Brussels, 12 May 2023

COST 014/23

DECISION

Subject: Memorandum of Understanding for the implementation of the COST Action "Behavioral Next Generation in Wireless Networks for Cyber Security" (BEiNG-WISE) CA22104

The COST Member Countries will find attached the Memorandum of Understanding for the COST Action Behavioral Next Generation in Wireless Networks for Cyber Security 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 CA22104
BEHAVIORAL NEXT GENERATION IN WIRELESS NETWORKS FOR CYBER SECURITY (BEiNG-WISE)

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 boost non-conventional wireless cyber-security solutions consisting of both technical and social characteristics. 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
The always-connected world we are living in, gives us an unprecedented plethora of new advanced services and automated applications requiring, more and more, less human intervention due to the increased integration of Machine Learning (ML), Artificial Intelligence (AI) approaches and sophisticated emerging wireless technologies.

On the other side, this connected world opens new breaches and creates new potential vulnerabilities for smart advanced cyber-attacks, namely attacks and offender relying on ML/AI and advanced wireless technology integration, to make their attack more effective and less detectable. If an increasing awareness by the users could help to contrast the security issues, it is not sufficient against the new generation of cyber-attacks. In this context, a drastic paradigm shift, putting human-being in the loop for the conception of novel and more effective cyber-security solutions, must be considered.

Human-beings have a double role in the cyber-connected world: as potential offender and potential victim. The focus of BEiNG-WISE will be on how these different human-being features can be combined with the advanced technological characteristics, in order to conceive non-conventional, responsible by design, cyber-security solutions accounting for both these factors. In this complex connected system, another fundamental aspect that needs to be accounted to, is the legal one, related to the conception of solutions that can be effectively employed in the real world. Also, legal aspects should be considered at the design stage. The Action relies on cross-domains expertise, ranging from cybersecurity, wireless communication technology, data science, sociology, psychology and law.

Areas of Expertise Relevant for the Action	**Keywords**
● Computer and Information Sciences: Cryptology, security, privacy ● Computer and Information Sciences: Ethics of computer and information sciences ● Law: Criminal law ● Media and communications: Media and communications, social aspects of information science and surveillance, socio-cultural communication	● Cybersecurity ● Human factor ● Wireless technologies ● Legal factors in Cyber-security

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

Research Coordination
● RCO-1: To serve as a pan-European scientific framework and realize the very ambitious objective of imposing and pushing a radical paradigm shift in cyber-secure wireless communications, by conceiving "responsible" and "sustainable" solutions.
● RCO-2: To develop and coordinate new approaches to raise awareness among the cyber users.
● RCO-3: To push interactions and multi-disciplinary research domains by defining new metrics that can account for human factors as well as technical aspects in a joint fashion, by design.
● RCO-4: To bring together members of the different communities into a multi-disciplinary sustainable community in order to analyse the specific open challenges of cyber security with a renewed point of view, enriched by the different specific perspectives of the different research domains.
● RCO-5: To support the 3-R's of the science, the Repeatability, Reproducibility & Replicability of the advancing security solutions designed in the Action and based on the technical and societal requirements,

through the dataset sharing.
● RCO-6: To support the development of a new scientific domain, where technical, social, and legal factors are considered in a joint and synergistic way, instead of being considered independently of each other.

Capacity Building
● CBO-1: To contribute to make the EU a leader on disruptive and unconventional cyber security solutions, by supporting the capacity to lead at an international level on wireless security and reliable communication systems.
● CBO-2: To build a network of Young Researchers and Innovators (YRIs) and create new profiles of researchers and technicians on innovative and high-multidisciplinary topics, involving technical, social, and legal competences.
● CBO-3: To widely promote the new paradigm of BEiNG-WISE encompassing societal, technical, and legal components at a global level.
● CBO-4: To establish a sustainable community of Groups of Experts on the different aspects of emerging technology, vulnerabilities, and countermeasures, able to provide technical and scientific know-how in Europe and beyond.
● CBO-5: To transfer knowledge in terms of expertise, scientific tools and human resources across the different disciplines and between academia and industry.
● CBO-6: To overcome the ’siloing’ of research topics by country and achieve geographical and demographical diversity, with special attention to COST Inclusiveness Target Countries and disseminate the results of the Action activities to the scientific community, the industry, the certification body, and the European institutions.

TECHNICAL ANNEX

1. S&T EXCELLENCE

1.1. SOUNDNESS OF THE CHALLENGE

1.1.1. DESCRIPTION OF THE STATE OF THE ART

Recent technological evolution and advancements in wireless communication systems are enabling millions of innovative cyberspace applications to connect to the Internet by anyone, anywhere. These applications are becoming an integral part of our daily life, in different sectors spanning from transport, health, energy, to deliver education, critical infrastructures, etc. The proliferation of disruptive technologies allows several opportunities to be (inter)connected and exchange significant amounts of data, by enabling the ***always-online-paradigm.***

The different wireless devices such as laptops, smart-phones, smart-watches allow an untethered access to data and information, which play a key role in enabling and developing a cyberspace intelligence, whose main scope should be to enhance collective human intelligence. Numerous cyberspace applications that could not have been imagined until a few years ago, since they are reliant on high data speed demand and high connections of devices, can be now enabled based on the innovative wireless technologies. These latter are at the basis of the capability to access and intelligent processing, based on the *any-paradigm*, ***any****one*, ***any****where*, ***any****time*.

Related to that, enterprise and service provider IT environments are experiencing an increased complexity in dealing with new security vulnerabilities. To be able to effectively thwart security attacks, there is a need for continued commitment to the adoption of security best practices. In this context, it is necessary to enhance and optimize security tools to mitigate threats, it is undeniable that security best practices are the right way to prevent them. However, security best practices cannot be imagined without full involvement of users. This is more urgent in respect to new paradigms such as the Internet of Things (IoT) and Bring Your Own Device (BYOD). BYOD is a policy that allows employees in an organization to use their personally owned devices for work-related activities. This has become more evident with the Smart Working policy widely adopted during the pandemic. In IoT and BYOD, different types of heterogeneous objects with different characteristics, capabilities and capacity are enabled to connect to the Internet and exchange information/data, that much contribute to the complexity growth.

In this rich and heterogeneous cyber world, it is difficult to understand the underlying data-sharing models and then to gauge the side effects of specific choices. The privacy and security management have become very intricate, and often tools used for guaranteeing privacy and security are very complex to be used and hinder the user's engagement instead of supporting it. Recently, the internet/Wi-Fi access is classified as one of the "most-basic" needs of humans. However, such need is always endangered as the Internet ecosystem is more vulnerable to different kinds of attacks, since the human component in security is often neglected, i.e., the focus is usually on the technical aspects of the security, which leaves the human/social aspects outside of the security management plan. This leaves the Internet ecosystem vulnerable to various non-technical (e.g., social) attacks. In this context, the main aim of the BEiNG-WISE COST Action is

to better understand human beings in wireless security systems and how to design usable security solutions.

