NATWORK

iti

CERTH
CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

Net-Zero self-adaptive activation of distributed self-resilient augmented services

Project Overview

Vision, Objectives, Architecture, Pilot Cases, Expectations

SNS Call 2 Projects Introduction Webinar

7 March 2024 - Online

Dr. Antonios Lalas
Postdoctoral Researcher
NATWORK Deputy COO & TM
lalas@iti.gr

Dr. Anastasios Drosou
Senior Researcher (Grade C')
NATWORK COO
drosou@iti.gr

Co-funded by the European Union

6GSNS

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

UK Research and Innovation

NATWORK project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101139285

Project's ID Card

- Short Name: ***NATWORK*** (GA No: 101139285)
- Full title: ***Net-Zero self-adaptive activation of distributed self-resilient augmented services***
- Start date: *1st of Jan. 2024*
- Duration: *36 months*
- Budget & EU Contribution:
  - Total budget: **6.111.179.00 €**
  - Total eligible costs: **3.828.075,00 €**
  - Max grant amount: **3.628.007,50 €**
- Coordinator: ***Dr. Anastasios Drosou (CERTH-ITI)***
- Deputy-Coordinator & TM: ***Dr. Antonios Lalas (CERTH-ITI)***

- Funded under the call: *HORIZON-JU-SNS-2023-STREAM-B-01-04: Reliable Services and Smart Security*

- Project Officer: ***Dr. Marinos Charalambides***

Co-funded by the European Union
6GSNS
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI
UK Research and Innovation

NATWORK consortium (1/2)

#	Short Name	Participant Organization Name	Type	Country
1	CERTH	Ethniko Kentro Erevnas kai Technologikis Anaptyxis	RTO	EL
2	GRAD	Fundacion Centro Tecnolóxico de Telecomunicacións de Galicia	RTO	ES
3	TSS	Tages	SME	FR
4	CNIT	Consorzio Nazionale Interuniversitario per le Telecomunicazioni	RTO	IT
5	ISRD	ISRD Sp. z o.o.	SME	PL
6	ELTE	Eötvös Loránd Tudományegyetem	UNI	HU
7	MONT	Montimage EURL	SME	FR
8	IMEC	Interuniversitair Micro-Electronica Centrum	RTO	BE
9	NEC	NEC Laboratories Europe GmbH	LI	DE
10	NOVA	Nova Telecommunications & Media Single Member SA	LI	EL
11	PNET	P-NET Anadyomena Diktya Neas Genias & Efarmoges Idiotiki Kefalaiouchiki Etaireia	SME	EL
12	ZHAW	Zürcher Hochschule für Angewandte Wissenschaften	UNI	CH
13	UZH	Universitat Zurich	UNI	CH
14	UESSEX	University of Essex	UNI	UK

