Brussels, 12 May 2023

COST 078/23

DECISION

Subject: Memorandum of Understanding for the implementation of the COST Action “Physical layer security for trustworthy and resilient 6G systems” (6G-PHYSEC) CA22168

The COST Member Countries will find attached the Memorandum of Understanding for the COST Action Physical layer security for trustworthy and resilient 6G systems approved by the Committee of Senior Officials through written procedure on 12 May 2023.

MEMORANDUM OF UNDERSTANDING

For the implementation of a COST Action designated as

COST Action CA22168
PHYSICAL LAYER SECURITY FOR TRUSTWORTHY AND RESILIENT 6G SYSTEMS (6G-PHYSEC)

The COST Members through the present Memorandum of Understanding (MoU) wish to undertake joint activities of mutual interest and declare their common intention to participate in the COST Action, referred to above and described in the Technical Annex of this MoU.

The Action will be carried out in accordance with the set of COST Implementation Rules approved by the Committee of Senior Officials (CSO), or any document amending or replacing them.

The main aim and objective of the Action is to address key security challenges in future generations of wireless and cyber-physical systems by proposing novel, context-aware, intelligent, sustainable, and adaptive security controls at all layers, with a particular focus on the physical layer (PHY), thus enabling trustworthiness and resilience in 6G systems. This will be achieved through the specific objectives detailed in the Technical Annex.

The present MoU enters into force on the date of the approval of the COST Action by the CSO.

OVERVIEW

Summary
Other than simply inheriting vulnerabilities from the previous generations, 6G will face new threat vectors, including in the radio and massive Internet of things (IoT) domains. The COST Action 6G-PHYSEC will thus focus on creating a European network of academia and industry experts that helps the development of trustworthy and resilient 6G that can instill trust, secure communications and privacy by proposing novel physical layer security (PLS) solutions.

The premise of 6G-PHYSEC is that in 6G, intelligent and adaptive security controls are needed at all layers, with adaptation enabled by the distillation of semantics and context. The focus of this Action is on exploiting the characteristics of physical phenomena to provide security functionalities; PLS can complement upper-layer security schemes to strengthen the overall system security and enhance trust. The Action will study the characteristics of different physical environments and hardware properties to develop efficient methods to authenticate users and devices and to provide key-based or keyless confidentiality schemes. This Action will also investigate the interplay between PLS and advances in artificial intelligence, joint communication and sensing, semantic communications and context awareness.

To enhance the trustworthiness of 6G, starting from the physical and hardware layers, 6G-PHYSEC forms a large network of internationally renowned experts in wireless communications and security, from both academia and industry. The Action has also involved researchers across the whole of Europe and has included distinguished international partners with established expertise. The Action promotes inclusiveness by welcoming the participation of young researchers and female researchers in particular.

Areas of Expertise Relevant for the Action	**Keywords**
● Electrical engineering, electronic engineering, Information engineering: Signal processing, 1-D and multidimensional signal processing, compression, signal acquisition ● Electrical engineering, electronic engineering, Information engineering: Communications engineering and systems (select for additional explanation) ● Computer and Information Sciences: Cryptology, security, privacy	● Trustworthiness ● 6G ● Physical Layer Security ● Resilience

Specific Objectives
To achieve the main objective described in this MoU, the following specific objectives shall be accomplished:

Research Coordination
● Primarily serve as a pan-European network for the research on PLS for 6G systems utilizing the diverse expertise of all technology-related participants in both academia and industry.
● Develop a common understanding on the challenges and opportunities of 6G systems, with the focus on both vulnerabilities and solutions, taking advantages of PHY properties.
● Lead the research on PLS internationally, taking into account key performance indicators, cross- layer considerations, implementation constraints, and emerging technologies such as JC&S, native-AI, and ML, to establish it as a viable addition to 6G security protocols.
● Enable collaborative research on the topics of interest between different groups across the COST Member countries and international partners, thus avoiding fragmentation of research and sharing research results and equipment to strengthen collaboration.
● Build strong links between academia and industry not only at the European level but also at the

international level, to develop trustworthy 6G systems.
● Coordinate the knowledge dissemination and knowledge transfer and contribute to creating a roadmap for EU and beyond on 6G security.
● Interface with the European Telecommunications Standardization Institute (ETSI), the International Telecommunications Union (ITU), and the Institute of Electrical and Electronics Engineers (IEEE) to impact 6G pre-standardization that is expected to start within the lifetime of the project.
● Collaborate with industry to standardize the security framework and associated protocols/ algorithms for 6G networks, through participation in the Global System for Mobile Communications Association (GSMA) and the third-generation partnership project (3GPP).

Capacity Building
● Promote EU as a global leader in providing safe, secure, and reliable telecommunications services.
● Foster collaborative and interdisciplinary research considering different aspects of security together with system requirements and real-world applications.
● Support and train young researchers to address security issues, both theoretically and experimentally.
● Share available resources and results, develop better understanding on the feasibility of PLS in 6G, considering both positive and negative results, and a realistic point of view.
● Support and enable the collaboration between academia and European companies to address the challenges in developing and deploying new security schemes.
● Promote the inclusiveness of the action by inviting new participants, accounting for gender balance, attract more participation of COST Near Neighbours and Inclusiveness Target Countries (ITC), international partners as well as companies.
● Provide a platform on which PLS and cryptographers / higher layer security experts can meet over the course of the Action, closing the gap between what was considered disparate research areas.

TECHNICAL ANNEX

1. S&T EXCELLENCE

1.1. SOUNDNESS OF THE CHALLENGE

1.1.1. DESCRIPTION OF THE STATE OF THE ART

Motivation

Unarguably, the security protocols of fifth generation (5G) systems are a significant improvement with respect to the long-term evolution (LTE) systems, resolving many, albeit not all, open issues. In particular, securing wireless links under overly aggressive latency constraints, scaling authentication, and key distribution to massive numbers of users (e.g., to accommodate massive Internet of things (IoT)) while providing resistance to quantum attacks for constrained devices, remain open issues (despite recent standardization of four post-quantum cryptographic algorithms from NIST). At the same time, sixth generation (6G) networks will interconnect intelligent and autonomous cyber-physical systems, including robots and vehicles. In the emerging "fusion" of digital and physical worlds, existing authentication and access control schemes are not enough to build trust and evaluate the trustworthiness of autonomous systems; for example, recent works have shown that positioning information is essential in building trust, e.g., Sybil attacks have been identified by using angle of arrival information in robotic systems [1]. Furthermore, as 6G will open up new THz bands and exploit joint communication and sensing (JC&S) approaches, new opportunities and challenges lie ahead. Opportunities for not only providing higher data rates but also higher accuracy in sensing and localization; for enhancing trust and securing wireless links with pencil sharp beamforming; for robust secret key generation and authentication leveraging the physical layer (PHY) as well as the hardware. Challenges arise to secure sensing itself and make the PHY resilient to denial of service and man-in-the-middle attacks.

