooting<br>🟢 QoE prediction for dynamic allocation |

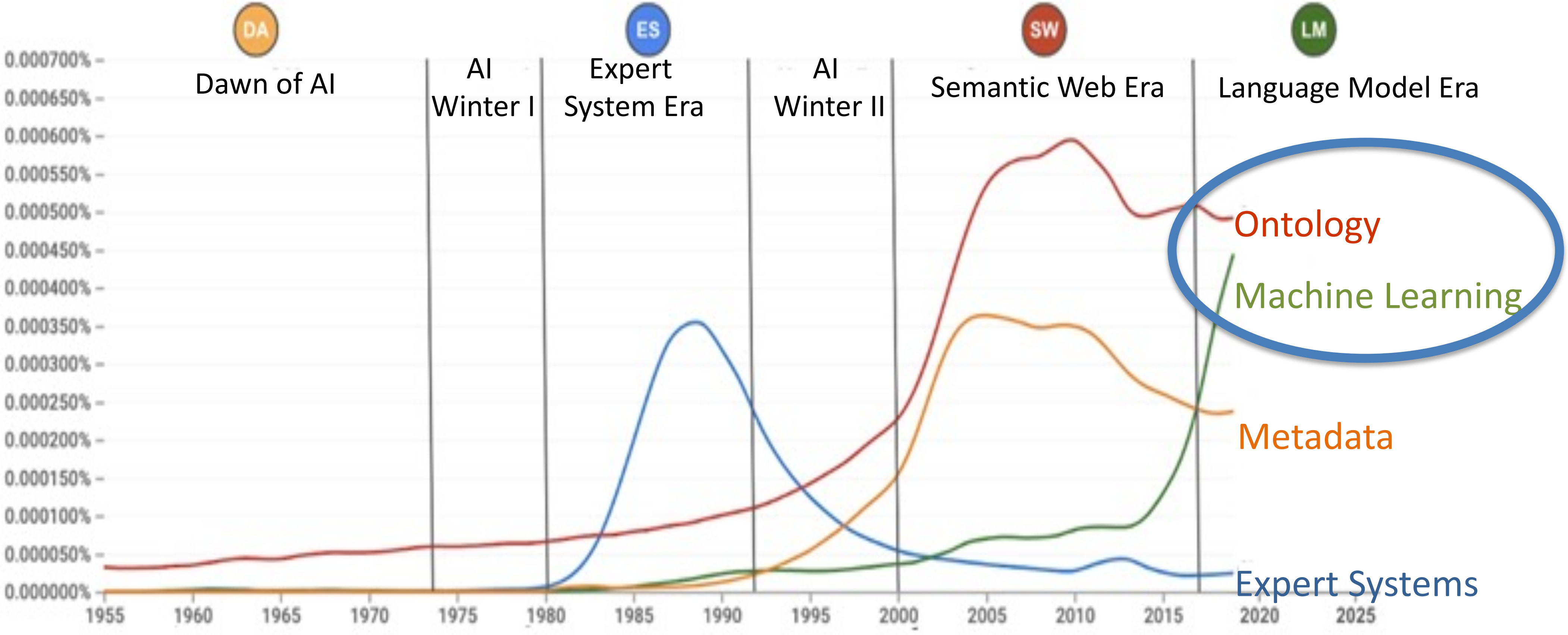
Source: GSMA ( June 2019)

# NETWORK AUTOMATION FORECASTING



*Forecast levels of network automation by MNOs worldwide 2018-2025 (Based on a survey of 76 Tier 1 and 2 MNOs worldwide, Q32018) (source: Analysis Mason)*

# AI TRENDS



*Percentage of n-grams in books published in English between 1955 and 2019 that are "expert systems", "ontology", "metadata", or "machine learning" [Google 2022]*

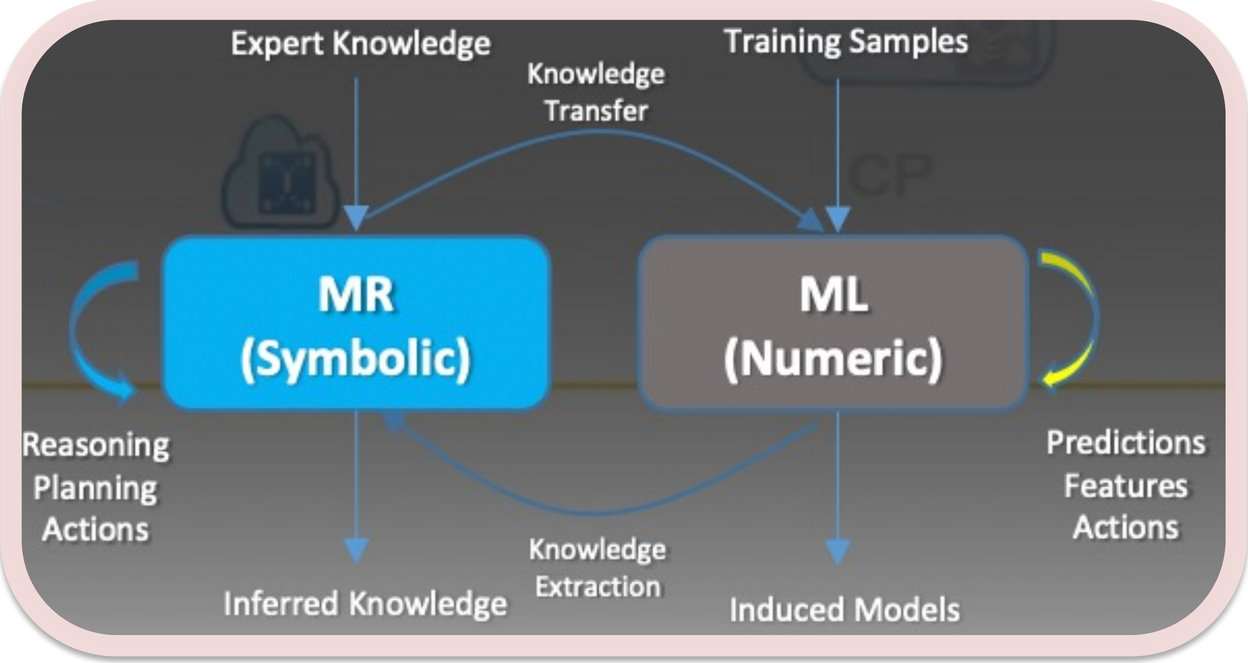
https://drops.dagstuhl.de/opus/volltexte/2023/17810/pdf/dagrep_v012_i009_p060_22372.pdf