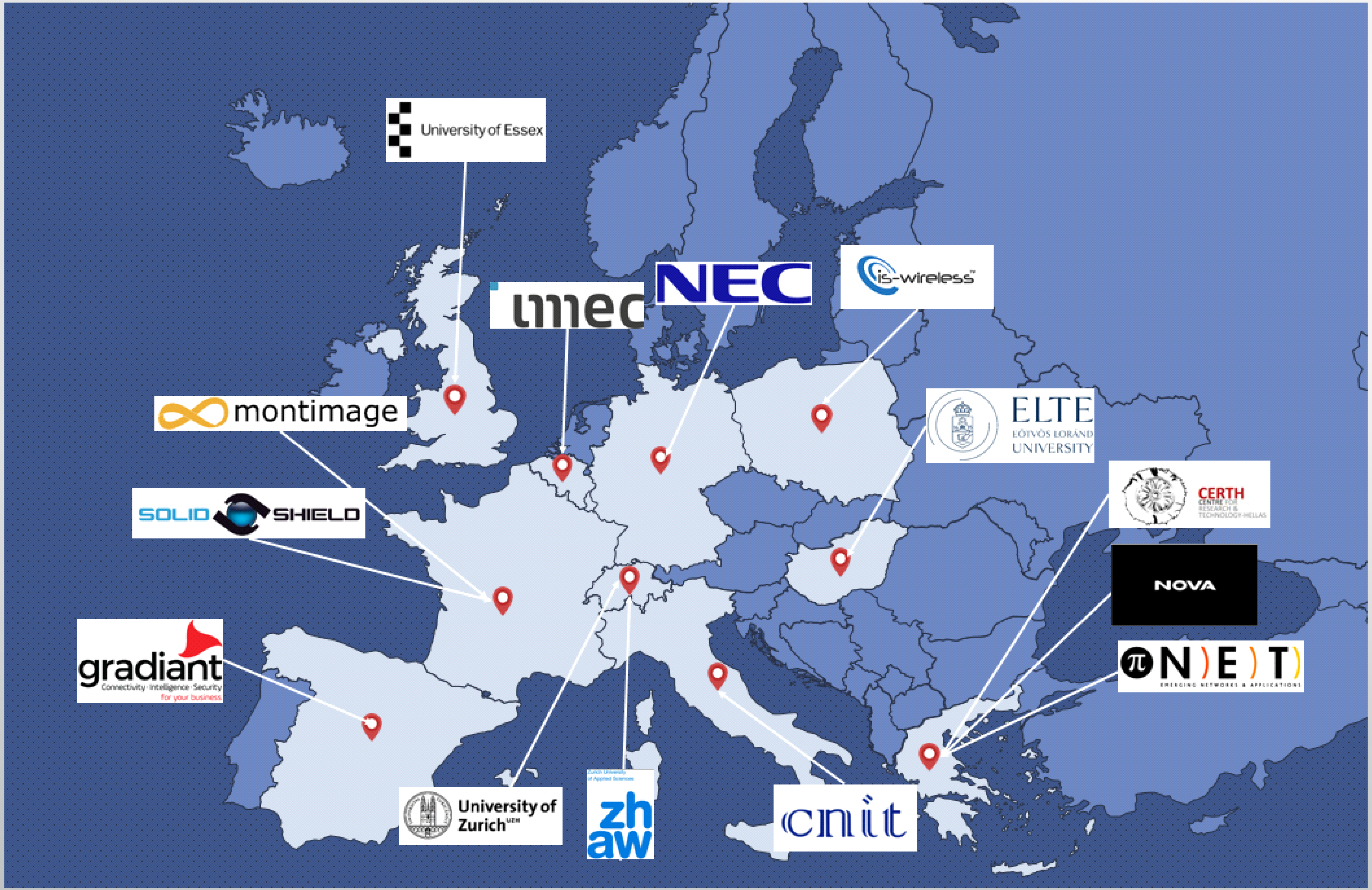
Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

UK Research and Innovation

NATWORK consortium (2/2)

Geographical Distribution



14 participants from
10 EU countries and
associated countries

Co-funded by the European Union

6G SNS

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

UK Research and Innovation

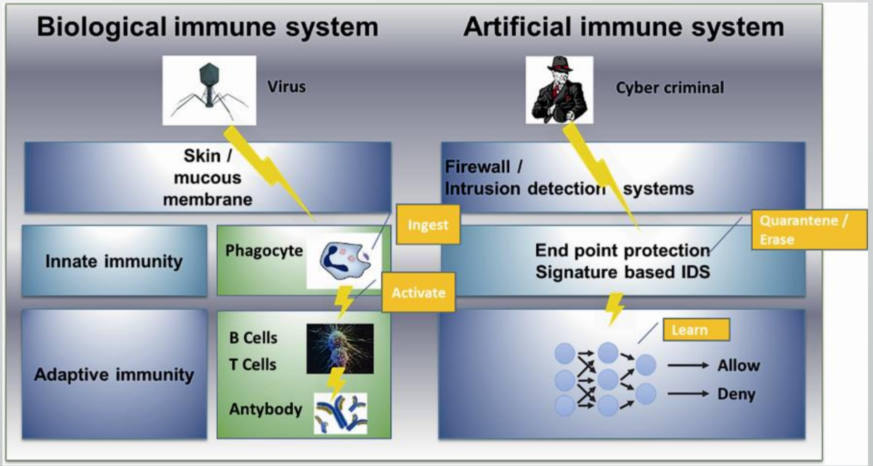
Rationale

Status

- The **architecture of the 6G network** will exhibit a highly dynamic and heterogeneous nature, thus **ensuring continuous security in such a complex and dynamic environment is considered a major challenge**.

