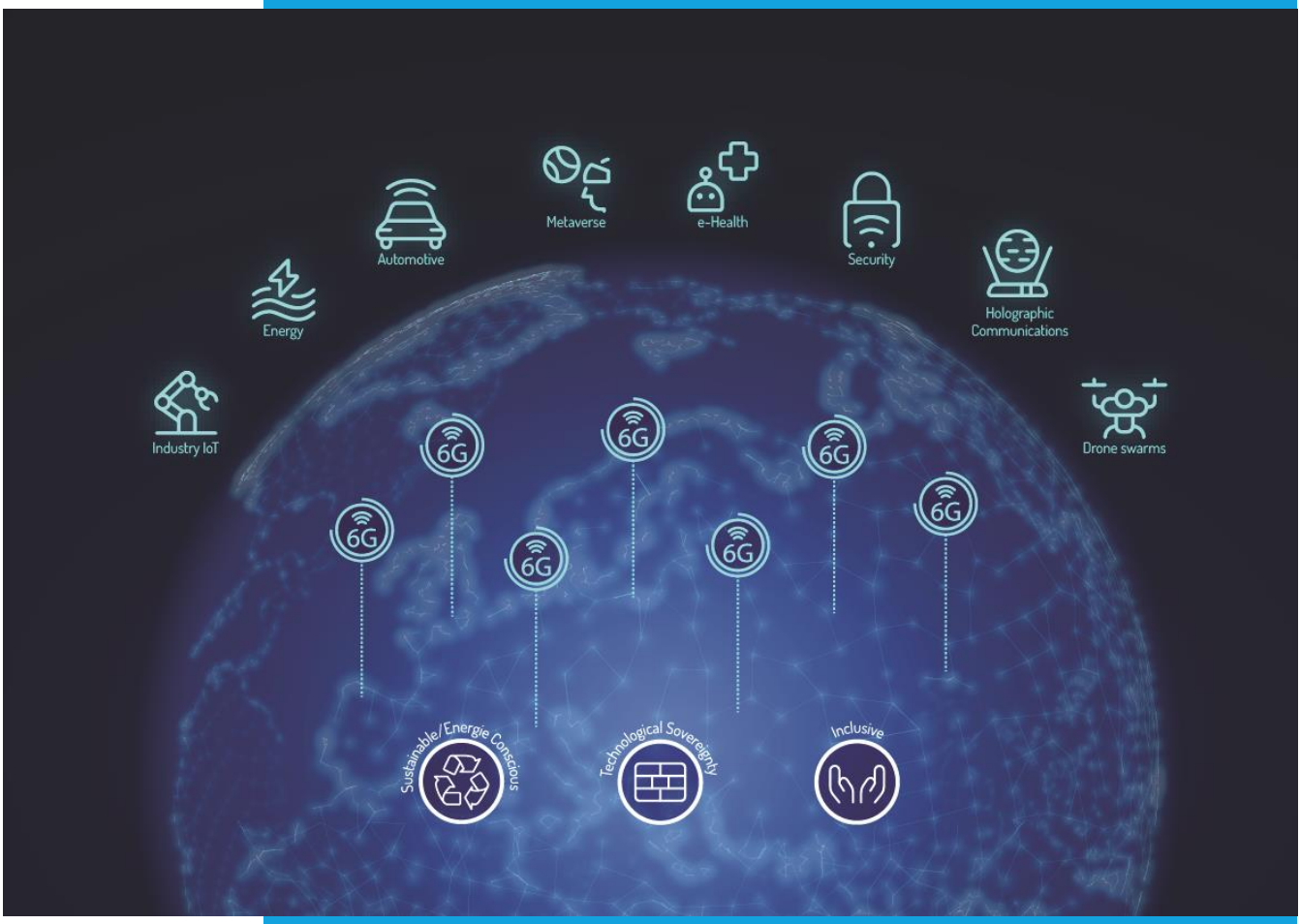
6G Smart Networks and Services Industry Association (6G-IA)



Version 1.0

mai 2024

Position paper

RESEARCH PRIORITIES ON 6G SECURITY

Editors : Emmanuel Dotaro

TABLE OF CONTENTS

1. INTRODUCTION

The Smart Networks and Services Joint Undertaking (SNS JU) is at a pivotal juncture. As it embarks on the second half of its journey within Horizon Europe's R&I Programme, ensuring the security of future 6G deployments is paramount. Recognizing this criticality, the 6G Infrastructure Association (6G-IA) convened a panel of experts for a workshop held on April 12th, 2024, in Brussels. The workshop's focus: defining strategic security priorities for the next phase of the SNS JU.