# ONTOLOGY VS MACHINE LEARNING

- Machine learning **learns from data** for different purposes:
  - ***Supervised learning****: classification (diagnosis, fraud detection, image recognition), regression (forecasting, predictions optimizations)*
  - ***Unsupervised learning****: clustering, dimensionality reduction (meangful compression, structure discovery)*
  - ***Reinforcement learning****: real time decisions, Game Ai, learning tasks, robot navigation*

- Ontologies **provide context** for representing knowledge in a domain model.

- Ontologies and ML **can complement each other**.



Source: D. Soldani, 6GWorld, 2021

# WHAT IS AN ONTOLOGY?

**An ontology is an**

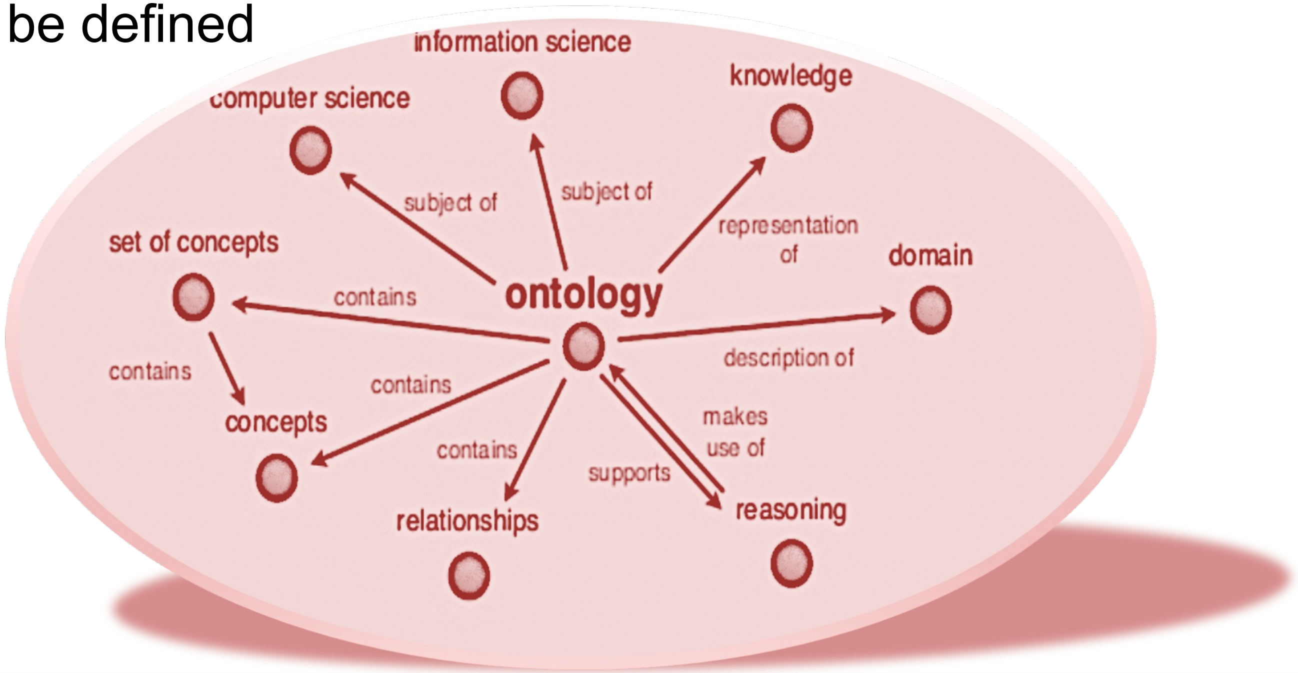
**explicit, formal specification of a shared conceptualization**

**conceptualization**: abstract model (domain, identified relevant concepts, relations)

**explicit**: meaning of all concepts must be defined

**formal**: machine understandable

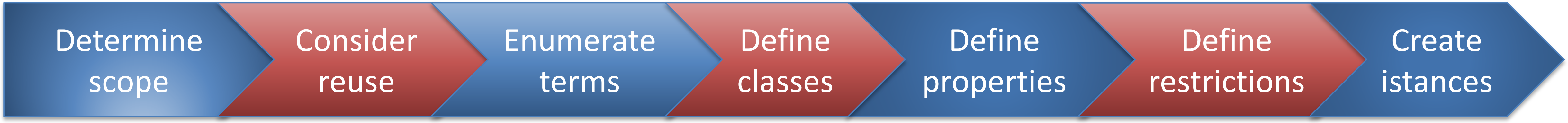
**shared**: consensus about ontology



# WHAT AN ONTOLOGY IS USEFUL FOR?

- **Meaningfully sharing information and knowledge** between humans and machine on a domain
- Enabling **reuse of domain knowledge**
  - *To avoid reinventing the wheel*
  - *To facilitate interoperability*
- Increasing **the ability to automate**
- Defining **correct configuration** templates
- Facilitating a multidisciplinary approach through **semantically data integration**
- Assisting in **semantics disambiguitation**
- Facilitating **more precise searches and complex queries**
- Supporting **reasoning to infer additional information** about the real world.

# HOW TO BUILD AN ONTOLOGY?



Determine scope

Consider reuse

Enumerate terms

Define classes

Define properties

Define restrictions

Create istances

- There is no unique way to design an ontology
- Identify competency questions that the ontology should be able to answer.
- The way you design the ontology is guided by the ontology application and competency questions
- Design the ontology is an iterative process.

