



# NETWORLD EUROPE

Strategic Research and Innovation Agenda Webinar  
12,13th January 2023

## SECURITY

Emmanuel Dotaro



# OVERVIEW

- 6G is changing of Architectures

- Significant diversity and complexity: Cellular, Cell-less, Edge, IoT, 3D, Public, Hybrid, Private, Mesh, highly distributed D2D/V2V, Adhoc, **Vertical specific architectures and Regulations**, Distributed Ledger Technologies, Quantum-based architectures, Cyber-Physical...
- Service orientation
- Digital Twins, Massive remote management/monitoring/sensing
- ...

- Change of Usages

- ICT + OT + AI → Systems & Services
- Up to Mission Critical & Human Centric

- 6G new technologies

Risks ever growing  
Attacks with exponential growth

- New Attack Surface
- Unprecedented attacks
- Unprecedented complexity
- Unprecedented fragmentation
  - Unprecedented dynamics
- Unprecedented expectations

17/01/2023

## EVALUATION & QUANTIFICATION

## STRATEGIES & PARADIGMS

Certification

Monitoring

OSINT

**GOVERNANCE incl. CTI**

CERTS

Threats  
Vulnerabilities  
Attacks  
Pentests  
Cyberrange  
Bugbounty

SOC(s)

Infra(s)OC

Users (incl vertical OT)

**AI-based Operational security**

SMART COMPOSITION (services w/ QoSec)

SMART PROTECTION ORCHESTRATION

SMART DETECTION

SecaaS

Distributed

## SECURITY ARCHITECTURES

(function of 6G architectures: distribution, DiffSec, AI, SBA, Computing continuum,...)

## DATA CENTRIC

## SOFTWARERIZATION

## HW for 6G SEC & PHY Layer

**Security functions (all phases)**

HSM/ PKI	XDR	SIEM	EBIOS RM	probes	DLT
IAM	SASE	SOAR	Data centric	...	

**Secured AI**

Secured 6G functions  
Secured subsystems  
Secured components



**CORPUS**

- *Security Distributions in 6G Architectures*
  - *As a function of overall 6G architectures, E2E, Multi-X, E2E policies management (incl. users !), Root of Trust, DT integration*
- *Differentiated 6G Security*
  - *No “one size fit all”, as a function of tenant & regulation policies, priority & precedence mechanisms*
- *Secure Artificial Intelligence (statistical, hybrid) for 6G*
  - *6G-AI models security toolbox (full life cycle), xAI*
- *Human-Centric Multi-Agent & Federative Learning*
  - *Secure w/ privacy preserving, adversarial attacks risks, the federated approaches incl. close-to-the-source monitoring and Multi Agents*
- *Service-Based Architectures*
  - *SSLA & SecaaS integration*
- *Security in the Computing Continuum*
  - *Secure AI and coordination in the computing architecture*

- *Beyond perimeteric strategies*
  - *Actual Zero Trust w/ confidential computing, Deception, MTD, Spatial data fragmentation,..*
- *Black-Boxes and new attack Tolerant Architectures*
  - *Countemeasure and mitigation ensuring overall security levels w/ untrusted areas*
- *Recovery strategies*
  - *Priorities, precedence, graceful remediation*
- *Per vertical specific security profile*
  - *Covering various specific requirements dimensions of security for verticals i.e. synchro, formal proof etc...*

- *Intra-6G (All type) Data Protection*
  - *PQC, SWAP constraints, BC, GDPR anomaly detection,..*
- *Intra-6G Data Processing*
  - *Including sticky policies, MPC, FHE, HW binfing,..*
- *Data powering 6G AI*
  - *CIA, inter-domain, ZKP usage,..abnormal data (biaised) detection*
- *Data security (CIA) in relation to exogenous impacts*
  - *In particular in sensing/com context but as secure enabler for DT in general*



- *Network Security Hardware*
  - *root of trust distribution (full life cycle), sec off loading, secret elements management,...*
- *Securing (new) Network Elements*
  - *LIS/RIS, clocks, flexible HW, supply chain **assurnace***
- *Bearer protection*
  - *Anti-jamming, intentional source of light, authentication, IMSI catcher,...*

- *6G Safe Code life cycle*
  - *AI attack surface via code, whole life cycle issues (updates, upgrades), forensic*
- *Full Security for 6G virtualization*
  - *Securing key components (orchestrators, PDP/PEP;...), performance issues*
- *Virtualized Security Functions*
  - *Scalability for crypto, knowledge sharing for xDR*

- *Security Policy Life Cycle*
  - *Intent-based where formal proof is sometime needed !*
- *Zero touch, autonomic and multi-agent*
  - *Towards true adaptive, DT for reasoning and validation, cooperative holistic security*
- *Root cause and Identification*

- *Quality of Security (QoSec) and relation to Security Service Level Attributes (SSLA)*
- *Continuous assessment of security conformance along life cycle*
  - *E2E provable composition & incremental methodologies*
  - *Platforms and data sets/lakes*
- *Economic and Societal impacts, liabilities*
  - *Bridging 6G security capabilities with societal impact at large using quantification*

- *Building Cooperative response to incident*
- *Private/public cooperation for a 6G CTI*



NETWORLD  
EUROPE

**THANK YOU FOR YOUR ATTENTION**

[networldeurope.eu](http://networldeurope.eu)