The SNS JU has long championed the importance of security for 6G. However, security is not a singular concern; it permeates the entire digital ecosystem, from the cloud to AI and the vast network of IoT devices. Each element presents unique vulnerabilities, contributing to the ever-evolving threat landscape. This very interconnectedness, where technologies and architectures converge, offers a unique opportunity for collaborative security efforts.

The workshop identified several areas ripe for further exploration, building upon the foundation laid by previous achievements in 5G security. This document delves into these priority areas, outlining potential pathways for collaborative research and innovation within the SNS JU framework. It emphasizes the importance of leveraging synergies with existing initiatives within Horizon Europe and Digital Europe to build a robust and secure 6G future.

Recognizing this potential and advocating for a holistic approach to secure 6G, multiple interfaces and potential collaborations are In scope. This includes in particular involvement of the cybersecurity industry as supplier of products and services but also as Research & Innovation actors on numerous common topics impacting 6G.

Other aspects that may be considered strategic for EU destiny is the technical foundation of potential policies enhancing users awareness and overall security and resilience.

2. CURRENT STATUS

The Smart Networks and Services Joint Undertaking (SNS JU) under Horizon Europe R&I Programme has reached its halfway point. To chart the course for the remaining years, the 6G Infrastructure Association (6G-IA) invited a panel of experts to a workshop Friday, April 12th, 2024 in Bruxelles focused on security strategies and priorities for the SNS JU's second term.

The SNS JU has already recognize the importance of security for future 6G deployments.

Security is not a single concern, but a thread woven throughout the entire digital infrastructures and services. From the cloud to AI and the vast network of IoT devices, each element presents unique vulnerabilities, participating to the threat landscape. This is precisely why 6G, standing at the intersection of these technologies and architectures, offers tremendous opportunities for collaboration. The inherent connections, shared interests, and potential synergies are undeniable. Recognizing this, the ECSO association was actively involved in this workshop, bringing its expertise to the table to ensure a holistic and secure future for 6G.

Some of the areas are already identified and part of the State of the Art, with among other the examples listed here below:

- Security and privacy for AI at the network edge
- Secure-by-design communication for deterministic performance
- Network-integrated security across user planes

- Infrastructure-agnostic software security
- Privacy preservation and automated security orchestration
- Proactive security provisioning and decentralized security analytics
- Privacy-aware network slicing and security service orchestration
- Enhanced authentication, integrity verification, and encryption
- Physical layer security schemes and zero-touch security deployment

Looking forward the workshop aims to define the strategic security priorities needs for the next phase of SNS, considering the evolving global landscape. Key objectives include:

- Reassess and confirm security priorities for the next three years
- Identify key European strengths and weaknesses in security R&I
- Develop a plan for deploying SNS solutions, starting with lower-level technologies and progressing towards high-TRL large-scale trials
- Understand key trends in 6G security and develop plans for the necessary underpinning technologies

The workshop's outcome will be shared with the Boards of 6G-IA, related Joint Undertakings, and Public Private Programmes to explore potential downstream partnerships; it will also be used to inform public consultations and suggestions across 6G-IA members during future Work Programme and exploitation strategy development

Building on Past Achievements

The workshop acknowledges the progress made on previous security challenges inherent to 5G and its evolution. These include objectives listed in the first term of the SNS JU:

- AI for secure edge architectures and resource management
- Blockchain for secure and intelligent networking and orchestration
- Post-quantum cryptography and confidential computing
- Holistic security frameworks for the IoT-Edge-Cloud lifecycle
- AI-driven security orchestration, trust management, and deployment
- Human-centric security, privacy-by-design security enablers
- End-to-end security for improved trust
- Energy-efficient security for sustainable networks
- Security and trust orchestration for 6G distributed cloud environments
- Zero-touch security management functionalities

It was suggested to consider a list of potential topics to be discussed compiled from the NetworldEurope SRIA, which is used as the basis for the SNS SRIA as well as lessons learnt from the event "6G Sec: Common Path and Cardinal Points (CP)²" that occurred in Paris, in January 2024.