# MAIN CHALLENGES WITH ONTOLOGIES

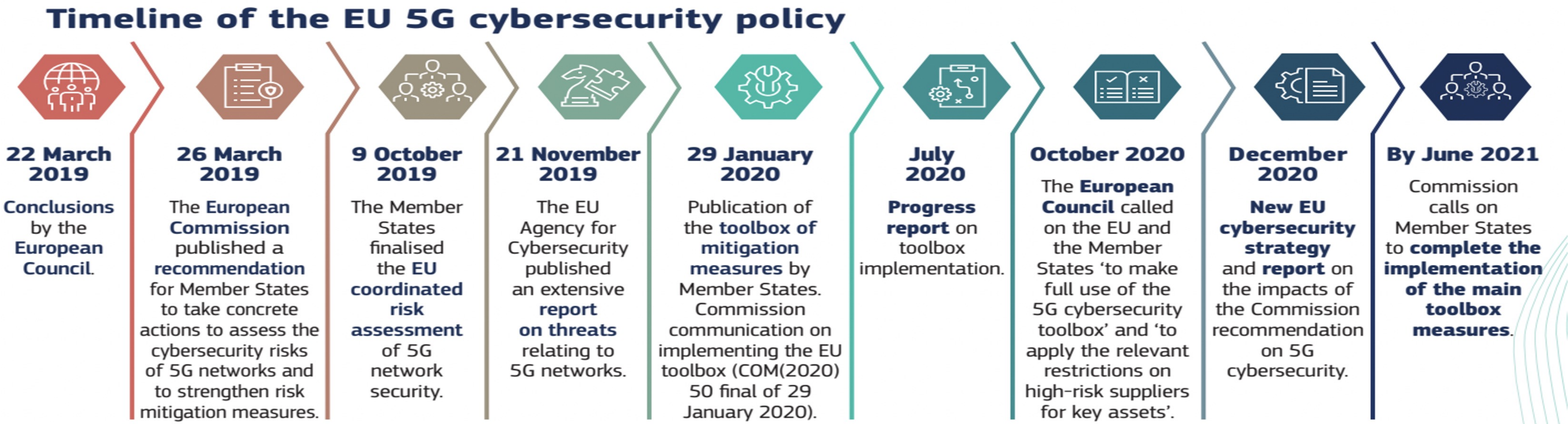
- Choose the right size for an ontology
- Ontology evaluation: how do we know is good enough?
- Ontology integration model (e.g include other concepts from other domains)
- Lack of formal standardized representation of relevant information
- Lack of coherent relationships between the different layers of abstraction in ontologies
- Ontology maintenace
- Ontology consensus

# MAIN EXISTING ONTOLOGIES IN THE CYBERSECURITY DOMAIN

- **Unified Cybersecurity Ontology (UCO)**
  - It connects different  cybersecurity resources (e.g. STIX, CAPEC, MAEC, CWE, CVE, CVSS, Cybox, CPE,  STUCCO)
- **Internet Of Things Security Ontology (IoTSec)**
- **NISTIR 8138 Draft 2016:**
  - Vulnerability Description Ontology (VDO). A Framework for Characterizing Vulnerabilities
- **TOCSA:** Threat Ontologies for Cybersecurity Analytics  (University of OSLO)
  - Aims at developing models and tools for automated or semi-automated classification and discovery of cyber threats based on ontologies and semantic reasoning
- **MITRE ATT&CK®** (MITRE Adversarial Tactics, Techniques, and Common Knowledge)
  - The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.

**...None of them  specifically  for 5G**

# ENISA FOR 5G SECURITY



## Timeline of the EU 5G cybersecurity policy

**22 March 2019**
**Conclusions** by the **European Council**.

**26 March 2019**
The **European Commission** published a **recommendation** for Member States to take concrete actions to assess the cybersecurity risks of 5G networks and to strengthen risk mitigation measures.

**9 October 2019**
The Member States finalised the **EU coordinated risk assessment** of 5G network security.

**21 November 2019**
The EU Agency for Cybersecurity published an extensive **report on threats** relating to 5G networks.

**29 January 2020**
Publication of the **toolbox of mitigation measures** by Member States. Commission communication on implementing the EU toolbox (COM(2020) 50 final of 29 January 2020).

**July 2020**
**Progress report** on toolbox implementation.

**October 2020**
The **European Council** called on the EU and the Member States 'to make full use of the 5G cybersecurity toolbox' and 'to apply the relevant restrictions on high-risk suppliers for key assets'.

