INTERDISCIPLINARY SECURITY ASPECTS OF NEXT-GENERATION WIRELESS NETWORKS AND SYSTEMS

BEiNG-WISE: State of Research and Future Research Steps

2025

2025

Edited By

Valeria Loscri
Iraklis Symeonidis
Martin Griesbacher
Virginie Deniau
Davide Andreoletti
Alessandro Chiumento
Vesna Dimitrova
Isabella Corradini
Hartmut Aden
Marcel Moritz

This publication is based upon work from COST Action BEiNG-WISE (CA22104), supported by COST (European Cooperation in Science and Technology).

COST (European Cooperation in Science and Technology) is a funding agency for research and innovation networks. Our Actions help connect research initiatives across Europe and enable scientists to grow their ideas by sharing them with their peers. This boosts their research, career, and innovation.

cost
EUROPEAN COOPERATION IN SCIENCE & TECHNOLOGY

Funded by the European Union

https://cost.eu/

Citation: Valeria Loscri, Iraklis Symeonidis, Martin Griesbacher, Virginie Deniau, Davide Andreoletti, Alessandro Chiumento, Vesna Dimitrova, Isabella Corradini, Hartmut Aden, Marcel Moritz (editors), "Interdisciplinary Security Aspects of Next-Generation Wireless Networks and Systems: BEiNG-WISE: State of Research and Future Research Steps", Report, January 2025, DOI: https://doi.org/10.4393/opushwr-4464

COST Action 22104 - BEiNG-WISE

Interdisciplinary Security Aspects of Next-Generation Wireless Networks and Systems

BEING-WISE: State of Research and Future Research Steps

Valeria Loscri[1], Iraklis Symeonidis[2], Martin Griesbacher[3], Virginie Deniau[4], Davide Andreoletti[5], Alessandro Chiumento[6], Vesna Dimitrova[7], Isabella Corradini[8], Hartmut Aden[9], Marcel Moritz[10]

[1] *Inria Lille - France*
[2] *RISE Research Institutes of Sweden AB*
[3] *Research Industrial Systems Engineering (RISE) GmbH - Austria*
[4] *University Gustave Eiffel - France*
[5] *University of Applied Sciences and Arts of Southern Switzerland - Switzerland*
[6] *University of Twente - Netherlands*
[7] *Ss. Cyril and Methodius University in Skopje - North Macedonia*
[8] *Themis Research Center - Italy*
[9] *Hochschule für Wirtschaft und Recht Berlin - Germany*
[10] *Université de Lille - CERAPS UMR 8026 - France*

Abstract

Next-Generation Wireless Networks and Systems (NGWN-Ss) are foundational to realizing a seamlessly connected world, unlocking transformative services and applications. However, the pervasive connectivity of NGWN-Ss introduces complex and new challenges in cybersecurity and privacy. Key concerns include the vast volumes of data exchanged, evolving user interactions with advanced technologies, and the increasing sophistication of cybercriminals utilizing these technologies for malicious purposes. The BEiNG-WISE Action highlights critical gaps in technologies, legislation, ethical considerations, and the integration of user-centric perspectives into technological development. Current regulatory frameworks lag behind the rapid pace of technological advancement, often neglecting the intricate needs of end-users. During the first year of collaborative efforts, the WGs identified key interdependencies across technical, legal, and sociological dimensions, underscoring the need for multidisciplinary approaches to address cybersecurity challenges comprehensively. This document synthesizes findings from various domains, ranging from the technical evolution of wireless systems (WG1) and the sociological dynamics of cybercrime (WG2) to innovative cybersecurity frameworks (WG3) and user-centered methodologies (WG4). A central theme is the interplay between advanced technology, human factors, and the evolving legal landscape (WG5). The chapters explore these connections and provide a foundation for re-imagining cybersecurity through a holistic, responsible-by-design approach. By integrating human, ethical, and regulatory dimensions, this work sets the foundations for novel cybersecurity solutions that balance technological innovation with societal impact.

Keywords: Security, Privacy, Wireless Communication, 5G/6G, Cyber Crime, Responsible, Human Factor, Legal and Ethical Factors

Contents

Glossary

AI Artificial Intelligence. 5, 8, 47, 60, 61

AR Augmented Reality. 9

CFR Charter of Fundamental Rights. 68

CoE Council of Europe. 68

ECHR European Convention on Human Rights. 68, 69

ENISA European Union Agency for Cybersecurity (ENISA). 70

ERCI European Repository of Cyber Incident. 30

GDPR General Data Protection Regulation. 68, 69

ICT Information and Communication Technology. 29

KPIs Key Performance Indicators. 46

LIME Local Interpretable Model-Agnostic Explanations. 47

ML Machine Learning. 5, 8, 60, 61

NGWN-Ss Next-Generation Wireless Networks and Systems. 1

OCSEA Online Child Sexual Exploitation and Abuse. 29

SDN Software-Defined Networking. 46

SHAP SHapley Additive exPlanations. 47

SMEs Small and Medium enterprises. 30

VR Virtual Reality. 9

WG Working Groups. 4

WGs Working Groups. 1

XAI Explainable AI. 47

0.1 Preliminaries - Background

This first deliverable represents the first year of activities of COST Action BEiNG-WISE. In particular, it is a joint effort of members of different Working Groups, with some members belonging and contributing on different Working Groups (WG) activities.

The key point of BEiNG-WISE, as the acronym suggests - Behavioral Next Generation in Wireless Networks for Cyber Security - is to bring the human and ethical factors in the technical solutions, be able to understand the extent and measure the impact of this integration.

When human being is related to network and communication security aspects, its dual nature in the cybersecurity context is quite straightforward. Indeed, human being can play the malicious role, by exploiting the technology for (cyber) criminal applications, or it is the weak ring of the chain, by making error or not implementing in a proper way the security solutions.

Based on that, after introducing a first Working Group on technical aspects related to the evolution of wireless communication networks, the WG1 - Cybersecurity in emerging wireless communications, it seemed natural considering the cyber crime activities, a condition sine qua non for cyber security practitioners to exist. The WG2 - A cybercrime perspective in wireless networks, traces the main theories that have been developed over time regarding the main rationale for committing cyber criminal activities. If, from one side, cyber crimes are considered, as mentioned before, the project relies on the double nature of human being, playing the role of offender or victim. That was a turning point to realize things concerning modern connected technologies, cyber security aspects are more complex and "just" considering double nature of human beings does not do justice to the complexity of the context and does not allow us to capture the subtleties necessary to advance in the complex connected world. It is for this reason, the other two WGs, the WG3 - Optimal security approaches and their impact on the user and WG4 - Human factors in wireless security, seemed necessary to better capture various facets of security challenges in modern communication technologies. In particular, in WG3 the "responsible by design" concept is considered as key factor for cyber security, and it is noticed as this concept has been always associated to Artificial Intelligence (AI) and Machine Learning (ML), but never considered for cyber security. This is very related, but still different from the Cyber Physical Human System (CPHS) introduced in WG4, where the interaction of the user with the technology is considered and for which it is paramount to account for psychological and sociological factors. On the other hand, these concepts are also fundamental to be considered in WG2, where an inspection of the main factors pushing the cybercriminal activity are examined, also from a sociological and psycological perspective. Last but not least it has been realized that the concept of cyber security, when the human factor is considered, is closely related to legal and ethical factors, that bring the attention on the necessity for lawyers and ethical practitioners, to get closer to the technology, to better understand it, in order to advance on regulations that appear with some important gaps. An important reflection in this sense is related to the apparent paradox of the ubiquitous technology, which tends to globalize the whole world, against fragmented and different laws existing in the different countries and that impacts on the way the technology is used and on the legal usage of the technologies.

An important premise, before delving into the different more detailed chapters, is that this first year of activities marks a first milestone, with an effort to make converging multidisciplinary domains, often using different vocabulary. The common thread is clear; the users are human, they are the main actors in the connected world. The technologies evolve and the way the user uses may have an impact on the user itself and on other users. Cyber security solutions should not be limited to simple technological methods, but should be able to capture these elements. On the other hand, who says technology also says "use and misuse" of technology. This aspect should be, in some ways, captured by security approaches. On the other hand, it is a kind of paradox, but the voluntary misuse of the technology, e.g. to create cyber attacks can be easier than the integration of protection, since no rules and regulations hinder the creation of advanced attacks or cyber criminal actions, while protection has to be realized by following not clear rules and regulations. This means that the technological evolution should be strictly followed by an evolution in the regulations, in order not to hinder the development of necessary protection. This closes the circle, but at this point we are quite lost and we realize that something more structured has to be developed to permit the putting on the table all these factors.

This premise represents a mandatory section to present the main very high ambitious goals of BEiNG-WISE, and provides the needed background to delve in the next chapter of this first deliverable.

0.2 Introduction

The main aim of BEiNG-WISE project is to advance towards a structured integration activity of the key factors of cyber security communication technologies. It is worth mentioning that this 1st year deliverable has not the scope to make the different actors of the project working in a structured way, but to reveal the potential points of interaction, and making the different pieces of the puzzle to be combined in order to obtain a unique structured vision of cyber security. The different sections of the deliverable focus on the most recent state-of-the-art on the specific domains of the WGs and have been conceived in a way to highlighting the potential interconnections among the different WGs.
In particular, WG1 retraces the evolution of wireless-based connected systems, by considering the integration of recent technologies as Artificial Intelligence (AI)/Machine Learning (ML) approaches. This WG1 contribution proposes an interesting categorization of the wireless connected systems, based on the bandwidth and range, encompassing in this way the most representative communication technologies. Chapter 1 is then devoted to the security gaps in the next-generation wireless systems, and this contribution includes "technical" aspects, without referring to neither human factors nor legal/ethical aspects, revealing the "traditional" attitude of technical people to keep regarding on technical aspects to fill in the gaps. In this context, the human factor appears in the very last part, considering the privacy challenges in next-generation networks, implying the consideration of a human being as potential victim. This concept is, on the other hand, also a connection point with the legal aspects developed in Chapter 7, where important points related to connected devices, such as data minimization, are discussed. This first connection point, on the other hand, permits one to put the focus on a fundamental aspect related to the connected world, namely the data. Data will be with a primary role in this Action, since it is at the basis of the attacks, it permits the victimization of cyber users. The adopted approach in WG1, while important from a technical point of view, since revealing interesting limitations in current solutions, with difficulties to cope with the fast technological evolution, also reveals its main limitations, since the main actor of the connected world, namely the user, is quasi not at all considered.

In the section concerning the WG2, the cybercrime aspects are considered, in order to understand if and how the knowledge of cybercrime can be exploited to improve the security aspects and face the open security challenges. The first interesting point that can be noticed is that by providing the definitions of cybercrime, a temporal approach following the evolution of technology is adopted. Indeed, in WG1 and WG2, it is notable that that the technological evolution is a common thread. In the first case, it is considered in terms of evolved attacks, while in the second case, it shows how the concept of cybercrime evolves with technological evolution, revealing an interesting parallel path.

On the other hand, the different theories presented and developed in chapter 2, show a tight relation with the legal factors developed in chapter 7.

By definition of crime: *"an action or omission that constitutes an offense that may be prosecuted by the state and is punishable by law"*, is related to law and regulation. Moreover, when the different cybercrimes prevention theories are explained, an interesting observation is related to the fact that cybercrimes theories are generally developed with three main elements/factors: -) a motivated offender, -) a suitable target, and -) absence of capable guardianship. In someway, these aspects can be considered from a technological point of view, permitting important advancement, with a completely new approach.

Contributions concerning the WG3 activities represent the "natural" and straightforward convergence of the other WG activities and outcomes. Introduces a paramount concept: **responsible cybersecurity**, that integrate new and unseen dimensions with respect to the traditional cybersecurity landscape. Although the concept of "responsible by design" has been investigated in respect of AI/ML, it has never been considered from a cyber security point of view. The concept of responsible is multifaceted and develops in different dimensions, by keeping the security concept the gravitational point. Lastly, data governance is introduced, creating a natural connection with the legal aspects related to managing data (WG5), considering a natural trend towards data sovereignty permitting a better development and control on data minimization application policy. The different dimensions are developed, starting from security, privacy, sustainability, inclusion, transparency, incentive compatibility, and data governance. Even some of the concepts are also analyzed in the previous sections, in this part the final user, namely the human being, plays a primary role, and the dimensions are evaluated in terms of impact on the user. This represents an early-stage tangible effort toward the integration of human factor in the cyber security domain.

In the chapter related to WG4 activities, the final user is again the key player in the connected world, by explicitly considering user-centric approaches. This WG4 is conceived with the main purpose to involving from the early-stage the users in the loop. The main rationale is quite simple and intuitive, if a solution is optimal from a technological point of view, but not well accepted by the final user, it will likely not be used. This can be translated with the clear need to build cyber-security solutions around the human-being, by trying as much as possible to account for different needs, and way to interact with the technology. In this sense, new research trend, explicitly revealing gender bias of cyber-security solutions, will allow to focus on key factors to be considered when the technology is developed. On the other hand, this chapter also retraces the important steps of final user needs, by including concepts as invisibility, explainability. Since technology is today pervasive and present in daily aspects as well as in sensitive infrastructures, these concepts cannot be just considered as an added-value, but have to be integrated as mandatory properties of the solutions. An explicit involvement of the end-user in the technology conception, will enable a better acceptance as well as an improved comprehension and experience. The ethical aspects become in this juncture a key point, making a clear clue with the WG5 activities.

Indeed, it has not been by chance, that the WG5 activities have been considered transversal in respect of all the WGs. In the chapter 7 the fundamental human rights are evoked, and the main challenge for this Action will be how to translate them with a technical and technological perspective, and how to integrate them by design in the cyber-security solutions. Moreover, by a quick look in the laws and regulation in cyber security matter, it clearly emerges the limitations and fragmentation aspects currently existing.

Chapter 1

WG1: Cybersecurity in emerging wireless communications

An Braeken[1] , **Alessandro Brighente** [2] , **Periklis Chatzimisios**[3], **Christophe Gransart**[4], **Miranda Harizaj, Salko Kovacic** [6], **Mustafa Mustafa**[7], **Vinod Puthuvat**[2], **Iraklis Symeonidis**[8] [1]

[1]Vrije Universiteit Brussel - Belgium
[2]University of Padua - Italy
[3]International Hellenic University - Greece
[4]University Gustave Eiffel - France
[5]Universiteti Politeknik I Tiranes - Albania
[6]Univerzitet Dzemal Bijedic u Mostaru - Bosnia and Herzegovina
[7]The University of Manchester - United Kingdom
[8]RISE Research Institutes of Sweden AB

[1]Authors sorted alphabetically by the surname

1.1 Introduction

In this chapter, we discuss the evolution of wireless communication systems towards new-generation technologies combined with the use of AI and ML, which bring us unprecedented opportunities for connectivity, efficiency, and new applications in all connected industries. However, the rapid evolution of these systems also opens the door to increased vulnerabilities, making cybersecurity a key concern. With the widespread use of the Internet of Things (IoT) and advanced mobile networks in verticals like industry, smart cities, healthcare, and autonomous vehicles, securing wireless communications has never been more crucial than now.

Next-generation wireless systems, including 5G, future 6G, and Wi-Fi 7/8 networks, represent connectivity, speed, and performance leaps. These technologies introduce advanced features such as ultra-low latency, massive machine-type communication, and enhanced mobile broadband. These improvements promise significant benefits, but they also present new security challenges/flaws that remain unaddressed since security has not kept pace with technological innovation.

For example, the increased number of connected devices through the IoT expands the attack surface, making systems more vulnerable to Distributed Denial of Service (DDoS) attacks, unauthorized access, and data breaches. Furthermore, the sheer complexity and increased reliance on software-driven architectures, virtualization, and edge computing introduce new attack surfaces that cybercriminals can exploit. In addition, the decentralization of network functions, along with virtualized environments such as Software-Defined Networking (SDN) and Network Functions Virtualization (NFV), introduces vulnerabilities that legacy systems were not exposed to in the past. Protecting these networks requires evolving approaches to security that consider both new and existing threats.

AI and ML have emerged as powerful tools to improve the performance and security of wireless networks. These technologies enable proactive threat detection, network optimization, and automated response mechanisms. However, AI and ML also present significant risks. Cybercriminals can use these same technologies to launch more sophisticated and unpredictable attacks, making them a double-edged sword. For example, adversarial machine learning can be used to deceive network defenses, while AI-driven attacks can overcome traditional security measures, leaving many systems vulnerable.

1.2 Task1: Evolution to Next-Generation Wireless Systems

The landscape of wireless technologies can be split into four large categories based on the dimensions of range and bandwidth capability: high bandwidth - high range, low bandwidth - high range, low bandwidth - low range, and high bandwidth - low range. In each of these categories, significant progress has been made during the last years. In some of the categories, this progress has been more disruptive than in others. The four categories are shown in Fig. 1.1 and summarized below.

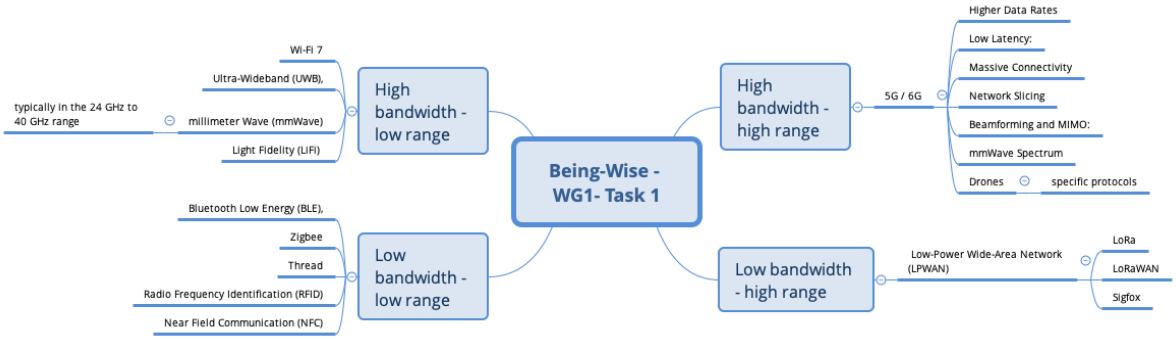

Figure 1.1: The big picture of the Wireless Systems.

1.2.1 High bandwidth - high range

The evolution in this domain had the aim of meeting the growing demand for higher data rates, lower latency, increased reliability, and enhanced connectivity for a wide range of applications and services. This evolution encompasses several generations of wireless technologies, each introducing new features, capabilities, and standards to improve wireless communication systems.

The first generation of cellular networks (1G), introduced in the 1980s, provided analog voice communication with basic mobile telephony services [225]. In the Second Generation (2G), digital voice communication has been added, enabling features such as SMS messaging and improved spectral efficiency [225]. The Third Generation (3G) introduced higher data rates and support for multimedia services such as video calling and mobile internet access [225]. In the Fourth Generation (4G) significant improvements have been made in data rates, spectral efficiency, and network capacity, enabling high-speed mobile broadband services, multimedia streaming, and mobile gaming [225]. Currently, the Fifth Generation (5G) represents the next leap in wireless technology, aiming to deliver ultra-fast data rates, ultra-low latency, massive connectivity, and improved network reliability [225]. The following key features and innovations can be distinguished.

- Higher Data Rates: 5G can offer peak data rates up to 20 Gbps, enabling faster downloads, streaming, and real-time communication.
- Low Latency: 5G can reduce latency to as low as 1 ms, enabling responsive applications such as online gaming, Augmented Reality (AR), and Virtual Reality (VR).
- Massive Connectivity: 5G supports massive IoT deployments, connecting billions of devices and sensors for applications such as smart cities, industrial automation, and healthcare monitoring.
- Network Slicing: 5G introduces network slicing, allowing operators to partition the network into virtual slices with customized characteristics for different use cases and applications.
- Beamforming and MIMO: 5G utilizes advanced antenna technologies such as beamforming and massive MIMO (Multiple Input Multiple Output) to improve coverage, capacity, and spectral efficiency.
- mmWave Spectrum: 5G utilizes a higher-frequency millimeter-wave (mmWave) spectrum to deliver high data rates and increased network capacity, although with a shorter range and limited penetration through obstacles.

Future horizons, called Beyond 5G (B5G) and 6G, are also currently being investigated [241]. B5G encompasses advancements beyond 5G, focusing on further improvements in data rates, latency, reliability,

and connectivity. Technologies may also include enhancements in spectrum utilization, AI-driven network optimization, and integration with emerging technologies such as edge computing and satellite communication.

6G envisions the next paradigm shift in wireless communication, aiming to unlock new capabilities such as terabit-per-second data rates, sub-millisecond latency, ubiquitous connectivity, and seamless integration with emerging technologies such as AI, blockchain, and quantum computing.

In the same category are drone communications, which are in the 2.4GHz and 5GHz free bands [17]. However, the new generations of drones are not based on Wi-Fi to exchange command/control messages between the remote command and the drone or for video feedback. The protocols are very often proprietary and are mainly based on Frequency-Hopping Spread Spectrum (FHSS).x Drones can communicate up to 20 km with the remote command and transmit also the video captured by the drone.

The evolution to next-generation wireless systems represents a continuous journey of innovation and advancement, driven by the evolving needs of users, businesses, and society as a whole. Each generation builds upon the achievements of its predecessors, pushing the boundaries of what is possible in wireless communication and paving the way for a more connected and digitally empowered future.

1.2.2 Low bandwidth - high range

The evolution to next-generation wireless systems for long-range and low bandwidth focuses on enhancing connectivity and extending the reach of wireless communication over significant distances while accommodating applications that require relatively low data rates. This evolution involves advancements in technologies and protocols tailored to address the specific requirements of long-range, low-bandwidth communication.

These wireless systems often utilize technologies optimized for extended coverage and reliable communication over large geographic areas. These include Low-Power Wide-Area Network (LPWAN) technologies [46] such as LoRaWAN and Sigfox, which are designed to provide long-range communication with low power consumption, making them suitable for applications such as smart agriculture, environmental monitoring, and asset tracking. Also, Narrowband IoT (NB-IoT) is a cellular IoT technology standardized by 3GPP, offering long-range communication over existing cellular networks with low data rates, making it suitable for applications such as smart meters, remote monitoring, and utility infrastructure. Another technology is the satellite communication system, which can provide ubiquitous coverage and long-range connectivity, enabling communication in remote or inaccessible areas where terrestrial networks may be unavailable or impractical.

Optimized protocols and standards are leveraged to maximize efficiency and reliability. Some protocols are designed specifically for long-range communication, such as LoRaWAN's chirp spread spectrum modulation or NB-IoT's narrowband communication to extend coverage and minimize power consumption. Other protocols are optimized for low-bandwidth communication often employing efficient packetization and framing techniques to minimize overhead and maximize the payload size, reducing the impact of protocol overhead on the available bandwidth. Also, error correction techniques have been enhanced, including Forward Error Correction (FEC) to improve reliability over long-distance communication links, reducing the impact of noise and interference on data transmission and reception.

In addition, a lot of focus has been given to energy-efficient design and operation to prolong battery life and reduce power consumption. This includes the use of radio transceivers with low-power sleep modes and efficient wake-up mechanisms to minimize energy consumption during idle periods, extending battery life in battery-powered devices. Also, effective power management techniques are implemented like duty cycling, adaptive transmission power control, and energy harvesting enabling efficient utilization of energy resources and reducing power consumption in wireless devices.

To extend coverage and optimize the range to reach remote or distant locations, several innovative techniques have been developed in different areas. First, there has been lots of progress in antenna design and placement, where directional antennas, antenna diversity, and smart antenna technologies help optimize coverage and extend the range of wireless communication systems, especially in challenging environments with obstacles or signal attenuation. Second, implementing relay nodes and mesh networking topologies enables communication over longer distances by relaying data between distant nodes, extending the effective coverage area, and improving connectivity in hard-to-reach locations. Finally, also selecting

appropriate frequency bands and optimizing channel planning help minimize interference and maximize signal propagation, improving communication reliability and range in long-range wireless systems.

Thanks to these advancements in technologies, protocols, design principles, and operational strategies tailored to meet the specific requirements of long-range communication with low data rates, it becomes possible to enable reliable, energy-efficient connectivity over extended distances, unlocking new possibilities for applications and services in remote, challenging, or resource-constrained environments.

1.2.3 Low bandwidth - low range

The evolution to next-generation wireless systems for low range and low bandwidth focuses on providing connectivity solutions optimized for short distances and applications with modest data requirements. These systems are designed to cater to use cases where the coverage area is limited, and the amount of data being transmitted is relatively small. Examples of applications are in consumer electronics, IoT, industrial automation, and smart infrastructure. There are many technologies in this domain, such as Bluetooth Low Energy (BLE), Zigbee, Thread, Radio Frequency Identification (RFID), Near Field Communication (NFC), etc [29].

Each of these technologies provides continuously new versions, including improvements of features aimed at enhancing connectivity, energy efficiency, security, usability, scalability, and interoperability.

1.2.4 High bandwidth - low range

The evolution to next-generation wireless systems for short-range networks with high bandwidth focuses on providing fast, reliable, and high-capacity connectivity for a variety of applications, including multimedia streaming, gaming, augmented reality (AR), virtual reality (VR), and ultra-low-latency communication.

One of the most important technologies in this domain is Wi-Fi. Wi-Fi 7 [69] is the latest iteration of the Wi-Fi standard, designed to deliver faster speeds, increased capacity, and improved performance in dense environments. It is offering remarkable advancements over its predecessors Wi-Fi 6 and Wi-Fi 6E, to meet our growing requirements. Differences between Wi-Fi and 5G/6G are discussed in [181].

Another important technology in this area is Ultra-Wideband (UWB), which utilizes a large bandwidth to transmit data rates of up to several gigabits per second over short distances with high precision and accuracy, making it suitable for applications such as wireless docking, file transfer, and multimedia streaming. UWB technology also enables precise indoor positioning and location tracking with centimeter-level accuracy, facilitating applications such as asset tracking, indoor navigation, and context-aware services [195].

Recently, also millimeter Wave (mmWave) technology utilizing high-frequency radio waves to transmit data over short distances with very high bandwidth, has grown in popularity [218]. mmWave technology offers extremely high data rates, reaching multi-gigabit speeds, making it suitable for applications such as 4K video streaming, VR/AR content delivery, and high-resolution gaming. The signals are highly directional and require line-of-sight communication between devices, making them ideal for short-range wireless networks in controlled environments such as stadiums, convention centers, and campus networks. 5G networks utilize mmWave frequencies (typically in the 24 GHz to 40 GHz range) to deliver ultra-fast data rates and support bandwidth-intensive applications. Mobile operators and technology companies have invested in mmWave infrastructure to deploy the 5G networks in urban areas and dense urban environments, where high-capacity, short-range communication is required to meet growing data demand.

Also, the Light Fidelity (LiFi) technology falls in this category of low range and high bandwidth [71]. The technology offers very high data rates, typically in the range of multiple gigabits per second (Gbps) or even higher, and is a short-range communication technology, for which the effective data range depends on factors such as the intensity of the light source, the sensitivity of the receiver, and environmental conditions. Typically, Li-Fi operates within a room or a confined area where light can be effectively transmitted and received. Recent advancements in Li-Fi technology have focused on improving performance, reliability, and practicality for a wide range of applications. As Li-Fi can complement 5G networks by providing high-speed, low-latency connectivity in indoor environments, urban areas, and other locations where traditional wireless technologies face challenges, researchers are exploring the integration of Li-Fi technology with 5G networks to create seamless and heterogeneous wireless communication ecosystems.

Thanks to these technological advancements, new opportunities for multimedia streaming, gaming, AR/VR experiences, and other immersive and data-intensive applications in various industries and sectors become possible.

1.3 Task2: Security Gaps in Next-Generation Wireless Systems

This section highlights the security gaps and challenges present in next-generation wireless systems, particularly in 5G and 6G technologies. While advancements in connectivity have revolutionized communications, significant security deficiencies remain. Key issues include vulnerabilities in protocol implementations, weak authentication, insufficient encryption, and the risks posed by IoT devices and supply chains. To counter these threats, an array of advanced security solutions, such as post-quantum cryptography, multi-factor authentication, and AI-based intrusion detection systems, are being actively developed and increasingly integrated into next-generation wireless networks. These solutions are designed to address the complex security challenges posed by 5G and 6G systems, ensuring robust protection against evolving cyber threats. While some of these technologies have already seen partial deployment, continuous enhancements, and broader implementation are necessary to fully safeguard the infrastructure and maintain the integrity of future wireless networks.

1.3.1 Current trends on security and privacy risks 5G/6G

In the dynamic evolution of wireless communication, each successive generation of networks has heralded significant technological advancements, fundamentally reshaping our connectivity and interactions. From the rudimentary analog systems of 1G to the highly sophisticated digital capabilities of 5G [8], the development of mobile networks has been marked by continuous innovation and growing demands for faster, more reliable, and more efficient communication. With the global roll-out of 5G setting the stage for an interconnected world, attention now turns towards the enhancement of the sixth-generation (6G) era [18] and dawn (7G) era. Even with the progress made in next-generation wireless systems, there remain notable security shortcomings and hurdles demanding attention to uphold the integrity, confidentiality, and accessibility of these networks [244]. A summary of the most critical security vulnerabilities identified in the next-generation wireless systems is provided in Table 1.1.