- All phases of 6G cybersecurity (NIST 2.0)
- Beyond-perimetric Architectures (incl. Zero-trust applications at network/computing & services levels)
- Physical layer security
- Security of softwares and virtualized environments
- Secure AI for secure 6G
- Data centric security
- E2E security distributed operations including beyond authority perimeter attacks
- Resilience & Service continuity
- Quantification and evaluation
- Security governance, knowledge sharing, CTI
- application of Quantum key distribution and post-quantum cryptography

One of the main driver is to establish a collaborative environment where key public and private players can conduct research activities; develop secure solutions for critical hardware and software components, foster end-to-end solutions compliant with European policies and legislation

The workshop represents a step towards achieving European technological leadership in security and privacy for 6G networks and structure the efforts, organize the synergies among the various initiatives

3. TOPICS FOR CONSIDERATION

- Considering the preliminary discussions that occurred during the workshop organized in Bruxelles in April 2024,

- Although in relation with the existing State of the art coming from previous SRIA actions and SNS projects,

the topics for consideration have been organized in four areas: Architectures, Operations, Services, Evaluation.

Each of them is derived in a list of specific clusters of topics. Each cluster is designed as a consistent set of research efforts but may be the purpose of further distribution depending on project size. As an example, the cluster of topics focused on “Zero Trust” may be legitimately derived into a focus on Confidential Computing relying on trusted zone as another one still from “Zero Trust” will focus on Access Control or even advanced cryptographic technologies such as FHE, MPC, ZKP,..

This structure is the synthesis from discussions and is not aiming at being neither exhaustive nor prescriptive.

While the workshop covered a comprehensive range of security topics, it's important to note that certain areas were not explicitly prioritized for dedicated focus. Physical layer security, traditionally addressed within specific domains like radio or optics, wasn't singled out for broader

collaboration. Additionally, disruptive security approaches like deception techniques or moving target defense weren't highlighted as immediate priorities. Finally, regarding quantum security, the focus was placed on Post-Quantum Cryptography (PQC) as a short-term need, with Quantum Key Distribution (QKD) not identified as a mandatory short term area, at least in the context of the SNS JU.

Potential implementation perspective in the SNS JU program is given in section "way forward" as well as potential synergies with other initiatives.

Building Secure 6G architectures

Zero Trust for Real: Integrating the Philosophy

One crucial area of research involves the genuine incorporation of Zero Trust (ZT) principles into 6G security architecture, especially in the network deployment context. Unlike traditional perimeter-based security, Zero Trust assumes constant breach and promise verification of every entity (user, device, application) before granting access. Research needs to define implementation methods for Zero Trust within 6G's dynamic environment, considering factors like decentralized identity management, least privilege principle, and continuous authorization checks. As ZT is the companion of Data Centric Security (DCS) focused on confidentiality, architectures should also integrate data policies in addition to extend the user point of view for critical application where availability and performance are the prime constraint. Specific usages of confidential computing, Full Homomorphic Encryption, Multi Party Computation, Zero Knowledge Proof as well as integration of secure (open) data spaces should complete the DCS integration.

Sensing the Threat Landscape: Integration with ISACs

Integrating advanced sensing capabilities with Information Sharing and Analysis Centers (ISACs) holds immense promise. Sensors within the network can gather real-time data on anomalies and potential threats. Research on 6G security architecture should focus on developing overall security with this new attack surface, meaning affordable secure communication protocols and mitigation of inherent threats. This may include specific orchestration patterns of the resources and integration of self-preservation properties to limit the impact of the potential threats and specific ISAC impacts on the control of the systems.