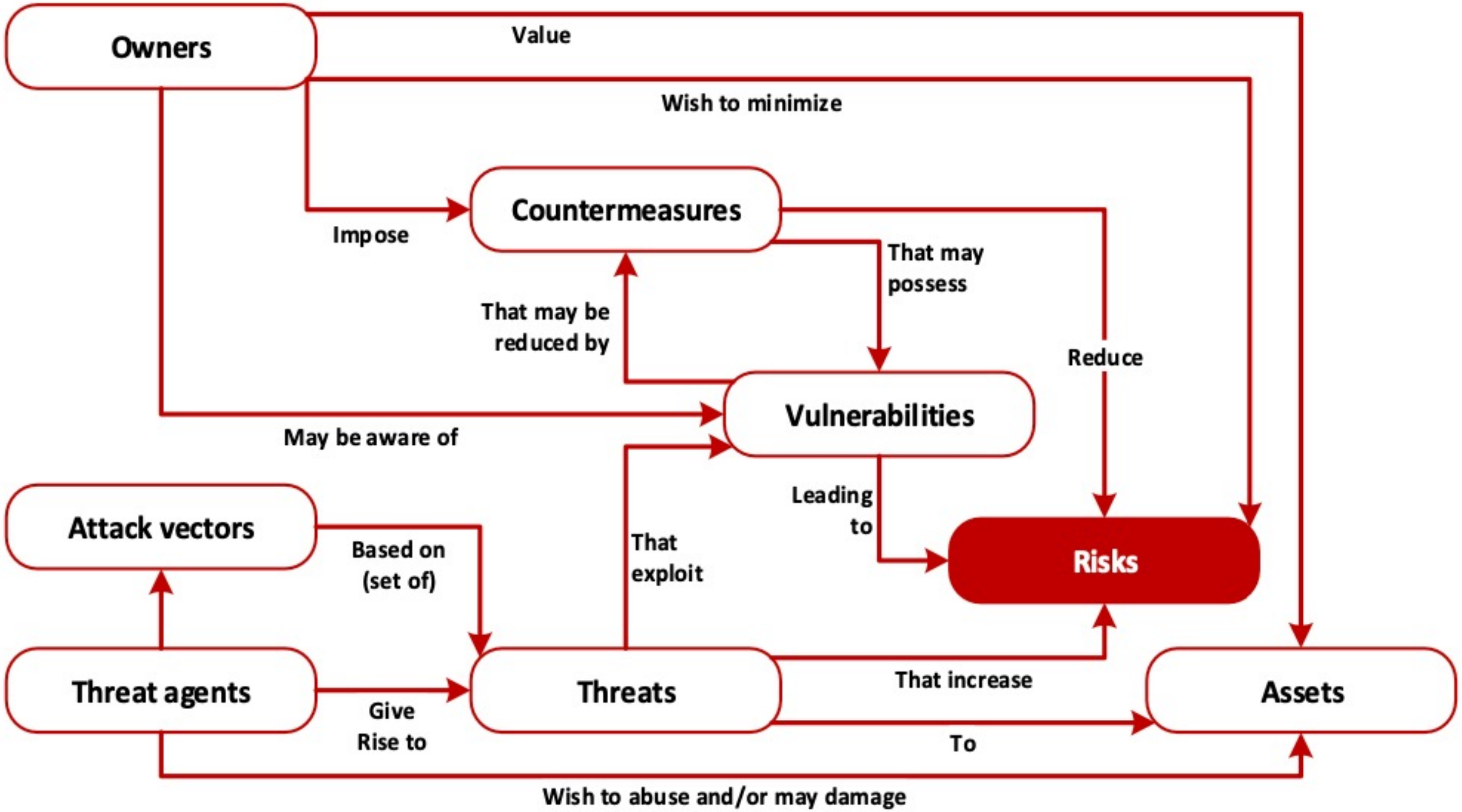
**December 2020**
**New EU cybersecurity strategy** and **report** on the impacts of the Commission recommendation on 5G cybersecurity.

**By June 2021**
Commission calls on Member States **to complete the implementation of the main toolbox measures**.

- ○ ENISA, EU Coordinated Risk Assessment of 5G Networks Security, 2019
- ○ ENISA, Threat Landscape for 5G Networks, 2019
- ○ ENISA, Threat Landscape for 5G networks - update, 2020
- ○ ENISA 5G toolbox, 2019
- ○ ENISA, Security in 5G Specifications, 2021
- ○ ENISA 5G Cybersecurity Standard (16/03/ 2022)
- ○ **EU 5G certification (tbd as of today)**