The Action 6G-PHYSEC aims at building on the opportunities stated above to address some of the key security challenges in future generations of wireless and cyber-physical systems by proposing novel, context-aware, intelligent, and adaptive security controls at all layers, with a particular focus on the PHY, which currently is largely missing. Since the problem is highly complex and involves many layers, the Action brings together experts from many diverse fields that, up to now, had limited possibilities to work together. This comprehensive network of wireless security experts will propel the incorporation of physical layer security (PLS) schemes in 6G security protocols. Exploiting the characteristics of physical phenomena to provide security, PLS can complement conventional upper-layer security schemes to strengthen overall trust and resilience of 6G. 6G-PHYSEC will study such possibilities in different physical environments ranging from sub-GHz to THz frequency bands and the potential use of intelligent reflective surfaces (IRSs), JC&S, high precision localization and radio frequency (RF) fingerprinting to enhance trust. Furthermore, the Action will propose lightweight and fast authentication and key agreement (AKA) mechanisms, including physical unclonable functions (PUFs) and secret key generation (SKG) from shared randomness. This Action will also consider the interplay between PLS and advances in artificial intelligence (AI) and machine learning (ML) around the design of efficient coding schemes and pre-processing / channel engineering. Furthermore, as 6G will be the first AI native generation, 6G-PHYSEC is interested in the role of semantics and context-awareness in the deployment of PLS-based solutions. Finally, this COST Action will formalize how medium complexity McEliece

cryptosystems can enhance the palette of quantum-resistant solutions, with a focus on constrained devices, for which the currently approved NIST post quantum cryptographic algorithms are still difficult to deploy.

State of the art

5G security enhancements present a significant improvement with respect to LTE, with the use of public key infrastructure (PKI) based protocols for AKA (5G-AKA, EAP-AKA, and EAP-TLS) message integrity checks, etc. However, as the complexity of the application scenarios increases with the introduction of ultra-reliable low latency communications (URLLC), massive machine-type communications (mMTC) and more generally IoT related verticals, novel security challenges arise that might be difficult to address using the standard paradigm of complexity-based classic cryptographic protocols. Future-proof security systems will rely on quantum-resistant schemes. However, the recently standardized post-quantum cryptographic algorithms are still relatively complex and there is a clear need for novel quantum-resistant solutions oriented to low-end IoT devices [2-3] as well as for adaptive cryptographic algorithms and protocols that dynamically adjust their configuration and parameters according to inputs from several layers and more generally from semantics and contexts [4].

In addition, 6G systems will operate under hugely diverse constraints. Operating under aggressive latency constraints, in massive connectivity regimes, with low energy footprint and low computational effort, while providing explicit security guarantees, can be challenging. Quite importantly, the massive scale deployment of low-end IoT nodes, often manufactured with non-homogeneous production processes poses pressing questions on the long-term IoT security. In addition, the extensive introduction of AI and ML and the rapid advances in quantum computing will further increase the attack surface of 6G systems and demand quantum-resistant solutions and ML mechanisms that are adversary-resistant and explainable.

Looking ahead, to provide scalable solutions for massive IoT and networks of cyber-physical systems, quality of security (QoSec) is expected to provide a flexible security framework for future networks, introducing different security levels and moving away from static security controls, captured currently in zero-trust security architectures. In parallel, the integration of communications and sensing, along with embedded and edge AI, provides the foundations for autonomous and adaptive security controls.

In this framework, it is envisioned that PLS solutions, which exploit the characteristics of physical phenomena to provide security, can complement conventional upper-layer security schemes and strengthen the overall trust and resilience of 6G [4,5]. PLS can be used to provide keyless and innately secure communications as well as to generate and distribute keys for symmetric encryption [6], by exploiting the propagation characteristics of the wireless channel at the PHY. This strategy is particularly useful for latency-constrained communications and resource-constrained radios. This is usually the case for high device densities under opportunistic self-organizing network formation paradigms or upcoming autonomously communicating device-to-device (D2D) nodes. Opportunistic self-organizing networks as well as autonomous D2D communications are two example scenarios where the traditional security mechanisms cannot be easily applied. In addition, authentication at PHY can be introduced to enable a quick and potentially continuous verification of legitimate user without upper layer processing, which is particularly beneficial for the heterogeneous environments of 6G networks. Therefore, PLS is expected to be incorporated in 6G security protocols, thus introducing security controls at all layers, for the first time.

1.1.2. DESCRIPTION OF THE CHALLENGE (MAIN AIM)

PLS mechanisms can be generally classified as keyless and key-based. In the former, which is commonly referred to as wiretap coding, code design and channel properties are exploited to provide secrecy [7,8]. On the other hand, the latter generates secret keys from wireless channels. As mentioned above, the physical properties can also be utilized to provide authentication. For instance, PUF method authenticates devices using the unique properties of the integrated circuits, whereas in RF fingerprinting the imperfections of analog front-ends in both the transceivers and the communication link are exploited

to provide authentication. The exciting prospect of incorporating PLS in 6G security protocols brings also challenges. Despite intense research interest on PLS for more than two decades, its use in actual security products remains elusive, with a few exceptions in terms of RF fingerprinting and multi-factor authentication. The use of wiretap coding, SKG from shared randomness (from the channel state information (CSI)), authentication using PUF and positioning / RF fingerprinting, are among the most prominent PLS solutions under consideration at the moment. All of these have been widely studied in the literature, but one has seen only a few practical implementations. There is, however, a new emerging reality ahead.