The Quantum Frontier: PQC and QKD

Research needs to evaluate the applicability of existing crypto schemes and potentially prioritize the integration of agile/flexible Post-Quantum Cryptography (PQC) algorithms into the 6G security architecture to ensure continued data confidentiality even with the arrival of quantum computers. Additionally, investigation of integration of Quantum Key Distribution (QKD) for key exchange, impact on 6G systems and their Key Management Systems is an open question. This may also includes the investigation of hybrid methods considering both PQC and QKD.

Convergence for a Secure Ecosystem: Cloud, IoT, and Beyond

6G won't exist in isolation; it will converge with existing technologies like

cloud computing and the Internet of Things (IoT). Research must focus on developing a holistic security framework that seamlessly integrates security solutions across these the various domains of the architecture (from far edge, through continuum up to applications & services). It may be noticed that this field comes beyond current challenges raised by network disaggregation and its consequences (openness, interfaces multiplication, virtualization, HW/SW binding,…) for security. This convergence should prioritize critical and strategic services, ensuring the highest level of protection for essential applications.

Redundancy and Resilience: Eliminating Single Points of Failure

Single points of failure pose a significant vulnerability. Research needs to address this by exploring redundancy in all aspects of the security architecture, including servers, communication links, and security control points. Beyond the redundancy design it should also encompass graceful degradation procedure/policies, priority/precedence policies, make-before-break/graceful restart, policy-based resource allocation, ensuring the availability of critical resources for response and recovery in case of various malicious attacks (incl. DDOS) as well as disasters.

Forensics in the Age of Complexity: Untangling the 6G Web

Investigating cyberattacks in a complex 6G environment presents unique challenges. Research should focus on developing advanced forensic tools and techniques tailored for the 6G architecture. The exploitation in forensic operations is fully dependent on the distributed capabilities of secure storage in sharing across the complexity of 6G systems. Tools should be capable of collecting and analyzing massive datasets from distributed network elements while maintaining data integrity and chain of custody for legal purposes.

Needs to embrace Automation and intelligence in Security Operations

The ever-evolving landscape of 6G necessitates a paradigm shift in security operations (SecOps). Conventional static security approaches will struggle to keep pace with the dynamic nature of 6G systems and services. Automation and intelligence are no longer optional – they are mandatory for ensuring a robust and secure 6G ecosystem. Beside real time constraints, the approaches should cover any type of 6G diversity in terms of architecture; highly distributed systems, fragmented, disaggregated and under multi-party authority perimeters.

While past research has explored automation in SecOps, significant gaps remain. Existing solutions often fall short in comprehensively addressing the intricate interplay between all system components and guaranteeing end-to-end interoperability. To address this, research must delve deeper, encompassing all phases (Govern, Identify, Protect, Detect, Respond and Recover) outlined within the NIST Cybersecurity Framework (v2.0).

End-to-End Attack Detection & Response in 6G with secure AI

A cornerstone of this research should be the extensive integration of various kind of Artificial Intelligence (AI), potentially including Generative AI or even autonomous multi-agents. AI has the potential to revolutionize SecOps

by automating (and beyond automation up to adaptive response) mundane tasks, analyzing vast amounts of data to identify threats, and facilitating real-time decision-making. By leveraging AI, security professionals can focus on strategic initiatives while AI handles the heavy lifting of threat detection, response, and mitigation. AI should be considered as a pre-requisite to scale the operations but is in turn the subject of potential attacks (adversarial, GAN-based, poisoning,…) and will have to secured all along the life cycle of the systems. As such avoiding poisoning of data, models, giving explainability to master the operations is a key focus, that have to be tailored to specific 6G statistical AI life cycles, specific 6G scenarios and policies as well as usage of Control Loops in automation.