Starting from the advanced technological aspects, BEiNG-WISE aims to analyse the human factors in the wireless systems from a security point of view, by considering the different declinations of the human being in the security wireless systems: the generation of attacks from a criminal perspective, the impact of the security solutions on the users and the impact on the implementation of the solutions, when the human factor is considered by design.

BEiNG-WISE will focus specifically on the following pillars:

- **Cybersecurity in emerging wireless communication** - Cybersecurity threats are growing faster than their corresponding mitigation measures. Related to that, one important question is "Will our individual and collective approach to managing cyber risks be sustainable in the face of the major technology trends taking place in the near future?". The BEiNG- WISE Action will try to rattle off the crucial points of the questions, to outline clear directions of the research and the paradigm shift necessary to be able to respond positively to this question. The key factor is that with the

evolving of the communication technologies, new paradigms such as the Internet of Everything (IoE), BYOD, always-online-paradigm are appearing and imposing their presence in daily life and in critical infrastructures. These paradigms are strictly correlated to each other. IoE is a kind of extension of the Internet of Things involving human beings, data and processes combined into a common interrelated system, with the main purpose of taking smarter decisions and improve experiences. In some way, this paradigm encompasses the other two concepts of BYOD, where the use of personal wireless devices is incentivised also by the companies and enterprises, and the always- connected-paradigm. The IoE paradigm puts in evidence the need for enhanced Quality of Service (QoS) parameters allowing to account for the perception and features of the users. New Quality of Human Perception and features (QoHPF) parameters need to be included to go beyond the classical metrics like throughput, latency, etc. by merging them with the human perception and human features.

- **A cyber-crime perspective in Wireless Networks** – The first declination of human factor in wireless security networks, is represented by the comprehension of the main reasons pushing human beings to create advanced attacks. A deep understanding of these aspects also permits to acquire better insights into the target effects an offender plans to generate. Prevention of cybercrime is strongly based on the understanding of the crime schemes in the cyberspace and the behaviours of the cyber criminals by the individual and the governments. The cybercrime services market growth is the effect of a sophisticated cyberattack landscape, and recently started to receive attention from media. Cyber criminality is often based on human prejudices exploitation and employs cognitive vulnerabilities to create effective attacks (see also in the domain of financial cybercrime, where the identification of the motivation behind cybercriminal attacks and the understanding of their modus operandi can support cybersecurity measures). These dark patterns and human psychology are often masterfully engineered to design sophisticated cyberattacks. Nevertheless, they have not received the same weights as for the “pure” technological aspects. In BEiNG-WISE, a synergic analysis of the two aspects will largely benefit the creation of more robust and resilient by design to attacks communication systems.
- **Optimal security approaches for wireless systems and impact on the user** – Wireless security is strongly relying on algorithms. This implies that the impact on final users, which can be an individual as well as a public or private sector, must be evaluated in terms of impact of algorithms, which bring us to the concept of responsible algorithms. Algorithms are increasingly used in several domains as part of decision-making processes, with a high potential impact on the individuals, private and public sectors. Recently, in the perspective to contribute to the legislative efforts of the EU towards transparency, accountability and fairness of algorithms, a detailed study has been dealt in the context of the European Parliamentary Technology Assessment (EPTA). In the perspective to contribute to the legislative efforts of the EU towards transparency, accountability and fairness of algorithms, a detailed study has been released. This study arises several interesting points about responsible algorithms, embracing different disciplines spanning from legal, technical, and sociologic aspects. Security and privacy algorithms are becoming essential components of several cyber-critical systems. It is fundamental to ensure that these algorithms do not discriminate against or harm the users. This is a very complex task, since it is demanding to study the whole process of the algorithm creation, starting from the theoretical design to the data sources to feed it, its implementation, and the potential impact on the people. This very complex process requires a pioneering methodology. The most touchable effect would consist in foreseeing the potential negative outcomes of the system and avoiding them when the solution is adopted by the users. For achieving this very ambitious target, it is necessary to adopt a broader perspective than that of a technical person, neglecting the specific context and the potential social impact of the developed tool, as it is in current solutions. A synergic combination of audit and technical design must be considered. These aspects and the need to think about algorithms design in the context of the security domain have been already object of consideration in different works. Additionally, an interdisciplinary approach to cybersecurity allows the implementation of an ethical European values and fundamental rights perspective. Digital security solutions within the European Union need to be designed in a way that the integrity of users is not compromised.
- **Human Factors in Wireless Security** – IoE paradigm presents several and interesting opportunities for designing new technologies in different sectors, from health to industrial, transport, energy, private and public organizations. In this context, for a matter of business continuity, several organizations are accepting these technologies, where the connection of the employee can be based on the organization’s premises and outside the organization. Based on these considerations, in the last few years, there has been a proliferation of Information Security experts, while there is a lack of experts on human factors and their relationships with cyber-attacks. In practice, the technological component, as a stand-alone aspect, is always more prevalent than the human

factor, even though this latter has been proven to be critical for advancing on cyber security solutions. Typically, the technology-centric approach for Communication and Infrastructure Security (CIS), has been the more recurrent approach to designing cyber-security solutions to overcome the limitations of achieving more reliable communications systems. Therefore, efforts to develop dedicated tools to tackle human factor-related cybersecurity issues should be continued and intensified.

1.1.2. DESCRIPTION OF THE CHALLENGE (MAIN AIM)

The identified challenge of the BEiNG-WISE Action is to boost non-conventional wireless cyber-security solutions consisting of both technical and social characteristics.

As largely demonstrated in the previous section, wireless network technologies for guaranteeing Ultra-Reliable Low Latency Communications (URLLC), are sufficiently addressed in several European and extra- European initiatives. However, the technical evolution of these technologies is not followed by an adequate analysis of the new risks and threats and above all, the human factor is often completely disregarded, or minimally considered. BEiNG-WISE will pursue a radical paradigm shift in contrast to the current trend, to be able to identify, detect novel vulnerabilities in wireless communication systems, and conceive effective countermeasures. This paradigm shift must rely on human features integration, since human being represents the source of the problem (the offender) and the target (the victim), playing a primary role in the cyber security wireless landscape. This double implication has not yet been addressed but would contribute to pave the way to novel more robust and reliable wireless communication networks. From one side, the understanding of the nature of the offender, the business model analysis beyond an attack, may convey on a deeper comprehension of the nature of the cyber-attacks, and this would play a double effect: 1) The developed security solutions can be more robust by design, preventing certain types of attacks; 2) The countermeasure solutions will be developed by including human components, to push wireless users to implement behaviours aimed at reducing the risks. From the victim's point of view, the identification of specific human factors, which can be considered as vulnerabilities, would help to design more "human" counterattacks. Of course, cyber solutions as envisaged in BEiNG-WISE require a deep awareness of jurisprudence. The problem is very complex and highly multidisciplinary, involving at least three different research domains: computer and communications science, social science, and law.