6G will introduce several changes, which may render PLS feasible, namely:

Channel engineering and channel controllability are key elements in 6G, enhancing the first steps taken in 5G with the introduction of millimeter waves (mmWaves). Channel engineering and controllability are under study, especially in the form of pencil sharp beamforming in ultra-massive Multiple Input Multiple Output (MIMO) systems at mmWaves and THz bands, allowing to make the case for wiretap channels, without relying on assumptions regarding the position or number of antennas of passive attackers. In this direction, secrecy maps and related concepts can be of great interest. Another related recent advancement concerns the use of IRS, drones, and multi-hop wireless networks to improve the received signal quality, so that explicit security guarantees can be provided in different scenarios.

The introduction of sensing in 6G will provide contextual information (including ranging capabilities) e.g., to identify when wiretap coding is applicable. Sensing capabilities will allow us to better assess the propagation environment to provide adaptive PLS solutions. Closely related to the latter is the concept of semantics and context enabled PLS in which PLS may further benefit by context awareness. Furthermore, the meaning / importance of exchanged messages is also of interest as it allows us to assess the value of information and make decisions regarding the required security level.

A full palette of countermeasures to address both passive (eavesdropping) and active attacks (man-in-the-middle, jamming) against PLS systems have recently been proposed. At the same time, the understanding of preprocessing techniques for the isolation of entropy-rich reciprocal components of the observed CSI can allow efficient implementation of SKG.

The analysis of the finite block-length for secrecy and reconciliation encoders, which allowed us to obtain a clear understanding of the trade-off between codelength, error packet rate and information leakage [9].

The fact that in 6G positioning is a default service. As a result, positioning integrity is of paramount importance and angle of arrival (AoA) in conjunction to ranging, camera depth estimations, etc., are studied to render positioning unforgeable. Several protocols have already been proposed that incorporate positioning information as a second soft authentication factor, while Sybil cyberattacks in robotic systems have been identified using AoA. Overall, positioning will be an important parameter for evaluating the trustworthiness of autonomous agents in 6G.

Advances in the understanding of PUFs and biometrics, analyses regarding strong and weak PUFs, the proposal of Wyner Ziv encoders for reconciliation, etc. There are currently numerous commercial products based on PUFs and a systematic study of the corresponding fuzzy extractors used is timely.

At the same time, new challenges emerge.

The challenges posed by emerging technologies: Fostered by advances in RF-sensing and channel controllability, sensing capabilities as an integral part of the network have been identified as a novel feature of future 6G networks. However, such integrated sensing and communication scenarios might induce serious privacy risks [10] and have been shown to be prone to active attacks. For instance, using RF sensing, an eavesdropper can track occupancy in a home, and other daily activities, an adversary can also redirect a portion of the sensitive communications by using a metasurface interacting with transmitter and receiver. To provide trustworthiness, one should therefore design positioning and sensing techniques robust to different attacks, a topic that is only now attracting attention [11]. In

addition, the expected intensive deployment of AI in 6G systems will increase the sophisticated intelligent attacks and needs to be investigated thoroughly.

The challenges posed by system requirements: Two of the envisioned pillars for 6G are "energy sustainable communications" and "security, privacy, and trustworthiness" [12]. In more detail, the broad objective of energy-sustainable communications includes the objectives of pJ/bit energy efficiency and the support of zero-energy device networks, among others. However, combining the pillars of energy sustainability and security is particularly challenging. When users are further constrained to use short packets due to the underlying traffic model as in D2D communications or latency requirements, meeting the stringent requirements on reliability and security becomes even more challenging; as an example, standard message authentication codes (MACs) have been shown not to meet data plane latency targets for URLLC [13]; thus, the need for fast integrity checks emerges. Furthermore, the deployment of massive IoT devices with diverse control and hardware will pose significant security and privacy risks to 6G.

Accounting for the above points, with the vision of enabling trustworthiness and resilience in 6G systems, the 6G-PHYSEC COST Action's **technical objectives,** around which the partners will collaborate in the Action, are the following:

- **OBJ1**: Provide trustworthiness to 6G systems, including explainable AI, security and privacy by design, semantic use of PHY attributes (e.g., positioning, fingerprinting and sensing), to infer cyberattacks and anomalies and measure trust.
- **OBJ2**: Make 6G systems resilient and explore several aspects ranging from position integrity to stealth waveform design, to the use of AI and context-awareness for adaptive security.
- **OBJ3**: Guarantee quantum-resistant solutions, make them suitable for constrained devices, looking at PLS and medium complexity code-based post quantum cryptography.
- **OBJ4**: Provide sustainable and scalable PLS security solutions for low energy and low footprint future networks.

The methodologies to obtain those objectives are presented in the following sections, along with the added value of interactions stemming from the collaboration between partners of the 6G-PHYSEC COST Action.

1.2. PROGRESS BEYOND THE STATE-OF-THE-ART

1.2.1. APPROACH TO THE CHALLENGE AND PROGRESS BEYOND THE STATE OF THE ART

As mentioned above, 6G networks will require the transmission and storage of big data volumes in secure and sustainable fashion. Consequently, development of post-quantum and post-Shannon techniques came recently into the research focus. In addition, future solutions should be efficient in terms of energy and computational resources. Therefore, the main goal of this collaborative action is to accelerate, through the proposed networking, dissemination and training activities, the development of adaptive techniques with information-theoretic security, in which different approaches will be combined, evaluated, and adapted to different applications with diverse requirements. This Action will investigate the main characteristics of future technologies and their interaction with the Action's objectives.

Hardware / channel modelling and spectrum technologies (**OBJ1**, **OBJ2**, **OBJ3**): 6G-PHYSEC will investigate channel and devices characteristics from sub-GHz to THz [14] and their security implications. Specifically, since 6G networks can operate in the THz bands, the need for high-gain directional antennas simultaneously at the transmitter and receiver makes THz frequencies difficult to intercept. To successfully intercept a THz signal, the eavesdropper must be within a very narrow beam coming from the transmitter. Beam discovery and tracking needed for a successful interception are challenging, especially since the transmitter does not cooperate with the eavesdropper.