Table 1.1: Major Security Deficiencies and Their Associated Risks in Next-Generation Wireless Systems

No.	Category of Deficiencies	Description	Potential Risks
1.	**Vulnerabilities in Protocol Implementations** [177, 207, 212]	Complex protocols may have security gaps due to implementation errors, making networks vulnerable to attacks.	- Unauthorized access - Denial of Service (DoS) - Jamming - Data breaches
2.	**Weak Authentication and Authorization** [177, 207]	Ineffective mechanisms can lead to unauthorized access, eavesdropping, especially in IoT environments.	- Data theft - Misuse of resources - Unauthorized device control
3.	**Insufficient Encryption and Data Protection** [177, 207]	Lack of robust end-to-end encryption leaves data susceptible to interception and eavesdropping.	- Data leaks - Identity theft - Communication interception
4.	**Security of IoT Devices and Endpoints** [177, 207, 212]	Many IoT devices have limited computational power and weak security, creating vulnerabilities in the network.	- Botnet formation - Network infiltration - Data exfiltration - Jamming
5.	**Supply Chain Risks** [177, 212]	Dependencies on diverse HW/SW vendors expose networks to risks from counterfeit components or compromised updates.	- Supply chain attacks - System compromise - Backdoor exploits
6.	**Privacy Concerns and Data Misuse** [163, 177, 207]	Massive data collection in 6G systems raises concerns over user privacy and potential misuse of personal information.	- Identity theft - Unauthorized profiling - Privacy violations
7.	**Emerging Threats and Cyberattacks** [163, 177, 207]	Next-generation wireless systems are prime targets for sophisticated attacks, including ransomware, and zero-day exploits.	- Financial losses - System sabotage - Espionage
8.	**Regulatory Compliance and Legal Challenges** [177]	Obligations to adhere to multifaceted regulatory frameworks related to data protection, communications, and cybersecurity.	- Data privacy violations - Cross-border data flow issues - IP disputes - Supply chain compliance

1.3.2 Approaches on solutions for 5G/6G

In the realm of next-generation wireless systems, various cybersecure technologies and solutions are being developed and deployed to enhance network security and address the sophisticated threats in 6G and beyond. These solutions not only ensure the integrity and availability of network infrastructure but also focus on privacy-preserving technologies to protect user data and maintain confidentiality. These

Table 1.2: Current cybersecurity technologies and solutions in next-generation wireless systems

Category	Technology/Solution	Description	Mitigated Threats from Table 1.1
Encryption and Data Protection	**Post-Quantum Cryptography (PQC)** [177, 191, 207, 212]	Strengthens encryption methods to protect against quantum computing attacks, ensuring long-term data security.	6, 7, 8
	End-to-End Encryption (E2EE) [177, 212]	Encrypts data across the entire transmission path, protecting against interception and eavesdropping.	2, 3, 4, 7
Authentication and Authorization	**Multi-Factor Authentication (MFA)** [177, 207]	Requires multiple forms of verification (e.g., passwords, biometrics) to ensure stronger user authentication and reduce unauthorized access.	1, 2, 6, 8
	Zero Trust Architecture (ZTA) [56, 177, 212]	Assumes that no device or user is trusted by default, applying strict identity verification at every network access point.	1, 2, 6, 8
Network Security	**Network Slicing Security** [144, 177, 212]	Ensures that individual network slices are isolated, preventing attacks from spreading across slices in 5G/6G networks.	1, 2, 3, 5, 7
	Software-Defined Networking (SDN) [177, 212]	Centralizes network control, improving the ability to detect, mitigate, and respond to security threats in real-time.	1, 2, 3, 4, 5, 7
IoT Security	**IoT Security Frameworks** [177, 207, 212]	Implement security protocols specific to IoT devices to protect them from being exploited as entry points for network attacks (e.g., botnets).	4
	Lightweight Cryptography [177, 207]	Ensures security for devices with limited computational power by using less resource-intensive crypto algorithms.	4
AI & ML	**Intrusion Detection Systems (IDS)** [163, 177, 207, 212]	Uses machine learning algorithms to detect and respond to unusual or malicious activity within the network, identifying threats faster and more accurately.	1, 2, 3, 4, 5, 6, 7, 8
	Behavioral Analytics [163, 177, 207, 212]	Monitors user behavior and flags deviations from normal patterns, enhancing the detection of insider threats and anomalies.	1, 2, 3, 4, 6, 7
Privacy Protection	**Federated Learning** [56, 163, 177, 191, 207]	Ensures data privacy by enabling AI models to be trained across multiple decentralized devices without transferring raw data to a central server.	1, 2, 3, 4, 5, 6, 7, 8
	Differential Privacy [163, 177, 207]	Adds noise to user data to ensure individual data points cannot be traced back to users, protecting personal information during data analysis.	1, 2, 3, 6, 7, 8
Edge and Cloud Security	**Secure Edge Computing** [144, 163, 177, 207, 212]	Secures data processed at the edge of the network, protecting against attacks targeting edge devices or compromising sensitive localized data.	1, 3, 4, 6, 7, 8
	Cloud Access Security Brokers (CASB) [163, 177, 207, 212]	Monitors data flows between on-premise and cloud infrastructure, enforcing security policies to safeguard sensitive data and prevent leaks.	2, 3, 6, 7, 8
Supply Chain Security	**Blockchain for Supply Chain** [177, 191, 212]	Utilizes blockchain to verify and secure the integrity of hardware and software components in the supply chain, reducing risks from counterfeit or malicious products.	5, 7, 8
Threat Detection and Response	**Extended Detection and Response (xDR)** [163, 177, 212]	Integrates multiple security products into a unified system, providing better threat detection across the entire IT environment, including network, cloud, and endpoints.	1, 2, 3, 4, 5, 7
	Threat Intelligence Platforms (TIPs) [163, 177, 207]	Aggregates real-time threat data from various sources to provide insights into emerging threats and vulnerabilities, enabling proactive defense.	1, 2, 3, 4, 5, 7

advanced methods are crucial to secure communication channels and meet evolving regulatory demands. Some of the key technologies are listed below.

By leveraging the outlined cybersecurity technologies and solutions in Table 1.2, next-generation wireless systems can significantly improve their security posture, addressing threats to ensure the integrity, confidentiality, and availability of wireless networks and services. Additionally, the incorporation of privacy-preserving technologies helps protect user privacy, build trust, and comply with regulatory requirements while still enabling the delivery of innovative services and applications in 6G and beyond. This approach provides a comprehensive defense against emerging cyber risks, promoting secure and trusted network environments.

1.4 Task3: AI and ML as a double sword in Next Generation Wireless Systems

The advances of AI and ML in the last decade increased the intelligence in wireless networks at different layers of the ISO/OSI stack. Indeed, we find examples of how AI/ML-based controllers can be used for scheduling, resource allocation, user tracking, mobility management, and energy savings. Despite the huge advantages provided by AI and ML techniques, it is nowadays clear that their role in the cybersecurity posture of their domain of application is paramount. Indeed, such models have been proven to be both a possible solution to increase the security and privacy of certain applications and a weak point that an attacker can leverage to disrupt the system [37, 38]. In this section, we provide examples from both the defense and attack point of view and discuss how AI/ML solutions should contribute to the enhanced security of the next generation of wireless networks.

1.4.1 Applications of AI and ML in Wireless Networks

The use of ML and AI techniques in wireless communications brought multiple advantages. The use of learning-based techniques provides a means to efficiently solve classical optimization problems in wireless networks. Examples include the dynamic allocation of power and spectrum [172], the optimal positioning of base stations [41], coverage and capacity planning [150], and network traffic pattern prediction [155]. Furthermore, classical signal processing algorithms rely on signal and channel models to perform tasks such as encoding and decoding [81], channel estimation and equalization [127], and direction of arrival estimation [250]. Thanks to learning-based techniques, it is possible to replace these analytical models with data-driven models to enhance the performance of these algorithms and reduce errors.

The data-driven decision capabilities of ML and AI algorithms allow for tasks such as intrusion and anomaly detection [234], failure prediction [26], and health monitoring [145] to be completely automated. Furthermore, this allows for the development of a general network that will adapt to the context where they are deployed. Lastly, AI and ML algorithms can efficiently leverage the data collected at the edge of the network to optimize the services provided to users, reducing latency and increasing throughput [82, 112, 242]. At the same time, this data-based approach allows for the efficiency differentiation of different types of traffic with the consequent assignment of different network resources (slicing) [216].

1.4.2 Attacks to AI/ML-Based Next Generation Wireless Systems

The evolution of AI and ML algorithms has recently been accompanied by the development of sophisticated attacks able to evade the tasks assigned to learning-based algorithms. A basic categorization of these attacks divides them into two sets [7]: i) attacks during the training phase, ii) and attacks during the testing phase.

Attacks during the training phase: Attacks during the training phase include *model poisoning* and *trojan injection*. With model poisoning, the attacker inserts malicious data into the training set to influence the decisions of the model in the successive testing phase. The attacker may either insert targeted values, for which they know the desired effects, or non-targeted values, which will simply degrade the performance of the system without a predefined clear objective. With trojans injection (or backdoors), the attacker inserts into the training set values that will cause the model to be affected by a trigger that the attacker can remotely activate. Upon receiving a specific input, the model will perform in an attacker's controlled fashion.

Attacks during the testing phase: With attacks during the testing phase, the attacker has no control over the training stage of a model. Rather, they interact with the deployed model and are only allowed to feed it with data to test. These attacks highly depend on the availability of information on the attacker's side, including knowledge of the model and training data. Some of the most notorious attacks in adversarial AI include the following. We focus on specific attacks highlighted in the literature for their significance and ability to uncover vulnerabilities, such as Fast Gradient Sign Method (FGSM) [98]; Basic Iterative Method (BIM) [146]; Carlini & Wagner (CW) [50]; Randomized Fast Gradient Sign Method (RFGSM) [235]; and Projected Gradient Descent (PGD) [162]. Besides the assumptions on the attacker's knowledge, in wireless networks, another important factor for the effectiveness of adversarial attacks is related to the location of the adversary. Indeed, the effectiveness of the attack may depend on whether

the malicious data is superimposed to the legitimate wireless signal, directly fed at the receiver's side, or via a compromised device that was previously a legitimate member of the network.

Examples of Adversarial Attacks to Wireless Networks. Chen et al. [54] propose DeepReceiver, an AI-based receiver that adjusts signals to minimize the bit error rate using an M-class classifier. They generate a signal to evade classification and reduce the bit error rate, leveraging FGSM and PGD based on the attacker's knowledge of the model and data. Qui et al. [194] develop an Intrusion Detection System (IDS) for IoT networks, where the adversary only has black-box access. They propose a model extraction technique and design a saliency map to predict the impact of malicious packets, followed by classical adversarial example generation methods. Flowers et al. [86] focus on adversarial attacks on ML-based radio frequency operations. They classify attacks based on attacker location, adapting FGSM for both direct input and over-the-air (OTA) transmission, showing adversarial samples are mitigated when OTA perturbations are used. Bahrmali et al. [28] model wireless adversarial perturbations as a constrained optimization problem. They consider white-box and black-box settings with constraints such as power undetectability and phase rotation, designing robust, input-agnostic adversarial attacks leveraging transferability and learnability. Shi et al. [222] use deep learning to generate adversarial signals for spoofing devices, leveraging a generative adversarial network to mimic victim signals and bypass physical layer authentication measures like RF fingerprinting. Liu et al. [156] develop a deep learning-based receiver for radio frequency identification. They formulate an optimization problem for an adversarial generation under full and partial Channel State Information (CSI), achieving higher spoofing success rates than FGSM.

1.4.3 ML for Network Traffic Analysis

Unlike Deep Packet Inspection, which relies on predefined rules, Machine Learning (ML) can adapt to network data. ML approaches are categorized as supervised, unsupervised, or semi-supervised. The general framework includes data collection, flow representation, and feature engineering. Supervised learning algorithms, such as SVMs, Naïve Bayes, Decision Trees, Random Forest, and kNN, use labeled datasets to classify traffic and detect malicious activities. Unsupervised learning, which does not require labeled data, identifies patterns by clustering similar data points. Clustering methods like K-means, hierarchical clustering, and Gaussian Mixture Models are common for network traffic analysis. Unsupervised learning, including K-means, has proven effective in tasks like flow grouping and real-time application identification. Hybrid or semi-supervised solutions combine both supervised and unsupervised methods. Typically, unsupervised techniques help with feature selection or labeling, followed by supervised algorithms for classification. This approach improves traffic classification by addressing the limitations of using either method alone. Research has enhanced standalone kNN performance through techniques like PCA and Fuzzy C-Mean clustering. For example, Zhang et al. [258] combined K-means and NCC to classify unknown traffic, while Glennan et al. developed a hybrid model for known and unknown traffic. Additionally, Fahad et al. [80] introduced SemTra, a framework that labels unlabeled data using multi-view representations and ensemble K-means clustering to improve classification. Furthermore, Zhang et al. [259] designed a Robust Statistical Traffic Classification (RSTC) system to identify zero-day applications and accurately discriminate predefined application classes.

1.4.4 Adversarial Network Traffic

Adversarial attacks exploit AI model vulnerabilities in network traffic analysis, where small perturbations in input data cause classifiers to misclassify traffic. These attacks raise concerns about the reliability of traffic classifiers in adversarial environments, affecting both the training and prediction phases by modifying traffic content or features. Most adversarial attacks, originally designed for image processing, cannot be directly applied to network traffic classification due to two main challenges: the dynamic nature of flows and the shared generation between entities. Sadeghzadeh et al. [205] address this by using Universal Adversarial Perturbation (UAP) injected into packets to reduce DL-based classifier performance. They also show that dummy packets with UAP can degrade classifier accuracy. The study by Duy et al.[76] demonstrates the vulnerability of ML-based Intrusion Detection Systems (IDS) to evasion attacks generated by Generative Adversarial Networks (GANs). Qiu et al.[193] propose an adversarial attack on DL-based IDS by replicating the black-box model and using a saliency map to target key packet attributes. Liu et al. [157] show how membership inference attacks reduce classifier performance, limiting deployment. In Federated Learning (FL), while raw data stays on devices, shared

model updates risk information leakage. Inference attacks can expose participants' data without direct access [101]. Researchers have found privacy risks in FL, such as membership inference, revealing training data details, or attackers learning unrelated information from model updates [108]. A central server breach could lead to a single-point-of-failure, compromising privacy in systems like traffic flow prediction [192].

1.4.5 Adversarial Attack Mitigation Approaches

Defending against membership inference and adversarial attacks, [157] developed the hierarchical differential privacy framework, which categorizes features of network traffic samples based on their security levels and introduces varying noise levels to each feature according to its security level.

To cope with these challenges discussed in Section 1.4.4, several studies have explored integrating Blockchain into FL (BCFL) to enhance privacy and security while reducing the risk of a single point of failure in traffic flow prediction [192] and the industrial Internet of Things [169, 250]. In ensuring the protection of model parameters from edge devices in networks beyond 5G, researchers have also integrated differential privacy with BCFL [240]. Moreover, studies incorporate a similar approach to enhance the system's privacy, adding noise to data generated using either Gaussian distribution[192, 206], Laplace distribution[240], and random distribution [55]. The trade-off between model performance and data privacy is the major drawback of differential privacy. Another approach to safeguarding the system employs homomorphic encryption-based BCFL, which enhances privacy by utilizing partial and fully homomorphic encryption, countering various inference and poisoning attacks with encrypted gradients [20, 217, 245]. Moreover, the researchers emphasize the effectiveness of hybrid approaches, which merge privacy-preserving techniques (differential privacy, homomorphic encryption, and secure multiparty computations) to mitigate security and privacy attacks in BCFL [105, 126, 262].

1.5 Research challenges

The future of wireless technologies will continue to evolve along the axes of range and bandwidth, with each category facing its own unique set of challenges. In particular, attention will be paid to energy efficiency, scalability, spectrum management (various bandwidths 2.4 GHz, 5 GHz, 6.5 GHz - 8.5 GHz, and also in the millimeter bandwidth 24 - 40 GHz), the integration of AI-driven optimization, and the appropriate security and privacy protection mechanisms. As we move towards 6G networks, satellite integration, and the explosion of IoT, overcoming these challenges will be essential to enable the next wave of innovations in wireless communication. In this section, we are focusing on the cybersecurity and privacy gaps as well as AI research challenges regarding traffic analysis.

1.5.1 Cybersecurity and privacy challenges in 5G and 6G

Managing security and privacy in the dynamic environment of next-generation wireless networks, while meeting Quality of Experience (QoE) demands, represents a complex optimization challenge. Addressing these concerns requires a holistic approach that includes rigorous risk assessment, comprehensive threat modeling, security and privacy by design principles, continuous monitoring, effective incident response strategies, and collaborative efforts among stakeholders to share threat intelligence and best practices. By taking proactive measures to tackle cybersecurity and privacy issues, these networks can strengthen their resilience and maintain user trust.

In particular, 5G and 6G networks are advancing rapidly, offering a wide range of benefits but also introducing significant cybersecurity and privacy challenges. Below, we outline key future research directions in these areas, with references to current literature to provide context for the ongoing work in this field.

1. **Security of Network Slicing:** Network slicing in 5G/6G enables the creation of isolated virtual networks on shared infrastructure. However, ensuring secure slice isolation and defending against cross-slice attacks remains a critical challenge. Research should focus on developing secure isolation mechanisms and dynamic real-time monitoring systems to detect and mitigate cross-slice breaches [144, 177, 212].
2. **Zero Trust Architecture (ZTA) for Distributed Networks:** Traditional perimeter-based security models are insufficient for the highly distributed and virtualized architectures of 5G/6G.

As these networks continue to evolve, ZTA must be adapted and scaled to ensure security across dynamically changing topologies. Research should explore how to implement ZTA in these environments without relying on fixed perimeters [56, 177, 212].

3. **Privacy-Preserving Mechanisms for IoT:** The proliferation of IoT devices in 5G and 6G networks brings significant privacy concerns regarding data collection, processing, and sharing. Scalable privacy-preserving mechanisms such as homomorphic encryption, federated learning, and differential privacy are needed to ensure the confidentiality of user data [56, 163, 177, 207].
4. **Quantum-Safe Cryptography:** The rise of quantum computing threatens current cryptographic methods, necessitating the development of quantum-safe or post-quantum cryptographic algorithms. Research should focus on exploring quantum-safe protocols and ensuring a smooth migration from classical to quantum-resistant solutions [177, 191, 207, 212].
5. **Blockchain for Secure, Decentralized Authentication:** Blockchain holds promise for providing decentralized trust in 5G/6G, but its scalability and latency issues present challenges. Future research should focus on integrating blockchain efficiently to ensure secure authentication and data integrity in these networks [177, 191, 212].
6. **Edge and Fog Computing Security:** The distributed structure of edge and fog computing in 5G/6G networks creates security risks, particularly for IoT devices with limited resources. Research into lightweight security protocols, such as efficient cryptography, is essential to protect against threats like botnets, network infiltration, and data theft, ensuring these devices remain secure entry points [144, 163, 177, 207, 212].
7. **Physical Layer Security:** The physical layer offers a promising yet underexplored opportunity to enhance security in 5G/6G networks. Research should explore how physical layer techniques, such as beamforming and interference management, can improve overall network security [93, 177, 212].
8. **User Privacy in Ultra-Dense Networks:** In ultra-dense 6G networks, where numerous devices are concentrated in small areas, protecting user privacy becomes more complex. Future research should focus on developing privacy-preserving mechanisms tailored for high-density environments [56, 163, 177, 191, 207].
9. **Cross-Layer and Holistic Security Approaches:** Attacks in 5G/6G may exploit vulnerabilities across multiple layers of the network stack, making a cross-layer and holistic security approach necessary. Future research should develop frameworks that integrate security solutions across all layers of the network [144].

1.5.2 AI and Wireless Network Traffic Analysis Challenges

Despite the significant advances in applying AI for wireless network traffic analysis, several key challenges remain that require further research [25]. These gaps include:

- **Autonomous Network Management:** AI can facilitate fully autonomous network management by automating network operations, controls, and maintenance functions without human intervention. However, current frameworks are not yet comprehensive in integrating AI-driven traffic analysis to optimize performance, security, and reliability. Future research must focus on designing intelligent systems that enable proactive, self-correcting mechanisms to enhance network performance [177, 212].
- **Scalability and Efficiency:** The growing complexity and scale of networks present challenges for AI-driven traffic analysis. Real-time data processing requires scalable AI models and distributed computing solutions, such as leveraging edge computing resources. Future work should focus on developing algorithms that can efficiently handle large volumes of data in real-time while maintaining performance [207].
- **Adversarial Attacks:** AI systems in wireless traffic analysis are vulnerable to adversarial attacks, such as evasion and poisoning attacks. These attacks can mislead classifiers into making incorrect decisions. Research must focus on enhancing the robustness of AI models through techniques like adversarial training and robust optimization to protect against these threats [97, 144].
- **Privacy-Preserving Analysis:** Ensuring user privacy in AI-driven traffic analysis remains a significant challenge. There is a need for privacy-preserving techniques that do not compromise

data integrity or require excessive computational resources. Future research should aim to develop methods that balance effective traffic analysis with user privacy [25, 177, 224].

- **Dataset Collection and Labeling:** The collection and labeling of traffic datasets for AI training are critical but challenging due to issues like data imbalance and the labor-intensive nature of labeling. Imbalanced datasets can skew classifier performance, leading to biased outcomes. Future work should focus on improving data collection methods and developing automated labeling techniques to mitigate bias and improve model accuracy [144, 212].

Chapter 2

WG2: A cybercrime perspective in wireless networks

Miguel Aguado[1], **Rasa Bruzgiene**[2], **Isabella Corradini**[3], **Virginie Deniau**[4], **Dalibor Dolezal**[5], **Christophe Gransart**[4], **Martin Griesbacher**[6], **Sarunas Grigaliunas**[7], **Steven Kemp**[8], **Valeria Loscri**[9], **Virginia Soldino**[10] [1]

[1]Universidad de Murcia - Spain
[2]Kaunas University of Technology - Lithuania
[3]Themis Research Center - Italy
[4]University Gustave Eiffel - France
[5]University of Zagreb - Croatia
[6]Research Industrial Systems Engineering (RISE) GmbH - Austria
[7]Kaunas University of Technology - Lithuania
[8]Universitat de Girona - Law Faculty - Spain
[9]Inria Lille - France
[10]Universitat de Valencia - Spain

[1]Authors sorted alphabetically by the surname

2.1 Introduction

The evolution of cybercrime over the years is strictly connected to the technological evolution. In this chapter, the concept of cybercrime is analyzed under different perspectives.

The first part of the chapter is devoted to the temporal evolution of the definitions of cybercrime, in order to capture all the facets of what cybercrime is. It is notable that a rich plethora of terms does exist, and it is noticed that also small differences may capture different aspects of cybercrime landscape. This part provides several taxonomies, based on the most relevant literature, presenting different types of cybercrimes. A quite comprehensive categorization of offenders permits then to distinguish among different criminals, based on their technological skills and motivations. Considering the double nature of human being in the context of cybercriminal activities – as cyber offenders and cyber victims – the chapter also focuses on one specific crime involving minors (online child sexual exploitation and abuse).

The second part of the chapter analyses the impacts of cybercrime on individuals and organizations from different viewpoints. The impact of cybercrime on workers represents an interesting perspective which integrates safety and security aspects. Hence, if on the one hand data leakage is a security problem, on the other hand it can have economic, psychosocial and reputational consequences for individuals and organizations.

Finally, the last part of the chapter considers the different approaches and theories developed for preventing cybercrimes and highlights their main gaps, essentially residing in the lack of evaluation and validation of these theories.

Based on a multidisciplinary approach, encompassing social and technical efforts, this chapter provides the criminological scenario, fundamental to understand the characteristics of cybercrime offenders and victims' vulnerabilities, and identify the most suitable cybersecurity solutions.

2.2 Task1: Identification of cybercrimes

2.3 Definitions of cybercrime

It is important to define cybercrime clearly because even small differences in definitions can affect the way it is measured. The problems in defining cybercrime start with the terminology itself. Various terms are used, sometimes in combination with the prefixes cyber, computer, e-, Internet, digital, or informational. The terms are used arbitrarily, highlighting overlaps in the content or pointing out important gaps [70]. Alternative terms for cybercrime include "crime in cyberspace", "computer crime", "electronic crime", "e-crime", "technology-enabled crime" and "high-tech crime". The variability of terms in the field of cybercrime illustrates the lack of a common language among experts specializing in this area [188]. Cybercrime refers to crimes "where the perpetrator uses specialized knowledge of cyberspace", while computer crime exists because "the perpetrator uses specialized knowledge of computer technology" [113]. In the mid-2000s, criminalologists adopted the term cybercrime to refer to criminal acts that are accessible through technology [113]. In this paper, the term "cybercrime" is used as a translation of the English term cybercrime. Phillips et al. [188] have reviewed the literature and concluded that there is no single, precise, comprehensive, and universally accepted definition of cybercrime. However, the definitions classify three groups:

- A term that encompasses a variety of criminal and harmful behaviors Cybercrime encompasses a variety of illegal acts or perceived illegal acts by individuals/groups against computers, computer-related devices, or information technology networks, as well as traditional crimes committed using the Internet and/or information technology [73]. Thus, although there is no single definition of computer crime, it is generally accepted that the term is used to describe a wide range of crimes and harmful behaviors. Wall (2001) states that computer crime "refers to little more than the occurrence of harmful behavior that is in some way associated with computers". Although such definitions are perhaps too broad and vague, they are nevertheless fundamentally correct [188].
- The most cited definitions of cybercrime Phillips et al. point out that the two most frequently cited academic definitions of cybercrime are those of Thomas and Loader and Gordon and Ford. Thomas and Loader [158] define cybercrime as "computer-mediated activities that are either illegal or perceived to be illegal by certain parties and that may be carried out over global electronic networks", while Gordon and Ford [99] state that cybercrime means "any crime committed using a computer, computer network, or device".
- Institutional and organizational definitions of cybercrime: At the organizational level, there are global differences in the definitions of cybercrime. The Convention on Cybercrime (2001) refers to a range of "practices directed against the secrecy, integrity and availability of computer systems, networks and data and their misuse, and providing for the criminalization of such conduct", while the Tenth United Nations Congress on the Prevention of Crime and the Management of Offenders provides the following definitions [10]:
  a. "any illegal behavior committed through electronic operations that targets the security of computer systems and the data they process"
  b. "any illegal conduct committed through a computer system or network, including offenses such as the illegal possession and offering or dissemination of information through a computer system or network."
  It is important to note that most organizational definitions are likely to refer to computer security crime and do not accept the broad interpretation of computer crime as defined in the academic literature [188].

2.4 Types of cybercrime

The most commonly used categorization system, consistently accepted by both researchers and policy makers, is the one that distinguishes two types of cybercrime: "cyber-enabled", i.e. computer-enabled, and "cyber-dependent", i.e. computer-focused crime [188]. This dual categorization is based on the definition originally presented by [40] and explicitly distinguishes cybercrime from so-called real crime, which migrates into cyberspace. "Cyber-enabled" crimes are traditional crimes that existed before technology and are now facilitated or enabled by information and communication technology. Alternative terms for this category include computer-enabled crime, computer-related crime and human-related

crime [188]. "Cyber-dependent" crime refers to criminal acts that occur with technology, without which they cannot exist outside the digital world. Different authors use different terms to describe these two categories. For example, "cyber-dependent" crimes are referred to as computer-focused crimes, computer crimes and technological crimes [188]. In [210], the authors develop this concept and it is interesting because of the breadth with which it adds a new dimension to cybercrime:

Type I cybercrime: crimes of a technical nature (e.g. hacking),

Type II cybercrime: offenses involving human contact (e.g. cyberbullying),

Type III cybercrime: offenses committed by artificial intelligence, robots/bots or self-learning technology.

The Wall's [239] three-category categorization system was one of the first to be published in the academic literature and is therefore often cited. It distinguishes between three types of crimes against machine:

"Crimes against computer integrity", known as crimes against computer integrity, e.g. hacking, cracking, denial of service (DoS) and distributed denial of service (DDoS),

"Computer-based crimes", also known as computer-based crimes, e.g. piracy, robbery and fraud,

"Offenses against computer content", which are identical to offenses against computer content, e.g. online hate, harassment, child pornography.

2.5 Types of economic actors

Economic cybercrime refers to illegal activities that aim to obtain illicit profits and in which ICT play a central role. This category consists of activities such as online fraud or ransomware that typically involve a chain of diverse actions, including phishing, malware infections, and money laundering. The actors behind economic cybercrime can work in a variety of structures ranging from lone attackers to loose networks to strict hierarchical organized crime groups. However, given the diversity of tasks involved in economic cybercrime, the lone attacker is infrequent, and most actors work in some form of collaboration. These collaboration networks and groups have been analyzed along a variety of spectrum; for instance, whether they are more low or high-tech, whether they are more local or international, or the degree with which they interact with victims (R. Leukfeldt et al., 2017b, 2017a) [153] and [154]. Research shows that, while cybercrime is frequently transnational in terms of attacks, the profit-motivated groups behind the attacks often have a local and even offline component. In this sense, hotspots for certain types of cybercrime specialization have been identified [43], [161]. For instance, Russia and Ukraine have been shown to be hotspots for technologically sophisticated economic cybercrime, whereas groups in Nigeria or India are known for focusing on scams in which social engineering plays a more prominent role than high level computer knowledge. The structure of some economic cybercrime groups has been compared to firms in the licit economy. Analysis of the Gozi ransomware group showed collaboration over an extended period of time and identified a certain degree of hierarchy with differentiated roles for leaders, middle-management, and lower-level employees [161]. Members of cybercrime firms typically have a particular specialized role, such as a coder or an administrator, and the firms externalize tasks when it is beneficial for their business goals. In this sense, the organizations involved in the profit-driven cybercrime ecosystem function in a similar manner to those in the licit economy, as they make cost and benefit decisions with the aim of maximizing profit. This links to rational choice and routine activities theory mentioned above.

Online criminal convergence settings can be important for online crime networks and groups, particularly those that are less experienced and those that do not have strong local and offline connections. Online criminal convergence settings are online places like forums, chat services and markets where criminals and potential criminals can meet [227]. These digital meeting points can perform a social, market and/or learning function [153]. Firstly, the social function of these meeting places consists of facilitating the expansion of existing criminal networks and the formation of new alliances. Secondly, the market function refers to the purchase and exchange of three types of products: data, tools and services. Much of the profit-driven cybercrime ecosystem focuses on making money through products and services that form part of a chain of activity, for example, phishing kits, ransomware rental services, or false identities. Finally, online criminal environments allow criminals and potential criminals to exchange knowledge and learn from each other, as mentioned in relation to social learning theory.

2.6 Cybercrime offenders - Topology and Motivations

Following a comprehensive review of previous categorization theories, Rogers [202] developed an updated continuum of computer criminals based on his earlier work. This continuum includes the following categories, which are mainly based on the criminals' technological skills and motivation

1. Novices (NV) are criminals with the least technical knowledge and skills. Members of this category are relatively new to the scene and use ready-made scripts/code and tools to commit computer crimes. Their main motivation is the thrill of breaking the law, gaining reputation and gratification [203]. They are mostly younger individuals who want to be accepted in the hacker subculture and to prove their worth, they strive to "collect trophies". This behavior is similar to that of youth gangs where the goal is to become a full-fledged member and to achieve this goal one must commit a crime that can be proven.

2. Cyber punks (CP) are the closest to the traditional stereotype of hackers. Members of this category are slightly more advanced than beginners. These criminals can create simple scripts and attack programs. Their typical behaviors include "crashing" websites, DDoS attacks5, card fraud and telecoms fraud. Their motivation is the need for attention, fame and financial gain, which they usually achieve by turning their crimes into a lucrative business.

3. Internals (IN) are former employees or disgruntled employees working in IT positions. Members of this category have an advantage over external attackers because of their job and status within the organization. Research shows that insider attackers are responsible for most computer crimes and financial losses. Their motivation is usually based on revenge for a perceived injustice (e.g. dismissal, lack of promotion). Authors in [219] have identified risk factors for this category and mention that they begin the attack in combination with appropriate environmental factors (e.g. stress). Risk factors such as lack of empathy, sense of justification and poor interpersonal skills are common among IT professionals in general.

4. Petty thieves (PT) are traditional criminals who have turned to technology to keep up with the times. These individuals are professional criminals whose motivation is primarily financial gain by stealing from banks, businesses and individuals.

5. The old guard (OG) hackers are computer criminals with advanced skills and technical knowledge. These individuals are responsible for writing many of the programmes used by less experienced beginners and computer rebels in their cyber-attacks; however, they are not criminals in the traditional sense. Their illegal behaviour is motivated by a desire for knowledge, curiosity and intellectual stimulation.