- The analogy of **another complex structure - human body** is employed, wherein the immune system is learning from **previous security incidents, forecasting potential future threats, and adjusting security protocols to accommodate shifting circumstances**.

- A breach in the security of the 6G network could lead to a **loss of information, loss of control over connected devices, loss of money and property, or even physical danger to people.**



Rationale

Challenges

- **Providing trustworthiness and security in a continuous manner in 6G** as a human-centred pervasive CPS.
- The **resilience and dependability of smart 6G services and devices** under novel malicious actors and threats with more advanced capabilities (e.g., AI-controlled weaponisation) in 6G.
- **Exploiting AI** as an explainable and robust security technology.
- **Net Zero AI and energy-efficient security** for sustainable networks.
- **Automated and zero-touch management and orchestration** of security via Security SLAs.
- **Integration of PLS and data plane security** for a full-stack security armament in 6G continuum.

Co-funded by the European Union
6GSNS
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI
UK Research and Innovation

Rationale

Ambition

The NATWORK project aims to set the foundations and deploy the very first **economically realistic, energy efficient and viable bio-inspired AI-based 6G cybersecurity and resilience framework** for intelligent networking and services, taking a holistic approach and considering all elements in a cross-sector business environment to address the diverse requirements and challenges that arise.

Opportunity

- The telecom industry starts **deploying b5G/6G testbeds**, that allow them to experiment on high quality novel intelligent networks and services, under a flexible and economically viable model.
- The major device manufactures are reaching a high technology level and are **almost ready to certify and deploy in the near future appropriate devices** to support the new 6G vision.
- The **AI development** is now mature enough providing a variety of services, and being able to take into account special requirements of the new infrastructure.
- The formulation of **AI-based 6G cybersecurity and resilience framework with novel services**, is no longer a revolution but an *evolution*, using new advanced technologies.

Co-funded by the European Union

Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

UK Research and Innovation

The Vision

- The NATWORK project aims to develop ***a novel AI-leveraged self-adaptive security mechanism for 6G networks based on resilient biomimicry principles***.
- The principle premise is to ***empower various entities of 6G ecosystems with the ability to self-regulate their conditions*** to provide service continuity in compliance with service SLAs.
- ***Trust-compliant orchestration and management of microservice applications in cloud-to-edge (fog) continuum*** will be progressed in this direction.
- NATWORK's SECaaS protects by hardening various forms of software payloads including WASM, prior to their deployment, ***leveraging hardware-based confidential computing technologies and/or software-based techniques according to the security objectives, payload mobility and associated energy costs***.
- ***Immunity of the E2E services exploits progressed AI-powered mechanisms deeply rooted down to the physical layer*** or inside data plane-located malware detection functions or finally at upper management layer with moving target defense.
- Physical Layer security will be progressed in view of delivering ***key-less perennial and net-zero resilience to wireless links attacks***.
- The ***Secure Federated Learning architecture of NATWORK will be based on decentralised defensive AI models*** embedded in disaggregated 6G network physical layer, smart Edge Network Interface Cards and RAN devices with P4-based programmable data plane and advanced DPU acceleration, with local feature extraction at wirespeed and AI model training.

Co-funded by the European Union
6GSNS
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI
UK Research and Innovation

The Objectives

NATWORK

✓ **Objective 1:** Define a detailed **extension to 6G architectures** by providing E2E security.

✓ **Objective 2:** Foster **secure-by-design composition and migration of novel 6G cloud-native slices** and secure distributed computations-network in the edge to cloud continuum.