Emerging technologies in sensing and channel control (**OBJ1**, **OBJ2**, **OBJ3**): It is also worth noticing that the availability of diversified and interacting relays in 6G networks, paves the way for new

PLS solutions, where the adaptability and flexibility of relay configuration under the control of the operator are put at the service of security. Indeed, the possibility to control the electromagnetic environment can be used to focus signals on certain positions (thus obtaining confidentiality by geofencing). Another security solution provides the use of IRS to alter the propagation channel in a controllable way that enables to check its consistency with the expected position of the transmitter, for authentication purposes. In general, the control of metasurfaces (including the control of their position when they are mobile) creates a controllable channel that can be exploited for security purposes. Existing PLS solutions do not take into account these features and suitable protocols and algorithms should be developed, together with a study on their performance. Similar observations hold for new meta-structures integrated with antennas, where the interaction between protocols and digital signal processing and an adaptive analog domain is to be explored and exploited for security purposes. Another emerging technology for 6G networks is the integration of communications and sensing or JC&S, which will bring the advantages of integrating radar/radio sensing and wireless communications into one physical system: higher spectral efficiency, and joint design and optimization of waveform, system, and network. JC&S has then the potential of perceiving the environment beyond localization and sensing, enabling the system to understand the environment, and creating perceptive mobile networks. At the same time, sensing human beings and the physical world brings serious concerns about privacy, as the radio channel is broadcast in nature. Therefore, it is essential that the transmissions employed for positioning and RF sensing are robust against attacks, guarantee privacy and provide trustworthy RF sensing. The design of PLS strategies for JC&S systems and advanced AI-based beamforming techniques will pave the path towards secure sensing.

Sustainable technologies (**OBJ3**, **OBJ4**): Energy efficient PLS mechanisms will also be addressed, which are compatible with the extreme requirements of energy-sustainable communications. To this end, the concept of providing PLS in a proactive way will be explored, while requiring minimum feedback by the energy constrained devices. More specifically, optimized PHY protocols will be developed, while the capabilities of smart radio environments will be explored, e.g., by using passive IRS to offer covert communication. The main characteristics of the developed protocols will be scalability and adaptiveness, to fit a wide range of scenarios and applications. To this end, tools from stochastic-geometry and stochastic optimization will be used. Also, ML is a useful tool to facilitate both model-free and model-based optimization and provision of PLS, considering user particularities. In addition, lightwave technology will be explored to meet the requirements of zero-energy devices.

Application of AI and ML, semantics, and context awareness (**OBJ1**, **OBJ2**, **OBJ3**, **OBJ4**): As mentioned above, to address the security challenges in 6G, a cross-layer, comprehensive solution involving different technologies is essential. To this end, the Action resorts to AI-based technologies to:

(i) correlate network events from all network parts (including radio access), to substantially improve the analysis and detection of anomalous traffic; (ii) mitigate harmful cyber-attacks and establishing trustworthiness by emphasising AI-explainability and exploiting the location information; and (iii) improve situational awareness, specifically targeting early anomaly detection. In the studies, this Action will take concrete steps to address privacy issues. 6G-PHYSEC will look at both privacy in localization and solutions based on local (on device) processing, e.g., using federated learning. To capture and analyse network events from the PHY to the application layer, advanced AI/ML techniques will be used to detect anomalies, reduce the number of false positives, and improve the detection of unknown attacks. The developed techniques will correlate events of the different layers with information from the physical infrastructure (notably, nodes' localisation), to detect and categorize ongoing attacks.

Clearly, the above key areas of research overlap as seen from their description; this fact will enable building bridges between academic partners focusing on distinct aspects of securing 6G. It will also facilitate the knowledge transfer to the industrial partners, looking at multiple potential benefits of some of the key technologies, and the same is true for impact on standardization activities.

1.2.2. OBJECTIVES

1.2.2.1. Research Coordination Objectives

Since 6G moves towards THz bands and is expected to incorporate network scalability, an exponentially growing number of heterogeneous devices, and advanced technologies such as AI and joint communication and sensing, security should be considered from different perspectives and under new constraints. In fact, the development of security protocols will not be standalone but requires the interaction with all other layers, e.g., for the distillation of semantics and context, and technologies, (including AI and JC&S). Thus, the design of the security will be coordinated with other research activities involving different layers. This will enable the Action to develop a new security framework which takes different points of view into account. For that, the network will form theoretical and experimental groups to enable a suitable helicoidal development process, using feedback (back and forth process). For instance, the analysis of fundamental limits, protocols, and algorithms will be built so that the latter can test the feasibility of the former, validate the performance of the security schemes considering realistic environments, and give feedback to the theoretical groups. As a consequence, the experimental results will enhance the understanding of real-world problems and enable the theoretical group to develop more realistic techniques and methodologies. More importantly, 6G-PHYSEC has involved many SMEs and large companies so that the Action can provide a “from idea-to-product" cycle. This research coordination also allows ease of knowledge transfer and makes the research more practical relevance.

The specific research coordination objectives are thus:

- Primarily serve as a pan-European network for the research on PLS for 6G systems utilizing the diverse expertise of all technology-related participants in both academia and industry.
- Develop a common understanding on the challenges and opportunities of 6G systems, with the focus on both vulnerabilities and solutions, taking advantages of PHY properties.
- Lead the research on PLS internationally, taking into account key performance indicators, cross-layer considerations, implementation constraints, and emerging technologies such as JC&S, native-AI, and ML, to establish it as a viable addition to 6G security protocols.
- Enable collaborative research on the topics of interest between different groups across the COST Member countries and international partners, thus avoiding fragmentation of research and sharing research results and equipment to strengthen collaboration.
- Build strong links between academia and industry not only at the European level but also at the international level, to develop trustworthy 6G systems.
- Coordinate the knowledge dissemination and knowledge transfer and contribute to creating a roadmap for EU and beyond on 6G security.
- Interface with the European Telecommunications Standardization Institute (ETSI), the International Telecommunications Union (ITU), and the Institute of Electrical and Electronics Engineers (IEEE) to impact 6G pre-standardization that is expected to start within the lifetime of the project.
- Collaborate with industry to standardize the security framework and associated protocols/ algorithms for 6G networks, through participation in the Global System for Mobile Communications Association (GSMA) and the third-generation partnership project (3GPP).

1.2.2.2. Capacity-building Objectives

The Action involves universities, research institutions, SMEs, and large companies to the joint effort of promoting trust and trustworthiness of 6G, exploiting PLS as a vital technology to this end. This diverse and inclusive network will strengthen the Action’s research and development of a suitable security framework, building on the established expertise of the partners. The specific capacity-building objectives are thus:

- Promote EU as a global leader in providing safe, secure, and reliable telecommunications services.
- Foster collaborative and interdisciplinary research considering different aspects of security together with system requirements and real-world applications.