FUB Fondazione Ugo Bordoni Ricerca e Innovazione

# METHODOLOGY FOR RISK ASSESSMENT (ISO 27005)

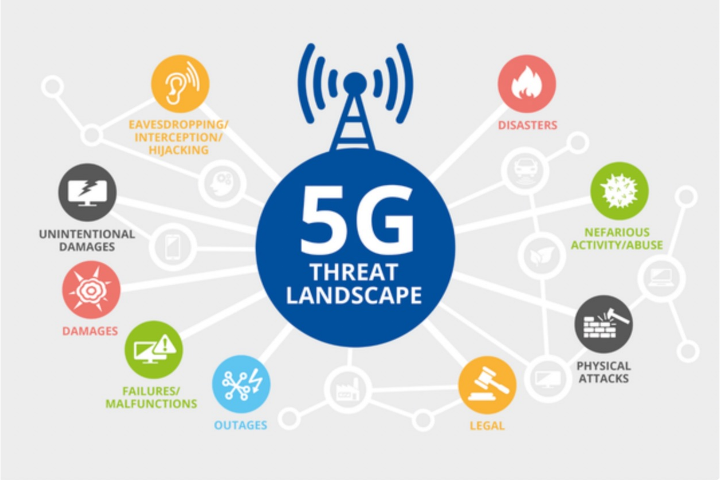


Source: Enisa 5G Threat Landscape – Update, 2020

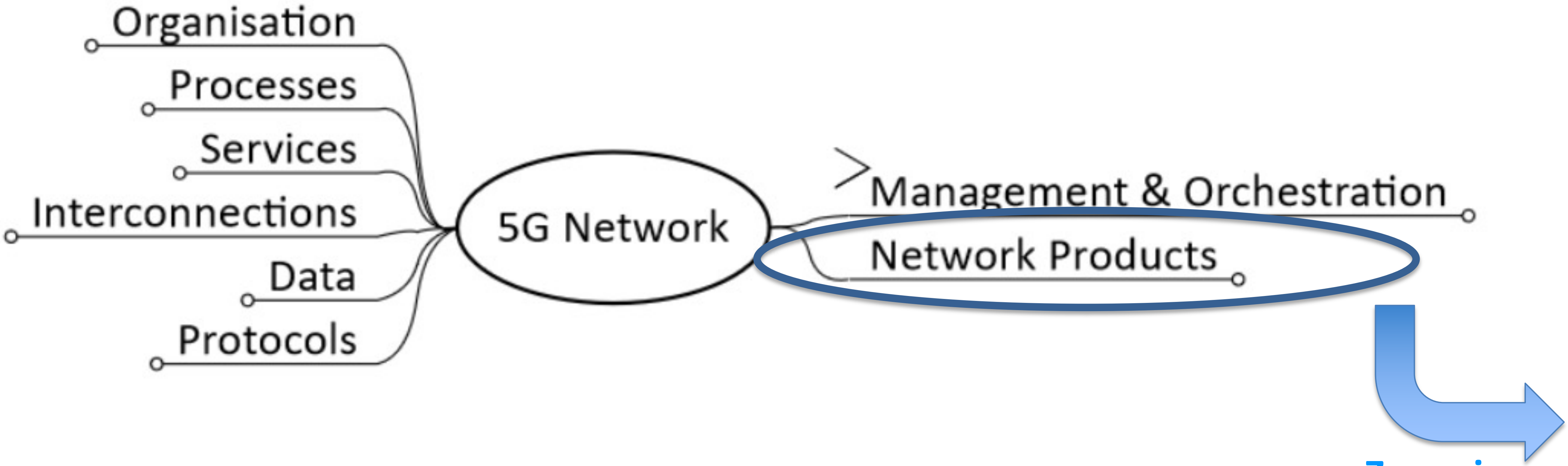
# ENISA THREAT LANSCAPE

ENISA’s 5G threat landscape is constituted by:

- 5G security architecture
- 5Gnetwork assets categories
- 5G threat taxonomy
- (5G attack vectors has not yet been implemented because are still unknown)
- Vulnerability assessment for the components of the 5G architecture:
  - *CORE NETWORK*
  - *NETWORK SLICING RADIO ACCESS NETWORK*
  - *NETWORK FUNCTION VIRTUALIZATION - MANO*
  - *SOFTWARE DEFINED NETWORKS*
  - *MULTI-ACCESS EDGE COMPUTING*
  - *SECURITY ARCHITECTURE*
  - *PHYSICAL INFRASTRUCTURE*
  - *IMPLEMENTATION OPTIONS*
  - *PROCESSES*