✓ **Objective 3:** Provide **Net-Zero AI-powered trustworthy and explainable management** to allow for highly malleable and attack-resilient networks

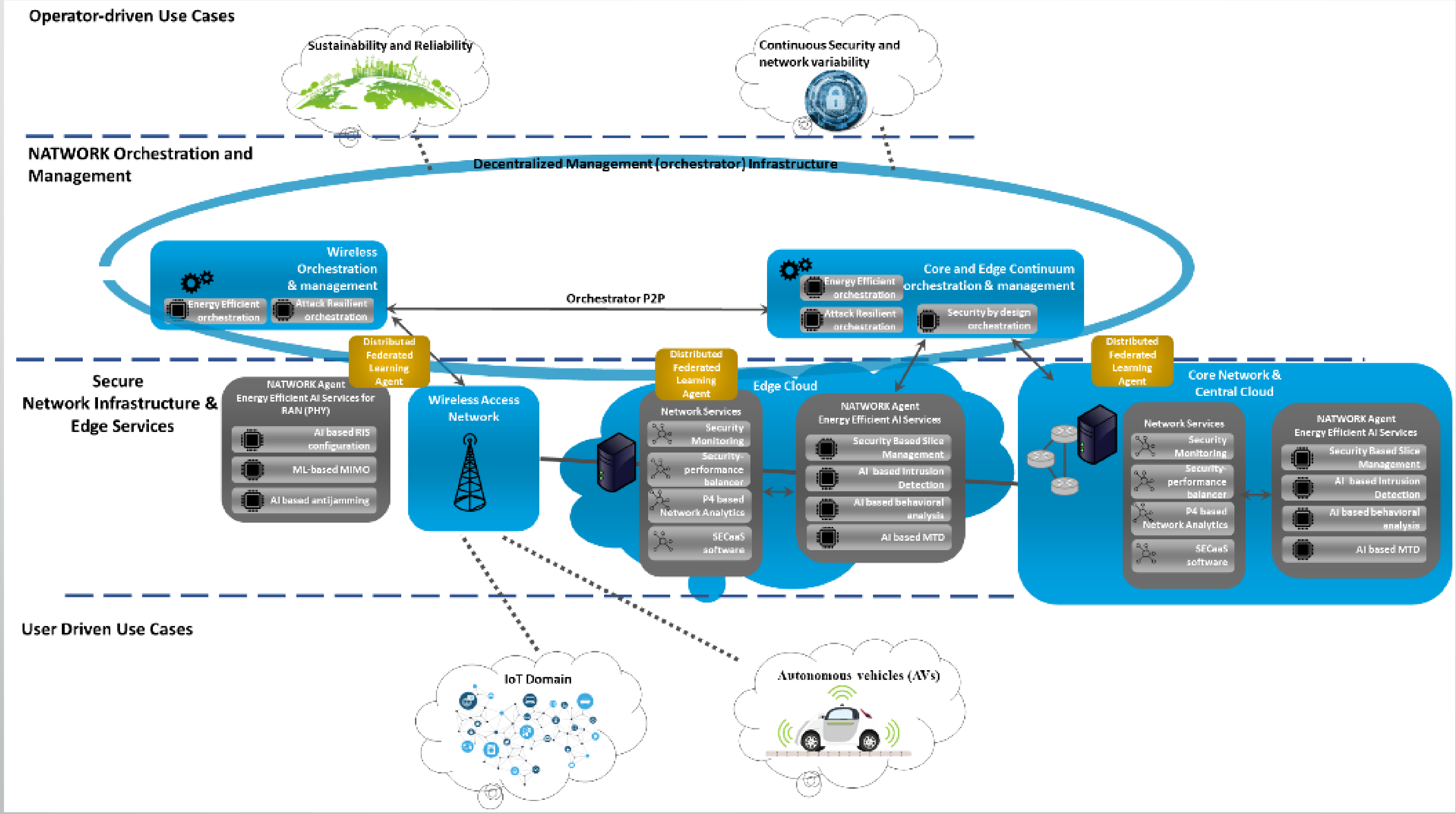
✓ **Objective 4:** Provide **Physical Layer Security** that supports encryption-free, **perennial self-resilience** of wireless links

✓ **Objective 5: Deployment & experimental implementation** of the security modules in relevant Use Cases.