Full-6G Resilient Infrastructure & Services

This research should be driven by the ultimate goal of bolstering the resilience of 6G infrastructure and services. Resilience in this case, refers to the ability to withstand, adapt to, and recover from cyberattacks. By incorporating secure AI and automation into all phases of the NIST framework, 6G networks can achieve a level of self-healing and proactive defense that traditional methods simply cannot match. It is worth to remind that intelligent security operations must not be agnostic to overall resource optimization (network, 3D, Sensing, compute…), the reverse being also easily understandable. 6G resilience is thus a holistic approach overcoming traditionally non-cooperative mechanisms

Continuous evolution of 6G security knowledge and cooperative mechanisms

At the governance chapter, Research should explore the potential of a dedicated Cyber Threat Intelligence (CTI) platform specifically tailored to the 6G landscape but capitalizing on existing technologies and/or sectors CTIs. This platform would serve as a central repository for threat data, threat actor profiles, and vulnerability information. By fostering real-time information sharing among stakeholders (including smaller actors such as SMEs), a CTI platform could significantly enhance situational awareness and enable a coordinated response to emerging cyber threats.

Ensuring the security of 6G networks demands a radical shift towards automation and intelligence in SecOps. Research focusing on integrating AI across all phases of the NIST framework, along with the development of a robust CTI platform, holds the key to building a resilient 6G ecosystem capable of withstanding the ever-increasing sophistication of cyberattacks. By prioritizing these research areas, we can pave the way for a secure and trustworthy 6G future.

Secure Services & Security services

Bridging the Gap: Research Needs for User-Centric Security in 6G Services

For 6G services to be truly successful, security needs to be more than just a technical hurdle; it must translate into tangible value for users. Research in 6G security and services needs to bridge the gap between technical advancements and user experience.

Security Made Visible: Exposing the Value Proposition

Users often perceive security as a complex and opaque concept. Research should explore innovative ways to showcase the security benefits of 6G services in a clear and user-friendly manner. This could involve developing security dashboards that display the current threat landscape, highlighting the specific security mechanisms employed by the service, and providing a quantifiable measure of security attributes of various 6G services. Application Programming Interfaces (APIs) will be the primary access point for interacting with 6G services. Research must address the security implications of APIs, exploring secure API design to access differentiated secure 6G services. One can notice that coming to AI-based security appliances and/or involvement of AI in overall security, qualitative description (linked to xAI) may improve the trust in the security level.

Security should not be an afterthought; it should be a prominent feature of all 6G services. Research should explore ways to integrate security attributes into service offerings, allowing users to compare security capabilities in addition to performance and choose services based on their specific security needs. This could involve standardized security labels specific of 6G or inherited from other ICT sectors similar to nutritional information on food products, clearly displaying the level of encryption, intrusion detection capabilities, and compliance with relevant security standards.

Intent-Based Security: Aligning User Policies with Service Delivery

The concept of Intent-based networking (IBN) holds considerable promise for 6G. IBN allows users to express their security policies and preferences, enabling the network to automatically configure and enforce those policies throughout the service lifecycle. Research should focus on developing robust user-friendly interfaces for defining security policies at the data level, application level, ensuring end-to-end security (infrastructure and services) that aligns with user intent. A full chain of AI applications are required here (ML, Generative AI,..), from semantic extraction in natural language from the towards systems configurations with adequate security levels, evluaiton, monitoring and assurance,

Collaboration for a Secure Ecosystem: MSSP Integration and Stakeholder Engagement

The complex nature of 6G security demands collaboration between different stakeholders. Research should explore ways to seamlessly integrate Managed Security Service Providers (MSSPs) into the 6G architecture. MSSPs can offer expertise and resources to manage security for user organizations, reducing the burden on individual users. Additionally, research should consider the needs of specific stakeholders such as critical infrastructure operators, ensuring their unique security requirements are addressed within the 6G ecosystem.

Enabling 6G Security Evaluation

The dynamic nature of 6G systems necessitates a paradigm shift in security evaluation methodologies. Traditional static assessments will be insufficient for ensuring continuous security posture in a constantly evolving environment. Research must focus on developing robust and adaptable frameworks for evaluating the security of 6G networks.