6. Virus writers (VW) do not fit into Rogers' taxonomy, mainly because this group of people has not been researched. Rogers (2006) states that this category is an anomaly because it is difficult to determine exactly where to categorise them within the classification. He also notes that they are an excellent example of how each group can contain its own subgroups. Gordon notes that there is a continuum of behaviour within this category and that individuals generally stop engaging in this deviant behaviour when they are in their mid to late twenties.

7. Professional criminals (PCs) tend to be older and more technologically equipped than the previous categories. Members of this category may be former government and intelligence agency employees who are motivated by financial gain. They often have access to advanced technology and are experienced in industrial espionage. They are considered one of the most dangerous types of computer criminals. They are often part of organised crime groups that have recognised the potential of using technology and the Internet in the criminal world [203].

8. Information Warriors (IW) are highly skilled operatives who carry out coordinated attacks on information systems to disable or destabilise infrastructure. This group may be motivated by loyalty and patriotism.

9. Political Activists (PA) include hackers who are motivated by political, social or religious reasons [203]. Authors in [68] have developed a topology based on five dimensions: Goals (people, business, public sector and critical infrastructure), Expertise, characterized by the level of knowledge and skills (high, medium and low), Resources (budget and free time), Organization (the level or way actors are structured to perform a task or achieve goals) and Motivation (personal, economic, ideological and geopolitical). With regard to the organizational dimension, a well-known distinction from institutional economics is used to increase analytical relevance and conceptual precision: Hierarchy, which relies on control and centralized authority to coordinate tasks; Market, which includes the purchase of security services and software; Networks, which do not have centralized authority but rely on long-term relationships and trust; and Collectives are the most weakly organized groups to which individuals with similar interests and expected benefits belong [68]. Their typology consists of the following categories:

Extortionists attack citizens, businesses, hospitals, schools, governments and critical infrastructure such as the energy sector and water management organizations. The authors rate the attackers' expertise in carrying out blackmail attacks as low to medium. In terms of resources, the assessment would be that the level of resources required for an extortion attack is low to medium. For the organizational dimension, the type of threat would be a hierarchy, a market or a network. Finally, the motivation would be categorized as personal or economic.

Data brokers may pose threats to the privacy of citizens, businesses and the public sector. They specialize in collecting and aggregating data, and sometimes this data can include sensitive details. Therefore, the scale and diversity of data held by these brokers make them a prime target for hackers and cybercriminals, that rely on this data to perform attacks.

The intensity of attack can range from medium to high. The number of resources required to obtain information and data through an attack can be categorized as low to medium. The tools to obtain these sources of information are readily available. For the organizational dimension, the type of threat could be classified as hierarchy, market or network. Finally, the motivation is economic. Crime facilitators have the same goals and motives as the previous category. Expertise in the development of new tools is constantly increasing and can be categorized as medium to high. The level of resources required to develop these tools and services is classified as medium, and the organisational structure that characterizes them is market and network.

Digital predators most often target individuals and often financial organizations, which suggests a commercial motivation. They have medium to high expertise and their attacks, the level of resources available is also classified as medium to high, and the organizational structure is network-based.

Scammers and fraudsters target private individuals, businesses and the public sector. The expertise required for this type of attack is categorized as low to medium, as is the level of resources. The organizational structures associated with these attacks are individual, market or network based, and the motivation is economic.

Hacktivists are ideologically motivated but poorly organized, either individually, in collectives or networks. The skill level of these attacks is low to medium.

Crackers can attack both public and private organizations as well as critical infrastructures. They are motivated by fun and the opportunity to show off their skills, which indicates personal motives, especially among younger individuals. Skill levels are categorized as low to medium as the availability of easy to use and potentially destructive tools increases. The number of resources available to them is categorized as low. Crackers tend to be relatively old and operate individually or in loosely organized collectives or networks.

Terrorists carry out attacks on companies, the public sector or critical infrastructures. This type of attack requires a high level of expertise and a medium to high level of resources. They usually use the organizational structures of the market or hierarchy to coordinate their attacks and the motivation is

ideological.

State actors represent traditional, covert attacks in which state actors target companies, the public sector or critical infrastructure to gain access to strategic information. The level of expertise and resources used in these attacks is classified as medium to high. The organizational structure used to carry out these attacks is hierarchical, and the motivation is geopolitical.

State-sponsored networks have dubious links to state actors. They mainly target citizens, businesses, the public sector and critical infrastructures. The level of expertise they display varies between medium and high. The level of resources is medium to high, as the attacks recorded are long-term campaigns. The organizational structure has network characteristics, and the motivation can be classified as ideological.

Insiders target the organizations in which they work, which may be public or private companies. The level of expertise can vary from medium to high if they are experienced and long-standing employees. The level of resources available for attacks can be categorized as low and the motivation as personal, economic or ideological.

Authors in [57] identified eleven classifications and typologies of computer criminals, most of which are mentioned in this article, published over three decades with the intention of summarizing the state of the art. They presented thirteen categories of offenders and seven unique motives, but one category and one motive were omitted from this paper on the grounds that they belong to sexually motivated offenses. Their summary and consequently the proposed typology is as follows [57]:

Novices: this group refers to hackers with little knowledge who rely heavily on online tools provided by other authors. Alternative terms are "script kiddies", "newbies" and "system challengers". They are motivated by curiosity, fun and fame. They use off-the-shelf code and scripts found on the internet and dark web, often with little or no modification. Their limited skills often mean that they are unable to cover their tracks. Their typical attacks include malware installation, phishing, password reuse and simple DDoS attacks.

Students (Eng. students): These individuals have no malicious intentions but hack only to gain knowledge. Their main motivation is curiosity. Like the previous category, students use existing code and scripts, but with some modifications, to investigate vulnerabilities in systems such as web servers, databases, etc. They usually report discovered vulnerabilities. They usually report discovered vulnerabilities to relevant companies, security researchers or authorities.

Cyberpunks: These are criminals with low to medium skills who cause damage for fun. They are also known as "crashers", "thugs" and "crackers". Their motives include financial gain, the desire for fame, revenge and fun. Computer rebels may use existing code or write their own to achieve their goals. Their methods include bricking (permanently disabling) computers, exploiting bugs in software, DDoS attacks, phishing, spam mails, SQL injections and stealing sensitive information such as credit card numbers.

Old guard hackers: Like students, these non-malicious hackers do not respect the privacy of others and fall into the aforementioned categories of "white hats", "trainers", "grey hats" and "tourists". Their motives are curiosity, celebrity, entertainment and ideology. They use custom code, scripts and penetration testing tools to discover vulnerabilities in existing systems. They may report these vulnerabilities to system owners, security researchers or the public and often work with security companies and authorities.

Insiders: Disgruntled current or former employees who abuse their access to get what they want. This group includes "internals", "user malcontents" and "corporate raiders" as categories of other authors. Their motives are financial gain, revenge and ideology. These individuals use their privileged access to steal sensitive data within the organization, such as customer or employee information. They may also inadvertently jeopardize the security of the network through carelessness.

Opportunist thieves: These are criminals who have shifted their activities to the Internet for financial reasons and revenge. They include extortionists, fraudsters, thieves and digital robbers. They use simple methods such as Trojan viruses, keylogging, phishing and ransomware to obtain financial information or extort money.

Digital pirates: These individuals, also known as copyright infringers, copy, distribute, download or sell illegally protected material. Their motivation is financial gain, and their strategies include stealing and distributing protected content such as music, films, games and software via websites, torrents and social media.

Crime facilitators: They provide cybercriminals with the necessary tools and technical knowledge, enabling them to carry out sophisticated attacks that would otherwise not be possible. They are usually motivated by financial gain. They offer services such as phishing campaigns, rental of malware and botnets, hosting services and hiding illegal transactions. They operate on forums and websites on the dark web and bring buyers and sellers together.

Professionals: These are highly skilled individuals who act as "hackers for hire" or to further develop their criminal empire. Their motivation is financial gain and revenge. They are also referred to as "black hats", "elites", "criminals", "organized criminals", "information brokers" and thieves. They carry out sophisticated attacks using a wide range of methods and customized code. Their operations are well disguised to avoid detection by the authorities. They operate independently, in small groups or in collaboration with criminal organizations.

Nation-state hackers: They are highly skilled and extremely skillful criminals who work directly or indirectly for a government to destabilize, disrupt and destroy the systems and networks of another state or government. Their motives are financial gain, revenge and ideology. This category includes "information warriors", "cyber terrorists", "cyber warriors", "state actors", "state-sponsored networks" and spies. They carry out complex, multi-stage attacks that include social engineering, installing malware, gaining administrative privileges and collecting data. Their operations are highly coordinated and target governments and critical infrastructures.

Crowdsources: These are individuals who come together to solve a problem, often using questionable methods or pursuing dubious goals. Their motivation is the desire for fame, revenge, entertainment and ideology. They operate together in hacker forums and work together to develop new malware, manage botnets and share infiltration techniques.

Hacktivists: Known as political activists and ideologues, they use their technical skills to further their political goals or use the internet as a tool for political change. Their motives are notoriety, revenge, entertainment and ideology. They work in groups and use methods such as SQL injections, DDoS attacks and compromising social media to draw attention to their goals. They also use platforms to spread fake news or phishing links.

Each of these hacker types uses specific strategies that fit their goals and capabilities and operate in different contexts and with different motivations. Although there are many typologies of hackers, many of them are often not comprehensive enough [57]. For this reason, Chng et al. [57] developed an updated framework for the typology of computer criminals and their motivations, which includes thirteen different offender groups and seven unique motivations. What is particularly important about this typology is that it identifies the typical attack strategies used by each of the thirteen proposed hacker types. This makes it possible to identify specific types of criminals, or at least the large groups to which they belong, by observing their activities when preparing or carrying out an attack. For example, if the target of the attack is a company or government infrastructure and sophisticated malware or scripts are used and the traces are difficult to detect, it can be concluded that the hackers are highly skilled. Depending on the complexity of the attack and the required expertise, it can be concluded whether several hackers (state hackers, hacktivists) or one (professional) were involved in the attack [57].

2.7 Online child sexual exploitation and abuse

Online Child Sexual Exploitation and Abuse (OCSEA), also known as technology-facilitated child sexual exploitation and abuse, refers to situations where Information and Communication Technology (ICT) are involved at some point during the abuse or exploitation continuum. This type of offense can occur entirely online or through a combination of online and in-person interactions between offenders and minors under the age of 18 (Interagency Working Group on Sexual Exploitation of Children, 2016; United Nations Children's Fund, 2021). OCSEA can manifest in various forms, including child sexual exploitation/abuse material (CSEM/CSAM), online child sexual grooming, live streaming of child sexual abuse, and online sexual extortion and coercion, among others (ECPAT International, 2020).Technological advancements facilitate these crimes by providing offenders with new methods to target and exploit children and young people. The widespread use of ICT by children and young people makes them accessible to offenders, who leverage various forms of ICT to target victims, often migrating to new and more suitable technologies as they become available [214]. The increasing ubiquity of the internet, social media platforms, encrypted messaging services, and emerging technologies like Next Generation Wireless Systems (NGWS), present new opportunities for exploitation. Understanding how these technological developments can potentially increase the prevalence and complexity of OCSEA is crucial. Here, we illustrate a technological advancement which facilitates crimes targeting teenagers. Very often, teenagers have a smartphone with a cheap phone subscription. So, they are constantly looking for open free Wi-Fi access to stay connected on social networks.

There are various apps, such as WiFi Map, WiFi Finder, Instabridge, Free Zone – Free WiFi Scanner and Wiman, designed to help users locate nearby available WiFi networks, offering a convenient way to stay connected. While these apps may seem useful, they often suggest open WiFi networks (SSIDs) that are not secure or trustworthy, and can even establish automatic connections to these networks without the user's active consent. This creates significant vulnerabilities, as anyone can set up an access point and use it to carry out a Man-in-the-Middle (MiTM) attack. In such an attack, a malicious actor intercepts the communication between the two parties, gaining access to personal information, such as login credentials, messages and sensitive data.

Of particular concern is the targeting of unwary individuals, who may unknowingly connect to these unprotected access points. Cybercriminals can take advantage of this opportunity to collect personal information from their victims, using them to initiate fraudulent contact and gain their trust for malicious purposes. These seemingly harmless free WiFi apps, while advancing technological convenience, inadvertently facilitate criminal activity by allowing attackers to easily compromise personal privacy and security. This highlights the urgent need for greater awareness, education and the development of robust cyber security measures to protect vulnerable users from such sophisticated attacks.

2.8 Task2: Impact of cybercrime

2.8.1 Vulnerability and Victimization / Victimization and target

Cybercrime is a hot topic concerning individuals and organizations, considering the increasingly use of digital technologies in workplace and in private life.

The risk of falling victim to the different forms of cybercrime depends on both personal and environmental factors [123]; however, research on victims' profiles can be very useful to identify the best security countermeasures. In regard to human collectives like businesses, several reports (e.g., Europol, 2024) highlight how all organizations - micro, Small and Medium enterprises (SMEs) as well as large-sized businesses - can be a target for cybercriminals. Some sectors appear particularly attractive: according to Statista, on the basis of data from European Repository of Cyber Incident (ERCI) critical infrastructure is top target, while the healthcare sector is exposed to an intense cybercrime activity, which includes ransomware attacks, the theft of confidential patient healthcare records and the disruption of care services in healthcare organizations [122]. Also, more macro-level social institutions like democracies can be targeted, e.g. in the form of disinformation campaigns.

On the individual level the concepts used for describing the effects of harmful events need to be used with care. The concepts of "vulnerability" and "victimization" are subject of discussion in term of their possible further negative effects on the mitigation of criminal events. Research in the domain of sexual violance is a primary source for this discussion as it can help to guide new interdisciplinary research perspectives developed in BEiNG-WISE (see for example [92]). Framing a human being in terms of it's vulnerabilites or as a "victim" can put them in a passive role as recpient of criminal attacks and take away their agency in actively mitigating the effects of the event. It is therefore particularily valuable, to take a closer look at the state of the art in research on child sexual exploitation and abuse to see how research should treat the question of impact of cybercrime on human beings.

2.9 Impact of cybercrime on individuals and organisations

By analyzing the impacts of cybercrime, the focus is usually on the economic aspects and reputational damage, while other relevant effects are often neglected. In this section we discuss these types of effects both on individuals and organizations, and a new perspective highlighting the impacts of cybercrime actions on workers' health and safety [119].

2.9.1 Individuals

The financial impact of economic cybercrime is very large. Action Fraud data on cybercrime reports in England and Wales shows that reported losses amounted to £2.3 billion in the 13 months to February 2024 (online available data). In the United States, the FBI's Internet Crime Report notes that the three categories of cybercrime that generated the largest losses were Business Email Compromise, Investment Scams, and Confidence/Romance Scams, with reported losses of $2.4 billion, $1.4 billion, and $950 million respectively. In addition to the direct financial losses suffered by victims of economic cybercrime, the time and financial costs of gathering evidence to report to the police and participate in the corresponding judicial process can also be considered costs arising from victimization.

The impacts described above are not distributed equally across citizens. For instance, younger adults are more likely to suffer victimization, but lose less money overall, which makes sense given that they tend to have less accumulated wealth. The difference is especially notable in certain types of online scams where older adults with greater personal wealth have more to lose, such as investment frauds [137].

While the most obvious consequence of economic cybercrime is financial harm, it is important to recognise that the impacts on individuals can go far beyond purely monetary losses and include negative impacts on mental and physical health. Studies of cyberfraud victims have documented loss of housing or work, problems with family relationships, or anger and depression, amongst other consequences [45].

Feelings of shame or embarrassment are also common and victims who explain the events to family or friends often experience negative reactions, such as being labelled naive, stupid or greedy. Moreover, these

reactions can also come from official institutions when the victim makes a report. Negative stereotyping of economic cybercrime victims as greedy or gullible and therefore deserving of victimisation can lead to secondary victimisation [135].

Indeed, although most online frauds do not involve any physical contact between the victim and the perpetrator, this does not preclude negative consequences for the physical health of the victim. For some victims, the stress and other consequences of victimisation worsen existing conditions (e.g. heart problems or high blood pressure).

2.10 Impact of Online Child Sexual Exploitation and Abuse on Children and Young People

Online child sexual exploitation and abuse (OCSEA) can have profound and lasting impacts on children and young people. Victims often experience immediate emotional and psychological effects, including guilt, self-blame, depression, and low mood [104], [107], [128], [131], [248]. These experiences are exacerbated with long-term feelings of fear, worry and anxiety related to the potential distribution of their images online [128], [248]. Children and young people frequently feel ashamed, guilty or humiliated, and they worry about who might see the images and whether others might mistakenly believe they were willing participants [90]. The sharing of child sexual abuse material (CSAM) poses a significant risk of repeated victimisation. Each time an image is viewed, sent, or received, the child is revictimised [42]. This can result in long-term psychological harm that extends into adulthood, affecting survivors' social and psychological well-being years after the initial abuse [213]. Many survivors struggle with their sense of self and experience difficulties in their relationships with friends, family, and romantic partners [129], [213], often feeling over-sexualised in social and romantic contexts [213].

Issues with self-image, body image, self-esteem, and self-acceptance are common among adult survivors [129]; [248]. Long-term mental health problems, including anxiety, self-harm, and persistent low mood, are also frequently reported [213]. Adult survivors often express ongoing fear and anxiety about their sexual images being distributed online [213], and they continue to suffer from guilt, self-blame, and shame [129], [90]. They worry about being recognised and judged by others who may see the images, or that the images could be used by other individuals for further exploitation [90]. The persistent availability of CSAM makes it extremely challenging for survivors to achieve closure [42]. The enduring impact of OCSEA underscores the necessity of developing effective cybercrime security countermeasures and strategies to identify and protect potential victims.

2.11 Workers health and safety and cybercrime: a new perspective

Cybercrime can produce several consequences for workers health and safety, in terms of psychological impacts, like anxiety, anger and depression [27]. Workers hit by cyberattacks can feel shamed, guilty, confused or frustrated, especially in the case of leakage of digital information. For example, the violation of privacy can have negative mental health effects on individuals, since this represents a psychological need strictly related to the development of personal identity [77].

Moreover, also people's life can be at risk during those working activities managed remotely, such in the the case of vehicles or machinery operating out of control because of interrupted wireless signals of equipment or when attacked by hackers. Given the variety of the impacts on workers' health and safety produced by cyberattacks, organizations should integrate occupational safety and health (OSH) in their cybersecurity risk assessment [119], so adopting a comprehensive approach.

2.11.1 Human Collectives

Organisations are increasingly exposed to many forms of online financial victimisation, suffering from ransomware, data breaches, and frauds, among others. The UK Cybersecurity Breaches Survey collects responses relating to the negative impacts and outcomes of cybercrime experienced by a representative sample of businesses and charities in the UK. In the 2024 sweep of the survey, among organisations

reporting incidents or attacks in the previous 12 months, phishing was often considered the most disruptive type of attack faced by organisations (for 61% of businesses and 56% of charities identifying an incident or attack). Online impersonation or attempted impersonation of the organisation was the second most disruptive attack, reported by 16% of businesses and 22% of charities. In comparison, ransomware, which often receives a lot of press and institutional attention, was rated as the most damaging attack by just 2% of businesses and 1% of charities.

Organisations affected by cybercrime experience a wide range of negative outcomes and impacts that are more complex than simply having money stolen. For instance, online services can be disrupted or taken down, or organisations can lose access to files and networks. These generate a myriad of costs such as having to refocus staff resources to deal with the attack, system repair or recovery costs, interruption of essential public services, or loss of sales [136].

A major negative consequence for organisations that suffer cybercrime is reputational damage. By means of an example, in recent years, there have been numerous cases of business email compromise frauds against Spanish local government institutions. Between 2021 and 2022, Barcelona City Council was defrauded of €350,000 through a phishing attack that impersonated a supplier. The payments made to the fake account were not recovered. Similar cases have occurred against the city councils of Seville, La Palma, Boiro, Ribeira, and the Córdoba Urban Planning Department, among many others. When public institutions lose large sums of public money through these types of phishing scams or when essential services are interrupted through a ransomware attack, this can have a negative impact on the reputation of public institutions in general and the perception of their ability to protect the interests of citizens in the digital era. Companies in the IT and financial sectors are also particularly concerned about the potential reputational damage cyberattacks may have on the company, as the loss of customer trust in financial products and digital services can have serious financial repercussions.

2.12 Task3: Cybercrimes prevention techniques

2.12.1 Criminological perspective on cybercrime

One of the more intriguing issues facing cybercrime scholarship relates to the efficacy or otherwise of established criminological theories in understanding or explaining patterns of online offending and victimization. While there are many criminological theories explaining criminal behaviour, there is still lack of scientific evaluation of these theories in the cybercrime context. Here are presented some of the theories that have been in the focus of scientific evaluation in the cybercrime context.

Routine Activity Theory

Routine Activity Theory (RAT) posits that crime occurs when three key elements converge in time and space: a motivated offender, a suitable target, and the absence of a capable guardian [59]. The choice of RAT as a "test case" for criminological theory's purchase on cybercrime arises from a number of factor: it is an established and widely mobilized theory that has been used to analyse various forms of criminal behaviour; its clear analytical schema permits relatively straightforward application across a range of scenarios and it offers clear cues for policy and crime-prevention, as seen in "situational crime prevention" strategies that draw on RAT [152]. This theory can be applied to cybercrime in the following way:

Motivated Offender: The internet lowers the barriers to entry for criminal activities, making it easier for individuals with varying levels of technical skill to engage in cybercrime. Motivations can range from financial gain (e.g., online fraud, ransomware attacks) to ideological purposes (e.g., hacktivism) or even thrill-seeking.

Suitable Target: Digital assets, such as personal data, intellectual property, or financial information, are considered suitable targets. The vast amount of data stored online makes it an appealing target for cybercriminals.

Absence of Capable Guardianship: The effectiveness of "guardianship" in cyberspace depends on cybersecurity measures such as firewalls, encryption, and user education but also capable guardians may take a variety of forms, including network administrators, forum moderators, users, and peers [255]. However, the rapid evolution of cyber threats often outpaces these defenses, leaving gaps that criminals can exploit.

Social Learning Theory

Social Learning Theory, developed by Albert Bandura [30], [31], [32] and improved by [11], posits that people learn criminal behaviour through their interactions with others, particularly when those behaviours are reinforced by positive outcomes or societal acceptance.

Given the nature of many cybercrime offenses, it makes intuitive sense that social learning theory applies to these crimes. For example, in very sophisticated forms of cybercrime (e.g., hacking, malware/virus distribution), offenders are unlikely to have the knowledge necessary to ensure success without associating with seasoned offenders. Thus, social learning theory is a powerful perspective in the understanding of cybercrime perpetration.

Most of the interaction between cybercrime offenders happens in the online communities, such as forums, chat rooms and social media platforms where individuals can learn and share techniques for committing cybercrimes. These communities can reinforce deviant behaviours by providing validation, support, and technical knowledge [113]. Within certain online subcultures, activities like hacking, piracy, or spreading malware may be normalized and even celebrated [114]. As individuals become more embedded in these communities, they may adopt these behaviours as part of their identity. In cybercrime, peers can play a crucial role in encouraging and guiding individuals towards criminal activities. The virtual nature of these interactions can make it easier for individuals to distance themselves from the consequences of their actions, further facilitating criminal behaviour.

Neutralization Theory

Neutralization theory, proposed by Sykes and Matza [229], suggests that offenders use rationalizations to justify their criminal behavior, thereby neutralizing feelings of guilt or shame. There are four core rationalizations in this theory which can be applied to cybercrime in this way.Denial of Responsibility: Studies have demonstrated that cyber offenders deny responsibility to rationalize their illicit behaviors online. For example, a survey into digital piracy found that digital pirates were unlikely to justify their behaviors due to copyright laws and instead opted to blame the cost of the product (Bryan, 2014). Denial of Injury: Cybercriminals may justify their actions by believing that their crimes do not cause real harm. For instance, a hacker might argue that stealing data from a large corporation is victimless because the company can afford the loss [57], [118].

Denial of the Victim: Offenders may rationalize their actions by portraying the victim as deserving of the crime. This is common in cases of hacktivism, where individuals justify attacks against entities they perceive as immoral or corrupt. Appeal to Higher Loyalties: Criminals involved in digital piracy and hacking, may claim that their actions serve a higher purpose, such as advancing social or political causes. This neutralization technique allows them to view their cybercrimes as acts of justice rather than criminal behavior [58], [117].

Condemnation of the Condemners: Cybercriminals might also discredit those who condemn their actions, such as law enforcement or government agencies, by portraying them as corrupt, oppressive, or hypocritical [44], [111].

Deterrence Theory

Deterrence theory argues that crime can be prevented if the perceived costs (e.g., punishment) outweigh the benefits. The theory is based on the idea that potential offenders make rational choices.

Legal Deterrence: The threat of legal punishment, such as imprisonment or fines, is intended to deter individuals from engaging in cybercrime. However, the effectiveness of this deterrence is often limited by the difficulties in identifying and prosecuting offenders, especially those operating in jurisdictions with weak cybercrime laws [74], [160].

Technical Deterrence: Cybersecurity measures (e.g., encryption, intrusion detection systems) can serve as a form of technical deterrence by increasing the difficulty and risk of committing cybercrimes. When the effort required to breach security measures outweighs the potential reward, offenders may be deterred [166].

Certainty vs. Severity: Research in deterrence theory suggests that the certainty of punishment is more effective than its severity. In the context of cybercrime, increasing the likelihood of apprehension and prosecution (certainty) may be more effective than imposing harsh penalties (severity) [171].

General Strain Theory (GST)

Robert Agnew's General Strain Theory expands on traditional strain theory by identifying three major sources of strain: the failure to achieve positively valued goals, the removal of positive stimuli, and the presence of negative stimuli.

Application to Cybercrime:

- Failure to Achieve Goals: Cybercrime may be a response to the inability to achieve personal or professional goals through legitimate means. For example, an individual frustrated by career setbacks might engage in cyber-espionage or data theft to gain an advantage.
- Loss of Positive Stimuli: Experiences such as job loss, relationship breakdowns, or social isolation (especially relevant in the context of online communities) can push individuals towards cybercrime as a way to regain control or vent frustration.

- Negative Stimuli: Exposure to negative stimuli, such as online harassment, cyberbullying, or discrimination, can lead individuals to retaliate through cyber-attacks, hacking, or other forms of cybercrime.

2.12.2 Prevention strategies for online child sexual exploitation and abuse

Public concern about 'online predators' has increased significantly, leading to substantial investment in legal responses and prevention resources [226], [249]. European law, through instruments like the Lanzarote and Budapest Conventions, highlights the need for international collaboration to identify, safeguard victims, and address online child sexual exploitation and abuse [51], [196]. Effective prevention of OCSEA requires a multifaceted approach [183], [249]; however, despite various preventive strategies implemented in recent years, many lack efficacy evaluation and a theory-driven approach [87], [130], [168], [249].

While offenders bear the ultimate responsibility for OCSEA, preventive activities targeting them are limited and primarily focus on individuals who have already committed offenses (i.e., tertiary prevention; [49], [87], [89], [141]. Implementing secondary preventive measures aimed at potential offenders before they commit abuse is essential to mitigate future crimes [139], [141], [226]. Support resources for individuals concerned about their own sexual thoughts and behaviors involving children have been increasing internationally ([89], [139], targeting mostly adults and fewer young people [89]. The Moore Center for the Prevention of Child Sexual Abuse has collated these support resources available in different languages on their website. Media and social media campaigns have successfully reached large numbers of offenders ([89]. The demand for secondary prevention services indicates at-risk individuals are seeking treatment voluntarily and often report numerous treatment-related benefits ([89]; [141].Educational initiatives targeting children and young people are a common preventive approach. These programs typically educate minors about online risks and provide guidelines for self-protection, such as avoiding dubious chat rooms, maintaining privacy, and minimizing sexual interactions with adults online [48], [67], [226], [249]. Efforts also focus on parents and caregivers to enhance communication about Internet safety [226], [249]. However, a review by Patterson et al. (2022) found that while these interventions improve knowledge retention, they do not significantly alter risky behaviors.

Changing the behavior of perpetrators and victims is challenging and costly, with limited evidence on effective crime reduction strategies [196]. However, modifying the contexts in which sexual crimes occur offers significant preventive potential [196], [226]. This includes policy and legislative changes and a stronger commitment from Internet-based companies to secure online spaces [196]. IT companies should support law enforcement, government, and non-profit agencies by sharing key technical and operational data, tackling child sexual abuse imagery, enhancing customer identity verification for domain registrations, and proactively identifying threat actors and vulnerable users (Child Dignity Alliance, 2019). In 2022, the European Commission adopted a legislative proposal mandating service providers to report OCSEA on their platforms and alert authorities. Additionally, online service providers would conduct risk assessments to detect child sexual abuse material on their services.

The fragmentation of preventive initiatives poses a significant challenge. It is crucial to establish an institutional public health strategy that incorporates primary, secondary, and tertiary prevention interventions. Developing comprehensive evidence-informed prevention strategies at local, national, or international levels is essential to effectively combat OCSEA [49], [87], [139], [141], [168], [151], [226].

Chapter 3

WG3: Optimal Security approaches and their impact on the user

Davide Andreoletti[1], Alessandro Chiumento[2], Gurjot Singh Gaba[3], Antonella Guzzo [4], Ana Respicio[5] Serguiu Sanduleac[6] [1]

[1]University of Applied Sciences and Arts of Southern Switzerland - Switzerland
[2]University of Twente - Netherlands
[3]Linkopings Universitet - Sweden
[4]University of Calabria - Italy
[5]RFundação da Faculdade de Ciências da Universidade de Lisboa - Portugal
[6]University - "Ion Creanga" State Pedagogical University of Chisinau - Moldova

[1]Authors sorted alphabetically by the surname

3.1 Introduction

Ensuring cybersecurity in wireless networks is notoriously more challenging than in wireline networks, due to the inherent vulnerabilities introduced by their broadcast and dynamic nature. For example, since transmissions are broadcast openly across space, wireless networks are exposed to greater risks of interference, eavesdropping, and unauthorized access. In addition to these inherent vulnerabilities, novel wireless systems, such as 5G, 6G, and the Internet of Things (IoT), have peculiarities that further exacerbate existing security challenges and introduce novel threats. These systems are marked by unprecedented connectivity between heterogeneous devices, complexity, interdependence, and data-driven automation. Specifically, these architectures are characterized by diverse devices, each generating different types of data, as well as network infrastructures that can span multiple jurisdictions, be shared among various operators, and heavily rely on data analysis through machine learning models, which play an increasingly critical role in automating network management. The convergence of these factors creates an environment that is not only highly interconnected but also intricately dependent on data-driven decision-making processes, which are vulnerable to manipulation, breaches, and misuse. All these factors are driving a shift in the risk landscape, with new threats that traditional security models are ill-equipped to manage. In particular, conventional security paradigms focused solely on safeguarding the well-known CIA triad (i.e., confidentiality, integrity, and availability) are no longer sufficient.