- Support and train young researchers to address security issues, both theoretically and experimentally.
- Share available resources and results, develop better understanding on the feasibility of PLS in 6G, considering both positive and negative results, and a realistic point of view.
- Support and enable the collaboration between academia and European companies to address the challenges in developing and deploying new security schemes.
- Promote the inclusiveness of the action by inviting new participants, accounting for gender balance, attract more participation of COST Near Neighbours and Inclusiveness Target Countries (ITC), international partners as well as companies.
- Provide a platform on which PLS and cryptographers / higher layer security experts can meet over the course of the Action, closing the gap between what was considered disparate research areas.

2. NETWORKING EXCELLENCE

2.1. ADDED VALUE OF NETWORKING IN S&T EXCELLENCE

2.1.1. ADDED VALUE IN RELATION TO EXISTING EFFORTS AT EUROPEAN AND/OR INTERNATIONAL LEVEL

There are projects on specific topics of PLS at national level of some EU countries but not pan-European or extra-EU initiatives. Projects on specific topics are, for instance,: the project PLAY SCATE (2018-2021, DFG, DE) aimed at understanding the fundamental properties of compound wiretap channels and arbitrarily varying wiretap channels with active eavesdroppers; the project SWING2 (2016- 2019, FCT, PT) studied the development and optimization of practical coding for secrecy schemes; the recently awarded American project RINGS Just-in-Time Security (2022-2025, NSF, US) which investigates the combination of hardware and software to provide hardware-based physical layer security solution; the project PHYLAWS (2012-2016, EU) involved five partners to design and prove new privacy concept for wireless communication exploiting radio channels. Recently, an IEEE Focus Group of mostly academics was put together in September 2021 as part of the IEEE Future Networks Initiative to provide an international forum on PLS. While these projects and initiatives established the fundamentals of PLS, there is still a gap in accepting this breakthrough concept between academics and industry, in the performance between theoretical studies and experiments [15]. Furthermore, extensive studies on its impact on existing services and new applications such as JC&S are needed in the context of 6G networks [16].

2.2. ADDED VALUE OF NETWORKING IN IMPACT

2.2.1. SECURING THE CRITICAL MASS, EXPERTISE AND GEOGRAPHICAL BALANCE WITHIN THE COST MEMBERS AND BEYOND

6G-PHYSEC already involves both industrial and academic partners with extensive experience in wireless communications and security. The initial network partners were selected from strong research groups/ institutions in wireless communications and security in both the physical and upper layers. Major companies and SMEs with expertise in the fields also participate, in addition to leading international partners. The initial consortium proposing this Action has already a critical mass and excellent expertise. Still, 6G-PHYSEC plans to involve more stakeholders into the Action. Additionally, this Action plans to collaborate with other COST Actions and projects on related topics to enable collaborative research and discussion beyond the Action. For instance, the following COST Actions are of interest to 6G-PHYSEC: INTERACT, NEWFOCUS, SyMat. Furthermore, this Action can interface with the 6G flagship project HEXA-X through the 6G-PHYSEC partners.

By involving partners from the COST Member states and beyond the Action aims to impact the research and development of new security concepts for 6G at a global level.

2.2.2. INVOLVEMENT OF STAKEHOLDERS

Breakthroughs and advances in wireless communications in science and technology are usually developed at universities and research institutions. After being tested and validated, they will be transferred to the industry, whose process relates to hardware/software providers, SMEs and large companies, standardization bodies, and policymakers. To guarantee the success of the Action, 6G-PHYSEC has involved many stakeholders, as described above, at the proposal stage. Thanks to the flexibility of the COST framework, new participants can join anytime during the duration of the Action, to assist/do collaborative research or provide advice and foster dissemination or standardization activities. In particular, this Action will reach out to potential stakeholders with different approaches, namely:

- **Researchers** / **scientists** / **students**: The Action will expand the networks by reaching out to peers, which is not limited to European ones, at conferences/workshops on the topics of interest. For example, the Action can hold workshops and special sessions at the well-known conferences such as IEEE GLOBECOM and IEEE ICC, to advertise the research and network. The selection will be based on the expertise and the diversity. Exploiting a network of institutional research centres and universities, this COST Action can also disseminate knowledge to their students and train young researchers at Training Schools.
- **Companies**: The Action already has several SMEs and big companies and plans to include more vendors, operators, as well as SMEs and large companies specializing in wireless communications and security, to maximize impact of the action on the industry. This Action will interact with companies at exhibitions and invite them. Note that 6G-PHYSEC has many partners with strong links to the industry which will benefit those activities. The Action also enables faster knowledge transfer so that companies including start-ups can benefit from the Action's research outcomes.
- **Professional organizations and standardization bodies**: The focus of the network is indeed on research for wireless communication and security; thus this COST Action will attract attention from professional organizations such as ACM and IEEE. Members of the initial group are also participating in standardization bodies such as ITU, ETSI, and 3GPP, thus they will help to reach out those stakeholders, including the European Union Agency for Cybersecurity (ENISA). The participation in those bodies will also attract more industrial partners and therefore expands the network.
- **Policymakers**: 6G-PHYSEC will invite representatives of national research funding agencies to attend outreach activities. The network also actively approaches participants in seminars/workshops on relevant topics at both national and international level to promote the discussion between the network and policymakers concerning privacy, trust, and security of 6G systems. More importantly, the Action will promote the inclusiveness of the research, favour the participation of ITC countries, ensure gender balance and attract young researchers, as promoted by COST.

3. IMPACT

3.1. IMPACT TO SCIENCE, SOCIETY AND COMPETITIVENESS, AND POTENTIAL FOR INNOVATION/BREAK-THROUGHS

3.1.1. SCIENTIFIC, TECHNOLOGICAL, AND/OR SOCIOECONOMIC IMPACTS (INCLUDING POTENTIAL INNOVATIONS AND/OR BREAKTHROUGHS)

In many white papers, (e.g., see the 6G research visions from 6G Flagship [17]), 6G systems are expected to introduce new technologies such as JC&S, IRS, AI and ML, and signal processing solutions at THz bands, to accommodate multiple constraints such as massive connectivity, high data rate, ultra-low latency, and low power consumption. Future networks also open new applications such as high-accuracy positioning and tracking, context-aware-based services, augmented/virtual reality, with a huge potential in healthcare and education, to name a few. Considering the existing level of advanced hacking methods, lack of trust, privacy, and security on current wireless systems and the Internet, building a trustworthy 6G is thus demanding. The unprecedented information collected from the physical world (e.g., IoT, eHealth, and body area networks) in 6G systems can be leaked and exploited unexpectedly,

with detrimental effects on both individuals and businesses. The Action thus aims at providing efficient solutions to those concerns.