In the long-term, the main scientific objectives that BEiNG-WISE implies are:

- O1: to perform fundamental research in the fields of emerging wireless communication and networks architectures and design secure communication systems;
- O2: to make wireless secure systems "responsible" and "sustainable" by design;
- O3: to pave the way towards a new paradigm integrating human factors in wireless cybersecurity systems.

In the next sections, the research directions identified to pursue the above objectives will be detailed.

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

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

The main innovative aspect behind BEiNG-WISE is to consider the cyber secure wireless communications by simultaneously addressing technological and social challenges. This means that human factors will be considered and integrated by design in the advanced cyber solutions. Moreover, the vulnerabilities of the wireless communication systems, will be studied by considering the human aspects and an economic business model approach, for better understanding the deep nature of the cyber-attacks. BEiNG-WISE will carry out extensive research coordination activities based on theoretical, simulation- based and experimental validation on four main applications areas, defined by considering the technical aspects, the human factor from an offender's point of view, the human components from the defender's point of view and the feasibility of advanced solutions. Each application area will be assigned to a specific WG: WG1 – Cybersecurity in emerging wireless communications; WG2 – A cyber-crime perspective in wireless networks; WG3 – Optimal security approaches and their impact on the users; WG4 – Human factors in wireless security. A fifth WG on legal factors (WG5) will be crossing all application areas.

Two original points considered in this Action, regard the legal aspects of cyber solutions considered in a transversal way for the different subjects considered, namely for the technical and human factors and the creation of mixed datasets based on data deriving from the "technical" aspects, i.e., channel, signal, networks, and data related to the users, its behaviour, its setting, and configuration in the use of devices, etc.

WG1 - Cybersecurity in emerging wireless communications (O1, O2): In March 2019, the first summit on 6G was held in Finland, with the main objective to draft the first-ever 6G white paper and let 6G officially start. Even though it is difficult to enclose 6G with a definition, it is sure that it will encompass a global evolution in terms of wireless communication technologies and will not just represent a "faster version" of the 5G network. Most of the researchers converge on the idea of 6G networks as fully AI-empowered, with a real and deep integration of Artificial Intelligence (AI) by design, to trigger a real ubiquitous communication. This evolution is accompanied by an evolution in the field, with the appearance of new vulnerabilities and threats, which can create a severe impact on cyber critical infrastructures. This WG will be mostly devoted to the identification and detection of new vulnerabilities and the conception of systems that are more secure by design. There is an increasing awareness of the fundamental role cybersecurity plays and will play tomorrow in developing sophisticated solutions, able to anticipate the risks, to promptly detect attacks and react in real-time. To accomplish these requirements, there is an increasing use of the AI/Machine Learning (ML) approaches, for designing more sophisticated solutions. The main problem is that these advanced technologies are a double-edged sword and can be used to create more effective and less detectable smart attacks. To create a better defence, the best approach is to attack first, Cybercrime-as-a-service is becoming the standard business model and new sophisticated cyber-attacks, following the evolution of wireless communication technologies can be developed. To create more effective attacks, a paradigm shift must be realised to account for the human component in it.

WG2 - A cybercrime perspective in wireless networks (O2, O3): Cybersecurity plays a key role in contemporary society due to the pervasive, ubiquitous interconnection of wireless communication systems and the constant and continuous evolution threats. Cyber-attack targets are spanning from individuals to companies, institutions, etc. In this context, the role played by human beings is fundamental, since it is the weakest part of the chain and the generation of successful advanced attacks (e.g., social engineering attacks), is based on the awareness of this vulnerability. In this trans-disciplinary WG, a special focus will be devoted to the analysis of cyber-crime profiles to derive a fine-grained perspective of the feasible advanced attacks. Accurate and deep analysis on types, methods, and effects of cybercrimes on a wireless network need to be investigated.

WG3 - Optimal security approaches and their impact on the user (O2, O3): This activity concerns “responsible by design” optimal security solutions. The starting point for feeding this WG is the increasing and pervasive use of technology in the daily life of human beings. This massive use of technology requires a deep reflection on the correlated aspects of cyber security and how it must be managed. In particular, optimal security solutions related to the massive use of disruptive technologies, should be thought in respect of ethics and human rights approaches to conceive security solutions that are responsible by design. There are three key stages for optimal responsible by design security tools and solutions: 1) the first phase is represented by the design and development; 2) the second part is concerning the deployment and 3) the last stage is the use and application (including the use of security measures). The universal acceptability of the solution by the final user is paramount for realizing successful security tools. In particular, the security algorithm perception as well as their impact on the human being need to be studied and considered in the design of the security algorithms. This WG requires technical and non-technical stakeholders to account for the key factors that integrate the responsible concept into the development, deployment, and use of optimal security solutions.

WG4 - Human factors in wireless security (O1, O2, O3): In this working group, cyber-physical systems and emerging wireless networks will be considered in strict relation with the human components, which is an integral part of the system. The new communication technologies systems will be regarded by considering the interaction with humans and by introducing a new paradigm shift, Cyber Physical Human Systems (CPHS). Human beings are a fundamental part of CPHS and play different roles as users, sources of problems in terms of security and the viable solution for the problem. Another main part of CPHS is the privacy and security component. Recently, there is an increasing interest on research activities regarding personalised and adaptive features to integrate into privacy and security user tasks. In this WG, the diversity of user’s characteristics, together with technology components will be considered for designing adaptive privacy and security technologies, accounting for the specific user context. As the wireless technology is imposing in the daily life of human beings, there is an increasing use of the proper own devices, both for personal and professional purposes. People are more and more used to publish personal information by the means of social networks without being aware of security and privacy issues. Even though there is an increasing attention and focus on the vulnerabilities for reducing sensitive data leakage and strengthening online communication, the manipulation of users based on social engineering attack is more complicated to be managed and deserve much attention. In practice, a social engineering attack targets the weakest link in the security chain, namely human beings. Different manipulation techniques can be used, and such a type of attacks requires an interdisciplinary

perspective and analysis. Indeed, it is deeply entrenched in the fields of social and human science and computer science.

WG5 - Legal factors in Cybersecurity Wireless Systems: A Vertical Approach (O1, O2, O3): the interconnection of many communicating objects means a huge amount of data to be moved from one point to another and data to be stored in some devices. Several questions arise about cybersecurity solutions and data treated in the wireless communication networks. One crucial aspect to be considered is who makes the connection between applications, networks, and services, and how the devices/objects based on different technologies can safely operate in the same environment. With the complex plethora of communication technologies in 6G, will it be possible to envisage global governance and security, or will it be necessary to figure out a local governance? To address these questions, a legal perspective needs to be considered, with experts in different domains, technical and legal, able to consider at the same time technical constraints and ethical issues, in the perspective of realizing "responsible" by design approaches.