To meet the demands of modern wireless systems, we propose a more comprehensive definition of cybersecurity, referred to as *responsible cybersecurity* that integrates multiple dimensions that account for ethical, operational, and environmental aspects. The dimension of **security** remains central to this framework, encompassing the traditional measures that ensure data confidentiality, integrity, and availability. However, in modern wireless systems, it is equally important to consider **privacy** as an integral part of security. Given that wireless systems continuously collect and transmit vast amounts of data, there is a higher risk of exposing sensitive information and behavioral patterns that could compromise individual privacy. Given the scale in the deployment and pervasiveness of wireless devices, **sustainability** emerges as another critical dimension, as it focuses on the long-term viability of cybersecurity efforts by minimizing the environmental and financial costs of maintaining protective measures. Sustainable cybersecurity practices ensure that the necessary protective mechanisms are in place without imposing excessive resource demands, making it feasible to secure wireless systems at scale without undue strain on the environment or budgets. The reliance on data-driven automated decisions requires the introduction of two additional dimensions, namely **inclusivity** and **transparency**. The dimension of inclusivity addresses the need for equitable security solutions where data-driven decisions do not discriminate based on sensitive information, such as gender and race. Transparency unveils the mechanisms that underpin security systems, and plays an essential role in ensuring accountability for the decisions taken. Then, the dimension of **incentive compatibility** ensures that secure behaviors are financially encouraged, while malicious behaviors are de-incentivized. Lastly, **data governance** forms the structural basis for managing data assets, establishing policies for data ownership, access, usage, and control. Paired with conventional cybersecurity practices, data governance provides a systematic approach to securing data assets by defining who can access and use data, thus reducing the risk of unauthorized disclosure or misuse. In the following sections, we will explore the specific challenges and solutions associated with each dimension and analyze their impacts on users, ultimately demonstrating how these elements shape the security landscape in wireless networks today.

3.2 Security

Security is defined as the set of measures aimed at ensuring confidentiality, integrity, and availability. A list of security problems, solutions, and their impact on the users is presented in the following, and summarized in Table 3.1.

SECURITY		
Problem	**Solution**	**Impact on the user**
Lack of End-to-End Encryption in resource-constrained IoT Devices	- Lightweight Cryptography Algorithms	- Increased Confidentiality - Increased Integrity - Performance trade-offs
Massive Connectivity in 5G/6G	- Isolated Network Slices - Edge Security - Software-Defined Networking (SDN) - Network Functions Virtualization (NFV)	- Improved Service Performance and Continuity - Enhanced Security
Vulnerabilities of Open Wi-Fi Networks to Man-in-the-Middle (MitM) Attacks	- Wi-Fi Protected Access 3 (WPA3)	- Enhanced Confidentiality - Enhanced Security
Eavesdropping	- Physical Layer Security (PLS)	- Enhanced Security - Efficiency - Seamless Integration
Jamming	- Spread spectrum techniques - Adaptive power control - Directional antennas - Machine learning jamming detection	- Improved Service Performance and Continuity - Enhanced Security

Table 3.1: Security problems, solutions, and impact on the user.

3.2.1 Lack of End-to-End Encryption in resource-constrained IoT Devices

IoT devices, such as sensors and smart appliances, often have limited computational resources, making it challenging to implement traditional encryption algorithms like RSA or AES [13]. In fact, these algorithms require significant memory and processing power, which can lead to performance bottlenecks and faster battery drain in resource-constrained IoT environments. As a result, IoT networks become vulnerable to data breaches and unauthorized access due to the lack of strong encryption techniques [16, 182]. This is particularly concerning in sensitive applications such as healthcare and smart homes, where data security is paramount [197].

Solution: Use Lightweight Cryptography Algorithms for Constrained Devices

To overcome the limitations of traditional encryption in IoT, lightweight cryptography algorithms have been developed. Specifically, these algorithms are designed to maximize security guarantees under the constraints posed by the underlying hardware and software implementations. Some examples of these algorithms are PRESENT [36], CLEFIA [223], SIMON and SPECK [34].

Impact on the user

Increased Confidentiality and Integrity: Lightweight cryptographic methods enhance the confidentiality and integrity of data in IoT networks by enabling secure communication between devices with minimal computational overhead. This ensures that sensitive data, such as health information or home automation details, remains protected from attackers [231]. However, the weaker encryption strength poses a risk in use cases requiring high-level security, such as critical infrastructure or industrial IoT [204], or when the processing of personal data (e.g., from medical devices) is involved [60]. Indeed, lightweight encryption schemes typically remain vulnerable to sophisticated attacks, such as algebraic attacks [256]. **Trade-offs:** While lightweight cryptography offers a promising solution for IoT security, there is no one-size-fits-all approach, as each implementation must balance various trade-offs. The **most prevalent trade-off is between security and efficiency** [231]. As security guarantees increase, so does computational load, which impacts the performance and power consumption of IoT devices. This requires users to carefully select the appropriate cryptographic mechanisms based on the specific compromises they are willing to accept. For example, a critical consideration is how a chosen cryptosystem affects battery life and the frequency of battery replacements in resource-constrained environments. Another important **trade-off is between security and flexibility** [34], which is defined as the ability of the cryptosystem to adapt to heterogeneous devices with different hardware and software implementations. In highly diverse IoT ecosystems, this means that the more heterogeneous the network is, the more challenging it becomes to select a cryptographic system that operates efficiently across all devices.

3.2.2 Expanded attack surface in massively-interconnected 5G/6G networks

The proliferation of connected devices, driven by the increasing demand for real-time services (e.g., autonomous vehicles, smart cities ...) in 5G and 6G networks, significantly expands the attack surface [63]. In fact, each device becomes a potential entry point for attackers, and the greater the number of devices, the more vectors exist for attackers to exploit vulnerable endpoints and amplify the scale of such attacks. In particular, the potential for large-scale distributed attacks like Distributed Denial of Service (DDoS) significantly increases.

Network slicing, the technique of dividing a single physical network into multiple logical slices, exacerbates the impact of DDoS attacks. Indeed, since these slices often share a common infrastructure, attacks targeting shared resources can compromise the entire network. DDoS attacks can disrupt multiple slices simultaneously, especially if attackers gain control of one slice and propagate the attack through the shared infrastructure (e.g., substrate nodes) [211]. This can lead to the degradation of critical services such as telemedicine or autonomous driving, both of which demand high availability and low latency.

Solution: Isolated Network Slices and Edge Security

To mitigate this increased attack surface, network slicing is employed to isolate services. By creating separate virtual network slices for different services (e.g., enhanced mobile broadband, ultra-reliable low-latency communications), the risk of one attack affecting other slices is minimized [63]. This can be further enhanced by slice isolation mechanisms, such as Reinforcement Learning-based algorithms, that dynamically allocate resources and monitor slices for potential threats, ensuring minimal cross-slice contamination [124].

Additionally, edge security can be enhanced by bringing security mechanisms closer to the network's periphery. Technologies like Software-Defined Networking (SDN) [167] and Network Functions Virtualization (NFV) [1] significantly augment control over the network by enabling centralized, programmable management of network resources. This increased control facilitates real-time detection and mitigation of threats at the edge of the network, allowing security mechanisms to dynamically adapt and respond to threats before they reach critical core infrastructure [2]. By leveraging SDN and NFV, security policies can be more efficiently deployed and enforced across the network, reducing the impact of attacks and improving overall resilience.

Impact on the user

Improved Availability and Resilience: The use of network slicing and isolation mechanisms enhances the availability of services, even during a DDoS attack. Critical applications, such as autonomous vehicles and smart city infrastructure, remain operational due to the segmented and isolated nature of

the slices. This ensures that users experience minimal disruption, maintaining the reliability required for real-time services like telemedicine and autonomous driving. **Enhanced Service Quality for Critical Applications:** For highly sensitive applications, such as telemedicine and industrial IoT, network slice isolation ensures that these services are less affected by attacks targeting non-critical services. This improves the overall quality of service for end users, ensuring uninterrupted and high-performance functionality for mission-critical applications.

3.2.3 Vulnerabilities of Open Wi-Fi Networks to Man-in-the-Middle (MitM) Attacks

Open Wi-Fi networks, commonly found in public spaces, are susceptible to man-in-the-middle (MitM) attacks. In these attacks, malicious actors intercept and manipulate communications between users and the network, leading to data breaches, identity theft, and unauthorized access to sensitive information. This is particularly concerning when users connect to insecure or unencrypted Wi-Fi networks [232].

Solution: Implementation of Wi-Fi Protected Access 3 (WPA3)

To mitigate the risks associated with open Wi-Fi networks, it is crucial to implement Wi-Fi Protected Access 3 (WPA3) across all Wi-Fi devices. WPA3 introduces enhanced encryption protocols, including 192-bit security, significantly improving protection against MitM attacks by securing user data even on public or shared networks. Additionally, WPA3 features individualized data encryption, ensuring that each user's connection remains unique and secure from eavesdropping [142].

Impact on the user

Enhanced Confidentiality and Security: By adopting WPA3, users benefit from advanced encryption protocols that protect their data from interception on public Wi-Fi networks. This enhancement is particularly valuable for individuals using public spaces or shared environments (e.g., airports, cafes) where security threats are more pronounced [233].

3.2.4 Eavesdropping

Eavesdropping remains a significant threat in wireless communications, where unauthorized entities intercept sensitive data transmitted over the air. The broadcast nature of wireless communication makes it vulnerable to eavesdropping, which has been a well-known security threat. Furthermore, continuing advances in computational power increase the capabilities of attackers. This type of passive attack is simple to execute and difficult to detect within a network. In such an attack, the intruder quietly monitors the network communication to gain access to private information. This can potentially compromise the system's data processing and analysis functions [66].

Solution: Physical Layer Security (PLS)

Physical Layer Security (PLS) offers a paradigm shift by leveraging the inherent properties of wireless channels, such as noise, fading, and interference, to secure communications. Unlike conventional cryptographic approaches, PLS focuses on ensuring that the legitimate receiver's channel is more favorable than that of any potential eavesdropper, thereby enhancing confidentiality. By focusing on the physical characteristics of wireless channels, PLS offers a robust and efficient means to safeguard communications against eavesdropping, complementing traditional security measures. PLS can be implemented in several ways, including the injection of artificial noise to degrade the eavesdropper's channel while maintaining the quality of the legitimate receiver's channel [23], directional modulation to ensure that only intended recipients can decode the information accurately [23], and the creation of spatial diversity by means of MIMO technologies to make it more challenging for eavesdroppers to intercept the complete message [221].

Impact on the user

Enhanced Security: Users benefit from increased protection against eavesdropping, as PLS techniques make it more difficult for unauthorized parties to intercept communications. **Efficiency:** PLS methods often require less computational power compared to traditional cryptographic approaches, leading to

improved performance, especially in resource-constrained devices. **Seamless Integration:** PLS can be integrated into existing wireless systems without significant changes to the user interface or experience, providing an additional layer of security transparently.

3.2.5 Jamming

Wireless jamming consists of the intentional emission of interfering signals to disrupt or block legitimate wireless communications. Jamming attacks can lead to service denial, data loss, and compromised security. Defending against jamming is particularly challenging in systems with a single communication interface, such as IoT devices, as they lack alternative pathways to maintain connectivity [189].

Solution: Anti-Jamming Strategies

Anti-jamming strategies span various techniques, including spread spectrum techniques, e.g., channel hopping, which spreads the signal over a wide frequency band, making it more resilient to jamming [189, 251], adaptive power control, which adjusts the transmission power dynamically [189], the use of directional antennas that focus the signal in specific directions to reduce the likelihood of interference from jammers [189], and the use of machine learning algorithms to detect jamming attacks in real-time [120].

Impact on the user

Improved Service Performance and Continuity: Users experience fewer disruptions, ensuring consistent access to higher-quality wireless services. **Enhanced Security:** Robust anti-jamming measures protect against malicious attempts to interfere with communications, safeguarding sensitive information and critical connectivity.

3.3 Privacy

Privacy is the ability to control the amount of information leaked from shared data. A list of privacy problems, solutions, and their impact on the users is presented in the following, and summarized in Table 3.2.

3.3.1 Leakage of Sensitive Information in Anomaly Detection

With real-time data transmission integral to IoT and 5G networks, there is a pressing need for anomaly detection to identify suspicious behaviors quickly. However, real-time monitoring often entails sharing sensitive, unencrypted data over networks, heightening privacy risks.

Solution: Lightweight Privacy-Preserving Anomaly Detection Frameworks

Privacy-preserving anomaly detection frameworks, such as PPAD (Privacy-Preserving Anomaly Detection), anonymize data before it is processed, reducing the risk of sensitive information exposure. By incorporating lightweight cryptographic techniques like homomorphic encryption, PPAD frameworks enable secure data processing while allowing effective real-time anomaly detection. This setup provides robust security and preserves user privacy even under high data volume and speed typical of 5G-enabled IoT networks [138, 180].

Impact on the user

For users, this solution balances privacy and efficiency, enabling secure real-time anomaly detection without extensive data exposure. In sensitive applications like healthcare or smart cities, users benefit from the immediate threat response without sacrificing privacy. Although cryptographic operations might slightly delay processing, these frameworks are optimized to minimize latency, ensuring real-time performance aligns closely with non-privacy-preserving alternatives.

PRIVACY		
Problem	**Solution**	**Impact on the user**
Leakage of Sensitive Information in Anomaly Detection	- Lightweight Privacy-Preserving Anomaly Detection	- Balancing privacy and efficiency - Immediate threat response
Leakage of Sensitive Information in Threat Intelligence Sharing	- Secure Multi-Party Computation - Trusted Execution Environments	- Secure and collaborative network environment - Trade-off between privacy and latency
Leakage of Sensitive Information in Training Cybersecurity Models for IoT and 5G Networks	- Federated Learning for Decentralized Model Training - Differential Privacy (DP) - Secure Multi-Party Computation (SMPC) - Homomorphic Encryption - Trusted Execution Environments	- Sensitive data kept on-device - Increased trust in IoT system - Trade-off between increased computations on the edge and privacy

Table 3.2: Privacy problems, solutions, and impact on the user.

3.3.2 Leakage of Sensitive Information in Threat Intelligence Sharing

The collaborative sharing of threat intelligence among IoT and 5G network nodes is crucial for rapid threat detection and mitigation. However, sharing detailed threat data between organizations or devices risks unauthorized data exposure and privacy breaches, which traditional sharing mechanisms cannot effectively prevent.

Solution: Secure Multi-Party Computation and Trusted Execution Environments

To address these privacy challenges, Secure Multi-Party Computation (SMPC) and Trusted Execution Environments (TEEs) enable multiple devices or organizations to jointly analyze and respond to threat intelligence without exposing individual datasets. SMPC allows data to be computed collaboratively while keeping inputs private, while TEEs create a secure hardware environment that protects data from unauthorized access during processing. Together, these methods allow for effective data collaboration without violating user privacy [91, 121].

Impact on the user

These privacy-preserving mechanisms foster a secure and collaborative network environment, enhancing overall cybersecurity without compromising user privacy. For users, this means an added layer of protection in IoT and 5G networks, as service providers can pool resources to combat threats while respecting individual privacy. The trade-off is a slight increase in latency due to secure computation processes, but this is generally outweighed by the enhanced security and privacy provided.

3.3.3 Leakage of Sensitive Information in Training Cybersecurity Models

In IoT and 5G networks, large amounts of sensitive data are generated by devices connected to the network. This data is invaluable for training machine learning models aimed at enhancing cybersecurity, particularly for tasks like intrusion detection, anomaly detection, and threat intelligence. However, the requirement to collect and centrally store this sensitive data for model training introduces significant

privacy risks. Transmitting raw data from devices to a central server exposes it to potential interception and breaches, raising serious privacy concerns for users.

Solution: Federated Learning for Decentralized Model Training

Federated Learning (FL) addresses this privacy challenge by enabling decentralized model training, where data remains on-device, and only model updates (rather than raw data) are shared with a central server. In FL, each device trains the model locally on its own data and then sends the computed model updates to a central aggregator, which combines the updates to improve the global model. This process allows effective model training without the need to transmit sensitive data off the devices, thereby preserving privacy. To further enhance privacy in FL, several techniques can be employed:

- **Differential Privacy (DP)**: Differential Privacy is applied to the model updates to prevent data leakage. By introducing controlled noise to the updates before they are shared, DP ensures that individual data points cannot be inferred from the aggregated model. This technique provides a strong layer of privacy, particularly important in 5G-enabled IoT networks where data sensitivity is high [138].
- **Secure Multi-Party Computation (SMPC)**: SMPC allows multiple devices to compute model updates collaboratively without exposing their data to each other. In the FL context, SMPC ensures that model updates can be aggregated securely, maintaining the privacy of each device's contribution. This is particularly useful in scenarios where collaborative threat intelligence is necessary across IoT networks [173, 180].
- **Homomorphic Encryption and Trusted Execution Environments (TEEs)**: Homomorphic encryption allows computations to be performed on encrypted data, while TEEs provide a secure hardware-based environment that protects data during processing. Both techniques enhance the security of FL by preventing unauthorized access to data during the aggregation process. Though computationally intensive, these techniques are effective for applications where data privacy is paramount [121].

Impact on the user

For users, FL offers significant privacy benefits by keeping their sensitive data on-device, reducing the risk of data breaches. This decentralized approach enables robust cybersecurity without compromising personal data security, making users more likely to trust IoT and 5G network services. However, FL does require computational resources on each device, which may impact device performance, battery life, and response time in real-time applications. Despite these trade-offs, the privacy-preserving capabilities of FL make it a powerful and suitable approach for cybersecurity applications in IoT and 5G networks.

3.4 Sustainability

Sustainability refers to ensuring that cybersecurity solutions can be effectively enforced without excessive consumption of resources, thereby supporting long-term viability by minimizing environmental and financial costs. A list of sustainability problems, solutions, and their impact on the users is presented in the following, and summarized in Table 3.3.

3.4.1 High Cost of Security in Large-Scale IoT Deployments

Securing large-scale IoT networks presents a considerable financial and logistical challenge, particularly when traditional security mechanisms, such as Trusted Platform Modules (TPMs), are required on every device within the network. Embedding such complex hardware into each device, especially low-cost sensors and actuators, leads to a significant increase in both manufacturing and operational expenses. This financial burden is further exacerbated in resource-constrained environments, making robust security financially unsustainable for many IoT applications, including smart cities and industrial IoT. Without feasible alternatives, organizations are often forced to compromise either on security, which poses risks, or on scalability, which limits the network's potential.

SUSTAINABILITY		
Problem	**Solution**	**Impact on the user**
High Cost of Security in Large-Scale IoT Deployments	- Lightweight hardware security features - Centralized protection functions	- Reduced financial and operational burden - Secure network infrastructure
Difficulty in Replacing End-of-Life IoT Devices	- Unique device identity, encrypted communication, and secure data storage within EoL devices - Replacement only when necessary	- Economic and environmental sustainability - No reliance on outdated software patches

Table 3.3: Sustainability problems, solutions, and impact on the user.

Solution: Lightweight hardware features and centralized architectures

Lightweight hardware security features, such as those provided by intrinsic device characteristics [21], offer a more cost-effective approach by leveraging unique device identifiers based on natural manufacturing variations, eliminating the need for added hardware. Additionally, security architectures that centralize protection functions into a few strategic network components (e.g., gateways) help distribute security resources efficiently. For example, frameworks designed to provide strong isolation and secure communication with minimal hardware extensions on selected network nodes, rather than embedding security hardware into each IoT device, enable scalable security management at a fraction of the cost [178].

Impact on the user

The proposed approaches reduce the financial and operational burdens for organizations deploying large IoT networks, allowing for secure, scalable deployments without the need to equip each device with costly security hardware. By focusing resources on a few critical nodes, users benefit from an affordable, robust security model, making IoT applications in smart cities, industry, and beyond more viable. The result is a secure network infrastructure that maintains performance, scalability, and long-term sustainability, while significantly lowering deployment costs.

3.4.2 Difficulty in replacing End-of-Life IoT Devices

Several studies [243, 254] examine the vulnerabilities of End-Of-Life (EoL) devices, identifying that millions of IoT devices, no longer supported by manufacturers, present serious security vulnerabilities that can be exploited by attackers. This issue highlights a critical challenge for the sustainability of IoT networks: security software necessary to counter emerging threats often requires more modern hardware, making it impractical or impossible to retrofit outdated devices with conventional solutions. As a result, the straightforward replacement of such devices is often seen as the only viable solution, but this approach leads to increased electronic waste and environmental impact, undermining the sustainability of cybersecurity practices.

Solution: Enhancing Longevity of IoT Security with Embedded Cryptographic Key Management
Instead of device replacement, Ref. [215] proposes a framework that offers a more sustainable approach by maintaining essential security functions, such as unique device identity, encrypted communication, and secure data storage, within EoL devices. This framework, referred to as RESCURE, leverages the inherent physical characteristics of device hardware (such as SRAM PUFs) to create and manage cryptographic keys directly on the device, eliminating reliance on external updates or retrofitted hardware. This solution allows EoL devices to uphold core security standards, supporting secure data transmission and protection, even when traditional updates are unavailable. By focusing on sustainable security solutions that extend the functional lifespan of IoT devices, RESCURE mitigates the environmental impact associated with frequent device replacements.

Impact on the user

For users, adopting a solution like RESCURE promotes both economic and environmental sustainability, reducing the costs and disruptions associated with replacing devices, while simultaneously decreasing electronic waste. In addition, users gain confidence in the continued security and privacy of their data, even on older devices, knowing that essential security features are preserved without relying on outdated software patches.

3.5 Inclusivity

Given that novel wireless systems are increasingly adopted by diverse types of users, with a high reliance on decisions based on personal data, inclusivity refers to ensuring that cybersecurity measures do not discriminate between users based on their sensitive characteristics. A list of inclusivity problems, solutions, and their impact on the users is presented in the following, and summarized in Table 3.4.

INCLUSIVITY		
Problem	**Solution**	**Impact on the User**
Complexity of Technical Explanations in Cybersecurity	- Audience-specific explanations using adaptive language models that adjust complexity based on the user's expertise	- Informed decisions based on AI insights - Increased trust - Improved response effectiveness - Enhanced inclusivity for non-experts
Interface Complexity and Limited Usability for Non-Experts	- User-centered design with intuitive interfaces - Conversational agents using natural language processing to reduce cognitive load	- Increased accessibility for novice users - Enhanced operational efficiency - Expanded user base for XAI tools - Reduced reliance on specialized personnel

Table 3.4: Inclusivity problems, solutions, and their impact on users.

3.5.1 Complexity of Technical Explanations in Cybersecurity

Many XAI models are developed with the assumption that users have a strong technical background, which limits their usefulness for individuals without deep expertise. In cybersecurity, where diverse stakeholders need to understand AI-driven insights to make informed decisions, the complexity of technical explanations creates significant barriers. For instance, current XAI techniques, such as Local Interpretable Model-Agnostic Explanations (LIME) or SHapley Additive exPlanations (SHAP), may require an understanding of machine learning principles that non-expert users do not possess [165, 185, 201].

Solution

One potential solution is to develop audience-specific explanations using adaptive language models that adjust the complexity of explanations based on the user's expertise. These models could simplify technical terms, use visual aids, and provide context-specific examples, making explanations more accessible to diverse audiences, from business professionals to cybersecurity staff with varying experience levels [85, 174].

Impact on the user

Such an approach enables users to make informed decisions based on AI insights, fostering trust and improving response effectiveness. For non-expert users, these tailored explanations can facilitate quicker comprehension, thereby reducing reliance on specialized personnel and promoting inclusivity within cybersecurity operations [201].

3.5.2 Interface Complexity and Limited Usability for Non-Experts

XAI tools in cybersecurity are often embedded within complex interfaces that require extensive training to operate. This complexity restricts their accessibility to skilled personnel, exacerbating the skills gap in cybersecurity. For example, many XAI tools demand familiarity with structured query languages and technical workflows, which can be overwhelming for novice users [85, 165].

Solution

To mitigate this, XAI systems can incorporate user-centered design principles, emphasizing intuitive interfaces and conversational agents based on natural language processing that can reduce cognitive load and provide an accessible means for novice users to interact with complex systems [174].

Impact on the user

By simplifying interfaces and introducing conversational guidance, these tools empower less-experienced cybersecurity staff to engage directly with XAI systems, enhancing their ability to manage security tasks independently. This not only improves operational efficiency but also broadens the user base capable of engaging with and benefiting from XAI-driven insights [85, 185].

3.6 Transparency

TRANSPARENCY		
Problem	**Solution**	**Impact on the User**
Root cause identification complicated by the complexity of 5G/6G networks	- Explainable AI (XAI)	- Increased network reliability and resilience - Enhanced trust in network integrity
Lack of accountability and fairness in AI-driven security decisions	- Explainable AI (XAI) - Counterfactual explanations	- Greater confidence in the fairness of security actions - Safeguards against potential biases

Table 3.5: Transparency challenges, solutions, and their impact on the user.

3.6.1 Root cause identification complicated by the complexity of 5G/6G networks

The complexity and heterogeneity of emerging mobile networks, including virtualized functions and Software-Defined Networking (SDN), coupled with a growing array of Key Performance Indicators (KPIs) across users, devices, services, and networks, make root cause diagnosis challenging [175]. In 5G and beyond, advanced technologies like Open Radio Access Networks (ORAN) and AI-driven security introduce multiple layers of complexity that complicate pinpointing the root causes of security breaches and failures. Attackers can exploit vulnerabilities across various sources, such as AI-based control nodes, virtualized functions, or cloud components, making it difficult for operators to quickly diagnose and

address specific security issues. This lack of visibility into the model's decision-making process can delay response times and increase the risk of recurring security breaches.

Solution:

To address this, Explainable AI (XAI) methods such as SHapley Additive exPlanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME) [35] provide insights into the features or inputs influencing AI-driven security alerts. XAI aids operators in identifying the model components contributing to security incidents, enabling swift identification and resolution of root causes in complex scenarios. For instance, recent work proposes RAFT, a real-time framework for root cause analysis in 5G vulnerability detection, which leverages log file fragments for high-accuracy identification of vulnerabilities in dynamic environments [187]. Additionally, other studies propose testbeds for evaluating AI-based modules for anomaly detection and root cause analysis in the 5G/ context [175], and self-organizing RAN systems with deep learning-based anomaly prediction and root cause analysis capabilities, achieving high accuracy in real-world cellular network data [261].

Impact on the User

XAI increases network reliability and resilience by enabling quicker, more accurate diagnosis of security issues, leading to faster resolutions and reduced disruption. For users, this results in a more secure network with fewer vulnerabilities and minimal downtime, reinforcing trust in the network's integrity.

3.6.2 Lack of Accountability and Fairness in AI-Driven Security Decisions

As 5G networks increasingly rely on AI to manage critical security functions like traffic filtering, anomaly detection, and access control, accountability for the actions taken by these systems becomes essential. In cybersecurity, decisions need to be not only effective in mitigating risks but also fair and justifiable, ensuring that all users are treated equitably and without bias. AI-driven cybersecurity decisions, however, are often opaque, making it challenging for operators to understand or explain why specific actions, such as restricting access or flagging certain behaviors, were taken. This lack of transparency raises significant concerns in instances where users may be unfairly affected, such as when false positives lead to unwarranted restrictions. Without mechanisms for accountability, it is difficult to verify that decisions adhere to regulatory standards, ethical guidelines, and fairness expectations. A cybersecurity system must not only justify its actions but also take responsibility for avoiding unfair treatment of users, ensuring that security interventions are both effective and equitable.

Solution:

XAI solutions provide essential tools for fostering accountability and fairness in AI-driven cybersecurity. By implementing techniques such as counterfactual explanations [24, 184], operators gain insights into how specific inputs influence AI decisions, revealing which factors contribute to actions like access restrictions. This understanding enables operators to assess the fairness of security interventions, identifying potential biases or inequitable treatment across user groups. Moreover, methods like SHAP and LIME clarify the role of individual features in decision-making, empowering operators to address biases and hold AI systems accountable for their actions. For example, various works [133, 134] propose using XAI methods, including SHAP and LIME, to enhance the classification accuracy of IoT devices connected to 5G and 6G networks, identifying the features responsible for decisions and thus increasing model accountability.

Impact on the User

Integrating XAI to ensure accountability and fairness in AI-driven cybersecurity systems builds user trust in the network. Users gain confidence that security actions are not only effective but also justifiable and equitable, leading to a more consistent and inclusive experience. By offering clear explanations for decisions, especially in cases where restrictions are imposed, XAI reassures users that they are protected by a transparent and responsible system. Additionally, accountability mechanisms provide users with a safeguard against potential biases, supporting a cybersecurity environment where trust, fairness, and regulatory compliance are central values.

3.7 Incentive Compatibility

Incentive compatibility ensures that cybersecurity systems are designed to financially encourage secure behaviors while discouraging malicious actions, aligning the interests of users and organizations with overall security goals. This approach motivates compliance with security best practices by making them the most beneficial and cost-effective choices. A list of problems related to incentive compatibility, corresponding solutions, and their impact on the users is presented in the following, and summarized in Table 3.6.

INCENTIVE COMPATIBILITY		
Problem	**Solution**	**Impact on the User**
High Cost of Securing IoT Networks	- Risk management approach assuming inevitable attacks - Cyber-insurance	- Reduced financial impact of potential cyber-attacks - More robust network of IoT devices
Lack of Economic Disincentives for Malicious Behaviors in Wireless Networks	- Dynamic cost adjustments and incentive mechanisms	- Added layer of security

Table 3.6: Incentive Compatibility problems, solutions, and impact on the user.

3.7.1 High Cost of Securing IoT Networks

Securing IoT networks is an expensive and complex endeavor due to several inherent challenges. First, IoT devices often have limited resources, such as processing power, memory, and battery life, which restricts the feasibility of implementing advanced security measures without incurring significant costs. The diversity of devices, ranging from sensors to smart home appliances, further complicates security efforts. This variety requires tailored solutions for each device type, adding to development and implementation costs. Additionally, the absence of standardized security protocols across the industry results in fragmented security practices, making it costly and challenging to ensure consistent protection across the entire network. In addition to these financial and technical barriers, there is often an underestimation of security risks in the IoT space. Users and manufacturers alike may overlook or downplay the threats, leading to common practices such as relying on default or weak passwords and neglecting regular maintenance or updates. This lack of security awareness, coupled with limited protective measures, makes IoT networks particularly vulnerable to advanced persistent threats (APTs), which involve sustained and covert attacks that are difficult to detect. Consequently, the high cost and underestimation of security risks collectively increase the likelihood of cyber-attacks, highlighting the pressing need for cost-effective security solutions in the IoT ecosystem.

Solution: Cyber insurance for Risk Management

A potential solution to address the high cost of IoT security is to adopt a risk management approach that assumes cyber-attacks are inevitable and focuses on mitigating the damage. Cyber insurance is an emerging approach that provides financial coverage for IoT owners in the event of an attack, helping them manage post-incident costs. For example, a study by [260] uses a game-theory framework to analyze the relationships among defenders, attackers, and insurers. This study introduces the concept of insurability for IoT networks, suggesting that the optimal incentive-compatible insurance contract would involve covering half of the defender's losses. Such coverage provides financial relief to IoT owners, encouraging them to invest in preventive measures while knowing that they are partially protected from the financial fallout of successful attacks.