Ultimately, 6G-PHYSEC contributes to building **trustworthy and resilient 6G**. Utilizing PLS, the most critical and vulnerable segments of the networks (e.g., physical devices such as IoT and sensors) will be secured. By taking advantage of the environment and devices characteristics to provide an extra level of security, this approach provides a lightweight and energy-efficient solution in comparison with traditional cryptography, which instead relies on complex mathematical computations. By bringing together all relevant parties working on different layers, from academia to industry, the Action strengthens the understanding and enables collaboration to develop breakthrough feasible solutions to address the security concerns. Thus, the Action will provide a set of potentially exploitable assets: (i) a reference architecture, designed to enable the project vision considering the inputs from the industries participating in the use cases; (ii) a set of sensing capabilities, operating at multiple network layers, including ground-breaking physical layer sensing, suitable for different telemetry purposes; (iii) a framework for the combination of sensor input and the distillation of context; (iv) a number of adaptive security controls, operating key management, cryptography parameters and network parameterization, and (v) tools for context-aware and semantics aware security.

Considering the dependence of the economy on wireless communications, which will deepen with 6G, this COST Action helps to secure the systems to provide a **sustainable development**. The interaction between physical and digital worlds via sensors and emerging technologies such as JC&S will be secured and trusted. In addition, privacy is perceived at different levels from vendors to countries and thus needs a coordinated action to involve all the stakeholders in discussion to provide a unified framework. By involving and participating in standardization bodies, 6G-PHYSEC also provides a worldwide solution and seamless and safe connections for end-users and the whole society. The impact from a business standpoint could translate into: (i) reducing costs and facilitating the inception, development, deployment and exploitation of future services, by addressing security-related considerations; (ii) reducing the complexity and costs of the security aspects of the network operation, improving the scalability of the network and (iii) facilitating the integration of new security related tools in the network enabling selective activation.

The 6G-PHYSEC COST Action also impacts **the societal, ethical, environmental, legal outcomes**. The automation of security measures poses ethical and legal questions. The fact that an algorithm or a set of AI rules, can determine the downgrade of the security level, and consequently a service becomes vulnerable, necessarily brings up the debate on the ultimate responsibility. The way which the trade-off between efficiency versus security is transferred into contractual terms is also subject to legal discussion. This Action will hopefully result in more efficient systems, less resource and power demanding, hence having a positive environmental impact.

The Action will also **bridge different stakeholders** in the society. Since this COST Action will work on enabling technologies for the trustworthiness of future networks, the Action will connect both academic and industrial partners to provide practical solutions. In addition, this Action will train young researchers being capable of developing security solutions and knowledgeable in both theory and applications. More importantly, this Action's solutions will benefit society at large by enabling trust, security, and privacy for next-generation networks.

3.2. MEASURES TO MAXIMISE IMPACT

3.2.1. KNOWLEDGE CREATION, TRANSFER OF KNOWLEDGE AND CAREER DEVELOPMENT

The COST Action involves both academic and industrial partners in wireless communications and security and is geographically diverse; it will thus strengthen this Action's research and create new technologies through collaborative work. 6G-PHYSEC will have annual meetings at both Working Group and management levels, to discuss emerging technologies and open issues. In addition, the Action will hold several workshops, seminars, and tutorials every year to share results and foster new research activities. This Action will also share the available labs and equipment, to the benefit of all participants.

Furthermore, more participants will be invited to fill the gap in expertise in other perspectives, thanks to the flexibility and openness of the framework.

In addition to knowledge creation, this Action will favour the transfer of knowledge, both within the network of institutions and partners and outside it. The members can access the shared resources and up-to-date results. Industry will benefit from the research and enable technologies for trustworthy 6G networks through conferences, workshops, seminars, and exhibitions. The participants of the Action will also investigate specific topics jointly with industrial partners or exchange researchers for scientific missions. The Action's knowledge transfer thus shortens the process from fundamental research to real product and helps to make the standardization process faster. Other stakeholders such as young researchers, other institutions will attend the Action's trainings, seminars, and workshops, and get access to published reports, white papers, and deliverables to enhance their knowledge.

Young researchers in particular will be empowered through different activities of the action. They will be invited to attend Working Groups' meetings and Training Schools focusing on fundamentals of PLS and cryptography, the interplay between PLS with other technologies such as JC&S, AI, and ML, the utilization of AI/ML and/or other emerging technologies such as AI, IRS to provide security. Participants can also apply for Short-Term Scientific Missions to carry out their research at other institutions and partners to learn about new technologies and interact with other groups directly, or simply make use of the available lab/equipment/devices. They can also get funded to present their work at workshops and conferences. Those activities will help to create a new generation of engineers with specific competences on PLS.

3.2.2. PLAN FOR DISSEMINATION AND/OR EXPLOITATION AND DIALOGUE WITH THE GENERAL PUBLIC OR POLICY

In addition to research and development of trustworthy 6G networks, 6G-PHYSEC believes that dissemination is a key action to increase awareness and support all relevant stakeholders in the society. More specifically, the Action plans the following dissemination activities:

- Create and maintain the Action website to provide a portal for not only participants but also interested people on the topics of security for 6G.
- Organize Training Schools, special workshops / tutorials on the topics relevant to the Action such as PLS, AI, and ML on top conferences such as IEEE ICC and IEEE GLOBECOM.
- Publish white papers on PLS and emerging technologies.
- Share reports after the annual meetings.
- Publish a newsletter every quarter to update the progress or new challenges in securing 6G systems.
- Maintain an active presence on social media such as LinkedIn, Twitter, and YouTube and post up-to-date interviews, podcasts, panels and / or demonstrations on PLS.
- Interact with other COST actions and projects such as INTERACT (CA20120), HEXA-X to organize joint seminars, workshops, or talks.