✓ **Objective 6: Evaluation, validation & verification** of the security framework performance.

Co-funded by the European Union
6GSNS
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI
UKRI UK Research and Innovation

Conceptual Architecture


Operator-driven Use Cases
Sustainability and Reliability
Continuous Security and network variability
NATWORK Orchestration and Management
Decentralized Management (orchestrator) Infrastructure
Wireless Orchestration & management
Energy Efficient orchestration
Attack Resilient orchestration
Orchestrator P2P
Core and Edge Continuum orchestration & management
Energy Efficient orchestration
Attack Resilient orchestration
Security by design orchestration
Distributed Federated Learning Agent
Distributed Federated Learning Agent
Distributed Federated Learning Agent
Secure Network Infrastructure & Edge Services
NATWORK Agent Energy Efficient AI Services for RAN (PHY)
AI based RIS configuration
ML-based MIMO
AI based antijamming
Wireless Access Network
Edge Cloud
Network Services
Security Monitoring
Security-performance balancer
P4 based Network Analytics
SECaaS software
NATWORK Agent Energy Efficient AI Services
Security Based Slice Management
AI based Intrusion Detection
AI based behavioral analysis
AI based MTD
Core Network & Central Cloud
Network Services
Security Monitoring
Security-performance balancer
P4 based Network Analytics
SECaaS software
NATWORK Agent Energy Efficient AI Services
Security Based Slice Management
AI based Intrusion Detection
AI based behavioral analysis
AI based MTD
User Driven Use Cases
IoT Domain
Autonomous vehicles (AVs)

Co-funded by the European Union
6GSNS
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI
UK Research and Innovation

Conceptual Architecture

Main Components & Modules

➢ Decentralized Orchestration

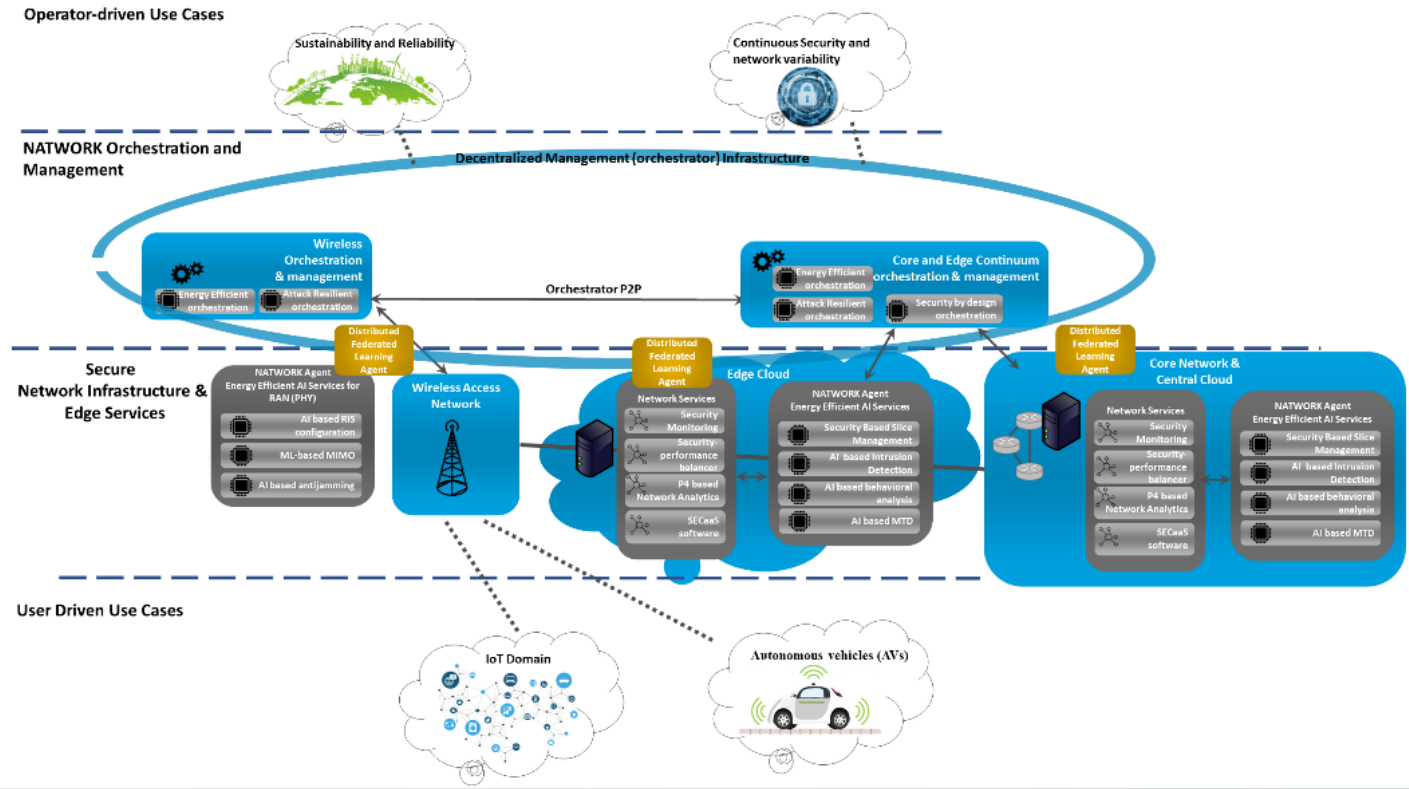
- Energy Efficient orchestration
- Attack Resilient orchestration
- Security-by-design orchestration Service