Continuous Security Assessment: Keeping Pace with Change

The dynamic nature of 6G, with its ever-changing network configurations, software updates (including in a DevSecOps mode), and evolving threats, demands a move from static to continuous security assessments. Research should explore innovative methods for real-time monitoring of security posture, with continuous conformity and vulnerability scanning tools. This will enable proactive identification and mitigation of security risks before they can be exploited and offer potential interworking within the parties involved. This research is to be considered as correlated (source) of smart and dynamic security adjustment, under resource constraints maintaining expected security level expected;

Standards for Security Quality:

Without standardized metrics for security quality, it becomes difficult to objectively evaluate the security posture of 6G networks. Research needs to focus on developing industry-wide standards that define different security levels based on factors like data sensitivity, network infrastructure complexity, security features implemented and potential attack surfaces. Quantitative risk analysis may of cyber threats woiuld be beneficial to the overall approach. These standards will provide a clear benchmark for evaluating the security of 6G services (thus allowing security level visibility, even when the user is not a security expert) and guide users in selecting the appropriate level of security for their specific needs. From an operational point of view this should take into account composition of the various services, segments, sub-systems and products (even as black boxes) actually involved end-to-end.

Security Measurement and Certification: Building Trust through Validation

Building trust in the security of 6G networks requires robust certification and regulatory frameworks. Research should explore the development of security level measurement tools that provide a quantifiable assessment of a network's security posture, potentially with support of Digital Twins. These measurements can participate as a basis for certification programs, allowing users to choose providers who have demonstrably met rigorous security standards. Regulatory bodies also need to adapt to address the unique security challenges of 6G, establishing clear guidelines and enforcing them to ensure a secure and trustworthy ecosystem. Measurement and certification of such complex and dynamic systems impose to rethink the process with paradigms such as composition of certification (end-to-end) and incremental as timing do not allow to restart from scratch at any modification.

Securing the Supply Chain: Addressing Vulnerabilities from Start to Finish

The security of a 6G network is only as strong as its weakest link. This highlights the importance of securing the entire supply chain, from software development to hardware manufacturing. Research should address the security implications of the 6G software lifecycle, focusing on secure coding practices, vulnerability management during development, and secure deployment and update procedures. This is to come with traceability of involved functions evolution (network, computing, security, …) Additionally, research should explore ways to track and verify the provenance of hardware components used

in 6G infrastructure, mitigating the risk of malicious actors introducing vulnerabilities at the manufacturing stage.

Open Source specifics

Research needs to investigate ways to leverage the benefits of open-source software while minimizing its security risks. This could involve fostering stronger collaboration among open-source developers, security researchers, and users to identify the whole life cycle process of OSS including certification fostering OSS potential usage in the landscape. Specific security focus on necessary open-source software for 6G network infrastructure shall be considered.

4. POSSIBLE WAY FORWARD

This document outlines some priorities for a strategic approach to 6G security research and innovation, recognizing its critical role in building a secure and trusted next-generation digital infrastructure. The presented focus areas prioritizes both timeliness and potential for collaboration with other instruments within Horizon Europe and Digital Europe initiatives. Here below, one can also find, topics not embedded in priorities table but suggesting collaboration with other communities or instrument.

- While certain 6G security vulnerabilities may manifest at the physical layer (radio or optical), true security demands a holistic approach. Jamming detection, for example, necessitates countermeasures beyond the physical, potentially leveraging intelligent reflecting surfaces (RIS) and AI-based management for optimal network defense. Similarly, research on physical layer fingerprinting could inform broader actions like blacklisting suspicious devices.
- The same way Hardware (HW) security, including potential root of trust coming with Confidential Computing (and also binding with virtualization technologies) may be handled through dedicated programs or at least with a fraction of it dedicated to 6G.
- 6G being at the crossroad of multiple technologies and architectures, there are several opportunities to collaborate and optimize synergies in the following areas:
- Security of cloud continuum/6G with corresponding existing IPCEI and/or other HPC HE/DE initiatives
- This critical area transcends 6G, offering valuable cross-cutting synergies. Research efforts should leverage existing regulations and initiatives on AI and data security. 6G's role as infrastructure for critical applications and data-intensive AI operations demands a particularly strong focus on this aspect
- AI and Data Security are also the purpose of many initiatives including regulations. 6G desereve at least two main reasons to collaborate in this field:
- 6G will serve as infrastructure and services for critical application
- 6G will be AI-based manipulating large amount of data impacting privacy.