Data in BEiNG-WISE: in BEiNG-WISE, it is expected that different types of data of various nature, will be managed. Due to the high multi-disciplinary nature of the network, at least three different types of data can be identified: a) "Technological Data" concerning the physical and environmental characterization of the communication systems; based on the wireless nature of the communication paradigms considered in this Action, it will be extremely interesting to collect and have access to data in both "normal working" conditions and when the systems are under attacks; b) Data concerning cybercrimes for characterising the probability, type and nature of cyber-attacks; and c) Data concerning human profiles for characterising the potential vulnerability related with the type of attacks, as well as the acceptance degree of the solutions conceived in the Action. In particular, the latter type of data will account for diversity in terms of culture, legal aspects of different countries, gender bias, etc. Among others, BEiNG-WISE will aim at collecting real-world data and compile anonymised datasets to be shared in the research and industry communities. Of course, legal concerns and GDPR requirements need to be considered as well as technical tools enabling to create such a significant database. The large size of proposers in the Action guarantees a sufficient amount and diversification of the data at an early stage of the Action lifetime. The Action will also consider the opportunity to combine/enrich these initial data with publicly available datasets.

1.2.2. OBJECTIVES

1.2.2.1. Research Coordination Objectives

Current research activity on cyber security in wireless networks disregards the human factor, both from an attacker/offender and a victim point of view. This implies the conception of solutions regardless of who will be the main final user. The primary objectives of cyber-security solutions are translated into technical requirements terms, which make the solution itself not suitable for the final user, most of the time. The main research coordination objectives of BEiNG-WISE are:

RCO-1: To serve as a pan-European scientific framework and realize the very ambitious objective of imposing and pushing a radical paradigm shift in cyber-secure wireless communications, by conceiving "responsible" and "sustainable" solutions.

RCO-2: To develop and coordinate new approaches to raise awareness among the cyber users.

RCO-3: To push interactions and multi-disciplinary research domains by defining new metrics that can account for human factors as well as technical aspects in a joint fashion, by design.

RCO-4: To bring together members of the different communities into a multi-disciplinary sustainable community in order to analyse the specific open challenges of cyber security with a renewed point of view, enriched by the different specific perspectives of the different research domains.

RCO-5: To support the 3-R's of the science, the Repeatability, Reproducibility & Replicability of the advancing security solutions designed in the Action and based on the technical and societal requirements, through the dataset sharing.

RCO-6: To support the development of a new scientific domain, where technical, social, and legal factors are considered in a joint and synergistic way, instead of being considered independently of each other.

1.2.2.2. Capacity-building Objectives

CBO-1: To contribute to make the EU a leader on disruptive and unconventional cyber security solutions, by supporting the capacity to lead at an international level on wireless security and reliable communication systems.

CBO-2: To build a network of Young Researchers and Innovators (YRIs) and create new profiles of researchers and technicians on innovative and high-multidisciplinary topics, involving technical, social, and legal competences.

CBO-3: To widely promote the new paradigm of BEiNG-WISE encompassing societal, technical, and legal components at a global level.

CBO-4: To establish a sustainable community of Groups of Experts on the different aspects of emerging technology, vulnerabilities, and countermeasures, able to provide technical and scientific know-how in Europe and beyond.

CBO-5: To transfer knowledge in terms of expertise, scientific tools, and human resources across the different disciplines and between academia and industry.

CBO-6: To overcome the 'siloing' of research topics by country and achieve geographical and demographical diversity, with special attention to COST Inclusiveness Target Countries and disseminate the results of the Action activities to the scientific community, the industry, the certification body, and the EU institutions.

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

BEiNG-WISE is the first COST Action focusing on non-conventional security approaches in wireless networks, integrating human beings from the two perspectives, the offender and the victim, and considering the legal and human aspects in the solution design.

Over the years, several initiatives at European level have been supported in different European programs considering security and trustworthy aspects in wireless communication systems. Among them, there are projects focusing on cyber security aspects in general, such as: 5G ENSURE (H2020, 2015-2017), CHARISMA (H2020, 2020-2024), SPIDER (H2020, 2019-2022), CYBERSANE (H2020, 2019-2022), SEMIOTICS (H2020, 2020-2023). Other projects are more focused on industry or transport applications, such as: C4IIoT (H2020, 2019-2022), RESIST (H2020, 2018-2022), COLLABS (H2020, 2020-2022), THREAT-ARREST (H2020, 2018-2021) or health applications, such as: HEIR (H2020, 2020-2023), SMART BEAR (H2020, 2019-2023), UNITI (H2020, 2020-2022), ASCAPE (H2020, 2020-2022), RETENTION (H2020, 2021-2025). A recent research project, CyberSec4Europe has as main focus to create a series of recommendations based on real-world use cases developed in different sectors such as healthcare, transports, etc. Another interesting project is a Marie Sklodowska-Curie Excellent Science action called LEADS and regarding legal aspects in data science. These two latter projects demonstrate the emergence to work on the creation of new experts in cross domains. IntelIIoT is one more recent European initiative considering human-in-the-loop. This is structured in three main applications, Agriculture, Healthcare and Shared Manufacture and the human component is considered in all the applications to take remote control, to receive updates and solicitations and to manage exceptions, since the solutions are AI-based and exceptional events could not be correctly managed by the system. Even though in IntelIIoT the human being factor is considered, the way to integrate and consider it is different in respect of the principles that will be developed in BEiNG-WISE.

Different COST Actions have been proposed in the years, concerning the evolution of wireless network technologies (in chronological order): IC0803: RF/Microwave Communication Subsystems for Emerging Wireless Technologies (RFCSET); IC0902: Cognitive Radio and Networking for Cooperative Coexistence of Heterogeneous Wireless Networks; IC1004: Cooperative Radio Communications for Green Smart Environments; IC1104: Random Network Coding and Designs over GF(q); CA15104: Inclusive Radio Communication Networks for 5G and beyond (IRACON); and CA20120: Intelligence-Enabling Radio Communications for Seamless Inclusive Interactions. None of them is considering security aspects and above all human behaviour-based solutions.

The main objective of the Action IS1410 - The digital literacy and multimodal practices of young children (DigiLitEY) is to create an interdisciplinary network that will advance understanding of young children's digital literacy and multimodal practices in the new media age. In this Action, the human interaction in respect of the Internet of Toys paradigm has been addressed and the societal aspects in terms of opportunities and risks have been considered. Even though some societal aspects have been considered in this Action, it is for a very specific application case, the IoToys and for a very specific

person category, young children. The COST Action IC1403 CRYPTACUS1 focuses on technical and societal aspects of security in the context of the Internet of Things and ubiquitous systems. Anyway, the main focus is on advanced aspects of cryptanalysis and analyse real-world scenarios with a specific focus on the data collected in the ubiquitous computing systems. The behavioural human factor is not considered in this Action.

Among international initiatives, the recently constituted research task group HFM-259 focuses on human systems integration in cyber security systems, with the main goal to promote and analyse cyber security as a socio-technical system and to consider the different aspects and features of such a complex system.

Based on the outcomes of this activity, it is clear the emergence to push research in this direction with a disruptive approach as the one that will be adopted in BEiNG-WISE.