➢ Energy Efficient AI Services for RAN (PHY)

- AI based RIS configuration
- ML-based MIMO
- AI based antijamming

➢ Edge/Core Cloud

- Security Monitoring
- Security-performance balancer
- P4 based Network Analytics
- SecaaS software
- Security Based Slice Management
- AI based Intrusion Detection
- AI based behavioral analysis
- AI based MTD
- Distributed Federated Learning across the continuum



Operator-driven Use Cases
Sustainability and Reliability
Continuous Security and network variability
NATWORK Orchestration and Management
Decentralized Management (orchestrator) Infrastructure
Wireless Orchestration & management
Energy Efficient orchestration
Attack Resilient orchestration
Orchestrator P2P
Core and Edge Continuum orchestration & management
Energy Efficient orchestration
Attack Resilient orchestration
Security by design orchestration
Distributed Federated Learning Agent
Distributed Federated Learning Agent
Distributed Federated Learning Agent
Secure Network Infrastructure & Edge Services
NATWORK Agent Energy Efficient AI Services for RAN (PHY)
AI based RIS configuration
ML-based MIMO
AI based antijamming
Wireless Access Network
Edge Cloud
Network Services
Security Monitoring
Security-performance balancer
P4 based Network Analytics
SECaaS software
NATWORK Agent Energy Efficient AI Services
Security Based Slice Management
AI based Intrusion Detection
AI based behavioral analysis
AI based MTD
Core Network & Central Cloud
Network Services
Security Monitoring
Security-performance balancer
P4 based Network Analytics
SECaaS software
NATWORK Agent Energy Efficient AI Services
Security Based Slice Management
AI based Intrusion Detection
AI based behavioral analysis
AI based MTD
User Driven Use Cases
IoT Domain
Autonomous vehicles (AVs)

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

UK Research and Innovation

Pilot Cases

Overview

Four (4) pilot cases

Target: test, monitor, and validate all its set of **10 NATWORK's Innovative Solutions**

- 4 different **realistic lab environments** as pilot sites
- **geographical diversity** of the pilots' ecosystem aims to enhance the impact of the project towards the EU-wide uptake of NATWORK.
- are expected to **assess of all the technical enablers** in a complementary manner

Co-funded by the European Union
6GSNS
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI
UK Research and Innovation