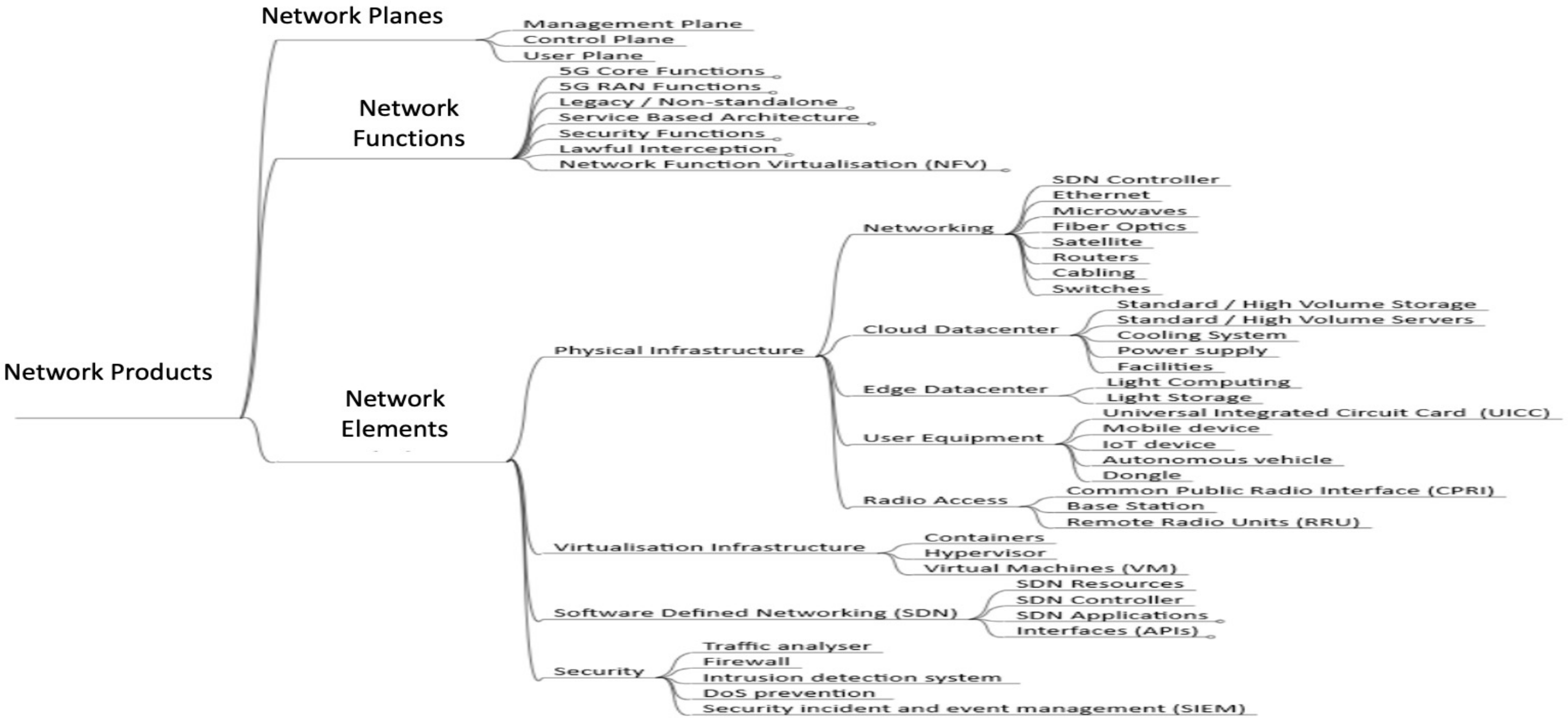


# ENISA 5G NETWORK ASSET CATEGORIES



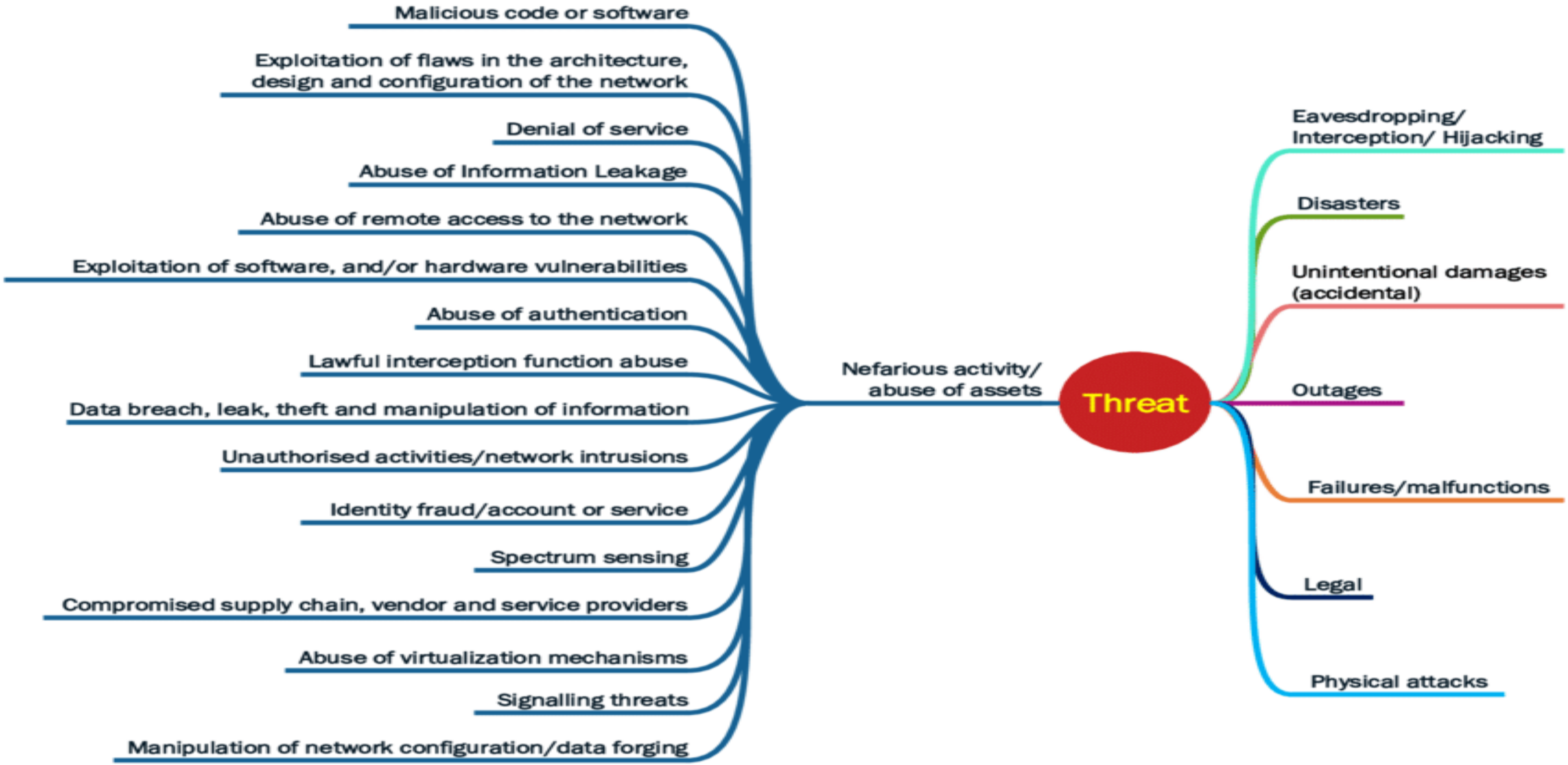
Zoom in

# ZOOM-IN OF NETWORK PRODUCTS CATEGORY



- Network Products
  - Network Planes
    - Management Plane
    - Control Plane
    - User Plane
  - Network Functions
    - 5G Core Functions
    - 5G RAN Functions
    - Legacy / Non-standalone
    - Service Based Architecture
    - Security Functions
    - Lawful Interception
    - Network Function Virtualisation (NFV)
  - Network Elements
    - Physical Infrastructure
      - Networking
        - SDN Controller
        - Ethernet
        - Microwaves
        - Fiber Optics
        - Satellite
        - Routers
        - Cabling
        - Switches
      - Cloud Datacenter
        - Standard / High Volume Storage
        - Standard / High Volume Servers
        - Cooling System
        - Power supply
        - Facilities
      - Edge Datacenter
        - Light Computing
        - Light Storage
      - User Equipment
        - Universal Integrated Circuit Card (UICC)
        - Mobile device
        - IoT device
        - Autonomous vehicle
        - Dongle
      - Radio Access
        - Common Public Radio Interface (CPRI)
        - Base Station
        - Remote Radio Units (RRU)
    - Virtualisation Infrastructure
      - Containers
      - Hypervisor
      - Virtual Machines (VM)
    - Software Defined Networking (SDN)
      - SDN Resources
      - SDN Controller
      - SDN Applications
      - Interfaces (APIs)
    - Security
      - Traffic analyser
      - Firewall
      - Intrusion detection system
      - DoS prevention
      - Security incident and event management (SIEM)