- Some of the 6G architectures such as 3D have a natural overlap with space domain programs
- Quantum topics and quantum technologies integration may be handled through existing flagships and initiatives
- Last but not least, 6G security has specific application of numerous security topics which fit under the umbrella of the European Cybersecurity Competence Center (ECCC). It is strongly recommended to reinforce synchronize the actions in research and Innovation (both HE and DE) and even beyond for regulation/certification.
    - Note that mention to ECCC is for the sake of simplification but has to be considered as overall actions taken by the European Commission in the context of cluster 3 and 4.

The table below summarize the topics discussed and potential implementation in SNS JU program

Topics/ranking interest/time frame ***** highest** **** medium** *** Lower**	**Short**	**Medium**	**Long**	**Synergies/suggestions**
Architectural issues				
Zero trust integration including Confidential computing, Data Centric Security and advanced cryptographic technologies applications (FHE, MPC, ZKP,…)	*******	******		**ECCC synchro** **Specific 6G application**
Securing ISAC with mitigation of unprecedented attack surface and self-preservation		******	*******	**Specific to 6G**
Integration of Post Quantum Cryptography in 6G systems with potential hybridation with Quantum Key Distribution	******* **(PQC)**		***** **(QKD)**	**ECCC synchro,** **(PQC) Specifc 6G application including constrained platforms (SWAP), performance and scalability, sustainability issues** **(QKD)Quantum flagship**

Converged security architectures allowing interworking within AI-native 6G including Cloud Continuum and IoT	**	***		**Cloud IPCEI**
Redundancy and Resilience: exploring Single Point of Failure banishment and recovery strategies (including post disaster)	**	***		**6G specific**
Forensic in the age of 6G complexity: collecting trustable data, legal and liabilities applications			***	**6G specific**
Operational issues				
End-to-End attack detection and Response in 6G with secure AI	***			**6G specific**
Full-6G Resilient Infrastructure & Services (Networks, 3D, Compute, sensing, AI..) in all NIST 2.0 phases		***	**	**6G specific**
Continuous evolution of 6G security knowledge and cooperative mechanisms		**	***	**6G specific**
Secure services and security services				
Security made visible: exposing the security attributes and value		***		**ECCC synchro: should be consistent with overall security standards and regulation**
Intent-Based Security: Aligning User Policies with Service Delivery			***	**ECCC synchro for policy extraction/solvers enabling 6G specifics**
Collaboration for a Secure Ecosystem: MSSP	***	**		**ECCC and Industrial Cybersecurity ecosystem**

Integration and Stakeholder Engagement				
Enabling 6G security evaluation				
Continuous Security Assessment: Keeping Pace with Change	**		***	**6G specific, potential synchro with cloud IPCEI**
Standards for security in the context of 6G		***	**	**6G specific**
Security measurement and certification (including composition and incremental issues		**	***	**6G specific coming into overall composition/incremental schemes (thus ECCC)**
Securing the supply chain including Open Source	***			**potential inheritance from SW/HW generic security (ECCC)**

5. ANNEX 1: LIST OF PARTICIPANTS TO THE WORKSHOP ON <DATE>

Surname	***Name***	***Company / Institute / University***
Amina	Boubendir	Airbus DS
Roberto	Cascella	ECSO
Marinos	Charalambides	SNS JU Office
Sergio	Cozzolino	TIM
Emmanuel	Dotaro	Thales (editor)
Erzsebet	Fitori	SNS JU Office
Pavlos	Fournogerakis	SNS JU Office
Joaquin	Garcia-Affaro	IMT
Artur	Hecker	Huawei MRC
Alexandros	Kaloxylos	6G-IA
Achilleas	Kemos	DG CNECT E1
Nicolas	Loriot	Airbus DS
Liyanage	Madhusanka	UCD
Samuel	Marechal	VTT
Michael	Montag	Nokia
Odysseas	Pyrovolakis	SNS JU Office
Cristina	Regueiro	Tecnalia
Bengt	Sahlin	Ericsson
Shuaib	Siddiqui	I2cat
Antonio	Skarmeta	Universidad de Murcia
Michela	Svelmio Moreolo	CTTC
Dimitris	Syridis	NKUA

6G-IA is the voice of European Industry and Reseach for Next Generation Networks and Services