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

The necessary skills and expertise were already present in the initial network of proposers of the BEiNG-WISE Action. This included **experts on wireless networks and emerging communication technologies, expert son cyber security, experts on social and human fields and experts on legal aspects related to cyber security systems**. Additional experts will be attracted around this initial group and thus consolidate the network. The cutting-edge research of BEiNG-WISE will be ensured by counting on leading European researchers, experts and industrial partners.

The initial Network of Proposers included 36 members, with secondary proposers from 20 COST countries, including 10 ITC (Croatia, Cyprus, Estonia, Greece, Hungary, Montenegro, Portugal, Romania, Slovenia, Turkey). They bring academic excellence and a proven track record of high-impact publications in the field. With this basis, the Action's broad geographical distribution will be ensured. Likewise, the interests and expertise of the initial network of proposers are complementary, spread evenly over the various working groups of the Action and with connections to relevant stakeholders in their fields of expertise. The Action will continue to actively seek out further participants, aiming at including as many young researchers as possible. During the Action lifetime, a commitment to gender balance will be applied, taking into account the proportion of women in the field. The Action's pronounced aim is to build capacity and leadership skills about a new multidisciplinary vision of cybersecurity in wireless network systems. The critical mass will be achieved, also by involving representatives from international companies that have expressed interest in being involved in the Action. This will allow to maintain the achievement of the ambitious goals considered. Key actors at international level for the different domains, will be also invited on a regular basis to participate to the meetings and provide inputs for the future research directions.

2.2.2. INVOLVEMENT OF STAKEHOLDERS

The network already relies on different stakeholders, including key institutions as universities, research institutes, SMEs, etc.

Stakeholder	**Examples**	**Plan for involvement**
Companies / Industries	Companies to raise the awareness of the users. Companies providing data to test the solutions on real- world cases.	Exploiting links of Action participants with the private sector to invite companies and industry representatives to join the Action.
Doctoral Students and Young Researchers	PhD students on wireless communications, cyber-security systems, PhD law Student, PhD sociology students	Through the contacts of the researchers and academic partners, doctoral schools will be most involved for training and dissemination activities.
Researchers from non-EU countries	Australia, Canada, USA, South-Corea, Israel, Japan, etc.	Exploiting links of Action participants with several non-EU researchers, these will be invited to contribute to the Action.

Standardization / Regulatory Bodies	ETSI, 3GPPP, ITU, etc.	Exploiting involvement of Action participants in standardization activities, the Action will be presented to them, and they will be invited to contribute to specific Action activities such conferences, workshops, etc.
Key bodies of international R&D organizations	IEEE, ACM, EURASIP, etc.	Exploiting links of Action participants with key R&D organizations, events for dissemination of the outcomes of the Action will explicitly be organised.

Based on the specific areas of interest and activities of the Action, the participation of International Organisations and International Standardisation Institutes (e.g., the National Institute of Standards and Technologies - NIST), and experts from COST Near Neighbour Countries (NNC) will benefit to each other. First of all, different metrics, parameters, models and scenarios can be considered, and an exchange will enrich the amount of information and possible measurements of the new solutions issued from the paradigm shift BEiNG- WISE is aiming to achieve. A variety of expertise in the different core subjects of the Action beyond European institutions, will enrich the uses cases and allow a better assessment of the founding key of the Action, creating a critical mass with a more complex and global perspective, which is a crucial factor in such a type of multidisciplinary initiative as BEiNG-WISE.

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)

BEiNG-WISE aims, via the WG activities, to achieve the scientific, technological, and socio-economic impacts outlined below:

Scientific short-term impacts:

- Generate new knowledge and resources for the research community (publications, cartography, gap analysis…) that will benefit all researchers working in the cross-domains: cybersecurity, social sciences and humanities, law, future networks generation.
- A deeper understanding of how human features can be considered to conceive innovative cyber-security countermeasures.
- Published results in top peer-reviewed international conferences and journals.
- Education of a new generation of researchers and engineers with acquired cross-domain competences: cybersecurity & social sciences and humanities, cybersecurity and law, cybersecurity and emerging networking (metaverse, cyber-objects, emerging wireless paradigms).
- Foster multidisciplinary collaboration at a larger scale: from mathematicians to humanities (lawyers, social humanities field).

Scientific medium to long-term impacts:

- Make the digital society safer and more secure and contribute to an increased trust in technology and science. Indeed, BEiNG-WISE will focus on the emerging wireless communication technologies, encompassing the concept of "smart-everything". This paradigm will allow to automatize several daily services and activities. The Action will specifically analyse the new vulnerabilities and security gaps, related to these emerging technologies, the direct and constant integration of ML and AI, the new vulnerabilities emerging in the Metaverse and in the Smart Reprogrammable Environment, and it will be done by putting the human being in the loop.
- An integrated European-wide research community on cybersecurity able to tackle problems that can only be done in an interdisciplinary and collaborative setting.

Technological impacts. Smart Wireless Networks can play a primary role in the society and economy. It is sufficient to think about the pervasiveness of the Intelligent Wireless Technologies to realise the Smart City, Smart Building, Intelligent and Connected Transports. New sensing applications, such as positioning and localization both indoor and outdoor, trigger and facilitate the integration of ICT and intelligent devices in the different above-mentioned sectors. Also, the Fourth Industrial Revolution, the so-called Industry 4.0, will boost a more aware productivity, keeping unchanged the quality factor of the products, but with a more improved usage of the energy and materials. This latter is a concept sadly familiar nowadays, with the direct consequences on the energy resources issues due to the war in

Ukraine. Even though embedding intelligence in the network seems the natural panacea to solve several modern issues, in the BEiNG-WISE proposer's vision this is not possible, unless a radical perspective change. More specifically, the increased ubiquity and "dependence" of humans on intelligent technology, is also the biggest vulnerability and this Smart Environment concept must be based on more reliable and secure design solutions.

Socio-economic impacts. The cutting-edge approach adopted in BEiNG-WISE, with a renewed human-centric vision, will have an enormous impact on the increasing awareness of a globally connected world and will contribute to improve its trustworthiness. Another key point is represented by the cost of cybercrime and cyber-attacks as impact on the global economy. In literature, it has been shown an increase of more than 50% in terms of cost since 2018. The research highlights the importance of standardised databases and actions to improve the awareness of users. One of the ambitions of BEiNG-WISE is to cut the costs and effects of cyber- attacks, without affecting the perceived quality of experience of the ICT users.

3.2. MEASURES TO MAXIMISE IMPACT

3.2.1. KNOWLEDGE CREATION, TRANSFER OF KNOWLEDGE AND CAREER DEVELOPMENT

The various measures aiming at maximising the impacts as well as pursuing the career development of young researchers will rely on the various dimensions outlined in Section 1.2.2.2, implemented via Transversal Activities, TAs, described in Section 4.