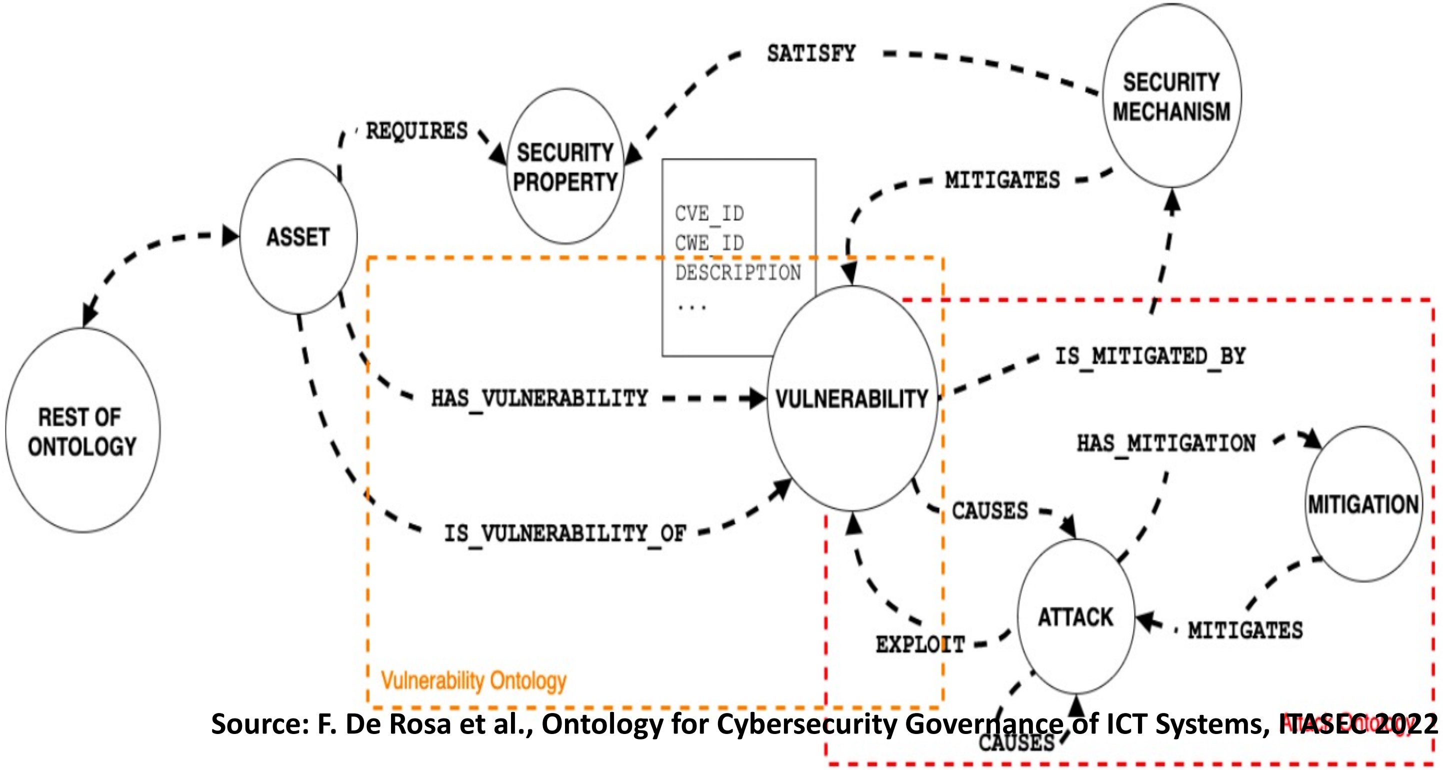
# ENISA 5G THREAT TAXONOMY


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 attacks

# ONTOLOGY BASED RISK ASSESSMENT

- NIS Directive: EU member states have to define measures to **ensure a high level of security of networks, information systems and services** on which essential functions depend

- Operators of essential services have to:
  - identify the ICT assets needed to perform the essential function or service
  - conduct a **risk assessment**
  - keeping it update

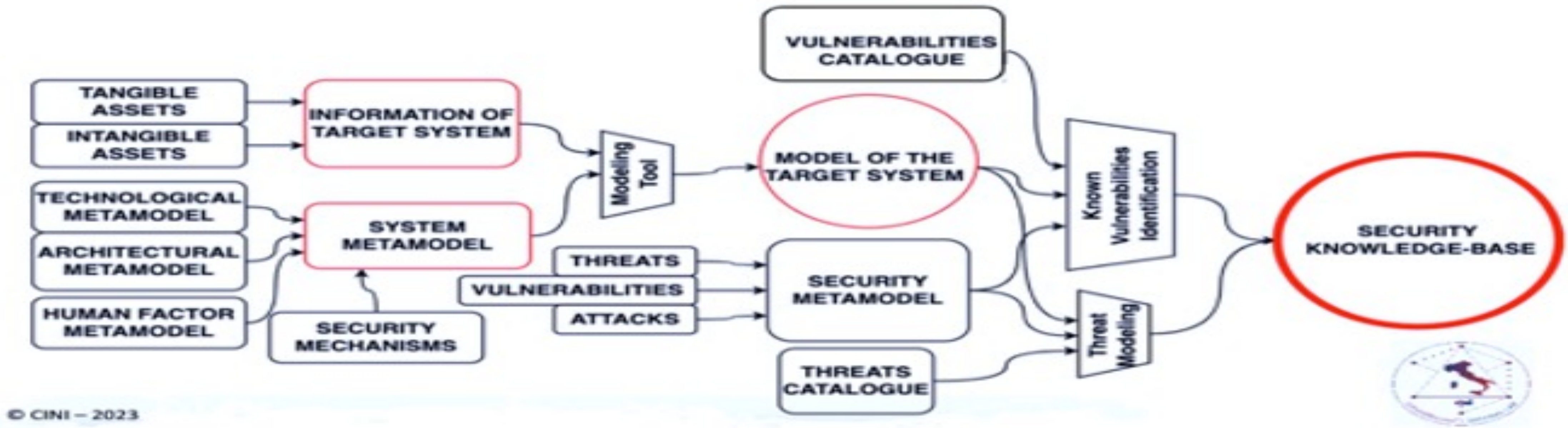


**Source: F. De Rosa et al., Ontology for Cybersecurity Governance of ICT Systems, ITASEC 2022**

Ontology is useful in organizing the information in a semantically rich knowledge–base where a level of automation can be introduced for that purpose