6G-PHYSEC's dissemination activities provide opportunities not only for the COST Action participants but also potential partners to exploit the resources, outcomes, or results. The initiatives for exploitation can be summarized as follows:

- Involve partners to propose European projects.
- Collaborate with other researchers in the network to work on the topics of interest.
- Share the available facilities and equipment, simulations, and results.
- Choose novel research / ideas to develop a possible business plan for a future COST innovators grant.
- Work with industry partners on developing hardware and software solutions for 6G security.
- Form a special group being responsible for submitting recommendations on adding PLS to 6G wireless security to standardization bodies.

Indeed, the advances in technologies need approval and acceptance from the general public and policymakers to make them feasible in practice. Therefore, the Action plans to communicate with the public, regulators, and policymakers in a regular manner to inform them about the progress and more importantly make them part of the development of the security concepts for 6G utilizing PLS. In addition to the dissemination activities mentioned above, this Action will also carry other activities to those target groups as follows:

- Provide public lectures / talks, open day and talks at schools.
- Dedicate a section on the website to explain the research to laypersons using less-technical terms and knowledge.
- Invite policymakers to regular meetings, demonstrations, exhibitions.
- Participate actively in seminars/workshops on 6G and 6G security held by relevant governmental agencies.
- Produce and participate in the writing of position papers promoting PLS for 6G systems.

To detail those activities, the Action classifies the relevant stakeholders into different target groups and identifies the corresponding activities and associated key performance indicators (KPIs) as presented in the following tables.

*Table 1- Activities targeted at **creating awareness***

Target audience	Activities	KPIs
Network operators and infrastructure providers	Number of multi-stakeholder events (e.g., Hackathon)	1
Technology providers	Trade fairs and exhibitions	2
Research community and academia	Workshops, keynotes, tutorials, summer schools, and magazine publications	20
General public	Science festivals, social network posts, and videos	15

*Table 2 -Activities targeted at **raising interest on the Action's results***

Target audience	Activities	KPIs
Research Community, ICT sector, and general audience	Communication of 6G-PHYSEC's news, events and results; Validation of concepts findings and advantages; Ideas' gathering and knowledge exchange; Increased awareness	40
Industry	Number of industry communities informed about the Action	15
Standardization organizations and associations	Communication of the Action's results; Validation of concepts, findings and advantages; Increased awareness – 6G-PHYSEC's presentations in standardization meetings (online or offline)	3
Research community and Stakeholders (industry, and SMEs)	Increasing visibility to stakeholders active in social media; Attainment of interest of stakeholders; Viral marketing by "word of mouth" through the followers; Direct communication mechanism with followers	300

Table 3- Activities targeted at communication with all stakeholders

Activity	Description	Target Audience	KPI
Website	Action website encompassing general information and means to follow-up for interested visitors	Structured with different sections for general audience, technical, and business	>3000 single visitors per year
Social media	Use several social media channels	All stakeholders	Number of followers on Twitter > 300, Number of followers on LinkedIn >100
Events & conferences	Events (hybrid as well as in presence) for disseminating 6G-PHYSEC's results as well as interacting with relevant stakeholder (including the general public); if possible, co-located or attached to existing events (e.g., exhibitions from museums, scientific conferences)	Stakeholders from industry, scientific community, policy makers, general public	at least 5 events
TV, printed press / other traditional non-online media	Dissemination of the Action's results towards the part of the population which is not "Internet affine" or is rather technology sceptic	Non "Internet affine" / technology sceptic parts of the population	Material ready for generic use, and at least 2 impacts

4. IMPLEMENTATION

4.1. COHERENCE AND EFFECTIVENESS OF THE WORK PLAN

4.1.1. DESCRIPTION OF WORKING GROUPS, TASKS AND ACTIVITIES

The structure of the Action is shown in Figure 1. In particular, the Core Group consists of the Chair, Vice-chair, Working Group Leaders; the steering committee will include Grant Holder, Grant Awarding Coordinator, Training, Science Communication, and Standardization Coordinators in addition to that of the Core Group. In addition, an advisory board comprising of groups of experts will assist and advise the research groups as well as the steering committee during the Action duration. The steering committee will coordinate activities from research, training, as well as dissemination activities, so that all planned objectives are fully achieved. The training and dissemination activities and their associated KPIs have been described in the previous section and will be framed together with research in Section 4.1.2 and 4.1.4. Regarding research activities, this Action is organized in five Working Groups as follows:

WG1-Trustworthy 6G: This group will work on the trustworthiness of the 6G system. The Action further creates three subgroups to focus on three important topics: security, trust, and privacy. This Action will involve not only physical layer investigators but also cryptographers and network investigators to the joint efforts, to provide a complete security framework at all layers.

WG2-Intelligent and resilient systems: The main objective of this Working Group is to investigate methods to improve the resilience of the systems to diverse attacks in 6G networks. More importantly,

this Action will learn intensively how to utilize AI and emerging technologies such as JC&S and IRSs to enable an intelligent secure 6G.

WG3-Quantum-resistant security: This Working Group will learn and develop quantum-resistant PLS schemes and efficient lightweight solutions. In addition, this Action will also investigate the utilization of different security schemes adaptively to provide proper quantum resistance guarantees.

WG4-Scalable and sustainable security: This group will study different aspects of system design to enable scalability and sustainability in addition to security. The group aims at investigating from hardware to software design, signal processing algorithms, and protocols to provide low-cost low complexity, and energy-efficient solutions.

WG5-Experiments and demonstrations: This Working Group will bridge the theoretical group to real-world solutions. They will work back-and-forth with the latter to provide a realistic framework for the security. They will also demonstrate security concepts at conferences, workshops, and exhibitions to attract the attention from both industry and end users.

In addition, 6G-PHYSEC will also create a group of experts in standardization (S-EG) to foster the Action's standardization activities. They will also give recommendations to the standardization organizations to promote the use of PLS in 6G systems. Furthermore, the Action will form a group of experts on AI and ML (AI-EG) to assist/collaborate with all Working Groups to develop specific applications and also the overall intelligent context-aware solution to 6G security.