Impact on the User

Implementing cyber-insurance in IoT networks creates a safety net for end-users, reducing the financial impact of potential cyber-attacks and promoting a proactive security culture. By alleviating some of the financial burdens associated with attacks, users are more likely to adopt enhanced security protocols and perform regular maintenance. This, in turn, helps create a more robust network of IoT devices. Additionally, insurance contracts with incentive-compatible structures—such as partial coverage of losses—can motivate manufacturers and service providers to develop devices with built-in security features to minimize the likelihood of successful attacks, ultimately benefiting both users and the wider ecosystem by improving baseline security standards across IoT products.

3.7.2 Lack of Economic Disincentives for Malicious Behaviors in Wireless Networks

In wireless networks, malicious behaviors such as eavesdropping, denial-of-service (DoS) attacks, and spectrum monopolization can often be executed at low or no economic cost to the attacker. This lack of financial deterrents enables potentially harmful users to exploit network resources without significant consequences, leading to an increased risk of security breaches. Without mechanisms to dynamically adjust access costs based on threat levels, malicious users face minimal barriers to misuse, undermining the overall security of wireless environments [159].

Solution: Dynamic Cost Adjustments and Incentive Mechanisms

Implementing dynamic cost adjustments and incentive mechanisms to counteract this issue, wireless networks can implement dynamic cost adjustments that increase the financial barriers for potential attackers. By raising access costs based on suspicious activity levels, networks can make it financially prohibitive for malicious users to carry out prolonged attacks like DoS. This approach relies on adaptive pricing mechanisms that respond to behavior patterns indicative of malicious intent, thus creating a direct economic disincentive for misuse. Additionally, legitimate users can be incentivized to engage in cooperative behaviors, such as jamming, to enhance physical layer security. For example, when legitimate users intentionally interfere with wireless signals in certain contexts, they can help secure the wireless channel by reducing the signal-to-noise ratio, thus making eavesdropping more difficult [252, 253]. This combined approach offers a flexible and scalable framework for promoting network security while creating an economically hostile environment for attackers.

Impact on the user

For end-users, dynamic cost adjustments, and incentive mechanisms introduce an added layer of security that directly impacts their network experience. By financially dissuading malicious users, these mechanisms reduce the likelihood of attacks, enhancing the stability and reliability of the network. For legitimate users, the possibility of earning incentives for cooperative security behaviors, such as engaging in authorized jamming, can result in a more interactive and secure networking environment. Moreover, these adaptive security measures create a balance that improves user trust in the network, as users can feel more confident that malicious actors face tangible deterrents. The increased cost-efficiency achieved through this strategy could also lower service costs over time, making secure access to wireless networks more affordable and accessible for a wider range of users.

3.8 Data Governance

Data governance is a structured framework for managing data assets, encompassing policies and practices that define data ownership, access, usage, and control. By establishing clear guidelines on who can access, modify, and use data, data governance plays a crucial role in enforcing the security of digital assets, making it a key pillar of any cybersecurity system. Identified data governance challenges, solutions, and their impact on users are presented below and summarized in Table 3.7.

3.8.1 Data Governance Complexity in Novel Wireless Networks

Data governance encompasses the organization's data assets, specifying data characteristics such as content, storage, value, and sensitivity, as well as policies regulating ownership, access, and usage

DATA GOVERNANCE		
Problem	**Solution**	**Impact on the User**
Data Governance Complexity in Novel Wireless Networks	- Intelligent Zero Trust Architecture (i-ZTA) - Blockchain technology	- Transparent real-time, verifiable access control mechanisms - Resilient governance framework

Table 3.7: Data Governance problems, solutions, and impact on the user.

rights. In conjunction with cybersecurity, which focuses on defending infrastructure and data against unauthorized access, damage, or misuse, data governance forms an essential component of a holistic security strategy. Effective data governance helps an organization evaluate the value of its data assets, allocating appropriate resources for protection and limiting access to sensitive data that could reveal valuable information. During cyber reconnaissance, for example, attackers often gather information about the organization, a phase where robust data governance frameworks can effectively reduce such risks [209]. However, implementing efficient data governance in novel wireless networks is increasingly challenging due to the scale and diversity of devices, high data transfer rates, and the sheer variety of data types in terms of format, sensitivity, volume, and access. Hence, in next-generation wireless networks, monitoring and enforcing data governance in real time is harder, as data flows across devices and systems that are not centrally controlled. The added complexity of device mobility, where sensitive data may cross multiple jurisdictions with distinct regulations, further complicates data management and compliance.

Solution: Integration of Zero Turst Architecture and Blockchain technologies

To address these governance complexities, integrating Intelligent Zero Trust Architecture (i-ZTA) [109] with blockchain technology offers a powerful solution. i-ZTA enforces continuous, data-centric security by assuming that no device, user, or service is inherently trustworthy. Instead, each access request is authenticated, monitored, and minimally authorized to perform specific tasks. This model leverages AI-driven components that dynamically assess risk and manage access in real-time, making it well-suited for the fast-paced, decentralized environments of 5G and 6G networks. An example of architecture integrating i-ZTA in future 5G/6G networks is presented in [199]. A critical component of this architecture is the reliance on AI models that continually analyze behavioral patterns and refine data access controls, ensuring governance policies are upheld across complex, decentralized networks. These AI models are trained using federated learning strategies, which allow collaborative training of security models across devices without centralizing sensitive data, preserving privacy while ensuring compliance with diverse governance policies.

The addition of blockchain for data governance [14] further enhances i-ZTA by establishing an immutable, tamper-resistant ledger that securely records every access request, data transaction, and security event. This immutability ensures that once an access log or audit trail is recorded, it cannot be altered or removed by attackers—even in the event of a compromised endpoint—preserving a trustworthy, auditable history of activity across the network. By preventing attackers from erasing traces of unauthorized actions, blockchain reinforces the integrity of security operations, making it easier to enforce compliance, audit data flow, and detect security breaches. In a distributed network environment, this decentralized and transparent model provides a unified governance framework, with all participants adhering to consistent data policies. When combined with i-ZTA, blockchain's immutability fortifies continuous data governance, maintaining data integrity and security as data traverses decentralized architectures.

Impact on the user

The combination of i-ZTA and blockchain technology greatly enhances user security by providing real-time, verifiable access control mechanisms that operate transparently across decentralized networks. Users benefit from a resilient governance framework that ensures data access and usage are both compliant and safeguarded, reducing the risk of unauthorized data access. This approach enables a seamless user

experience by adapting security and governance protocols to individual behavior without sacrificing data integrity or accessibility.

Chapter 4

WG4: Human factor in wireless security

Sonay Caner-Yildirim[1], **Argyris Constantinides**[2], **Isabella Corradini**[3], **Vesna Dimitrova**[4], **Gurjot Singh Gaba**[5], **Mohamad Gharib**[6], **Martin Griesbacher**[7], **Abdulsamet Haşiloğlu**[8], **Basak Ozan Ozparlak**[9], **Mustafa Şenol**[10], **Denis Trček**[11], **Anatolijs Zabašta**[12] [1]

[1]Erzincan Binali Yıldırım University - Türkiye
[2]Cognitive UX Ltd - Cyprus
[3]Themis Research Center - Italy
[4]Ss. Cyril and Methodius University in Skopje - North Macedonia
[5]Linköpings Universitet - Sweden
[6]Tartu Ulikool - Estonia
[7]Research Industrial Systems Engineering (RISE) GmbH - Austria
[8]Istanbul Gelisim University - Türkiye
[9]Ozyegin Universitesi - Türkiye
[10]Istanbul Gelisim University - Türkiye
[11]University of Ljubljana, Faculty of Computer and Information Science - Slovenia
[12]Rigas Tehniska Universitate - Latvia

[1]Authors sorted alphabetically by the surname

4.1 Introduction

The growing reliance on wireless networks has made security a critical concern, as these networks often become the target of cyber threats. Although technical solutions are vital, human factors play an equally important role in the security of wireless systems. Personalized cybersecurity solutions that consider user behavior, experience, and ethical concerns are necessary to ensure robust yet user-friendly protection mechanisms. This section explores human factors in wireless security through the following interconnected tasks.

- Task 4.1: Identification of Human-Centric Models for Personalized Security Solutions,
- Task 4.2: Evaluation of the Impact of Personalized Cybersecurity Solutions and
- Task 4.3: Ethical Aspects in Personalized Cybersecurity Solutions.

The first task focuses on identifying human-centric models that integrate security and privacy into IT systems with minimal disruption to the user experience. By involving users during both the design and operational phases, the goal is to create security solutions that are intuitive, seamless, and aligned to performance target, ensuring they are effective without complicating normal workflows.
The second task assesses how personalized cybersecurity measures impact users and overall system security. There is a delicate balance between robust security and a positive user experience. By measuring specific parameters, the task aims to evaluate whether the solutions are secure and user-friendly enough to be widely accepted by end-users, without negatively affecting their interaction with the system. The final task addresses the ethical challenges in developing personalized cybersecurity solutions. As AI and machine learning increasingly process personal data, the definition of "personal data" becomes more fluid. This task introduces an Ethical Design approach to ensure that personalized security measures respect user privacy and data protection laws, while maintaining transparency and trust in how personal data is handled. Together, these tasks form a comprehensive approach to designing personalized cybersecurity solutions that are effective, user-friendly, and ethically sound.

4.2 Task1: Identification of Human-Centric Models for Personalized Security Solutions

To ensure IT systems' security and privacy with minimal impact on user workflow, a variety of human-centric models can be implemented, focusing on user-friendly security systems. By integrating User-Centric Design (UCD), the entire development lifecycle includes user feedback, catering to their needs and behaviors to create seamless security measures [179]. Simplification of security protocols, such as using single sign-on systems, helps reduce complexity without compromising security, making security routines a natural part of user workflows. Transparent security measures operate in the background, like automatic data encryption and anomaly detection through machine learning, ensuring uninterrupted user experience. Moreover, the use of adaptive security mechanisms adapts security levels to the context of user activities, enhancing protection, when necessary, without extra effort from the user [236]. Implementing comprehensive feedback systems provides users with clear and actionable security notifications. Privacy by Design is fundamental in integrating privacy from the ground up, aligning with legal standards like GDPR. Regular security assessments and updates ensure the system remains robust against new threats and user-friendly [147]. These strategies underscore that effective security should support the user experience seamlessly, requiring a multidisciplinary approach that includes cybersecurity, user experience design, and behavioral science [103]. In modern communication technologies, user-centric security models play a pivotal role in enhancing both usability and security [83]. For instance, in cellular wireless technologies ranging from 2G to 6G, there's a focus on simplifying authentication processes and ensuring data encryption remains transparent to the user. Similarly, in WLAN/Wi-Fi networks, streamlined setup procedures are designed to reduce user effort while enhancing the understanding of security settings. The integration of IoT devices within 5G private networks leverages adaptive security based on context and behavior to minimize user input. In vehicular communications, including ITS G5 and 5G systems, the emphasis is on user-friendly interfaces that manage communication settings and automate security updates. For short-range IoT communications like Bluetooth and Zigbee, automatic secure pairing processes and straightforward privacy settings are prioritized to ensure ease of use. Lastly, long-range IoT communications utilizing technologies like LoRa and 5G focus on automated security protocols that adapt to device behavior and user patterns, thus bridging the gap between security and user convenience.

4.2.1 Relevant Aspects

Involving End Users in the Design and Implementation of Usable Security Systems

The increasing reliance on IT systems necessitates robust security measures that ensure both security and privacy. However, these measures often complicate user workflows, reducing efficiency and satisfaction. To identify the best human-centric models for personalized security solutions, it is needed to involve end users in designing and implementing security systems. The goal is to create usable security systems that do not impede regular IT system use, ensuring transparency and minimal impact on user workflows. Human-centered design (HCD) principles can be effectively applied to achieve usable security and privacy in digital systems, i.e., how end-users can protect their information without hindering system usability [100]. Consequently, enhancing overall security and user satisfaction.

Trust in Security Solutions and a Model Proposal

Research of security-related technological solutions highlights the vital role of human trust in these systems. Trust is primarily considered in the context of human-to-human and social relationships, even though trust is clearly not limited to social settings – trust may be also about a technological artifact to function as expected, where security and privacy are among top concerns by users. However, it is crucial that solutions act as anthropomorphic artifacts [106]. Trust can be affected by the system transparency, usability, unobtrusive user engagement, also communications about the system (social element), etc. Since trust is a multifaceted and dynamic phenomenon, a BEiNG-WISE model should consider the following key elements:

- Users may perceive a security solution as secure, even though the solutions is not secure. The key issue is how to "enforce" that users properly perceive secure solutions as secure. Transparency is often emphasized for this goal, but for a security expert, this concept has a different meaning compared to a casual user. Moreover, this perception mostly depends on the context of deployment.

Additionally, it is important to consider the risk perception of users, given that this can affect their security behavior.

- The solution has to be as much invisible as possible, but if this is not possible, it must be minimally obtrusive (by being highly intuitive, for example). The key question is what minimally invasive solutions are, and how to provide it. Usability is often exposed here, but similar as in the above case of transparency, usability is a concept studied from different perspectives, and differs a lot across populations depending on their age, education, willingness to learn new things (early adopters!), etc.
- The solution should be part of a continuous loop of interactions with users in a way that increases trust. The key question is how to achieve this. It is often suggested that the basis is an effective and continuous communication about threats and benefits, but even such communication can easily become irritating or obtrusive for users. Reliability of a solution can be an important factor here, besides, of course, the minimization of incidents.
- Privacy provisioning should be a high priority for a security providing device. If possible, it should be privacy focused, as any leakage of private data will reduce trust, and consequently use of a solution. This is very important to prevent any fear of surveillance – so privacy by design is almost a must.
- When deploying AI, due to the recent ChatGPT hype, users clearly became aware of the importance of explainability. While the problem is clear, it is hard to explain this issue.
- When deploying a security solution, the social factors range from the recommendations and others opinions (including reviews) to institutions (which may impose required ways of use and compliance). An issue is how to address this enough and incorporate this in security solution deployment.

The model proposed will be based on system dynamics, because this is intended to model natural, technical, social, and socio-technical systems [88]. It has been successfully applied in many settings and is one of the best fits for the purpose of WG4 - BEiNG-WISE. System dynamics-based models can provide qualitative as well as quantitative models. While the first kind of models enables better understanding of the observed structure and related concepts, the second kind of models enables quantitative evaluation with simulations. The modeling starts with graphical diagram development, called causal loops diagrams. First, the observed variables have to be identified. By providing causal links between identified variables, these diagrams are obtained. The links can have positive polarity when increased driving variable increases the driven variable, while when decreased driving variable leads to increased output (and vice-versa), links are negative. Variables can be material or non-material (e.g. beliefs). Further, they can be stocks, rates and constants. During the mentioned linking process, loops emerge. These causal loops (also called feedback loops) can be positive (reinforcing) or negative (balancing, stabilizing). These qualitative diagrams provide an insight into systems structure and functioning. They serve as a basis for quantitative models, when backed by formulae that quantify variables and their relationships. So, the basic model proposed for WG4 BEiNG-WISE is given in Fig. 1 (it belongs to the so-called archetype models [96]. It actually contains three layers:

1. The bottom one covers user motivations (a wish to be secure, minimal interference...) and incentives (from legal requirements to positive behavior stimulation).
2. The upper one covers trust, which differs basically in two ways – the first kind of trust is the traditional one, while the second kind of trust is that which is related to a technological solution.
3. The third layer is the central goal of our research, which is the resulting behavior and deployment, which ensures optimal security related to the whole context in a minimally obtrusive way for a user.

Note that this basic model, shown in Figure 4.1 assumes different kinds of technologies, which may require different addressing of the mentioned issues (e.g., they may differ for particular environments like Wi-Fi, VANs, etc.).

Starting from this model, it is possible to discuss through an interdisciplinary approach its different aspects and implement it through the experimental findings achieved during the project.

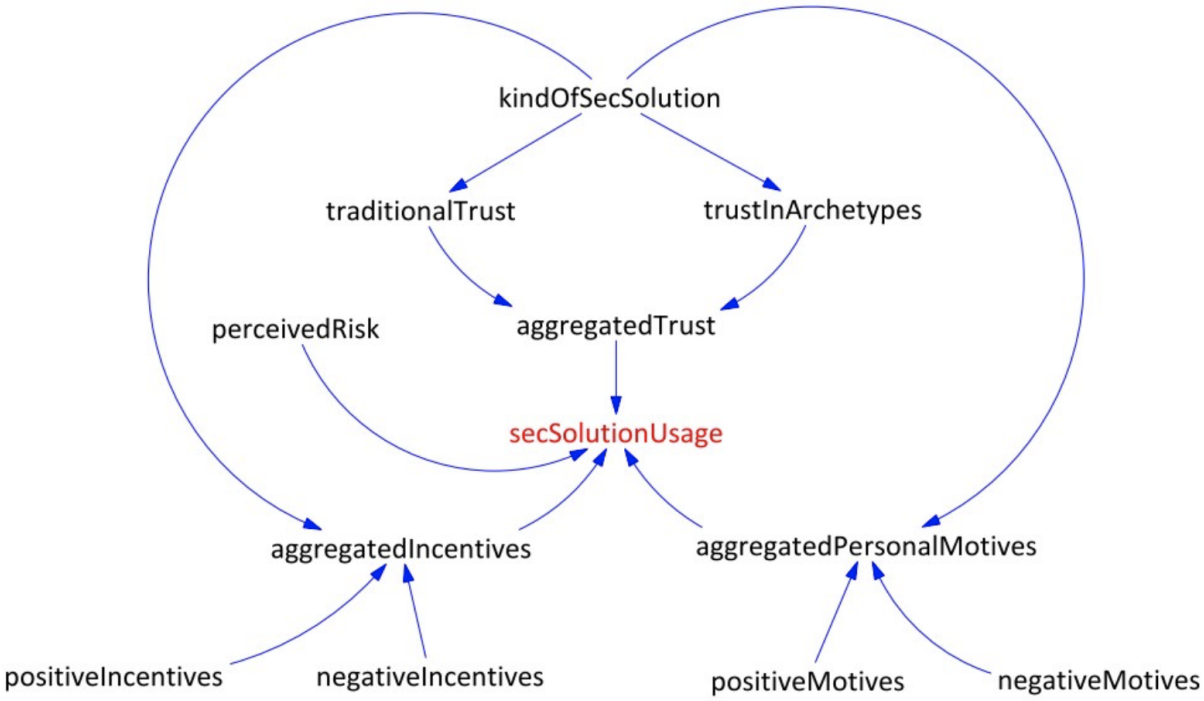

Figure 4.1: Base WG4 BEiNG-WISE model for human factors related to wireless security.

4.2.2 Current Trends

Enhancing Usability
Usability is critical for the effective adoption of security systems. Traditional security measures often neglect the user experience, leading to cumbersome and inefficient processes. Involving end users in the design phase ensures that security features align with their workflows and preferences, making them more intuitive and less intrusive. Research indicates that security systems designed with user input are more likely to be accepted and correctly utilized [4].

Improving Security Outcomes
User involvement can also enhance security outcomes. Users are more likely to comply with security protocols if they find reasonable and easy to follow. When users are engaged in the design process, they provide valuable insight into potential security gaps and practical implementation challenges. This collaborative approach can lead to the development of security measures that are not only robust but also practical and user-friendly [65].

Participatory Design
A systematic literature review [164] has investigated how Privacy-By-Design and Privacy-By-Default principles can be translated into software requirements and how these principles can be integrated into a Human-Centered Design process. The analysis of the resulting publications led to the identification of several software requirements and business processes organized along 8 data-oriented and process-oriented privacy design strategies. The authors identified an initial framework, reporting a set of solutions that different stakeholders can use during the different phases of the software development lifecycle. Participatory design involves users directly in the design process; therefore, it is important to use active methodologies, such as workshops, focus groups, and iterative testing. This approach ensures that the security system evolves based on continuous user feedback. For example, involving users in the creation of password policies can lead to the development of guidelines that balance security and usability, such as creating passwords that are both secure and memorable [208]. This activity can be an example of helpful exercises in organizations, since it can explore employees' sensitivity to cybersecurity issues, encourage them in awareness programs and contribute to the development of a cybersecurity culture [64].
Co-creation workshops bring together users, designers, and security experts to collaboratively develop

security solutions. These workshops facilitate a mutual understanding of security needs and usability concerns. Through brainstorming sessions and collaborative prototyping, participants can devise innovative solutions that meet security requirements without compromising usability [208].

User-Centered Design (UCD)
User-centered design (UCD) is a framework that places the user at the forefront of the design process. UCD involves several stages, including user research, prototyping, and usability testing. By understanding user needs and behaviors, designers can create security solutions tailored to the actual use cases of the system. This iterative process ensures that the final product is both secure and user-friendly [186].

Personalized Security Solutions in the Context of the Relevant "Technologies/Application Domains"

Cellular Wireless Technologies (2/3/4/5/6G)
The rapid evolution of cellular wireless technologies from 1G to 6G presents unique challenges to ensure seamless security while maintaining high performance and good user experience. Each generation of cellular technology has introduced new features and capabilities, necessitating adaptive and transparent security measures [176]. Accordingly, user involvement in the design phase can help identify potential usability issues and ensure that security measures are seamlessly integrated into daily mobile usage. Recent works have explored the aspects of personalization in the realm of cellular wireless networks. More specifically, a research work leveraged Artificial Intelligence (AI), big data analytics, and real-time, non-intrusive user feedback to personalize wireless networks [15]. The proposed personalization framework gathers data from the user environment and the network, anticipates user needs and tolerance to service quality, and optimizes resource allocation to minimize costs while maintaining certain levels of user satisfaction. To facilitate the tracking and measurements of user feedback, the authors also introduced a user satisfaction model based on the concept of the Zone of Tolerance, which refers to "the range of service performance a customer would consider satisfactory". Another work proposed a data-driven architecture tailored for personalized Quality of Experience (QoE) in 5G networks [246]. The proposed architecture includes a monitoring system that gathers real-time data on the applications users are utilizing and the current Quality of Service (QoS) status. The architecture also includes a data mining scheme to predict users' application preferences, and it manages communication resources based on the QoS status and the predicted user preferences to ensure a satisfactory QoE. Nonetheless, the use of data analysis and AI by mobile network operators and service providers to personalize and enhance user experience in future cellular networks poses significant privacy risks, as it can lead to fine-grained privacy invasion and potential leakage of user information if not properly managed [125]. Moreover, improper handling of subscriber identifiers (e.g., Radio Network Temporary Identifier, Globally Unique Temporary Identifier, etc.) can allow attackers to track users' locations.

Wireless Local Area Networks (WLAN/Wi-Fi) and IoT

As smart cities and smart home environments evolve, the need for personalized security solutions is increasing. In such smart environments, accurately identifying individuals is crucial for providing personalized services (e.g., preventing children and the elderly from using hazardous electronic appliances, such as, stove and dryer). A recent work suggested that existing WiFi signals from indoor Internet of Things (IoT) devices can capture unique human physiological and behavioral characteristics to authenticate users during daily activities [220]. The proposed device-free system uses a single pair of WiFi-enabled devices to extract amplitude and relative phase from Channel State Information (CSI) for accurate authentication of users without their active participation. The authors developed a deep-learning model that captures distinct WiFi fingerprints and identifies users, and integrated a spoofing detection mechanism based on a support vector machine. Furthermore, to mitigate the interference from other individuals, the authors proposed to extract features from multiple antennas and designed an architecture based on convolutional neural networks for reliable user authentication. Finally, the authors designed a transfer-learning mechanism to reduce training efforts when updating models for new users or environments. A similar approach for non-intrusive and device-free user authentication based on WiFi signals was proposed in [143]. The proposed user authentication system, coined FingerPass, uses CSI from WiFi signals to continuously authenticate users through finger gestures. The system has two stages: i)

login stage: in this stage, a deep learning-based approach extracts behavioral characteristics from finger gestures for accurate user identification; and ii) interaction stage: in this stage, lightweight classifiers provide continuous real-time authentication to ensure a satisfactory user experience. Designing personalized IoT applications involves dealing with human variability, which encompasses intra-human variability (different behaviors among individuals), inter-human variability (changes in behavior over time within the same individual), and multi-human variability (influence of others in the environment) [78]. To address human variability, the author proposed a reinforcement learning-based framework, coined FaiR-IoT, for adaptive and fairness-aware human-in-the-loop IoT applications. The framework monitors the change in the human reaction and behavior during interactions with the IoT systems and uses three levels of reinforcement learning agents to consider all three forms of human variability. The framework was validated on two IoT applications in simulated environments. Results indicated the positive aspect of adapting to human's variability, in terms of improving the human experience and enhancing the fairness of the multi-human system.

4.2.3 Future Directions

Increased Integration of AI and Machine Learning

Future security systems may increasingly integrate AI and machine learning to adapt to user behaviors and preferences dynamically. This approach can enhance both security and usability by providing personalized security measures that learn from user interactions and adjust accordingly.

Expanding User Involvement
Expanding the scope of user involvement in security design can lead to more comprehensive security solutions. This might include not just end users, but also stakeholders such as IT administrators, security experts, and organizational leaders, ensuring a holistic approach to security design.

Emphasis on Continuous Feedback Loops
Implementing continuous feedback loops where users can report issues and suggest improvements in real-time can help maintain the usability of security systems over time. This ongoing dialogue between users and designers can lead to iterative enhancements that keep security measures effective and user-friendly.

Developing Cross-Platform Usability Standards
As users increasingly operate across multiple devices and platforms, developing cross-platform usability standards for security measures will be crucial. Ensuring a consistent and intuitive user experience across different environments can enhance both security compliance and user satisfaction.

4.2.4 Remarks

By prioritizing user involvement, Task 4.1 aims to identify human-centric models that ensure security without compromising usability, ultimately enhancing both security and user satisfaction. Involving end users in the design and implementation of security systems is crucial for developing solutions that are both secure and usable. Through participatory design, user-centered design, and co-creation workshops, designers can create security measures that align with user workflows and preferences.

4.3 Task2: Evaluation of the Impact of Personalized Cybersecurity Solutions

The impact of cybersecurity solutions on end users is vital to overall system security. Security and user experience have a delicate, interdependent relationship: while users want their connected devices to be reliable and secure, security measures should not compromise the user experience. Therefore, involving users is essential to create personalized security solutions, with their impact assessed through specific metrics that determine the security assurance level and predict whether the solution will be accepted by users.

4.3.1 Relevant aspects

User-Centric Assessment of Personalized Cybersecurity Solutions
The increasing prevalence of cyber threats necessitates the development of cybersecurity solutions that are both effective and user-friendly. As cyber threats evolve, the need for robust cybersecurity measures becomes paramount. The primary goal of personalized cybersecurity solutions is to create a balance between robust security measures and seamless user experience [75]. Users demand their connected devices to be trustworthy and secure, but implementing security should not compromise usability. This delicate balance underscores the importance of involving users in the development of personalized cybersecurity solutions and measuring their impact through specific parameters to ensure security effectiveness and user acceptance. Several user-centric models have been published in journals and in conferences, highlighting how the key factor for the success of these solutions is the convenience for users [12].

Measurement Issues and User Cases
If on the one hand user involvement is needed to develop personalized security solutions, on the other hand the impact of these solutions 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. This is an important challenge, considering that usually the approach adopted is focused on a technology-centric viewpoint, where end users' processes and motivations are largely underestimated [94] [9]. Therefore, a number of non-technical countermeasures need to be considered in cybersecurity management and measurement, like usable rules and practices [190]. In this sense, user cases analyzing both methods used by attackers and victims' perception can help to identify appropriate measures. According to the Swedbank Financial Institute survey (2021), for example, not only the intensity of fraudsters' activity has changed, but also the methods of reaching potential victims. Moreover, the public's general opinion shows that fraud victims and the rest of society have different perceptions of the techniques used by fraudsters, which make them trust their offers. The most effective are the tactics used by fraudsters to hurry up, forcing them to quickly decide in their own interests or those of their loved ones (53%), the ability to create the feeling that the communication is with a representative of a bank or other reliable institution (50%), and the promise of a guaranteed and great financial gain (45%). Meanwhile, victims of fraudsters cite emotional attraction and the ability to gain the potential victim's trust as the primary reason (48%), followed by rush tactics (45%).

4.3.2 Current Trends

Traditional "one-size-fits-all" security solutions might fall short in addressing everyone's needs, since users have varying levels of technical expertise and risk tolerance. With the involvement of users in the design stage and the runtime phase, security solutions can be tailored to their specific needs and preferences. Nonetheless, simply providing a personalized security solution is not adequate. Such solutions must be evaluated based on their security guarantee levels, as well as the impact on the user's experience. Therefore, specific metrics for quantifying this impact are necessary.

In the context of personalized knowledge-based user authentication solutions, indicative metrics for establishing the security level guarantee include: i) number of guesses required to crack the password; ii) password strength meters; and iii) entropy [247], [132], [61], [62]. Furthermore, prior works conducted human guessing attacks studies to investigate whether personalized security solutions suffer from human guessing vulnerabilities [61], [62]. Moreover, by measuring user impact, we can observe whether the solution actually improves security behavior. If users find the solution cumbersome and bypass it, the overall security guarantee level might be weakened. Ultimately, if users find the security solution too

intrusive or difficult to use, they might abandon it altogether. Measuring user impact helps ensure the solution is not only secure but also usable and accepted by the users. Common metrics for quantifying the impact of personalized knowledge-based user authentication solutions include: i) usability dimensions (e.g., task efficiency, task effectiveness, user preference, memorability)[132]; ii) perceived security, memorability, trust, and likeability towards the security solution using questionnaires tailored to the domain the security solution is applied [61] [84]; and iii) perceived usability using the System Usability Scale questionnaire Brooke et al., 1996), which is widely used in security studies [61], [84]. Recent years have seen significant advancements in personalized cybersecurity solutions. These innovations include adaptive security measures that tailor protections based on individual user behaviors and preferences.

Behavioural Biometrics
Behavioral biometrics involve leveraging user behavior patterns for authentication purposes. This reduces reliance on traditional passwords, enhancing security without compromising usability. For example, typing patterns, mouse movements, and touchscreen interactions can be used to verify user identity. Research indicates that behavioral biometrics offer a high level of security while being unobtrusive to the user [102].

Adaptive Security
Adaptive security systems dynamically adjust security measures based on real-time risk assessments and user behavior. This approach allows for tailored protection that responds to the current threat landscape. Adaptive security can significantly improve protection by providing context-aware responses to potential threats.

AI and Machine Learning
Artificial Intelligence (AI) and Machine Learning (ML) are increasingly used in cybersecurity to predict and respond to threats in a personalized manner. These technologies can analyze vast amounts of data to identify patterns and anomalies, offering proactive security measures. AI and ML play a significant role in enhancing personalized cybersecurity by enabling systems to learn and adapt to individual user behaviors.