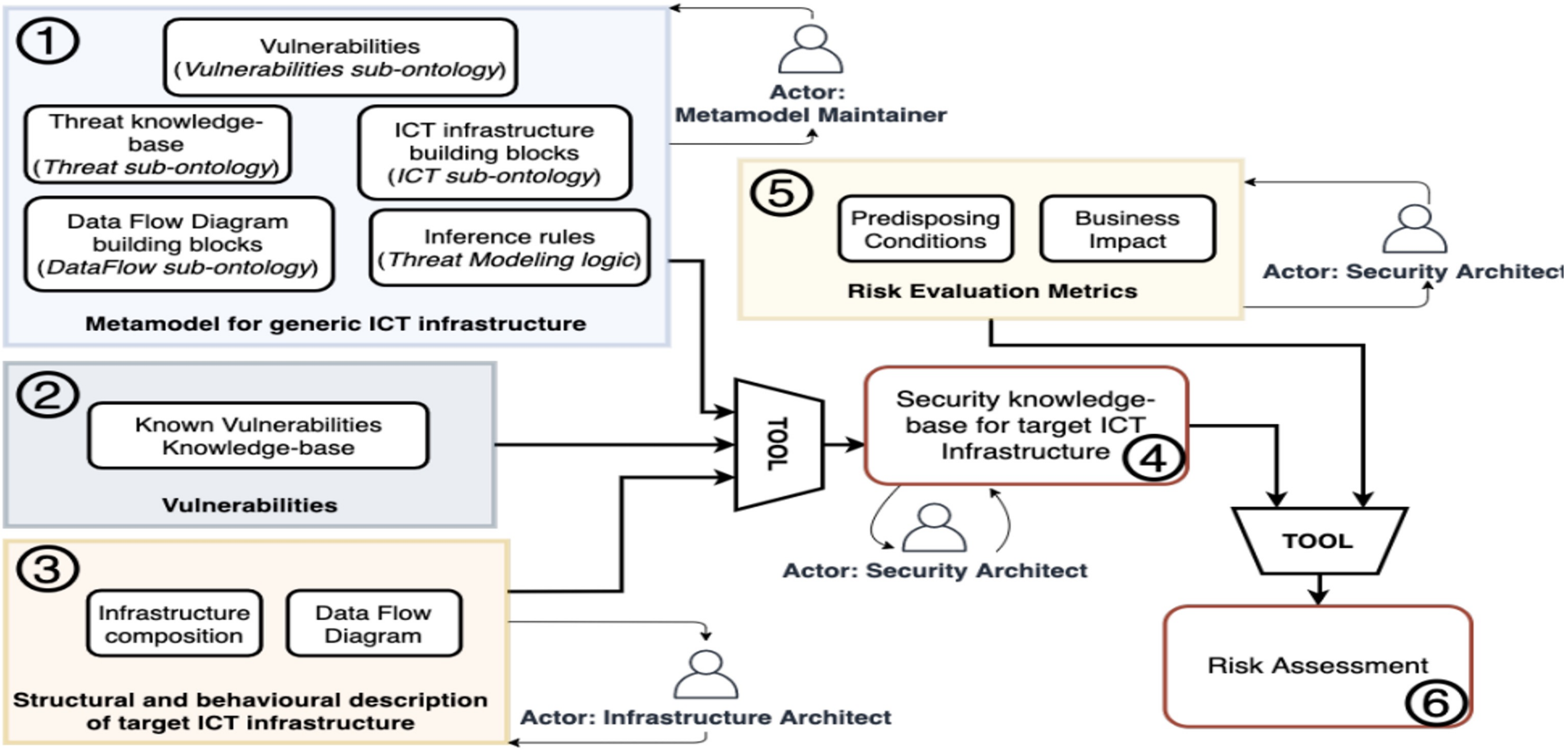
# SECURITY KNOWLEDGE BASED OF A TARGET ICT SYSTEM: ERACLITO Project

**Eraclito** is one of the 27 projects of PNRR extended Partnership **"SERICS - Security and Rights in CyberSpace"** aiming at developing ontologies, methodologies, guidelines, best practices, and tools for improvement of the security posture of the ITC assets (i.e., networks, IT/OT systems and services) included within Cybersecurity National Perimeter



Source: F. De Rosa et al., Ontology for Cybersecurity Governance of ICT Systems, ITASEC 2022

# METHODOLOGY


1
Vulnerabilities (Vulnerabilities sub-ontology)
Threat knowledge-base (Threat sub-ontology)
ICT infrastructure building blocks (ICT sub-ontology)
Data Flow Diagram building blocks (DataFlow sub-ontology)
Inference rules (Threat Modeling logic)
Metamodel for generic ICT infrastructure
Actor: Metamodel Maintainer
2
Known Vulnerabilities Knowledge-base
Vulnerabilities
3
Infrastructure composition
Data Flow Diagram
Structural and behavioural description of target ICT infrastructure
Actor: Infrastructure Architect
TOOL
Security knowledge-base for target ICT Infrastructure
4
Actor: Security Architect
5
Predisposing Conditions
Business Impact
Risk Evaluation Metrics
Actor: Security Architect
TOOL
Risk Assessment
6

Source: F. De Rosa et al, 2022

# TAKEAWAYS

- The dependence of many critical services on 5G networks  make the cybersecurity of 5G networks a strategic issue

- Complexity of  5G networks, calls for automation and artificial Intelligence

- Ontology based approaches are key for building cybersecurity knowledge-base of a target system
    - *Extract system infrastructure from assent discovery and asset inventory tools*
    - *Perform threat modeling and extract system known vulnerabilities automatically*
    - *Develop innovative tools for risk assessment*

- There are many ontologies to be reused in the cybersecurity domain, but not in 5G domain: ENISA plays a key role in integrating 5G architecture and assets, with cybersecurity features, (e.g threats, risks, and vulnerabilities) and is a main reference for building 5G ontology.

- Populating the ontology with information from 5G use cases is the challenge we are aiming at!!!

# AKNOWLEDGEMENTS

*I wish to thank my colleague Andrea Bernardini from FUB for collaboration and fruitful discussions and Paolo Prinetto, Fabio De Rosa, Nicolò Maunero from Cini for providing insight, expertise and coordination that greatly assist the research in the Eraclito Project.*

**This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.**

Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

# Q & A

***To keep in contact:***

*msettembre@fub.it*