Knowledge creation: a publication policy and plan will be put in place at the start of the Action. Young Researchers and Innovators (YRIs) will be encouraged to take the lead on the publications and position themselves as first authors as a means of enhancing their career perspectives (TA). Facilitating measures include the number of meetings (three per year), the various training schools/tutorials (in particular, those enabling researchers to adopt AI as a tool), as well as the extensive share of knowledge, information and results (through the BEiNG-WISE database under the supervision of TA3).

Transfer of knowledge: to fulfil the long-term vision of BEiNG-WISE it is necessary for knowledge and know-how to both be shared and transferred across categories of researchers and stakeholders. For this reason, BEiNG-WISE has put in place a strong capacity building programme (TA1 and TA2) (CBOs) which will ensure: i) transfer of technical know-how amongst scientists, SMEs/industries and society including professional training organisations. ii) transfer of scientific knowledge amongst researchers notably to YRIs.

Career Development: A number of actions will be put in place (TA1 and TA2) to enable the YRIs involved in BEiNG-WISE to boost their career potential notably through the possibility of at least 12 STSMs in 4 years (minimum 3/y). Because unfamiliar connections will be made amongst stakeholders, scientists will have new opportunities to be involved as experts in varied scientific councils of authorities (e.g., Special Interests Groups of IEEE ComSoc).

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

At the beginning of the Action, the Science Communication coordinator (TA2 leader) with the dissemination focus group mainly composed of YRIs (see Section 3.2) will elaborate a dissemination and exploitation plan describing in detail activities that will enforce the impact of the Action. This plan will include the sharing of knowledge between the participants and will increase awareness to favour the most efficient use of social media and new communication technology at all levels to the public and end-users. An initial strategy for dissemination activities will be outlined in consultation with stakeholders and this strategy will be shared with stakeholder representatives in the early stage of the Action to ensure its relevance and impact.

Web-site and general dissemination materials: website, logo, templates, leaflet, and other dissemination materials that create identity, consistency and awareness of the BEiNG-WISE COST Action. The website will serve as the front-face portal, containing all activities including participants profiles, progress reports, publications, presentations, tutorials, case studies, etc. Public and a private access will be made possible. The private access will serve as a collaborative platform for the Action participants to discuss, work on common papers etc. A leaflet will be prepared to introduce the Action to all relevant stakeholders and the general public. Annual scientific reports on research outcomes will be produced together with semi-annual newsletters targeting a wider audience. White papers will be issued on the views of the Action Cybersecurity.

Publications: Action members will regularly publish joint papers in international high-quality journals (e.g., IEEE TCOM, IEEE Transactions on Wireless Communications, TIFS, etc.) and conferences (e.g.,

EUCNC, INFOCOM, PerCom, ESORICS, CNS, WiSec, etc.). Special issues, surveys/tutorial papers will be particularly pursued to increase awareness on cybersecurity based on different cross-domains. At the end of the Action, a book will highlight the scientific/technological advances achieved.

Networking with scientific community: BEiNG-WISE will organise annual workshops, serving as international forums to bring together Action participants and researchers on emerging wireless technology and cybersecurity; and special sessions and symposiums on cybersecurity based on new communication paradigms at high-profile international conferences (GLOBECOM, ICC, CNS, etc.). Relations will be also set up with other COST Actions, Horizon2020 and Horizon Europe projects and large-scale international initiatives to increase awareness, dissemination and establish collaborations.

Training schools and courses: A Training school coordinator will be appointed to supervise the organization of courses and schools at least once a year, targeting PhD students, engineers, and junior researchers. Publications of tutorials, videos, and massive open online courses (MOOC) will be encouraged as well.

Industrial engagement: A meeting per year will be held. Key industrial players and distinguished external experts will be invited to give talks, exchange knowledge, and expand the Action network.

Exploitation planning: Plans for exploitation will be addressed within the management structure of BEiNG-WISE from the beginning. Key exploitation issues will be how to maintain the hub after the Action ends and how also to ensure that all Action results, notably the research roadmap and guidelines, are adopted by the relevant stakeholders to ensure maximum impact. BEiNG-WISE partners aim to maintain the network post-funded phase, to ensure such a continuation and options for creating a self-sustaining community will therefore be explored both within Management Committee (MC) and Core Group (CG) meetings, but also in consultation with all participating stakeholders.

IPR Management: All BEiNG-WISE members will collaborate closely with the technology transfer units of their respective institutions or with private patent offices. A key objective of BEiNG-WISE is to integrate and add value to existing results that, in some cases, may already have IP constraints. The Science Communication coordinator, in collaboration with the Action MC, will oversee the correct handling of existing IP as well as ensuring that no dissemination activity could potentially harm any potential for new IP either by partners or participants to the WGs.

4. IMPLEMENTATION

4.1. COHERENCE AND EFFECTIVENESS OF THE WORK PLAN

4.1.1. DESCRIPTION OF WORKING GROUPS, TASKS AND ACTIVITIES

The Action will establish a Core Group, constituted by the Action leadership roles (Chair, Vice-Chair, Grant Holder Scientific Representative, WG Leaders, the Grant Awarding Coordinator, the Science Communication Coordinator, and Training School Coordinator). Leaders of the Transversal Activities will be involved whenever relevant and necessary. The Action Core Group will interact and work together for the achievement of the Action objectives, to support the Management Committee.

Working Groups

WG1 – Cybersecurity in emerging wireless communications

Task 1.1- Evolution to Next-Generation Wireless Systems This task will focus on studying all technologies that are expected to transform the wireless communication by offering sustainable higher coverage, with less energy consumption and better spectral efficiency. The following technologies will be considered: Artificial Intelligence (AI), Machine Learning (ML), Visible Light Communication (VLC), Reconfigurable Intelligent Surfaces (RIS), Metaverse.

Task 1.2 - Security gaps in Next Generation Wireless Systems the Internet of Everything (IoE) paradigm, will come with new security issues also related to the 6G use cases, where the security requirements are stricter than 5G uses cases. New connected devices, encompassing underwater, air and ground nodes with high mobility, make the interconnection among the different systems more challenging, with an important impact on security. In this task, not only the gaps and new challenges related to the NG wireless systems will be considered and analysed, but new solutions based on decentralised security approaches will be studied, that can meet the new requirements of massive data and massive traffic processing of 6G networks.

Task 1.3 - AI and ML as a double sword in Next Generation Wireless Systems AI and ML will play a primary role in the NGWS, so much so that *network intelligentization* term has been coined, that will

replace the virtualization concept that characterised 5G networks. As a matter of fact, AI and ML are changing the cybersecurity world, for better or worse. Indeed, from one side AI and ML can be adopted to improve the performance of the networks, enhancing their robustness and resilience. On the other hand, they can be used to create sophisticated cyberattacks. New advancements in AI/ML-based attacks and countermeasures will be analysed in this task.

WG2 – A cybercrime perspective in wireless networks

Task 2.1 - Identification of cybercrimes Cybercrime is strictly tied to technological development and cybersecurity. Several aspects of human lives are automated, with an increased interaction of human beings and technology, and this trend is destined to grow in the next few years. In this task, the types of cybercrimes that will evolve and increase based on the technological advances considered in the WG1, will be considered.