User Education and Awareness
Educating users about cybersecurity threats and best practices is crucial for fostering a security-conscious culture. User education is essential in preventing security breaches and ensuring that users can effectively utilize security tools.

4.3.3 Discussion

To understand the practical implications of personalized cybersecurity solutions, it is essential to examine real-world case studies, such as the following described.

Behavioral Biometrics in Banking
A leading financial institution implemented behavioral biometrics for user authentication. By analyzing typing patterns and mouse movements, the bank was able to significantly reduce fraudulent activities without disrupting the user experience (FasterCapital, 2024). This case study demonstrates the effectiveness of behavioral biometrics in enhancing security while maintaining usability.

Adaptive Security in Enterprise Networks
A large enterprise adopted adaptive security measures to protect its network infrastructure. The system dynamically adjusted security protocols based on real-time risk assessments and user behavior. This approach resulted in a marked decrease in security breaches and improved user satisfaction due to fewer intrusive security checks (Securus Communication, 2024). This case highlights the benefits of adaptive security in providing tailored protection.

AI and ML in Personalized Threat Detection
A tech company integrated AI and ML into its cybersecurity framework to detect and respond to threats. The AI system analyzes user behavior and network patterns to identify anomalies and potential threats proactively. The implementation led to faster threat detection and response times, enhancing overall

security without compromising user convenience. This example illustrates the transformative potential of AI and ML in personalized cybersecurity (Gaur, 2023).

Tailored User Education Programs
A financial institution implemented a personalized cybersecurity training program for its customers. The program analyzed user transactions and online behaviors to provide customized security advice and alerts. This initiative resulted in a notable decrease in phishing incidents and unauthorized transactions, highlighting the value of personalized user education in enhancing overall security. The expected rapid development of AI/LLM technologies during the year could potentially provide innovative technological solutions for defense capabilities and more effective tools to combat cyber threats. Looking ahead, cyber threat detection tools will be the next logical step for most companies to invest in. Ultimately, early detection and effective response capabilities will be key to mitigating the impact of cyber-attacks. AI/LLM tools will also be used by attackers to analyze and react in real-time to the cyber defense methods used by the victim when conducting attacks. AI/LLM will also be offered as a service, giving attackers ample opportunities to prepare fraudulent attacks to retrieve personal data and payment information faster and easier, in particular, it could facilitate the preparation of targeted cyber-attacks (spear phishing), which is a labor-intensive process. AI/LLM will also provide an opportunity to automate fraudulent phone calls, reducing the human resources needed to carry out attacks. This means that the number and intensity of such fraudulent attacks will increase and users will have to make even greater efforts to protect their data.

4.3.4 Future Directions

The future of personalized cybersecurity solutions lies in further integrating AI and machine learning to create even more sophisticated and user-friendly security measures. Potential advancements include:

- Predictive Security and Improved Usability Utilizing AI to predict potential security threats based on user behaviour and historical data, allowing preemptive actions to be taken. Developing security solutions that are intuitive and unobtrusive is essential for minimizing friction in user interactions.
- Enhanced Biometric Technologies and User Involvement Developing more advanced biometric authentication methods that are harder to spoof and more convenient for users. User involvement in the design and implementation of security measures ensures they are both effective and user-friendly [198].
- Holistic User Profiles and Context-Aware Security Creating comprehensive user profiles that encompass not just digital behaviors but also physical and contextual factors to provide a more complete security assessment. Integrating context-aware systems that consider the user's environment and behavior can provide more accurate and personalized security measures.
- Privacy Preservation Ensuring that personalized cybersecurity solutions do not compromise user privacy is crucial. This involves transparent data handling practices and robust encryption mechanisms. The importance of privacy preservation in the context of personalized cybersecurity cannot be overstated, as secure data management practices are vital.
- Interdisciplinary Research Collaboration between cybersecurity experts, behavioral scientists, and usability researchers can lead to the development of holistic solutions that address both security and user experience. "Interdisciplinary research can provide insights into user behavior and preferences, informing the design of more effective security measures (Rich, M. S. and Aiken, M. P. (2024). Additionally, fostering a culture of cybersecurity awareness through continuous, personalized education will remain crucial. As threats evolve, so must the strategies to educate and protect users, ensuring they are always one step ahead of potential cyber risks.

4.3.5 Remarks

The assessment of personalized cybersecurity solutions underscores the delicate balance between security and user experience. By focusing on user-centric approaches, these solutions can achieve high levels of security without compromising usability. Involving users in the development process, leveraging advanced technologies, and continuously evaluating the impact of these solutions are key to their success. Case studies demonstrate the effectiveness of adaptive security systems, biometric authentication, and

tailored user education programs in various contexts. Looking ahead, integrating advanced technologies and enhancing user education will be pivotal in developing next-generation personalized cybersecurity solutions that are both effective and user-friendly.

4.4 Task3: Ethical aspects in personalised cyber-security solutions

Designing personalized cybersecurity solutions and defining user-friendly security measures through user-centric approaches make ethical considerations increasingly complex. In both the EU and USA, regulations clearly mandate that personal data must be protected, regardless of processing activities. In a highly interconnected digital world with extensive AI and ML usage, defining "personal data" becomes challenging, as the transformation of input data through algorithmic processing can evolve their status into "personal." It's also essential for users to understand how their data is used to stay informed about privacy and security risks. Broadly speaking, personal data includes a significant portion of connected devices, adding complexity to the design of personalized security solutions. These factors point to the need for an Ethical Design approach in creating these solutions, which is the main objective of this task.

4.4.1 Relevant Aspects

Interdisciplinary Studies
Security and privacy are the most challenging yet crucial ethical aspects for next generation wireless networks which are requiring a diminishing level of human intervention and more AI-based network governance. Furthermore, the classification of data as "personal" or "non-personal" will be inadequate for establishing ethical and regulatory standards in the near future. Regardless of the generation of the wireless system, as data flow becomes more ubiquitous thanks to massive sensors and AI-driven technology, the inadequacy of current data protection legal frameworks has long been under debate. In its updated Recommendation on AI, OECD underlines the importance of human intervention when an AI system causes undue harm with regards to safety (OECD Recommendations, 2024 updated version). Different from its predecessors 6G network will not only alter the technological aspects but it will also cause revolutionary changes to the everyday lives of human beings with the novel societal and economical trends. This is one of the reasons that next generation wireless networks require interdisciplinary studies to tackle these novel ethical challenges.

Gender Perspectives in Next-Generation Wireless Networks
The advent of next-generation wireless networks promises unprecedented connectivity and integration of technology into daily life. However, alongside these technological advancements come ethical challenges, particularly concerning gender disparities in cybersecurity knowledge, awareness, and participation. Personalized cybersecurity solutions, which tailor security measures based on individual user characteristics and behaviors, are becoming increasingly prevalent across various wireless technologies, including 5G networks, IoT devices, vehicular communications, and satellite systems. The gender dimension of such personalization raises important ethical considerations that need to be addressed to ensure equitable and secure access for all users in the evolving digital world.

4.4.2 Current Trends

Considering fair competition as an ethical standard for a trustworthy AI in a data driven economy gains much more importance even for security reasons. Depending on only a few cloud and service providers might jeopardize not only innovative initiatives by SME level companies or newcomers to the market but also hinders the ability for sanction mechanisms for security standards against market dominant companies. By establishing fair access to data and limiting data merging between a few companies, not only digital divide but also jeopardizing all the other underlined ethical aspects would be hindered. Human bodies with body-in and body-on sensors will be included as an element of the network with the 6G wireless system. Human body in the network will inevitably involve the human brain with the rapid developments and investments on brain-machine interface technologies. Thus, beginning from the privacy, autonomy and security of the individual human beings must be safeguarded with establishment of trustworthy AI. Next generation wireless systems not only differentiate from today's technology by integrating human beings into the network, but the network will also be highly automated by AI. This leads to an AI ethical framework as a priority area to be focused on. Since the Asilomar principles which were established as an outcome of the Asilomar Conference organized by Future of Life Institute in 2017, many ethical frameworks have been studied and shared across the globe both at national and international levels. As the European Union AI Act has been published in the Official Journal in 2024, it is worth mentioning here that the ethical principle of this regulation is based on the https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf. As pointed out as one of the

seven (accountability, transparency, technical robustness, human oversight, privacy and data governance, diversity-non discrimination and fairness, environmental and societal well-being) ethical principles within this report, robust AI, infers a safe and secure AI system. To mitigate the risks for health, safety and fundamental rights, robustness and human oversight are considered among the requirements that should apply to high-risk AI systems in the AI Act (Recital 66). Also Recital 6 and Recital 66 emphasize a human-centric approach ensuring that AI serves society and respects human dignity. Also with a special emphasis on cyber security measures, Article 14 of the AI Act underlines the importance of human oversight in high risk AI systems. Evaluating the European Union's digital legal framework with a focus of next generation wireless system's cybersecurity requirements from a human centric perspective is highly important for the WG studies of this COST Action.

Current Ethical Challenges from a Gender Perspective
Recent studies have highlighted persistent gender disparities in cybersecurity knowledge and behavior across different cultural contexts. In [149], the authors found that in the United States, females tend to have a lower level of cybersecurity knowledge compared to males. Their research indicated that gender, along with socio-economic status and ethnicity, significantly influences individuals' cybersecurity awareness and behaviors. In a developing country context, Khan et al. (2022) examined cybersecurity and risky behaviors among university students in Pakistan. Their study revealed significant differences in cybersecurity posture and risky Internet behaviors in terms of gender, age, and digital divide variables. Notably, females exhibited less risky behavior than males, although no significant gender difference was found in cybersecurity behavior. Younger students (aged 18–20) showed less risky behavior compared to older students (aged 21–25). The personalization of cybersecurity solutions introduces additional ethical challenges related to gender. AI and machine learning algorithms used in personalized cybersecurity may inadvertently perpetuate gender biases present in training data or reflect societal stereotypes [148]. This can lead to differential treatment or protection levels based on gender, potentially disadvantaging certain groups [33]. Women and gender minorities often face heightened privacy risks online, making the ethical handling of personal data in cybersecurity solutions particularly crucial for these groups [110]. Furthermore, the lack of ethics education in computer science curricula exacerbates these gender disparities. Authors in O'Sullivan et al. (2023) note that ethics is often a missing element in computer science education, and when it is included, it is frequently taught as a standalone subject rather than integrated throughout the curriculum. This gap in education limits the ability of future technology developers to consider ethical implications, including gender biases, in their work. The 2024 EDUCAUSE Horizon Report on Cybersecurity and Privacy emphasises the importance of ethics in shaping cybersecurity practices (EDUCAUSE, 2024). While the report does not explicitly address gendered perspectives, it highlights the need for transparency, trust, and inclusion in cybersecurity efforts. These principles are essential for addressing gender disparities, as they promote an environment where diverse perspectives are valued and considered in cybersecurity strategies. Several factors contribute to these disparities:

Gender Bias in AI-Driven Security Systems AI algorithms used in personalized cybersecurity may perpetuate existing gender biases, leading to unfair treatment or protection levels based on gender [95]. This is a critical concern as next-generation networks increasingly rely on AI for security measures.

Privacy Concerns
Women and gender minorities often face heightened privacy risks online, including technology-facilitated harassment and abuse [110]. Ethical handling of personal data in cybersecurity solutions is crucial to protect these groups. Furthermore, the integration of AI into cybersecurity raises ethical concerns about the balance between security needs and privacy rights [95]. Women and gender minorities often face heightened privacy risks online, making ethical handling of personal data crucial.

Intersectionality
The intersection of gender with other identity factors such as race, age, and socio-economic status creates complex ethical challenges in designing inclusive and fair personalized security measures [263]. Authors in [140] found that digital divides exacerbate gender disparities, with students who have less frequent Internet access exhibiting weaker cybersecurity behaviors.

User Understanding and Consent There is a growing need for transparent and accessible explanations

of how personalized cybersecurity solutions use gender-related data, especially given varying levels of technical literacy across genders [22]. Users must understand and consent to how their data is used to ensure ethical practices.

4.4.3 Discussion of Ethical Challenges from a Gender Perspective

The implications of gender disparities in cybersecurity are multifaceted. From an ethical standpoint, unequal access to technology education and career opportunities violates principles of fairness and equity. Moreover, it undermines the potential effectiveness of cybersecurity measures in next-generation networks. Ethical considerations in gender-aware personalized cybersecurity solutions include: **Fairness and Non-Discrimination**
Ensuring that security measures do not unfairly advantage or disadvantage users based on gender, while still accounting for genuine gender-specific security needs [33]. This requires careful design and testing of AI algorithms to mitigate biases. **Data Minimization and Purpose Limitation**
Balancing the collection and use of gender-related data for security purposes with principles of data minimization to protect user privacy [238]. Excessive data collection can lead to privacy violations, especially for vulnerable groups.

Transparency and Consent
Providing clear and accessible information about how personalized cybersecurity solutions use personal data, including gender-related information, to enable informed user consent [22]. This is essential for building trust and ensuring ethical practices.

Inclusivity and Representation
Incorporating diverse perspectives in the design and testing of personalized security solutions, ensuring representation across gender identities [72]. Diverse teams can help identify and address potential biases in security systems. Addressing these ethical challenges requires a comprehensive approach that considers both technical and human factors. It involves recognizing and dismantling gender biases and creating inclusive environments that encourage participation from all genders. This includes:
Educational Initiatives
Developing programs that encourage girls and women to pursue interests in STEM and cybersecurity from a young age [200]. Education should challenge stereotypes and provide equal opportunities for skill development. Integrating ethics education that includes gender perspectives can enhance awareness and interest [228]. Authors in [140] suggest that tailored cybersecurity training, considering gender and digital divide variables, can improve cybersecurity behaviors among students.
Ethical AI Practices
Implementing fairness-aware machine learning techniques to reduce biases in AI-driven security systems [33]. This involves using diverse and representative datasets, as well as continuous monitoring for unintended biases.
Policy and Regulation
Developing and enforcing regulations that protect against discriminatory practices in personalized cybersecurity solutions [237]. Policies should promote transparency, accountability, and fairness in AI applications.
User Empowerment
Enhancing user understanding of personalized cybersecurity solutions through transparent communication and education [3]. Empowered users are better equipped to make informed decisions about their privacy and security. From an ethical perspective, stakeholders, including governments, educational institutions, and industry leaders, have a responsibility to address these disparities. The EDUCAUSE report notes that institutions face financial constraints but are investing more in cybersecurity and privacy programs. Allocating resources to diversity and inclusion initiatives is essential for building a resilient cybersecurity workforce capable of addressing the complex challenges posed by next-generation wireless networks EDUCAUSE, 2024.

4.4.4 Future directions for Ethical Challenges from a Gender Perspective

Gender disparities in cybersecurity knowledge, participation, and the ethical challenges posed by personalized cybersecurity solutions present significant issues in the context of next-generation wireless networks. These disparities are rooted in societal stereotypes, lack of representation, and unequal access to education

and opportunities. Incorporating ethics education, as advocated by [228], addressing cultural and socio-economic factors, as highlighted by [140], and ensuring fairness in AI-driven security systems are vital steps in addressing these issues. The 2024 EDUCAUSE Horizon Report underscores the importance of ethics, transparency, and inclusion in shaping the future of cybersecurity and privacy. Even not explicitly focused on gender, the principles outlined in the report are essential for addressing gender disparities and building a diverse cybersecurity workforce. Addressing these challenges is not only a matter of fairness but is essential for enhancing the security and effectiveness of emerging technologies. By actively working to close the gender gap and ensuring ethical practices in personalized cybersecurity solutions, we can foster a more diverse and inclusive cybersecurity context. This diversity is crucial for innovation and for developing comprehensive strategies to combat evolving cyber threats. It is imperative that all stakeholders collaborate to implement inclusive policies, provide equal opportunities, and challenge societal biases. Such efforts will ensure that next-generation wireless networks are secure, resilient, and accessible to all, upholding ethical standards of equity and justice.

4.4.5 Remarks

The rapid advancements in AI and next-generation wireless technologies, including the integration of human-centric elements, highlight the need for robust ethical frameworks. The European Union AI Act and similar regulatory efforts emphasize the importance of human oversight, privacy, and security to safeguard individual rights. From a gender perspective, addressing disparities in cybersecurity knowledge and behavior is essential. The ethical design of personalized cybersecurity solutions must mitigate gender biases in AI systems, protect the privacy of vulnerable groups, and promote inclusivity. Incorporating diverse perspectives and providing equal opportunities in education and career development are crucial steps in creating a more inclusive cybersecurity landscape. Future efforts must focus on integrating ethics into technology development, ensuring transparency, and fostering collaboration among stakeholders. By addressing these ethical challenges and disparities, we can build a secure, equitable, and innovative digital future that respects and upholds human dignity and rights.

4.5 Conclusion

The human factor in wireless security is as critical as the technical measures employed. Tasks 4.1, 4.2, and 4.3 highlight the importance of designing personalized, user-centric cybersecurity solutions that protect wireless networks without disrupting user experience or violating ethical standards. By focusing on human-centric models, evaluating the impact on users, and considering ethical aspects, wireless security solutions can be designed to meet both technical requirements and user expectations. These solutions ensure robust security without compromising usability or trust, which is essential for widespread adoption and effective protection in the modern wireless ecosystem. As a final remark, we think that human-centric models should not be reduced to the only questions of early end-user involvement but also consider approaches which focus on design principles like privacy by design, legality by design, data access by design. Maybe, we could propose that whatever model we decide to use, it should be based on “human dignity by design” principle.

Chapter 5

WG5: Legal factors in cybersecurity for wireless systems: a vertical approach

Hartmut Aden[1], **Müge Çetīn**[2], **Periklis Chatzimisios**[3], **Morten Falch**[4], **Ana Ferreira**[5], **José Luis Gómez-Barroso**[6], **Marcel Moritz**[7], **Başak Ozan Özparlak**[2], **Eirini Kanaki**[8] [1]

[1] Authors sorted alphabetically by the surname

5.1 Introduction

From a legal perspective, next-generation wireless communication technologies such as Wireless Fidelity (WiFi), 5G and the upcoming 6G do not constitute a separate area of law. Thus, for legal scholars, these technologies do not constitute a distinct research area but are rather part of broader discussions about the regulation of digital systems. Wireless communication is based on and related to data transmission and processing, and therefore falls within the broader context of digitization and datafication. This chapter summarizes how legal aspects and regulatory frameworks are relevant for research on wireless systems, on cybercrime related to these systems and on humans as central actors – with a specific focus on aspects that are relevant in the framework of the COST Action BEiNG-WISE. In this context, the main purpose of legal research is to adopt legal approaches that have been developed for other areas of digitization and apply these to wireless systems. Another target of the current chapter is the identification of research gaps related to particularities of these emerging wireless technologies that require attention, modifications to existing laws and potential new regulatory approaches. As the BEiNG-WISE COST Action primarily includes researchers from European Union (EU) and Council of Europe (CoE) countries, the chapter more specifically looks at the legal frameworks established at EU and CoE level. However, certain legal issues that are relevant for wireless communication systems are not yet regulated at EU level, remaining under the member states' legislative authority. This means that considerable differences persist concerning the regulatory frameworks and their application across different jurisdictions. This is particularly the case for criminal law and criminal procedure. Thus, in some respect, comparative approaches can help to understand the scope of the legal frameworks applicable to wireless communication systems.

5.2 Wireless systems and fundamental rights

Fundamental rights are the central focus of any legal analysis in a rule of law context. This is even more the case in the perspective of analyzing the role – and the rights – of individuals in the framework of technology development. Processing personal data mainly concerns the fundamental right to privacy and data protection, as it is protected in the European Union by Articles 7 and 8 of the Charter of Fundamental Rights (CFR) that became binding primary EU law with the Treaty of Lisbon in 2009 and by Article 8 of the CoE's European Convention on Human Rights (ECHR). The wording of Article 8 EU-CFR defines the right to data protection and clearly summarizes the main requirements for the processing of personal data that follow from this fundamental right: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority." (Article 8 EU-CFR; main elements highlighted in italics by the authors) Even if fundamental rights are primarily meant to protect citizens against encroachments by public authorities [170], they are also of high relevance for regulatory approaches for data processing by private entities and for the interpretation of these approaches by the courts. This is even more so the case since the EU's General Data Protection Regulation (GDPR) (= Regulation (EU) 2016/679, see further below in section 3) transferred the rules and principles laid down in Article 8 CFR into legal requirements for data processing by private entities, when processing data of EU citizens and public authorities (with the exemption of law enforcement covered by a separate Directive (EU) 2016/680). The use of wireless communication systems may also encroach upon other fundamental rights beyond privacy and data protection. For example, the freedom of expression and information including the freedom of the media (Article 11 EU-CFR) may be directly concerned by the way in which wireless communication systems are designed, used or misused. In particular, wireless communication systems, as essential components of modern digital infrastructure, directly influence how information is transmitted, accessed, and shared. Another right that may be impacted by wireless communication systems is the right to non-discrimination, which is protected under Article 2 of the Universal Declaration of Human Rights (UDHR) and Article 21 of the EU-CFR. In the context of wireless communications, these rights include the obligation to ensure equal and fair access to wireless services and infrastructure, without unfair or biased treatment based on characteristics such as race, gender, ethnicity, nationality, disability, or other protected characteristics. Legal frameworks governing wireless communication systems must also promote digital inclusivity for economically disadvantaged individuals. In particular, this concerns vulnerable groups and those living in remote or rural areas, ensuring they are not excluded from essential communication services. This includes the obligation to create policies that encourage the development of infrastructure in under-

served areas and ensuring that wireless services are designed with accessibility and inclusivity at their core. Indirectly, several other fundamental rights may be concerned: For example, the right to integrity of the person (Article 3 CFR) may be concerned if someone suffers physical damage due to wrongly processed information. The right to liberty and security will be impacted if someone is unduly arrested because of data that has been wrongly processed. In the event of data collected for evidential purposes, Article 6 ECHRcould also apply.

5.3 Wireless systems, EU Data Protection Law and Privacy by Design

With the EU's General Data Protection Regulation (GDPR) (= Regulation (EU) 2016/679), the EU has combined a number of elements that are relevant for data processing in a legal framework that is directly binding – even beyond the EU if data processing concerns the personal data of individuals located in the EU (Article 3(2) GDPR). This has been labelled as the "Brussels effect" of EU law upon the law of third countries [39]. The GDPR defines numerous requirements that are directly applicable for both the developers and users of wireless systems. Linked to the BEiNG-WISE COST Action, it should be emphasized that personal data is given a broad definition, including a wide range of technical data (such as IP or MAC addresses, device identifiers, and other metadata that may be generated during the operation of wireless systems). In some situations, cookies may also be regarded as personal data and fall under the regulations governing personal data within the regulatory scope of the GDPR (Recital 30 GDPR). According to one of the most important requirements, the processing of personal data needs to be based on an adequate legal basis, such as informed consent (Articles 6 and 7 GDPR). If the data subject is a child, the consent for processing personal data is valid only if the child is over 16. However, member states can lower this age limit to 13. For children under the age of consent, data processing is lawful only with the approval of the parents (Article 8). More restrictive rules apply to sensitive data such as information about political or sexual preferences and biometric data (Article 9). The way in which personal data is processed needs to be made transparent to the data subjects (Article 12). This could mean that wireless system developers and operators need to make sure that such information is clearly communicated to data subjects in a transparent, concise, and easily accessible manner, especially given the often complex nature of these systems. Restrictive rules also apply to automated decision-making based on data on individuals and to profiling (Article 21). These are particularly relevant for wireless systems that use artificial intelligence (AI) or machine learning algorithms to process data. In cases of major data breaches, the data controller will have to inform the relevant supervisory authority within 72 hours of becoming aware of the breach (Article 33). Violations of the GDPR can be sanctioned with up to 4 Despite this Europeanization of privacy and data protection law through the GDPR, differences may remain across Europe with respect to the implementation of data protection rules. Users may be more or less concerned by privacy, depending upon the cultural context in which they are living [5] or age. In some cases, even if users are concerned about privacy, they might not know how to exercise their rights (especially younger users or those with limited digital literacy). Companies may be more or less willing to comply with the GDPR correctly. Whether they comply, may either depend upon their business models where data protection friendly settings may be useful to build trust and, thus, get access to (potential) customers. In this case, they might even be willing to implement higher data protection standards than those strictly required by the GDPR in order to differentiate themselves in a competitive market. Other companies may simply try to avoid fines and, thus, just implement the minimum of what the GDPR requires. The principle of privacy by design and by default (Article 25 GDPR) directly links legal requirements and technology development: "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects" (Article 25(1) GDPR). Technology developers should ideally implement the principle of privacy by design by ensuring that privacy does not depend upon the behavior of the users of their systems, but that the technology can only be used in a data protection-compliant way. "Privacy by design" is not a recent expression. However, it has been more focused in Europe since the introduction of the GDPR, which

came into force in 2018. In this regulation, the term used is Privacy by Technology Design which, in a nutshell, aims to guarantee data protection through technology design. Technology should, in principle, promote privacy and protect data. But how can we guarantee and validate that it does? Moreover, in wireless systems and technologies? According to the European Union Agency for Cybersecurity (ENISA) (ENISA), the research community should continue to explore the deployment of (security) techniques and technologies that can support the practical implementation of data protection principles. To reach such practical implementation, we need to start from more theoretical definitions and requirements and then move along to more specific measures and mechanisms, which can translate those ideas into practice. Cavoukian [53] defined seven Foundational Principles of Privacy by Design (PbD) that describe what PbD systems must integrate (Fig. 5.1).

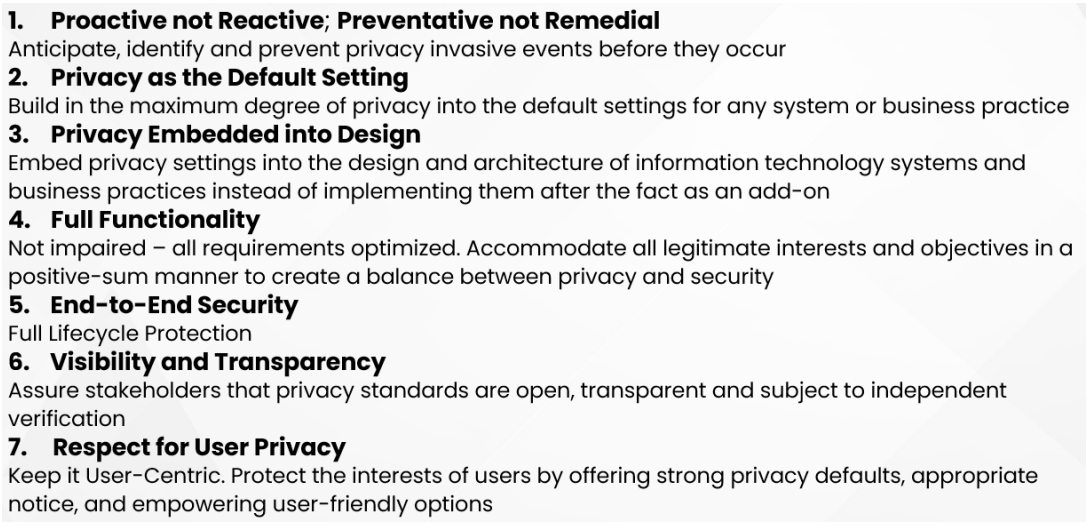

Figure 5.1: Foundational Principles of Privacy by Design.

Similarly, Article 5 GDPR defines principles for data protection in the processing of personal data (Figure 2, on the right).

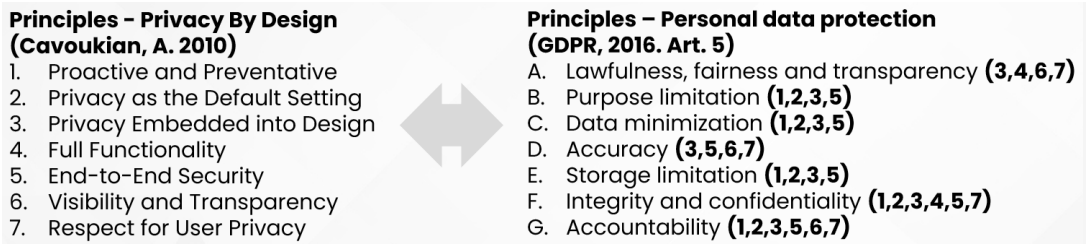

Figure 5.2: GDPR Principles for Data Protection.

From a general analysis of both principles, it is clear that they are related. Focusing on the practicality of implementing GDPR principles described in Article 5 and helping the seven principles of PbD to be integrated within end solutions, we can present examples of solutions or mechanisms that can be used. For example, to comply with Principle 3 - "Privacy Embedded into Design", all GDPR principles need to be taken into consideration, and we can think of a few technologies and mechanisms to focus on those principles:

- A. (Privacy preserving and enhancing techniques, Blockchain, Interaction Design);
- B. (Trusted Execution Environments, Access Control);
- C. (Homomorphic encryption, Differential privacy);
- D. (Trusted Execution Environments, Cryptography, Blockchain, Interaction Design);
- E. (Data retention policy, Audit, Data anonymization);

- F. (Cryptography, Privacy preserving and enhancing techniques, Blockchain, Homomorphic encryption, Differential Privacy, Quantum & Post-quantum cryptography);
- G. (Access Control, Blockchain, Backup policy).

Moreover, emerging technologies can support PbD by optimizing and monitoring most of the GDPR principles of data protection (using AI for instance), or improving traceability (using blockchain for instance). In particular, AI algorithms can help in identifying and mitigating privacy risks in real-time, providing ongoing monitoring and compliance checks that are adaptive to changing environments or data usage patterns. On the other hand, technologies like blockchain can improve traceability and transparency by facilitating decentralized data storage and management, providing users with greater control over their personal information and ensuring that data access is both secure and verifiable. Similarly, this can be done for other PbD Principles, and although more testing needs to be performed, the identified connections between various principles (Figure 2) can be used to identify requirements, and associate those with technologies that need to be applied for the specific architecture components. Wireless communication systems, by their very nature, cannot operate in isolation and they must be integrated into a wider (most likely wired) architecture with specific communication channels (user-systems and between systems themselves), storage spaces (which can be varied, from a mobile application, to a server in a faraway institution), contexts (health, finance, energy, etc) and user interactions (type/size of device, design, content, actions, etc). This is very complex and challenging, especially because wireless technologies have their own vulnerabilities and require specific expertise in terms of cybersecurity and risk assessment to be well understood, developed and configured. To give a few examples of vulnerabilities in the wireless space we can list, with the systems communication channel or at rest: side-channel attacks; vulnerabilities of the wireless protocols; interferences and jamming or no physical pre-defined perimeter; battery consumption; power or acoustic analysis or other vulnerabilities that can be introduced via third parties. With the user-systems channel there are also usability or design problems if this channel was not adequately tested or adapted to the specificities of the context where the systems were set up. Moreover, while some devices are personal and usually attended by their owners, others (e.g., sensors or robots) are generally left unattended and could be placed in remote and/or hostile locations. This greatly increases their vulnerability to physical and/or logical attacks. A thorough risk assessment needs to be performed right from the start of the technology ideation and development process so that appropriate security measures are chosen to tackle the required privacy aspects throughout the entire lifecycle of the technology. Nevertheless, the time and resources spent performing those analyses beforehand will pay off later, meaning less time needed to manage and correct or mitigate risks that were clearly stated from the beginning.