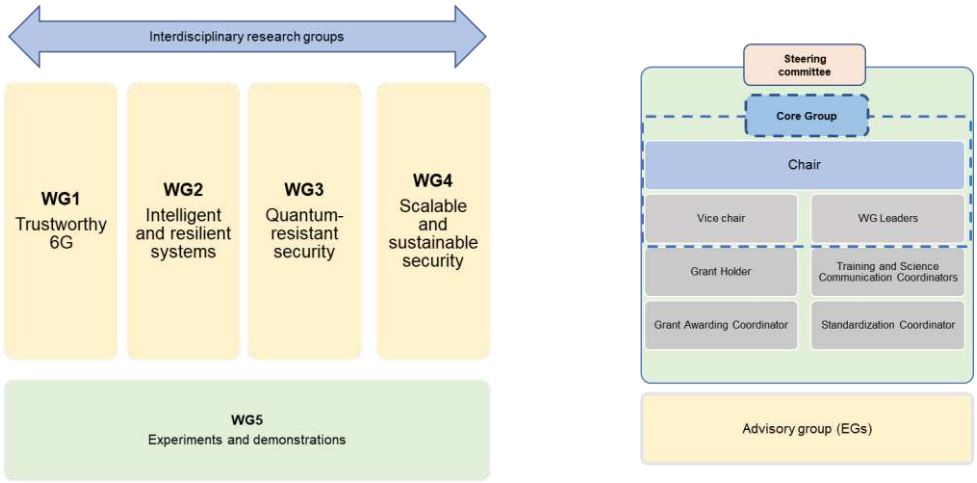

Figure 1- Organizational structure of COST Action 6G-PHYSEC

4.1.2. DESCRIPTION OF DELIVERABLES AND TIMEFRAME

As previously mentioned, each WG will carry specific tasks to complete the specified topics. In the first phase, the general task is to identify challenges and plan for theoretical / experimental activities. Generally, every group will interact with the experimental and demonstration group to evaluate the performance of the proposed approaches/protocols/algorithms in realistic scenarios following by analysis and recommendations. 6G-PHYSEC also attracts new participants/stakeholders during the duration of the Action. Furthermore, the Action will take new economical/societal challenges into this Action's consideration and enable disciplinary, interdisciplinary, and collaborative research. The network of participants plans to publish at least 10 joint papers and book chapters quarterly not only within the groups of the Action but also with other research groups outside the Action.

A plan for deliverables is presented in Table 4.

Table 4- Deliverables of the Action

Number	Deliverables
D1.1	Trustworthy model and metrics
D1.2	A general framework to guarantee trustworthiness in 6G systems
D2.1	(Intelligent) Attacks and countermeasures
D2.2	Context-aware solutions to enable the resilience of 6G
D3.1	Quantum-resistant algorithms and design
D3.2	Adaptive algorithms for the post-quantum era
D4.1	System design for sustainable wireless networks
D4.2	Recommendation for scalable and sustainable 6G
D5.1	PLS demonstration, dataset at the first phase
D5.2	Experiments, demonstrations on context-aware 6G security, and shared dataset

In addition, this Action plans to issue 12 newsletters (N), 3 whitepapers (W), and 5 tutorials (T) during a 4-year period. Every year, the Action will hold one special sessions (SS) at well-known conferences such as IEEE GLOBECOM or IEEE ICC, one coordinated meeting (CM) with other projects or COST actions, and actively participate to standardization activities (S). This COST Action will also run one Training School (TS) annually and start Short-Term Scientific Missions (STSMs) from the first running year. At the end of Action, 6G-PHYSEC will prepare and release the final report (FRP). The details of the plan for deliverables and dissemination activities are in Section 4.1.4.

4.1.3. RISK ANALYSIS AND CONTINGENCY PLANS

The table below indicates risks identified by the consortium at the time of proposing this Action. The Action also propose some actions to mitigate the impact of those risks in the following table.

Table 5- Major risks and mitigation measures

Description of risk	Likelihood	Severity	Proposed risk-mitigation measures
Complexity in management	Low	Medium	Most of the partners have either collaborated in the past or are reliable partners from the network links.
Partner leaving the consortium	Low	Medium	COST Actions are open and thus can always invite new participants and even substitutes.
Partner is underperforming	Medium	Low	**Quarterly meeting** and reporting and continuous monitoring will avoid undiscovered underperforming. The mitigation plan includes reactivating the partners and in the worst case remove / replace as necessary.
Difficulties in data collection	Medium	High	Building block and corresponding logging system developers will be involved since the beginning of the project in the definition of the data collection methodology
Insufficient and/or poor evaluation activity	Low	High	The Action will propose to periodically synchronize activities during the evaluation phase to ensure that the evaluation will be performed on time

4.1.4. GANTT DIAGRAM

WG	Title	Year 1			Year 2			Year 3			Year 4		
		Q1	Q2	Q3	Q1	Q2	Q3	Q1	Q2	Q3	Q1	Q2	Q3
WG1	**Trustworthy 6G**					D1.1						D1.2	FRP
T1.1	Identification												
T1.2	Theory Development/ Metrics definitions												
T1.3	Experiment & Data analysis												
T1.4	Model/ Framework												
WG2	**Intelligent and resilient systems**					D2.1						D2.2	FRP
T2.1	Identification												
T2.2	Protocol design												
T2.3	Attacks and countermeasure experiment												
T2.4	Data analysis and Context-aware protocols												
WG3	**Quantum-resistant security**							D3.1				D3.2	FRP
T3.1	Identification												
T3.2	Algorithm design												
T3.3	Experiments and Data analysis												
T3.4	Adaptive algorithms												
WG4	**Scalable and sustainable security**							D4.1				D4.2	FRP
T4.1	Identification												
T4.2	Hardware and Software design												
T4.3	Experiments and Measurement												
T4.4	Data analysis and Recommendation												
WG5	**Experiments and demonstrations**								D5.1			D5.2	FRP
T5.1	Identification												

T5.2	Experiments, analysis, and feedback											
Dissemination activities												
Website & social media												
Newsletters		N1	N2	N3	N4	N5	N6	N7	N8	N9	N10	N11	N12
White paper					W1			W2			W3		
Special sessions/workshops				SS1			SS2			SS3			SS4
Coordinated/joint meetings			CM1		CM2			CM3			CM4		
Standardization activities				S1			S2			S3			S4
Training Schools				TS1		TS2			TS3			TS4	
Tutorials			T1		T2		T3		T4		T5		
Joint publications													
STSMs													