Task 2.2 - Impact of cybercrime new types of cybercrimes will create an impact on business, National defence, and the awareness of the type of damages caused by cybercrime victimisation is paramount. The identification of potential victims is a tough while necessary task, for being able to advance on cybercrime security countermeasures.

Task 2.3 - Cybercrimes prevention techniques This task is strictly related to the previous ones. Based on different scenarios, new applications and services enabled by the new technological progresses realised in the context of NGWS, a profile analysis of the potential offender as well as the potential cybercrime with the associated level of effectiveness, will be considered to conceive advanced cybercrimes prevention techniques.

WG3 – Optimal Security approaches and their impact on the user

Task 3.1- Responsible Cybersecurity Algorithms The main purpose of this task is to achieve a holistic understanding of the relations between cybersecurity systems and humans. The starting point will be represented by an inclusive definition of the social responsibility of cybersecurity. Recently, some efforts in this direction have been accomplished to define Social Responsibility of AI. The rationale to introduce a similar concept for cybersecurity is threefold. From the one hand, in the previous WGs it was remarked an increasing tie between AI and cybersecurity, with a double use of it to increase the protection of communication systems as well as to improve the cyberattacks effectiveness. From another point of view, the increasing ubiquity of wireless networks in our daily life, intended for different population ages and involving more and more younger people, oblige to define new ethical principles and policies, to be established in consultation with lawyers. Finally, the interconnection between AI and cybersecurity is paramount for a protected society, and thus it is fundamental to include AI (and XAI) aspects in cybersecurity. New metrics accounting for the different aspects, namely legal, technical, and ethical need to be defined.

Task 3.2 – New metrics for ethical, legal and effective cyber solutions This task will be devoted to the highly challenging objective to account for the different aspects highlighted in T3.1 and in the other WGs, in order to define new metrics or at least guidelines for cyber solutions that have to be acknowledged as responsible by design, while keeping their effectiveness to protect the communication systems and make them robust to advanced attacks.

WG4 – Human factors in wireless security

This WG4 will focus on the specific attacks beyond the technical manipulation, for obtaining sensitive data. It will consider specific attacks based on the profile of potentially vulnerable users. It is based on the illegitimate acquisition of data, and it is related to WG1, where advanced wireless communication will be considered with a very high data rate for the communication making the offender able to steal a high amount of information in a reduced time. Moreover, based on the profile of the cybercriminal and how they select the targeted victims, new and more effective countermeasure techniques can be realised (in relation to WG2). Finally, the solutions for preventing a social engineer attack to be successful are much related to the impact of the solution on the final user as considered in WG3.

Task 4.1- Identification of human-centric models for personalised security solutions the main aim of this task is to understand how IT systems security and privacy can be guaranteed, without or with a minimal impact on the workflow ‘user. Security and privacy do not have to complicate the "normal" usage of the IT system and must be transparent for the final user. This challenging objective cannot be achieved, without the involvement of the final users, both in the design stage and the run-time phase. The final objective is to identify human-centric models, to design usable security systems that are consistent with the performance targets established in the WG1.

Task 4.2 – Evaluation of the impact of personalised cybersecurity solutions Impact of cybersecurity solutions on final users is crucial to the system security. Security and user experience are in a double-edged relationship. Users aim for their connected objects to be trustable and secured, but security must not have impact on user experience. Based on these reflections, it is clear how user involvement is needed to give it personalised security solutions and impact on it must be measured through specific parameters that can allow to establish the security guarantee level and if the solution will be successfully, namely accepted or not by the user.

Task 4.3 – Ethical aspects in personalised cyber-security solutions Personalised cybersecurity solutions and the definition of usable security solutions based on user-centric approaches, make ethical aspects considerations more challenging. Both in EU and USA, it is clearly established that independently of the undertaking processing, personal data must be protected. The definition of "personal data" is complicated in a highly connected cyber-world and with a massive use of AI/ ML based on a huge amount of data and "transforming" input data in such a way that their status of "personal" could evolve under algorithmic processing. Also, users must understand the use of their data to be aware of privacy and security risks. As a general consideration, personal data encompasses a large part of interconnected objects, making the design of personalised security solutions more complicated. These considerations lead us to introduce an Ethic Design approach to be adopted for conceiving personalised solutions and is the main objective of this task.

WG5 - Legal Factors in Cybersecurity Wireless Systems: a vertical approach

The proliferation of inter-connected objects and heterogeneous technologies need legal framework for security to adapt to. This aspect is strictly related to the WG1 and WG3. The evolution of heterogeneous communication technologies implies a huge amount of data and misuse of devices/objects or data can be turned into a criminal offense. There is in this sense a lack of international regulation, which will result in lack of clarity. This aspect is specifically related to the capacity of a nation to fight against cybercrime. This aspect is strictly related to WG2. With the expected technological developments, the final users need to be convinced about the trustworthiness of emerging technologies (in relation to WG1 and WG4). Recently, it has been highlighted as lack of unity in the Internet governance means lack of unity in cybersecurity". The cybersecurity world can be divided into two main categories: risk-based and control-based cybersecurity models. Risk-based model is completely open and with a complete exposure to all the threats, while the control-based is more conservative with prevention techniques, intellectual property protection, but with sub-optimal interoperability. In BEiNG-WISE, the two approaches will be explored in terms of cybersecurity solutions whose feasibility and impact will be analysed and evaluated. Whichever will be the adopted model, there is a clear need of more lawyers and cybercrime specialists to foster new collaborative opportunities and new approaches to cybersecurity.

Transversal Activities

TA1 – Training activities and STSMs. This activity relates to two tasks, namely training schools and STSMs. The former will be led by the Training School Coordinator, while the latter by the STSM Coordinator. ***TA1.1*** STSM organization. Promotion of joint research activities and interactions between the different Action members will be taken through funding of STSM. ***TA1.2*** **Training Schools** will be organised by the BEiNG-WISE participants and experts on the different disciplines. Transversal tutorials considering human factor and legal aspects on cybersecurity, will be organised. Training activities will explicitly prioritise YRI as target group.

TA2 – Dissemination, this activity will be led by the Science Communication Coordinator and will be based on the following tasks.***TA2.1*** Creation and maintenance of Action website, publicity, and diffusion of the news regarding the Action on social media as Facebook, LinkedIn, Twitter, etc. ***TA2.2*** Redaction of position/white paper. ***TA2.3*** Two Newsletters/year and the creation of a Leaflet summarizing the key points of the Action, to be distributed to final users and during the conferences. ***TA2.4*** Networking with scientific community: workshops and special sessions in conjunction with recognised international and national conferences will be regularly organised. ***TA2.5*** **Publications:** Action Members will be encouraged to contribute on joint publications in high target international journals and conferences. An edited book summarizing and highlighting the most important results achieved will be published as one of the Action outcomes. ***TA2.6*** A Special Interest Group (SIG), mostly composed by experts in standardization activities, will be set to produce specific recommendations for international bodies of standardization.