5.4 Wireless systems and *legality by design*

The idea that technologies should be designed in a manner that helps humans to use them in a legal way is not limited to privacy and data protection. Thus, it can and should be more broadly extended to a concept of legality by design [6]. The concept of legality by design represents a proactive approach that goes beyond privacy concerns and can be applied across a wide range of legal domains. It actually suggests that technology developers have a responsibility to embed legal and regulatory requirements directly into the design and architecture of their products. This proactive approach can prevent misuse and ensure that both the technology and its users operate within legal boundaries, mitigating risks for companies, users, and society across various sectors. The idea behind legality by design is, then, to design artifacts lawfully from the beginning. In other words, the goal is to consider legal requirements early in the system's development process. For that, a major problem is that the formulation of laws sometimes makes it difficult for practitioners to extract and operationalize legal requirements. An optimal solution would be the codification of legal knowledge in design patterns. Design patterns are solutions for recurring problems that codify complex domain knowledge in an accessible and applicable way for non-domain experts [79]. Another – second-best – solution is to keep on hand guidelines available to assist in the development process. The European Data Protection Board, which promotes general guidance (including guidelines, recommendations and best practice) to clarify the law and to promote common understanding of EU data protection laws, has delivered a number of interesting documents, including two particular examples of guidelines. One of them is dedicated to facial recognition technologies (European Data Protection Board, 2023), which are, it goes without saying, very sensitive tools. The other one, (European Data Protection Board, 2023), is devoted to the use of virtual voice assistants (VVAs). VVAs serve as an intermediary between users and their computing devices and online services, including search

engines and online shops. As a result of their function, VVAs, currently available on most smartphones and tablets, have access to a vast quantity of personal data, including all users' commands (e.g., browsing or search history) and responses (e.g., appointments in the agenda), that may be transferred to remote VVA servers. Legality by design can be particularly valuable when applied to wireless systems, as these technologies are at the core of many critical infrastructures and involve the processing of sensitive data. For example, procedural requirements for the use of a wireless device may be implemented in a way that the system only opens this application if the completion of the requirement has been confirmed – and even better double-checked by technical means. Where more than one technical option is available, priority should be given to the technical solution that best fulfills the legal requirements. Furthermore, since wireless systems are inherently vulnerable to a variety of cyber threats, legality by design could also ensure secure communications and prevent unauthorized access to critical networks by implementing strong multi-factor authentication protocols by default (i.e., require from WiFI users to authenticate not only with a password but also with a second factor, such as a biometric verification). Another example could be in the context of cybersecurity, in which technologies could be designed to ensure that users follow security best practices, such as using strong passwords or multi-factor authentication, by making these features default and mandatory rather than optional. Legality by design may represent a step forward, but it can never be a definitive ("the") solution to the complex challenges of security and legal compliance. Its promises might be characterized as overly optimistic, as "the struggle for security is really a perpetual Sisyphean task of moving a rock between various degrees of vulnerability [...] and given the extreme erosion in recent years of the basic societal bedrock supporting privacy" [47].

5.5 Wireless systems and the emerging Artificial Intelligence law - EU AI Act and comparative perspectives

Wireless systems are increasingly combined with tools based on AI. Until recently, there was no specific law related to AI in the EU. As AI applications rely on big quantities of data (datasets) for their training and testing, the GDPR applies to AI systems that might be used in combination with wireless systems. This can be a challenge for the development of AI systems, as the relevant data will often not have been collected for the purpose of AI development, but such as through gathered user data from Internet of Things (IoT) devices or mobile applications. Thus, a GDPR-compliant AI development requires data that has been either explicitly collected for the purpose of AI development – with the data subjects' consent - or relying on a legal base. This situation is expected to remain a major topic of political and legal debates in the upcoming years. In 2021, the European Commission published a proposal for a regulation on AI ("AI Act") that was passed in 2024 as Regulation (EU) 2024/1689 after intensive and controversial debates. This regulation establishes a comprehensive legal framework for the development, deployment, and use of AI systems across the EU. Thus, the use of AI in the context of wireless systems will now also have to comply with the rules laid down in this legal instrument that is directly applicable in all EU member states (with some transitional rules). The EU AI Act uses a risk-based approach, defining enhanced obligations for the higher risk categories. Thus, for AI systems in the context of wireless systems, a classification according to the AI Act's risk categories will be required. An AI system classified as highly risky (Annex III of Regulation (EU) 2024/1689) or even as prohibited will require specific attention, as its use might not be permitted outside narrow (mostly law enforcement) exemptions or bound to procedural rules. The technical implementation of such procedural rules should be combined with privacy by design and legality by design approaches (see above). Despite these points in common, there is also a difference in philosophy between the GDPR and the AI Act: while the GDPR is based on a principled and personalistic approach, the AI Act is inspired by the regulations applicable to product safety and develops an approach based on risks apprehended at the level of social groups and particular uses. The practical combination of these two regulations is therefore of great scientific interest.

5.6 Wireless systems and cybersecurity law - criminal law, protection of critical infrastructure: EU rules and comparative aspects

Cybersecurity law is another sub-domain of the law related to digitalisation and datafication. Therefore, data protection and privacy are highly relevant elements in this area [115], [116]. The definition of cybercrime in terms of criminal law is still under the authority of the single European states, which means that definitions, procedures and sanctions may vary from country to country. Besides this, the EU and

the CoE play a major role for the harmonisation of legal (minimum) standards and for administrative rules concerning the protection against cyberattacks, namely for critical infrastructure. In 2001, the CoE passed the Budapest Convention on Cybercrime, a comprehensive legal framework to combat cybercrime at an international level, with member states far beyond the geographical scope of the CoE's membership. In this context, the Octopus conventions can also be mentioned as a tangible instrument for developing cooperation among countries in the fight against cybercrime. Later, Directive 2013/40/EU (often referred to as the Cybercrime Directive), a legal framework of reference for combating cybercrime, expanded and further specified both the content of the Budapest Convention and the Council Framework Decision 2005/222 on attacks against information systems. This directive serves as the primary legal framework for combating cybercrime within the EU by expanding and refining many of the previously introduced legal principles and provisions. The European cybersecurity legal framework includes:

- Directive (EU) 2022/2555 ("NIS 2 directive") that obliges the member states to establish a national cybersecurity strategy (Article 7) and a national cyber crisis management framework (Article 9) to comply with minimum standards for cybersecurity. The member states also have to impose risk management and reporting obligations upon relevant public and private entities (Articles 20 to 21). In particular, the Directive applies to public or private entities which qualify as large and medium-sized enterprises and, regardless of their size, applies to providers of public electronic communications networks or of publicly available electronic communications services; trust service providers; top-level domain name registries and domain name system service providers. Cybersecurity risk-management measures should be based on an all-hazards approach, which aims to protect network and information systems and the physical environment of those systems.
- Directive (EU) 2022/2557, also known as the Directive on the Resilience of Critical Entities (CER Directive), aims to enhance the resilience of critical entities and their ability to provide essential services within the Union, by establishing harmonised minimum rules as well as providing assistance through coherent and specific support and supervisory measures. The particular regime established by the NIS 2 directive makes that obligations laid down in this Directive on the resilience of critical entities "should not apply to entities belonging to the digital infrastructure sector in order to avoid duplication and unnecessary administrative burden". However, Member States should identify those entities belonging to the digital infrastructure sector that have to be defined as critical entities. Consequently, the strategies, the Member State risk assessments and part of the support measures set out in the Directive on the resilience of critical entities do apply. The Cybersecurity Act (Regulation (EU) 2019/881), established a cybersecurity certification framework for products and services. This regulation constitutes the EU's broader strategy to enhance cybersecurity across the EU by creating a comprehensive cybersecurity certification framework for products, services, and processes. The regulation aims to support cybersecurity of digital products and services by introducing standardised certification schemes that ensure a consistent level of security across the EU.

Cybersecurity is also addressed in Article 15 of the AI Act, which claims that "high-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity" and mandates to adhere to specific security requirements, including cybersecurity measures. The 2022 proposals for a regulation on cybersecurity requirements for products with digital elements (Cyber Resilience Act) and for a European Cybersecurity Alert System to improve the detection, analysis and response to cyber threats (Cyber Solidarity Act), are also of great importance. The European Cybersecurity Certification Scheme for Cloud Services which is in the final stages of development is also expected in the near future, aiming to harmonise cybersecurity standards for cloud services across the EU and taking into account international specifications, best industry practices, and the national certifications of EU Member States. Existing and future wireless systems will have to comply with these standards, as far as the entities concerned fall under the scope of these and other legal rules on cybersecurity. As with any defective product, the issue is obviously that of proving the defect. Cybersecurity is an emerging area in regulation of communication networks. 5G and 6G networks are expected to connect billions of IoT devices. If these devices are not properly protected, they can be used for cyberattacks and the diffusion of malware and ransomware.

5.7 Wireless systems and legal aspects of Data Governance

Data Governance as an umbrella term covers the ways in which public and private entities organize their data. Thus, this is not primarily a legal, but rather an organizational and managerial topic. Data governance focuses on managing data flows to ensure privacy, security and quality. With Regulation (EU) 2022/868, the EU has developed a directly binding legal framework for data governance ("Data Governance Act", DGA). The Data Governance Act aims to strengthen frameworks that build trust in data sharing while increasing the availability of data. It is a part of the European Data Strategy. The purpose of this regulation is to facilitate the (re-)use of available data. This regulation does not impose specific rules on wireless systems, however it may be relevant to how data is shared in such systems. In particular, wireless systems are part of the "secure processing environment" provided (or controlled) by a public sector body when impact assessments, the application of privacy-preserving techniques (such as anonymisation, differential privacy, generalisation, suppression and randomisation, or the use of synthetic data) or other safeguards are needed. The DGA establishes specific common European data spaces for data sharing and data pooling. These spaces could cover areas such as health, mobility, manufacturing, financial services, energy or agriculture, or a combination of such areas. The DGA highlights that Common European data spaces should implement the FAIR data principles (findable, accessible, interoperable, re-usable) while ensuring a high level of cybersecurity (Recital 2). The DGA introduces a specific variation of data sharing called data altruism (Article 2(16)). Data altruism refers to situations where data subjects consent to the processing of their personal data for purposes of public interest, such as improving healthcare services, combating climate change, enhancing mobility, and facilitating the development, production, and dissemination of official statistics and improving the provision of public services. The data altruism organisation shall take measures to ensure security for the storage and processing of non-personal data that is collected based on data altruism (Article 14(4)). This may apply to situations where data is stored or processed in connection with wireless systems. The Data Act (Regulation (EU) 2023/2854) is also of interest for wireless systems, as it sets out rules to encourage greater openness of data from the Internet of Things. It aims to provide clear rules for data use and transfer, prevent unfair contracts, allow public sector access to private data in emergencies or legal cases, and make it easier for users to switch between data service providers [52]. It establishes clear rules for data usage permissions, purposes and accessibility. Together with the DGA it plays an important role in the European Data Strategy. This does not impose specific rules on the developers and users of wireless systems, but may be relevant for data generated by such systems.

5.8 Wireless systems and aspects of responsibility and liability

Responsibility is not a purely legal concept, but equally relevant as a philosophical concept and empirically in the perspective of social sciences. In the context of digitalization and datafication, responsibility is a multifaceted concept. It covers the attribution of obligations to the various actors involved. This attribution is in many cases defined in procedural legal rules, for example concerning the obligation to carry out impact assessments or to establish risk management plans. 6G networks will be managed across a disaggregated network and powered by AI and machine learning techniques. The actors in such a scenario will be of very different types, such as, for example, multi-layer service aggregators, network service aggregators, infrastructure aggregators, data centre gatekeepers, or spectrum managers. These roles may also be performed through service provision activities and may operate in cross-border or mixed public-private network environments. Defining responsibilities in this swarm is not an easy task, especially as a result of intelligent automation in decision-making, which is often opaque. Responsibility also includes private law aspects, namely liability for damages that occur. In this context, the attribution of responsibility concerns the question of who will be liable for damages that may be caused by wireless systems and their users. In the interest of transparency, the relevance of the so-called right to explanation – if an automated system makes a decision about us, then we have a right to an explanation of that decision [230] – has to be explored. As with any defective product, the issue is obviously that of proving the defect. Cybersecurity is an emerging area in regulation of communication networks. 5G and 6G networks are expected to connect billions of IoT devices. If these devices are not properly protected, they can be used as remedies for cyberattacks and diffusion of malware and ransomware. This issue is addressed in the EU legislation through the Cybersecurity Act and the forthcoming Cyber Resilience Act. While the Cybersecurity Act aims to create a general framework for certification of products with digital elements, the Cyber Resilience Act defines requirements directly for the manufacturers.

5.9 Standardization of wireless systems and the law

Legal regulation and standardization are two distinct, but interconnected normative approaches to technology regulation. The novelties that 6G will introduce, and its enabling technologies, will require novel interpretation of laws in force and might even trigger additional regulatory frameworks. As underlined in the sections above, many regulatory frameworks already cover recent and future digital transformation in the EU, which are intertwined. Those legal frameworks will be fully in force before 6G is commercially available in 2030. On the other hand, 6G standardization by eminent entities like the International Telecommunication Union (ITU) and the 3rd Generation Partnership Project (3GPP) have already begun. In 2022, the ITU published a framework (ITU 2022), updated in February 2024 (ITU, 2024), to develop 6G standards and radio interface technologies. In this framework regarding regulation and standardization, the ITU defined security and resilience as one of the overarching aspects among sustainability, connecting the unconnected and ubiquitous intelligence, to act as design principles applicable to all use cases (ITU, 2024). Each of these principles is reflected in the already existing regulatory framework in the EU, such as the GDPR, the AI Act, the Data Act, the Data Governance Act, and the Cybersecurity Act. However, a new perspective and novel regulatory mechanisms will also be required to fulfill the expected outcomes of 6G, with a special emphasis on security. In a report released by the ITU in 2022 (ITU, 2022), it is underlined that new international mobile telecommunications (IMT) service and application trends will include empowering citizens as knowledge producers with human-centric innovation, contribution to pluralism and increased diversity. The crucial role of regulation is at this moment undeniable. Instead of falling behind and responding to developments after they rise, regulatory works must proceed in sync and proactively with the innovation and technology regarding the next-generation wireless network during their development phase. In addition to interpreting regulations in force in light of new technologies, it is also necessary to work on and discuss legal issues that are already clearly unable to address new technologies in the 6G era. For example, as one of the 6G services, creating human digital twins will require a new set of rules determining the legal status and legal impacts of a human digital twin, whether it will be deemed as part of a person's identity or a mere digital agent, and the liability issues with respect to the cyber security of the digital twin's software. Also, to present a comparative perspective on 6G, it is interesting to note that the governments of the United States, Australia, Canada, the Czech Republic, Finland, France, Japan, the Republic of Korea, Sweden, and the United Kingdom agreed on a set of common principles for the research and development of 6G wireless communication systems.

These are:

1. Trusted Technology and Protective of National Security
2. Secure, Resilient, and Protective of Privacy
3. Global Industry-led and Inclusive Standard Setting & International Collaborations
4. Cooperation to Enable Open and Interoperable Innovation
5. Affordability, Sustainability, and Global Connectivity
6. Spectrum and Manufacturing.

Nonetheless, while regional agreements are vital, a global set of standards to be established at both national and multinational levels would serve an inclusive and fair next generation network security. One of the novelties of the 6G network is that humans will be an integral part of the 6G network with the body in and body on sensors [257]. In order to provide trust for the network, putting humans at the centre of the next-generation wireless networks is essential. The human body in the network will inevitably involve the human brain with the rapid developments and investments in brain-machine interface technologies. Thus, cybersecurity, privacy, and autonomy of individual human beings must be safeguarded by industry standards and by legislation. One of the dilemmas of regulations in this regard would be conferring data control mechanisms to the data subjects themselves and, at the same time, ensuring cybersecurity. The next-generation wireless system will not only be different from today's technology by integrating human beings into the network, but the network will also be highly automated by AI. This leads to the AI ethical framework being a priority area to be focused on. With its novelty, the 6G network will blur the boundaries between what is online and what is physical. This will have a significant impact on the perception of cybersecurity as it will not be a mere concept belonging to a digital realm; it will have severe impacts on the physical domain as well. This is why an embedded trust

in the 6G network will be essential. Legislation and standardization play a crucial role in establishing a trusted network. Contractual relations between different and new stakeholders of the communication ecosystem will also be significant areas of legal research and disputes in the 6G era. Policymakers and regulators need to reassess existing spectrum management policies to meet the specific needs of 6G since the implementation of 6G will necessitate a fundamental change in spectrum management, as spectrum sharing will play a critical role in the efficient use of limited resources [19]. Today, big tech companies already have significant data and control power. They are well prepared to determine how the digital world will operate through the control of data and even through digital currencies. If this question is left unanswered, human rights may be jeopardized, and 6G may not achieve the expected social benefits or inclusive development for all. Depending on only a few cloud and service providers might jeopardize innovative initiatives by SME-level companies or newcomers to the market and hinder the ability for sanctioning mechanisms for security standards against market-dominant companies. By establishing fair access to data and limiting data merging between a few companies, overcoming the digital divide and all the other underlying ethical aspects would be hindered. Research on regulation and standardization for next generation wireless networks is relevant today, as in the beginning of 2027, relevant stakeholders will submit proposals for the IMT-2030 Radio Interface Technology (RIT) for ITU-R consideration to be evaluated for the 6G technology standards to be approved by 2030.

5.10 Conclusion

This chapter has shown that the state of the art of research on legal aspects of current and future wireless systems is characterized by multiple aspects. The chapter has selected aspects that are of specific relevance for wireless systems and the risks occurred at the development stage of such systems. Technological developments are mostly much faster than legislative reactions to them. The law therefore has to evaluate new technological developments and define the necessary reactions and adaptations, especially with respect to the protection of the fundamental rights of those concerned. If this evaluation takes place in cooperation with technology development, this helps to implement technical solutions that enable high standards of legality and of protection of fundamental rights. Privacy by design and legality by design approaches, as they have been described in this chapter are therefore of particular relevance for interdisciplinary cooperation between legal scholars and scholars from informatics and other disciplines on future wireless communication systems.

Chapter 6

Conclusion

The journey around different facets of cyber security is far to be easy or to be concluded, it is an open challenge, with several (important) issues. After delving on this first year of BEiNG-WISE activities, it is also more convincing that a drastic paradigm shift is needed. A different perspective, with the integration of the final user/human being by design may appear clear, logic, but the reading of this document through the different WGs permit to confirm that it is not the case up to day, and it is not straightforward. Generally, the technology evolves fast, often with de-facto standards that impose, without having the same evolution in terms of legal and ethical regulations. Moreover, users are more and more with different expertise level, age, gender: all these factors have an impact on the use of the technology and how the users interact with it. Some important connection points have been identified in this manuscript, by developing the different "threads" with a separate approach, to establish the status-quo of the cybersecurity approaches. This permits to identify in a clearer way the next step towards the implementation of BEiNG-WISE vision in terms of cyber security.

Acknowledgements We express our heartfelt gratitude and appreciation to all the individuals who have contributed to the successful completion of this first report. A special thanks to Hartmut Aden, Mohamad Gharib and Salko Kovacic for having reviewed the document and Sonay Caner-Yildirim for the cover.

Bibliography

[1] Sherif Abdelwahab, Bechir Hamdaoui, Mohsen Guizani, and Taieb Znati. Network function virtualization in 5g. *IEEE Communications Magazine*, 54(4):84–91, 2016.

[2] Ihsan H Abdulqadder, Deqing Zou, Israa T Aziz, Bin Yuan, and Weiqi Dai. Deployment of robust security scheme in sdn based 5g network over nfv enabled cloud environment. *IEEE Transactions on Emerging Topics in Computing*, 9(2):866–877, 2018.

[3] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Comput. Surv.*, 50(3), August 2017. ISSN 0360-0300. doi:10.1145/3054926. URL https://doi.org/10.1145/3054926.

[4] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun. ACM*, 42(12):40–46, December 1999. ISSN 0001-0782. doi:10.1145/322796.322806. URL https://doi.org/10.1145/322796.322806.

[5] Hartmut Aden. *Privacy and Security: German Perspectives, European Trends and Ethical Implications*, pages 119–129. 01 2022. isbn:978-1-80262-414-4. doi:10.1108/S2398-601820210000008009.

[6] Hartmut Aden and Jan Fährmann. Data protection assessment and transparency deficits in technology use: An analysis using the example of police data processing. *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis*, 29(3):24–29, Dec. 2020. doi:10.14512/tatup.29.3.24. URL https://www.tatup.de/index.php/tatup/article/view/6832.

[7] Damilola Adesina, Chung-Chu Hsieh, Yalin E. Sagduyu, and Lijun Qian. Adversarial machine learning in wireless communications using rf data: A review. *IEEE Communications Surveys & Tutorials*, 25(1):77–100, 2023. doi:10.1109/COMST.2022.3205184.

[8] Mamta Agiwal, Abhishek Roy, and Navrati Saxena. Next generation 5g wireless networks: A comprehensive survey. *IEEE Communications Surveys Tutorials*, 18(3):1617–1655, 2016. doi:10.1109/COMST.2016.2532458.

[9] Rachid Ait Maalem Lahcen, Ram Mohapatra, and Manish Kumar. *Cybersecurity: A Survey of Vulnerability Analysis and Attack Graphs: ICMC 2018, Varanasi, India, January 9-11, Selected Contributions*, pages 97–111. 09 2018. isbn:978-981-13-2094-1. doi:10.1007/978-981-13-2095-8_9.

[10] N. Akdemir and B. Sungur. *i Başaranel*. B. (2020). Examining the challenges of policing economiccybercrime in the UK. GüvenlikBilimleri Dergisi, (International Security Congress Special Issue), 2020.

[11] R. L. Akers. *Social Learning and Social Structure: A General Theory of Crime and Deviance*. Boston, MA: Northeastern University Press, 1998.

[12] Raja Naeem Akram, Hsiao-Hwa Chen, Javier Lopez, Damien Sauveron, and Laurence T. Yang. Security, privacy and trust of user-centric solutions. *Future Generation Computer Systems*, 80: 417–420, 2018. ISSN 0167-739X. doi:https://doi.org/10.1016/j.future.2017.11.026. URL https://www.sciencedirect.com/science/article/pii/S0167739X17326146.

[13] Abdullah Al Hasib and Abul Ahsan Md Mahmudul Haque. A comparative study of the performance and security issues of aes and rsa cryptography. In *2008 third international conference on convergence and hybrid information technology*, volume 2, pages 505–510. IEEE, 2008.

[14] Lampis Alevizos, Vinh Thong Ta, and Max Hashem Eiza. Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. *Security and privacy*, 5(1):e191, 2022.

[15] Rawan Alkurd and Ibrahim Abualhaol. Big-data-driven and ai-based framework to enable personalization in wireless networks. *IEEE Communications Magazine*, 58:18–24, 03 2020. doi:10.1109/MCOM.001.1900533.

[16] Ala Saleh D Alluhaidan and P Prabu. End-to-end encryption in resource-constrained iot device. *IEEE Access*, 11:70040–70051, 2023.

[17] Ihab Almaameri and László Blázovics. An overview of drones communication, application and challenge in 5g network. In *2023 6th International Conference on Engineering Technology and its Applications (IICETA)*, pages 67–73. IEEE, 2023.

[18] Muntadher Alsabah, Marwah Abdulrazzaq Naser, Basheera M. Mahmmod, Sadiq H. Abdulhussain, Mohammad R. Eissa, Ahmed Al-Baidhani, Nor K. Noordin, Sadiq M. Sait, Khaled A. Al-Utaibi, and Fazirul Hashim. 6g wireless communications networks: A comprehensive survey. *IEEE Access*, 9:148191–148243, 2021. doi:10.1109/ACCESS.2021.3124812.

[19] Wijdan Alsaedi, Hamed Ahmadi, Zaheer Khan, and David Grace. Spectrum options and allocations for 6g: A regulatory and standardization review. *IEEE Open Journal of the Communications Society*, PP:1–1, 01 2023. doi:10.1109/OJCOMS.2023.3301630.

[20] Jafar A. Alzubi, Omar A. Alzubi, Ashish Singh, and Manikandan Ramachandran. Cloud-iiot-based electronic health record privacy-preserving by cnn and blockchain-enabled federated learning. *IEEE Transactions on Industrial Informatics*, 19(1):1080–1087, 2022.

[21] Nikolaos Athanasios Anagnostopoulos, Saad Ahmad, Tolga Arul, Daniel Steinmetzer, Matthias Hollick, and Stefan Katzenbeisser. Low-cost security for next-generation iot networks. *ACM Transactions on Internet Technology (TOIT)*, 20(3):1–31, 2020.

[22] Mike Ananny and Kate Crawford. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, 20(3):973–989, 2018. doi:10.1177/1461444816676645. https://doi.org/10.1177/1461444816676645. URL https://doi.org/10.1177/1461444816676645.

[23] Omar Ansari and Muhammad Amin. Directional modulation techniques for secure wireless communication: a comprehensive survey. *EURASIP Journal on Wireless Communications and Networking*, 2022(1):93, 2022.

[24] Emre Ates, Burak Aksar, Vitus J Leung, and Ayse K Coskun. Counterfactual explanations for multivariate time series. In *2021 international conference on applied artificial intelligence (ICAPAI)*, pages 1–8. IEEE, 2021.

[25] Ahmad Azab, Mahmoud Khasawneh, Saed Alrabaee, Kim-Kwang Raymond Choo, and Maysa Sarsour. Network traffic classification: Techniques, datasets, and challenges. *Digital Communications and Networks*, 2022.

[26] Imen Azzouz, Boumedyen Boussaid, Ahmed Zouinkhi, and M. Naceur Abdelkrim. Multi-faults classification in wsn: A deep learning approach. In *2020 20th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, pages 343–348, 2020. doi:10.1109/STA50679.2020.9329325.

[27] Maria Bada and Jason Nurse. *The social and psychological impact of cyberattacks*, pages 73–92. 01 2020. isbn:9780128162033. doi:10.1016/B978-0-12-816203-3.00004-6.

[28] Alireza Bahramali, Milad Nasr, Amir Houmansadr, Dennis Goeckel, and Don Towsley. Robust adversarial attacks against dnn-based wireless communication systems. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 126–140, 2021.

[29] Billy Baker, John Woods, Martin J Reed, and Martin Afford. A survey of short-range wireless communication for ultra-low-power embedded systems. *Journal of Low Power Electronics and Applications*, 14(2):27, 2024.

[30] A. Bandura. Behavioral modification through modeling procedures. In L. Krasner and L. P. Ullman, editors, *Research in behavior modification*. Holt, New York, NY, 1965.

[31] A. Bandura. *Principles of behavior modification*. New York, NY: Holt, Rinehart Winston, 1969.

[32] A. Bandura. *Social learning theory*. Englewood Cliffs, NJ: Prentice Hall, 1977.

[33] Solon Barocas, Moritz Hardt, and Arvind Narayanan. *Fairness and Machine Learning: Limitations and Opportunities*. MIT Press, 2023.

[34] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The simon and speck lightweight block ciphers. In *Proceedings of the 52nd annual design automation conference*, pages 1–6, 2015.

[35] Aditya Bhattacharya. *Applied Machine Learning Explainability Techniques: Make ML models explainable and trustworthy for practical applications using LIME, SHAP, and more*. Packt Publishing Ltd, 2022.

[36] Andrey Bogdanov, Lars R Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin, and Charlotte Vikkelsoe. Present: An ultra-lightweight block cipher. In *Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9*, pages 450–466. Springer, 2007.

[37] Emilie Bout, Valeria Loscri, and Antoine Gallais. Evolution of iot security: The era of smart attacks. *IEEE Internet of Things Magazine*, 5(1):108–113, 2022. doi:10.1109/IOTM.001.2100183.

[38] Emilie Bout, Valeria Loscri, and Antoine Gallais. How machine learning changes the nature of cyberattacks on iot networks: A survey. *IEEE Communications Surveys Tutorials*, 24(1):248–279, 2022. doi:10.1109/COMST.2021.3127267.

[39] Anu Bradford. *The Brussels Effect: How the European Union Rules the World*. Oxford University Press, 02 2020. isbn:9780190088583. doi:10.1093/oso/9780190088583.001.0001. URL https://doi.org/10.1093/oso/9780190088583.001.0001.

[40] J. S. Brenner. american academy of pediatrics council on sports medicine and fitness (2007). *Overuse injuries, overtraining, and burnout in child and adolescent athletes. Pediatrics*, 119(6), 2007.

[41] Alessandro Brighente, Francesco Formaggio, Marco Centenaro, Giorgio Maria Di Nunzio, and Stefano Tomasin. Location-verification and network planning via machine learning approaches. In *2019 International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOPT)*, pages 1–7, 2019. doi:10.23919/WiOPT47501.2019.9144111.

[42] S. Brown. *(2023)*. Key messages from research on child sexual abuse by adults in online contexts.

[43] M. Bruce, J. Lusthaus, R. Kashyap, N. Phair, and F. Varese. (2024). *Mapping the global geography of cybercrime with the World Cybercrime Index. PLOS ONE*, 19(4).

[44] A. Bryan. Digital piracy: Neutralising piracy on the digital waves. *Plymouth Law and Criminal Justice Review*, 6(1):214–235, 2014.

[45] M. Button and C. Cross. *Cyber Frauds, Scams and their Victims*. Routledge, 2017.

[46] Ismail Butun and Ian F Akyildiz. Low-power wide-area networks: Opportunities, challenges, risks and threats. 2023.

[47] Lee A Bygrave. Security by design: Aspirations and realities in a regulatory context. *Oslo Law Review*, (3):126–177, 2022.

[48] E. Calvete, I. Orue, and M. Gámez-Guadix. A preventive intervention to reduce risk of online grooming among adolescents. *Psychosocial Intervention*, 31(3):177–184, 2022.

[49] R. L. Cant, M. Harries, and C. Chamarette. Using a public health approach to prevent child sexual abuse by targeting those at risk of harming children. *International Journal on Child Maltreatment: Research, Policy and Practice*, 5:573–592, 2022.

[50] N. Carlini and D. Wagner. Towards evaluating the robustness of neural networks. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 39–57. IEEE Computer Society, may 2017. doi:10.1109/SP.2017.49.

[51] J. Carr. *Mechanisms for collective action to prevent and combat online child sexual exploitation and abuse*. Council of Europe, 2019.