Pilot-Case #1

NAT WORK

<table>
<tr><th colspan="2">Use Case #1: Sustainability and reliability of 6G Slices and services</th></tr>
<tr><td><b><u>Objective</u>:</b> Explore innovative energy solutions that can support reliable connectivity and high-quality services while reducing energy costs and minimising environmental impact</td><td>UEssex, IMEC, TSS, ISRD</td></tr>
<tr><td colspan="2"><b>Approach:</b>
1. UC1.1. - Decentralised management and orchestration service for intent-compliant end-to-end service resiliency and continuity
2. UC1.2 - SECaaS for the pre-deployment of dependable software generation
3. UC1.3 - Intelligent workload placement taking into account green energy availability</td></tr>
<tr><td><b>Key Performance Indicators/ Expected Improvements</b></td><td>• <b>KPI 1.1 -</b> End-to-end compliance with latency tolerance (UC#1.1, 10%),
• <b>KPI 1.2</b> - Energy waste (UC#1.1, UC#1.3, 10%),
• <b>KPI 1.3</b> - Respective x86 native payloads latency at start, performance degradation during runtime and overall energy waste for the aggregation of confidentiality, integrity runtime and correct execution monitoring (UC#1.2, <1sec, <10%, <10%).
• <b>KPI 1.4 -</b> WASM security enforcement (according to our security challenge results), equivalent to x86 native implementation.</td></tr>
</table>

Co-funded by the European Union

6GSNS

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

UK Research and Innovation

Pilot-Case #2

<table>
<tr><th colspan="2">Use Case #2: Anti-jamming technologies for AVs</th></tr>
<tr><td><b><u>Objective</u>:</b> Detect, classify, and mitigate jamming attacks in real-time, utilizing Machine learning and AI techniques, by analysing signal patterns.</td><td>CERTH, GRAD, ISRD</td></tr>
<tr><td colspan="2"><b>Approach:</b>
1. UC#2.1: Enabling multi-antenna systems for resilience against jamming attacks.
2. UC#2.2: Empowering AI-based jamming detection and mitigation for multi-path routing in 6G networks.
3. UC#2.3: Adaptive modulation techniques for anti-jamming autonomous recovery
4. UC#2.4: Improving 6G security in 6G spectrum bands</td></tr>
<tr><td><b>Key Performance Indicators/ Expected Improvements:</b></td><td>• <b>KPI2.1 -</b> Jamming attacks detected and mitigated (increase of at least 30% in the detection of attacks)
• <b>KPI2.2 -</b> Time needed to detect and prevent a jamming attack (in the order of a few seconds, target <5s)
• <b>KPI2.3 -</b> Time needed to recover from a jamming attack (reduction by 30% in the order of seconds)
• <b>KPI2.4 -</b> Downtime prevented (less downtime at least 20%), KPI2.5 Throughput enhancement during jamming attack of at least 40%</td></tr>
</table>

Call 2 projects introduction webinar - 7 March 2024
Co-funded by the European Union
6GSNS
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI
UK Research and Innovation
14

Pilot-Case #3

Use Case #3: IoT security	
<u>Objective</u>: Ensuring the security and privacy of IoT devices and their data in 6G networks utilizing advanced threat detection and mitigation mechanisms.	MONT, CERTH, ELTE
Approach: 1. UC#3.1: Enabling anomaly detection using machine learning automated techniques for attack detection. 2. UC#3.2: Validating AI-driven penetration testing and vulnerability assessment for attack mitigation. 3. UC#3.3: Enhancing blockchain-based security and trust management end-to-end security	
Key Performance Indicators/ Expected Improvements:	• **KPI 3.1 -** Mean Time to Detect (MTTD): <5 minutes, <10ms (for MMT rules not based on ML) • **KPI 3.2** - Number of False Positive (FP): <1 % (involving injection of at least 5 different attack types) • **KPI 3.3** - Number False Negative (FN): <1 % (involving injection of at least 5 different attack types) • **KPI 3.4** - Packet Loss Ratio (PLR): <0.001% (for low bandwidth traffic) • **KPI 3.5** - Mean Time to Resolve (MTTR): <10 minutes

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

UK Research and Innovation

Pilot-Case #4

Use Case #4: Improving variability of network with continuous security

Objective: To ensure robust and continuous security in the highly dynamic and heterogeneous 6G network architecture, employing machine learning and AI for real-time security analysis, adaptation, and proactive defense against emerging threats across diverse devices, services, and mobile users.