TA1 and **TA2** will contribute to meet the Capacity Building Objectives (CBO).

TA3 – Data Management, the main objective is to create the basis for sharing data, measurements,

simulation tools and to make the access open to the participants of the Action. Depending on the specific nature and the "sensitiveness" of the data, they can be also shared in open- source platforms. The tasks to be considered are: ***TA3.1*** definition of the rules for sharing data and how/where store them (i.e., database, open/partially open platforms, etc.). ***TA3.2*** pushing incentive actions for sharing data respecting the (pre)-established rules and maintaining of the database.

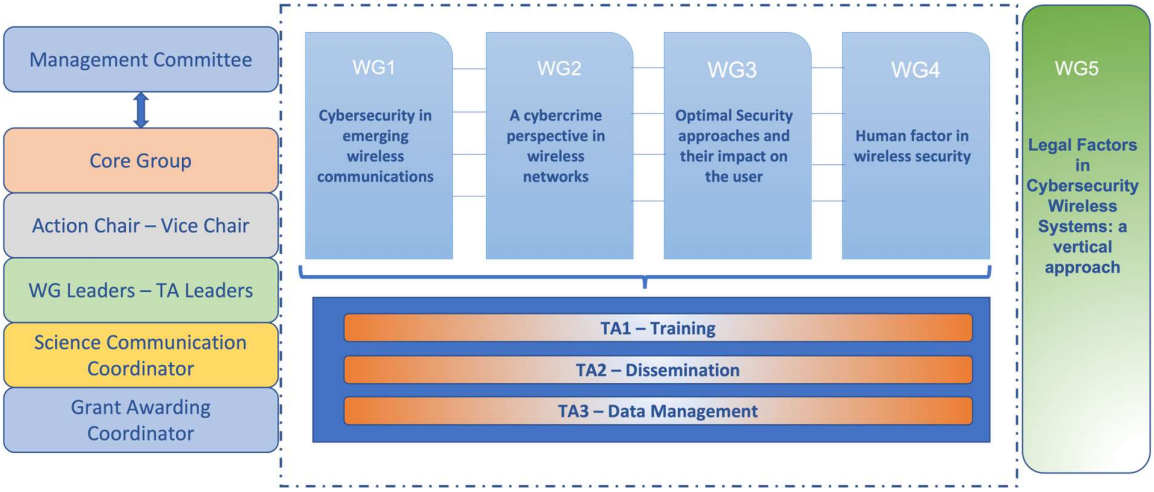

Figure 1 Pert Diagram and Organization structure of BEiNG-WISE Action

4.1.2. DESCRIPTION OF DELIVERABLES AND TIMEFRAME

D: Deliverable, DB: Database, OAB: Open Access Book, WP: White Papers

Deliverable n°	Related WG	Delivery date	Title
D1	TA2	M3	Action Website.
D2	All WGs	M6	Science Communication Plan.
D3	All WGs	M12	Report on state of the art of the field and its gaps.
D4	All WGs	M12	Data Management Plan and definition of joint publications, organization of special issues, international conferences.
D5	WG5 Legal factors	M24	Report with conceptual framework - cross layer approach defined for all the WGs.
D6	All WGs	M36	Report with the elaboration of solutions beyond the existing approaches for each domain considered stand- alone.
D7	TA3, WG1	M36	Database definition for the wireless features and the human characteristics.
D8	TA3 and all WGs	M48	Publication of a database merging wireless channel features and human being characteristics.
D9	All	M48	An Open Access Book will be delivered at the end of the Action, highlighting the main outcomes and the future directions.
D10	WG1, WG2 WG3	M48	Three White Papers (first one with WG1 in lead by M18; second with WG2 in lead by M36; third one with WG3 in lead by M48) addressing specific challenges and issues identified in the Action.

4.1.3. RISK ANALYSIS AND CONTINGENCY PLANS

The Management Committee, with the support of the Core Group, will closely monitor the progress of reaching the Action objectives and mitigate any risks to ensure timely provision of the deliverables. The following table shows the major identified risks and the corresponding mitigating actions and contingency plans.

Risk description	**P***	**I***	**Contingency plan**
Lack of time of the Action members: there is a risk that Action members do not have enough time to work in the different activities which consequently leads to a delay on the different tasks and deliverables.	M	H	• Encourage Your Researchers and Innovators (YRI) to lead the different working groups: these researchers need to foster their research career and therefore are the best positioned to actively promote the working group activities. • Have co-working group leaders in each working group: this person will oversee supporting the working group leader. YRI will also be encouraged to occupy this position. • Involve young researchers in the Action: the participation of PhD students will be encouraged in order to support or lead the achievement of the different tasks.
Creation and feeding of the database	M	M	The TA3 will start the activity based on existing databases and then, it will be proactive to relaunch the different partners in order to minimize the risk. In order to mitigate this risk, the Core Group will also be in contact with other EC projects consortia, to evaluate the possibility to rely on other databases as well.
Industrial partners too reluctant in onboarding and/or participation	M	M	Redefine scope for potential industrial partners. More networking activities with a focus on industry partners. Drastically lower entrance hurdle for new industry partners.
Lack of communication in the working groups: there is a possibility that communication within the Action is not adequate.	L	L	Bi-yearly meetings together with different specific communication channels (i.e., action website, social networks, etc) to alleviate this risk.
Restrictions due to Covid-19 situation	L	L	Remote tools will be used to perform the different activities planned in the Action should restrictions be adopted due to health crisis.
Gender imbalance	L	L	Include female participants in core decisions and organization. Reserve core functions to female participants. Re-allocate funds to increase and support the involvement of female researchers. Organize events and training schools targeting female researchers.

P = Probability*, I*= Impact H=High M= Medium, L= Low

4.1.4. GANTT DIAGRAM

	Year 1				Year 2				Year 3				Year 4			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
WG 1 - CyberSecurity in emerging wireless communications																
T1.1: Evolution to Next Generation Wireless Systems																
T1.2: Security gaps in Next Generation Wireless Systems																
T1.3: AI and ML as a double sword in Next Generation Wireless Systems																
WG 2 - A cybercrime perspective in wireless networks																
T2.1: Identification of cybercrimes																
T2.2: Impact of cybercrimes																
T2.3: Cybercrimes prention tecniques																
WG 3 - Optimal Security approaches and their impact on the user																
T3.1: Responsible Cybersecurity Algorithms																
T3.2: New metrics for ethical, legal and effective cybersolutions																
WG 4 - Human factor in wireless security																
T4.1: Identification of human-center models for personalized security solutions																
T4.2: Evaluation of the impact of personalized cyber-sercurity solutions																
T4.3: Ethical aspects in personalised cyber-security solutions																
WG 5 - Legal Factors (Transversal)																
Transversal Activities																
TA 1 - Training																
TA 2 - Dissemination																
TA 3 - Data Management																
MC Meeting	X			X				X				X				X
CG Meeting		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Deliverables																