MONT, CERTH, ZHAW, TSS, ELTE, CNIT, ISRD

Approach:

1. UC#4.1: Enabling software-defined networking and network function virtualisation by employing security aware dynamic resource allocation and monitoring.
2. UC#4.2: Including AI-assisted network slicing for efficient resource utilisation and continuous monitoring and analysis.
3. UC#4.3: Employing software-defined radio for agile payload communication
4. UC#4.4: AI-driven microservices orchestration in 6G networks
5. UC#4.5: Enabling optimised and explainable MTD for 6G edge-to-cloud continuum.

Key Performance Indicators/ Expected Improvements:

- **KPI 4.1** - DFE processing latency <50us with data plane device scalability up to 10k different flow rules. - DFE computational efficiency should be 50% higher than existing methods (raw in-band telemetry). Additionally, it reduces power consumption by 20% compared to standard software-based feature selection and extraction at computational engines.
- **KPI 4.2 -** WAI-based latency purely on hardware < 10 microseconds, latency on software-based WAI < 100 microseconds. 50% less power consumption compared to outsourced AI systems that run on cloud or edge nodes.
- **KPI 4.3 -** Delivery of specifications a PoC exploiting control flow metadata extraction and AI-based DoS attack inference
- **KPI 4.4 -** Probability of detection of DoS attack inference:>80%,
- **KPI 4.5 -** Probability of false detection <5%. Same KPI concerning the monitoring and detection as in UC #3

Co-funded by the European Union
6GSNS
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI
UK Research and Innovation

Expected Outcomes (1/2)

EO#1: Availability of **technologies supporting the necessary levels of trustworthiness, resilience, openness, transparency, and dependability** expected under the EU regulations (such as GDPR and Cyber Security Act, including associated provisions including new certification processes) across a complete continuum

- **incorporating the human-cyber-physical system including connectivity-service provision,**
- **supporting complex human centric multimodal communications**, including entangled devices.

EO#2: Availability of **technologies ensuring secure, privacy preserving and trustworthy services in the context of a programmable platform accessed by multi-stakeholders and tenants** including vertical industries as users, for increasingly fleeting and dynamic scenarios

EO#3: Secure host-neutral infrastructure where multiple infrastructure providers are involved in the deployment, hosting and orchestration of the network service, especially in the context of stringent requirements for the communications.

Co-funded by the European Union
6GSNS
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI
UK Research and Innovation

Expected Outcomes (2/2)

EO#4: Identification of the **life cycle of smart services security and trust requirements including development, provision, operation, maintenance and of their business impact** on the stakeholders' ecosystem

EO#5: AI technology can be applied to security and service deployment in several ways:

i) correct application of AI to enhance security and service deployment in 6G

ii) consideration of potential security threats using AI

EO#6: Operational security: **End-to-End, system wide Security policies composition and management among multiple stakeholders** based on trusted and eventually certified services, eventually providing technology solutions in the context of regulatory initiatives like the cybersecurity toolbox

EO#7: New services and security technologies that will fulfil 6G needs and EU policies in this area.

Co-funded by the European Union 6GSNS Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI UK Research and Innovation

Questions & Answers

NATWORK

THANK YOU!

Contact Details: *Dr. Antonios Lalas* *lalas@iti.gr*
Dr. Anastasios Drosou *drosou@iti.gr*

iti

Centre of Research & Technology - Hellas
Information Technologies Institute

CERTH
CENTRE FOR
RESEARCH & TECHNOLOGY
HELLAS

Co-funded by
the European Union

6GSNS

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI

UKRI
UK Research
and Innovation