[52] Federico Casolari, Carlotta Buttaboni, and Luciano Floridi. The eu data act in context: a legal assessment. *International Journal of Law and Information Technology*, 31(4):399–412, 02 2024. ISSN 0967-0769. doi:10.1093/ijlit/eaae005. https://academic.oup.com/ijlit/article-pdf/31/4/399/56963829/eaae005.pdf. URL https://doi.org/10.1093/ijlit/eaae005.

[53] Ann Cavoukian. Privacy by design: The 7 foundational principles: Implementation and mapping of fair information practices. Toronto: Information & Privacy Commissioner of Ontario., 2010.

[54] Jinyin Chen, Jie Ge, Shilian Zheng, Linhui Ye, Haibin Zheng, Weiguo Shen, Keqiang Yue, and Xiaoniu Yang. Air: Threats of adversarial attacks on deep learning-based information recovery. *IEEE Transactions on Wireless Communications*, pages 1–1, 2024. doi:10.1109/TWC.2024.3374699.

[55] Junbao Chen, Jingfeng Xue, Yong Wang, Lu Huang, Thar Baker, and Zhixiong Zhou. Privacy-preserving and traceable federated learning for data sharing in industrial iot applications. *Expert Systems with Applications*, 213:119036, 2023.

[56] Shaolei Chen, Neng Zhao, Meng Ding, Yuan Liang, Haizhou Tang, Chengshi Zhao, and Fei Lin. Vision, requirements, and network architecture of 6g mobile network beyond 2030. *IEEE Network*, 34(6):36–43, 2020.

[57] Samuel Chng and Lu. Han and kumar. *Ayush and Yau, David. (2022). Hacker types, motivations and strategies: A comprehensive framework. Computers in Human Behavior Reports. 5. 100167*, 5.(10.):100167., 2022.

[58] Y. T. Chua, /, and T. J. Holt. A cross-national examination of the techniques of neutralization to account for hacking behaviors. *Victims and Offenders*, 11(4):534–555, 2016.

[59] L. E. Cohen and M. Felson. *On estimating the social costs of national economic policy: A critical examination of the Brenner study*. Social Indicators Research6, 1979.

[60] Amparo Coiduras-Sanagustín, Eduardo Manchado-Pérez, and César García-Hernández. Understanding perspectives on personal data privacy in internet of things (iot): A systematic literature review (slr). *Heliyon*, 2024.

[61] Argyris Constantinides, Christos Fidas, Marios Belk, Anna Pietron, Ting Han, and Andreas Pitsillides. From hot-spots towards experience-spots: Leveraging on users' sociocultural experiences to enhance security in cued-recall graphical authentication. *International Journal of Human-Computer Studies*, 149:102602, 02 2021. doi:10.1016/j.ijhcs.2021.102602.

[62] Argyris Constantinides, Marios Belk, Christos Fidas, Roy Beumers, David Vidal, Wanting Huang, Juliana Bowles, Thais Webber, Agastya Silvina, and Andreas Pitsillides. Security and usability of a personalized user authentication paradigm: Insights from a longitudinal study with three healthcare organizations. *ACM Trans. Comput. Healthcare*, 4(1), February 2023. doi:10.1145/3564610. URL https://doi.org/10.1145/3564610.

[63] Jonathan Cook, Sabih Ur Rehman, and M Arif Khan. Security and privacy for low power iot devices on 5g and beyond networks: Challenges and future directions. *IEEE Access*, 11:39295–39317, 2023.

[64] Isabella Corradini. *Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology*. 01 2020. isbn:978-3-030-43998-9. doi:10.1007/978-3-030-43999-6.

[65] Lorrie Faith Cranor. A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*, UPSEC'08, USA, 2008. USENIX Association.

[66] Hong-Ning Dai, Hao Wang, Hong Xiao, Xuran Li, and Qiu Wang. On eavesdropping attacks in wireless networks. In *2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES)*, pages 138–141, 2016. doi:10.1109/CSE-EUC-DCABES.2016.173.

[67] J. Davidson, E. Martellozzo, and M. Lorenz. *Evaluation of CEOP ThinkUKnow internet safety programme and exploration of young people's internet safety knowledge.* Centre for Abuse Trauma Studies and Kingston University, 2009.

[68] Karin De Bruijn, Joost Buurman, Marjolein Mens, Ruben Dahm, and F. Klijn. Resilience in practice: Five principles to enable societies to cope with extreme weather events. *Environmental Science Policy*, 70:21–30, 02 2017. doi:10.1016/j.envsci.2017.02.001.

[69] Cailian Deng, Xuming Fang, Xiao Han, Xianbin Wang, Li Yan, Rong He, Yan Long, and Yuchen Guo. Ieee 802.11 be wi-fi 7: New challenges and opportunities. *IEEE Communications Surveys & Tutorials*, 22(4):2136–2166, 2020.

[70] Van der Hulst, R. C. ; Neve, and R. J. *High Tech Crime Literature Review about Crimes and Their Offenders; WODC (Research and Documentation Centre): The Hague, The Netherlands.* 2008.

[71] G Devi, N Jayanthi, S Rahul, M Saran Karthick, S Gokul Raghavendra, and M Anand. A critical review on li-fi technology and its future applications. In *AIP Conference Proceedings*, volume 2690. AIP Publishing, 2023.

[72] Catherine D'Ignazio and Lauren F. Klein. *Data Feminism.* The MIT Press, 03 2020. isbn:9780262358521. doi:10.7551/mitpress/11805.001.0001. https://direct.mit.edu/book-pdf/2390355/book_9780262358521.pdf. URL https://doi.org/10.7551/mitpress/11805.001.0001.

[73] Charlette Donalds and Kweku-Muata Osei-Bryson. (2019). *Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. International Journal of Information Management. 51. 102056*, 51.(10.):102056., 2019.

[74] B. Dupont. Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law, and Social Change*, 67:97–116, 2017.

[75] Saurabh Dutta, Stuart Madnick, and Ger Joyce. Secureuse: Balancing security and usability within system design. volume 617, pages 471–475, 06 2016. isbn:978-3-319-40547-6. doi:10.1007/978-3-319-40548-3_78.

[76] Phan The Duy, Nghi Hoang Khoa, Hien Do Hoang, and Van-Hau Pham. Investigating on the robustness of flow-based intrusion detection system against adversarial samples using generative adversarial networks. *Journal of Information Security and Applications*, 74:103472, 2023.

[77] Aboujaoude E. Protecting privacy to protect mental health: the new ethical imperative. *Journal of medical ethics*, 45(9), 2018.

[78] Salma Elmalaki. Fair-iot: Fairness-aware human-in-the-loop reinforcement learning for harnessing human variability in personalized iot. In *Proceedings of the International Conference on Internet-of-Things Design and Implementation*, IoTDI '21, page 119–132, New York, NY, USA, 2021. Association for Computing Machinery. isbn:9781450383547. doi:10.1145/3450268.3453525. URL https://doi.org/10.1145/3450268.3453525.

[79] Matthias Söllner Ernestine Dickhaut, Andreas Janson and Jan Marco Leimeister. Lawfulness by design – development and evaluation of lawful design patterns to consider legal requirements. *European Journal of Information Systems*, 33(4):441–468, 2024. doi:10.1080/0960085X.2023.2174050. https://doi.org/10.1080/0960085X.2023.2174050. URL https://doi.org/10.1080/0960085X.2023.2174050.

[80] Adil Fahad, Abdulmohsen Almalawi, Zahir Tari, Kurayman Alharthi, Fawaz S. Al Qahtani, and Mohamed Cheriet. Semtra: A semi-supervised approach to traffic flow labeling with minimal human effort. *Pattern Recognition*, 91:1–12, 2019.

[81] Alexander Felix, Sebastian Cammerer, Sebastian Dörner, Jakob Hoydis, and Stephan Ten Brink. Ofdm-autoencoder for end-to-end learning of communications systems. In *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pages 1–5, 2018. doi:10.1109/SPAWC.2018.8445920.

[82] Wanmei Feng, Jie Tang, Nan Zhao, Xiuyin Zhang, Xianbin Wang, and Kai-Kit Wong. A deep learning-based approach to resource allocation in uav-aided wireless powered mec networks. In *ICC 2021 - IEEE International Conference on Communications*, pages 1–6, 2021. doi:10.1109/ICC42927.2021.9500582.

[83] Mohamed Amine Ferrag, Leandros Maglaras, Antonios Argyriou, Dimitrios Kosmanos, and Helge Janicke. Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, 101:55–82, 2018. ISSN 1084-8045. doi:https://doi.org/10.1016/j.jnca.2017.10.017. URL https://www.sciencedirect.com/science/article/pii/S1084804517303521.

[84] Christos A. Fidas, Marios Belk, Argyris Constantinides, David Portugal, Pedro Martins, Anna Maria Pietron, Andreas Pitsillides, and Nikolaos Avouris. Ensuring academic integrity and trust in online learning environments: A longitudinal study of an ai-centered proctoring system in tertiary educational institutions. *Education Sciences*, 13(6), 2023. ISSN 2227-7102. doi:10.3390/educsci13060566. URL https://www.mdpi.com/2227-7102/13/6/566.

[85] Bobby Filar, Richard Seymour, and Matthew Park. Ask me anything: A conversational interface to augment information security workers. In *SOUPS*, 2017.

[86] Bryse Flowers, R. Michael Buehrer, and William C. Headley. Evaluating adversarial evasion attacks in the context of wireless communications. *IEEE Transactions on Information Forensics and Security*, 15:1102–1113, 2020. doi:10.1109/TIFS.2019.2934069.

[87] G. Forni, A. Pietronigro, N. Tiwana, C. E. Gandolfi, Del Castillo, Mosillo G., M., and A. Pellai. (2020). *Little red riding hood in the social forest. Online grooming as a public health issue: A narrative review. Annali di Igiene: Medicina Preventiva e di Comunita*, 32(3):305–318, 2020.

[88] Jay W. Forrester. System dynamics, systems thinking, and soft or. *System Dynamics Review*, 10: 245–256, 1994. URL https://api.semanticscholar.org/CorpusID:62114666.

[89] A. Gannoni, A. Voce, S. Napier, H. Boxall, and D. Thomsen. Preventing child sexual abuse material offending: An international review of initiatives. *Research Report no*, 28., 2023.

[90] A. Gewirtz-Meydan, W. Walsh, J. Wolak, and D. Finkelhor. The complex experience of child pornography survivors. *Child Abuse Neglect*, 80:238–248, 2018.

[91] Bimal Ghimire and Danda B Rawat. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. *IEEE Internet of Things Journal*, 9(11): 8229–8249, 2022.

[92] E. C. Gilson. Vulnerability and victimization: Rethinking key concepts in feminist discourses on sexual violence. *Signs: Journal of Women in Culture and Society*, 42(1):71–98, 2016.

[93] Marco Giordani, Michele Polese, Arjun Roy, Sangjoon Doo, Sundeep Rangan, and Michele Zorzi. Toward 6g networks: Use cases and technologies. *IEEE Communications Magazine*, 58(3):55–61, 2020.

[94] Henry Glaspie and Waldemar Karwowski. Human factors in information security culture: A literature review. pages 269–280, 07 2018. isbn:978-3-319-60584-5. doi:10.1007/978-3-319-60585-2_25.

[95] Pawan Kumar Goel. *Ethical considerations in implementing artificial intelligence in cybersecurity: Balancing security and privacy concerns. In Redefining Security with Cyber AI*, pages 85–104. IGI Global, 2024. URL https://orcid.org/0000-0003-3601-102X.

[96] Jose Gonzalez and Denis Trcek. Proper incentives for proper it security management - a system dynamics approach. 01 2017. doi:10.24251/HICSS.2017.289.

[97] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. In *Proceedings of the International Conference on Learning Representations (ICLR)*, 2015. URL https://arxiv.org/abs/1412.6572.

[98] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples, 2015.

[99] Sarah Gordon and Richard Ford. On the definition and classification of cybercrime. *Journal in Computer Virology 2*, 2006.

[100] Eduard Groen, Denis Feth, Svenja Polst, Jan Tolsdorf, Stephan Wiefling, Luigi Lo Iacono, and Hartmut Schmitt. *Achieving Usable Security and Privacy Through Human-Centered Design*, pages 83–113. Springer, 03 2023. isbn:978-3-031-28642-1. doi:10.1007/978-3-031-28643-8_5.

[101] Y. Gu, Y. Bai, and S. Xu. Cs-mia: Membership inference attack based on prediction confidence series in federated learning. *Journal of Information Security and Applications*, 67:103201, 2022.

[102] Fatma Gümüş, Oğuz Ata, and Hasan Hüseyin Balık. Davranışsal biyometrinin 5 yılı: Kimlik doğrulama ve anomali tespit uygulamaları. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 30(1): 345–364, 2018.

[103] Lee Hadlington. Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7): e00346, 2017. ISSN 2405-8440. doi:https://doi.org/10.1016/j.heliyon.2017.e00346. URL https://www.sciencedirect.com/science/article/pii/S2405844017309982.

[104] C. Hamilton-Giachritsis, E. Hanson, H. Whittle, F. Alves-Costa, and A. Beech. (2020). *Technology assisted child sexual abuse in the UK: Young people's views on the impact of online sexual abuse. Children and Youth Services Review*, 119:105451., 2020.

[105] Djallel Hamouda, Mohamed Amine Ferrag, Nadjette Benhamida, and Hamid Seridi. Ppss: A privacy-preserving secure framework using blockchain-enabled federated deep learning for industrial iots. *Pervasive and Mobile Computing*, 88:101738, 2023.

[106] P. A. Hancock, Theresa T. Kessler, Alexandra D. Kaplan, John C. Brill, and James L. Szalma. Evolving trust in robots: Specification through sequential and comparative meta-analyses. *Human Factors*, 63(7):1196–1229, 2021. doi:10.1177/0018720820922080. https://doi.org/10.1177/0018720820922080. URL https://doi.org/10.1177/0018720820922080. PMID: 32519902.

[107] E. Hanson. The impact of online sexual abuse on children and young people. In J. Brown, editor, *Online risk to children: Impact, protection and prevention*, pages 98–122. 2017.

[108] Xinlong He, Yang Xu, Sicong Zhang, Weida Xu, and Jiale Yan. Enhance membership inference attacks in federated learning. *Computers & Security*, 136:103535, 2024.

[109] Yuanhang He, Daochao Huang, Lei Chen, Yi Ni, and Xiangjie Ma. A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, 2022(1):6476274, 2022.

[110] Nicola Henry and Anastasia Powell. Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse*, 19(2):195–208, 2018. doi:10.1177/1524838016650189. https://doi.org/10.1177/1524838016650189. URL https://doi.org/10.1177/1524838016650189. PMID: 27311818.

[111] S. Hinduja. *Neutralization theory and online software piracy: An empirical analysis.* Ethics Inf Technol9, 2007.

[112] Tai Manh Ho and Kim-Khoa Nguyen. Joint server selection, cooperative offloading and handover in multi-access edge computing wireless network: A deep reinforcement learning approach. *IEEE Transactions on Mobile Computing*, 21(7):2421–2435, 2022. doi:10.1109/TMC.2020.3043736.

[113] T. Holt and A. Bossler. *Cybercrime in Progress.* New York: Routledge, 2016.

[114] T. J. Holt. Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*, 28:171–198, 2007.

[115] Hartmut Aden Hugo Loiseau, Daniel Ventre. Cybersecurity and data protection – research strategies and limitations in a legal and public policy perspective. In *Cybersecurity in Humanities and Social Sciences*, chapter 3, pages 67–84. John Wiley Sons, Ltd, 2020. isbn:9781119777588. doi:https://doi.org/10.1002/9781119777588.ch3. URL https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119777588.ch3.

[116] Hartmut Aden Hugo Loiseau, Daniel Ventre. Cybersécurité et protection des données : stratégies de recherche et limites dans une perspective juridique et de politique publique. In *a cybersécurité en sciences humaines et sociales - méthodologies de recherche*, pages 75–92. ISTE Editions, 2021. isbn:978-1-78406-757-1.

[117] A. Hutchings. Hacking and fraud: Qualitative analysis of online offending and victimization. In *Global criminology: Crime and victimization in a globalized era*, pages 93–114. CRC Press, Boca Raton, 2013.

[118] A. Hutchings and R. Clayton. Exploring the provision of online booter services. *Deviant Behavior*, 37(10):1163–1178, 2016.

[119] Corradini I. *Incorporating Occupational Safety and Health in the Assessment of Cybersecurity Risks*. European Agency for Safety and Health at Work, 2022.

[120] Marko Jacovic, Xaime Rivas Rey, Geoffrey Mainland, and Kapil R Dandekar. Mitigating rf jamming attacks at the physical layer with machine learning. *IET communications*, 17(1):12–28, 2023.

[121] Mian Ahmad Jan, Fazlullah Khan, Rahim Khan, Spyridon Mastorakis, Varun G Menon, Mamoun Alazab, and Paul Watters. Lightweight mutual authentication and privacy-preservation scheme for intelligent wearable devices in industrial-cps. *IEEE transactions on industrial informatics*, 17(8): 5829–5839, 2020.

[122] Akshai Jansen. *These sectors are top targets for cybercrime.* and other cybersecurity news to know this month, 2024.

[123] Jurjen Jansen and Eric Leukfeldt. Coping with cybercrime victimization: An exploratory study into the impact and change. *Journal of Qualitative Criminal Justice Criminology*, 08 2017. doi:10.21428/88de04a1.976bcaf6.

[124] Amir Javadpour, Forough Ja'fari, Tarik Taleb, and Chafika Benzaïd. Reinforcement learning-based slice isolation against ddos attacks in beyond 5g networks. *IEEE Transactions on Network and Service Management*, 20(3):3930–3946, 2023.

[125] DongHyun Je, Jungsoo Jung, and Sunghyun Choi. Toward 6g security: Technology trends, threats, and solutions. *IEEE Communications Standards Magazine*, 5(3):64–71, 2021. doi:10.1109/MCOMSTD.011.2000065.

[126] Bin Jia, Xiaosong Zhang, Jiewen Liu, Yang Zhang, Ke Huang, and Yongquan Liang. Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in iiot. *IEEE Transactions on Industrial Informatics*, 18(6):4049–4058, 2021.

[127] Yu Jin, Jiayi Zhang, Bo Ai, and Xiaodan Zhang. Channel estimation for mmwave massive mimo with convolutional blind denoising network. *IEEE Communications Letters*, 24(1):95–98, 2020. doi:10.1109/LCOMM.2019.2952845.

[128] M. Joleby, S. Landström, C. Lunde, and L. S. Jonsson. (2020a). *Experiences and psychological health among children exposed to online child sexual abuse – a mixed methods study of court verdicts. Psychology, Crime Law*, 27(2):159–181, 2020.

[129] M. Joleby, C. Lunde, S. Landström, and L. S. Jonsson. (2020b). *All of Me Is Completely Different: Experiences and Consequences Among Victims of Technology-Assisted Child Sexual Abuse. Frontiers in Psychology*, 11:606218., 2020.

[130] L. M. Jones, Kimberly J. Mitchell, and W. A. Walsh. *A content analysis of youth internet safety programs: Are effective prevention strategies being used? Crimes Against Children Research Center (CCRC).* University of New Hampshire, 2014.

[131] L. S. Jonsson, C. Fredlund, G. Priebe, M. Wadsby, and C. G. Svedin. Online sexual abuse of adolescents by a perpetrator met online: A cross-sectional study. *Child and Adolescent Psychiatry and Mental Health*, 13(32.), 2019.

[132] Christina Katsini, Marios Belk, Christos Fidas, Nikolaos Avouris, and George Samaras. Security and usability in knowledge-based user authentication: A review. In *Proceedings of the 20th Pan-Hellenic Conference on Informatics*, PCI '16, New York, NY, USA, 2016. Association for Computing Machinery. isbn:9781450347891. doi:10.1145/3003733.3003764. URL https://doi.org/10.1145/3003733.3003764.

[133] Navneet Kaur and Lav Gupta. An approach to enhance iot security in 6g networks through explainable ai. *arXiv preprint arXiv:2410.05310*, 2024.

[134] Navneet Kaur and Lav Gupta. Enhancing iot security in 6g environment with transparent ai: Leveraging xgboost, shap and lime. In *2024 IEEE 10th International Conference on Network Softwarization (NetSoft)*, pages 180–184. IEEE, 2024.

[135] S. Kemp. Fraud reporting in Catalonia in the internet era: Determinants and motives. *European Journal of Criminology*, 19(5):994–1015, 2022.

[136] S. Kemp. Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach. *Computers & Security*, 127:103089., 2023.

[137] S. Kemp. *(2024).* Las Ciberestafas: Tendencias, Infractores, Víctimas y Prevención, Barcelona, 2024.

[138] Marwa Keshk, Elena Sitnikova, Nour Moustafa, Jiankun Hu, and Ibrahim Khalil. An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems. *IEEE Transactions on Sustainable Computing*, 6(1):66–79, 2019.

[139] S. Kewley, R. Mhlanga-Gunda, Van Hout, and M. C. (2021). *Preventing child sexual abuse before it occurs: Examining the scale and nature of secondary public health prevention approaches. Journal of Sexual Aggression*, 29(1):1–33, 2021.

[140] Naurin Khan, Naveed Ikram, Sumera Saleem, and Saad Zafar. Cyber-security and risky behaviors in a developing country context: a pakistani perspective. *Security Journal*, 36:1–33, 05 2022. doi:10.1057/s41284-022-00343-4.

[141] N. Knack, B. Winder, L. Murphy, and J. P. Fedoroff. Primary and secondary prevention of child sexual abuse. *International Review of Psychiatry*, 31(2):181–194, 2018.

[142] Christopher P Kohlios and Thaier Hayajneh. A comprehensive attack flow model and security analysis for wi-fi and wpa3. *Electronics*, 7(11):284, 2018.

[143] Hao Kong, Li Lu, Jiadi Yu, Yingying Chen, and Feilong Tang. Continuous authentication through finger gesture interaction for smart homes using wifi. *IEEE Transactions on Mobile Computing*, 20:3148–3162, 2021. URL https://api.semanticscholar.org/CorpusID:219460710.

[144] Diego Kreutz, Fernando M V Ramos, Paulo Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky, and Steve Uhlig. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1):14–76, 2015.

[145] Merima Kulin, Tarik Kazaz, Ingrid Moerman, and Eli De Poorter. End-to-end learning from spectrum data: A deep learning approach for wireless signal identification in spectrum monitoring applications. *IEEE Access*, 6:18484–18501, 2018. doi:10.1109/ACCESS.2018.2818794.

[146] Alexey Kurakin, Ian Goodfellow, and Samy Bengio. Adversarial examples in the physical world, 2017.

[147] Marc Langheinrich. Privacy by design - principles of privacy-aware ubiquitous systems. In *Proceedings of the 3rd International Conference on Ubiquitous Computing*, UbiComp '01, page 273–291, Berlin, Heidelberg, 2001. Springer-Verlag. isbn:3540426140.

[148] Susan Leavy. Gender bias in artificial intelligence: The need for diversity and gender theory in machine learning. In *2018 IEEE/ACM 1st International Workshop on Gender Equality in Software Engineering (GE)*, pages 14–16, 2018.

[149] Claire Seungeun Lee and Yi Ting Chua. The role of cybersecurity knowledge and awareness in cybersecurity intention and behavior in the united states. *Crime & Delinquency*, 70(9):2250–2277, 2024. doi:10.1177/00111287231180093. https://doi.org/10.1177/00111287231180093. URL https://doi.org/10.1177/00111287231180093.

[150] Hoon Lee, Sang Hyun Lee, and Tony Q. S. Quek. Deep learning for distributed optimization: Applications to wireless resource management. *IEEE Journal on Selected Areas in Communications*, 37(10):2251–2266, 2019. doi:10.1109/JSAC.2019.2933890.

[151] E. J. Letourneau, W. W. Eaton, J. Bass, F. S. Berlin, and S. G. Moore. The need for a comprehensive public health approach to preventing child sexual abuse. *Public Health Reports*, 129(3):222–228, 2014.

[152] E. R. Leukfeldt and M. Yar. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3):263–280, 2015.

[153] E. R. Leukfeldt, E. R. Kleemans, and W. P. Stol. Origin, growth and criminal capabilities of cybercriminal networks. *An international empirical analysis. Crime, Law and Social Change*, 67 (1):39–53, 2017.

[154] R. Leukfeldt, E. Kleemans, and W. Stol. The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist*, 61(11):1387–1402, 2018.

[155] Ming Li, Yuewen Wang, Zhaowen Wang, and Huiying Zheng. A deep learning method based on an attention mechanism for wireless network traffic prediction. *Ad Hoc Networks*, 107:102258, 2020. ISSN 1570-8705. doi:https://doi.org/10.1016/j.adhoc.2020.102258. URL https://www.sciencedirect.com/science/article/pii/S1570870519310923.

[156] Boyang Liu, Haoran Zhang, Yiyao Wan, Fuhui Zhou, Qihui Wu, and Derrick Wing Kwan Ng. Robust adversarial attacks on deep learning-based rf fingerprint identification. *IEEE Wireless Communications Letters*, 12(6):1037–1041, 2023. doi:10.1109/LWC.2023.3259432.

[157] Guangrui Liu, Weizhe Zhang, Xurun Wang, Stephen King, and Shui Yu. A membership inference and adversarial attack defense framework for network traffic classifiers. *IEEE Transactions on Artificial Intelligence*, 2024.

[158] B. D. Loader, and D. (Eds.). Thomas. *(2000).* Routledge.

[159] Nguyen Cong Luong, Dinh Thai Hoang, Ping Wang, Dusit Niyato, and Zhu Han. Applications of economic and pricing models for wireless network security: A survey. *IEEE Communications Surveys & Tutorials*, 19(4):2735–2767, 2017.

[160] A. Lupovici. Cyber warfare and deterrence: trends and challenges in research. *Military and Strategic Affairs*, 3(3):49–62, 2011.

[161] J. Lusthaus, J. van Oss, and P. Amann. (2023). *The Gozi group: A criminal firm in cyberspace? European Journal of Criminology*, 20(5):1701–1718.

[162] Aleksander Madry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. Towards deep learning models resistant to adversarial attacks, 2019.

[163] Bomin Mao, Jiajia Liu, Yingying Wu, and Nei Kato. Security and privacy on 6g network edge: A survey. 25(2), 2023. ISSN 1553-877X. doi:10.1109/COMST.2023.3244674. URL https://doi.org/10.1109/COMST.2023.3244674.

[164] Rosa Lanzilotti Marco Saltarella, Giuseppe Desolda and Vita Santa Barletta. Translating privacy design principles into human-centered software lifecycle: A literature review. *International Journal of Human–Computer Interaction*, 40(17):4465–4483, 2024. doi:10.1080/10447318.2023.2219964. https://doi.org/10.1080/10447318.2023.2219964. URL https://doi.org/10.1080/10447318.2023.2219964.

[165] Philip Mavrepis, Georgios Makridis, Georgios Fatouros, Vasileios Koukos, Maria Margarita Separdani, and Dimosthenis Kyriazis. Xai for all: Can large language models simplify explainable ai? *arXiv preprint arXiv:2401.13110*, 2024.

[166] J. Mayer. *Cybercrime Litigation.* Downloaded on September 4th, 2024.

[167] Nick McKeown. Software-defined networking. *INFOCOM keynote talk*, 17(2):30–32, 2009.

[168] G. McKibbin and C. Humphreys. (2020). *Future directions in child sexual abuse prevention: An Australian perspective. Child Abuse Neglect*, 105:104422., 2020.

[169] Collin Meese, Hang Chen, Wanxin Li, Danielle Lee, Hao Guo, Chien-Chung Shen, and Mark Nejad. Adaptive traffic prediction at the its edge with online models and blockchain-based federated learning. *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[170] M. Moritz. La soumission des pouvoirs publics aux obligations de vigilance et diligence. le cas des technologies numériques utilisées à des fins de police. *Beaucillon C. Gallo (eds.), Vigilance et diligence en droit public*, pages 71–86, 2024.

[171] D. S. Nagin. Deterrence in the twenty-first century. *Crime and Justice*, 42(1):199–263, 2013.

[172] Yasar Sinan Nasir and Dongning Guo. Multi-agent deep reinforcement learning for dynamic power allocation in wireless networks. *IEEE Journal on Selected Areas in Communications*, 37(10):2239–2250, 2019. doi:10.1109/JSAC.2019.2933973.

[173] Zia Ul Islam Nasir, Adnan Iqbal, and Hassaan Khaliq Qureshi. Securing cyber-physical systems: A decentralized framework for collaborative intrusion detection with privacy preservation. *IEEE Transactions on Industrial Cyber-Physical Systems*, 2024.

[174] Liqaa Nawaf. Inclusivity, diversity, and gender equality in cybersecurity. 2023.

[175] Manh-Dung Nguyen, Vinh Hoa La, R Cavalli, and Edgardo Montes De Oca. Towards improving explainability, resilience and performance of cybersecurity analysis of 5g/iot networks (work-in-progress paper). In *2022 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pages 7–10. IEEE, 2022.

[176] Van-Linh Nguyen, Po-Ching Lin, Bo-Chao Cheng, Ren-Hung Hwang, and Ying-Dar Lin. Security and privacy for 6g: A survey on prospective technologies and challenges. *IEEE Communications Surveys Tutorials*, 23(4):2384–2428, 2021. doi:10.1109/COMST.2021.3108618.

[177] Van-Linh Nguyen, Po-Ching Lin, Bo-Chao Cheng, Ren-Hung Hwang, and Y.R. Lin. Security and privacy for 6g: A survey on prospective technologies and challenges. *IEEE Communications Surveys Tutorials*, 08 2021. doi:10.1109/COMST.2021.3108618.

[178] Job Noorman, Jo Van Bulck, Jan Tobias Mühlberg, Frank Piessens, Pieter Maene, Bart Preneel, Ingrid Verbauwhede, Johannes Götzfried, Tilo Müller, and Felix Freiling. Sancus 2.0: A low-cost security architecture for iot devices. *ACM Transactions on Privacy and Security (TOPS)*, 20(3): 1–33, 2017.

[179] Don Norman. *The Design of Everyday Things: Revised and Expanded Edition.* New York: Basic Books, 2013. isbn:9780465050659. URL https://shepherd.com/book/the-design-of-everyday-things.

[180] Ernest Ntizikira, Wang Lei, Fahad Alblehai, Kiran Saleem, and Muhammad Ali Lodhi. Secure and privacy-preserving intrusion detection and prevention in the internet of unmanned aerial vehicles. *Sensors*, 23(19):8077, 2023.

[181] Edward Oughton, Giovanni Geraci, Michele Polese, and Vijay Shah. Prospective evaluation of next generation wireless broadband technologies: 6g versus wi-fi 7/8. *Available at SSRN 4528119*, 2023.

[182] Pejman Panahi, Cüneyt Bayılmış, Unal Çavuşoğlu, and Sezgin Kaçar. Performance evaluation of lightweight encryption algorithms for iot-based applications. *Arabian Journal for Science and Engineering*, 46(4):4015–4037, 2021.

[183] A. Patterson, L. Ryckman, and C. Guerra. A systematic review of the education and awareness interventions to prevent online child sexual abuse. *Journal of Child Adolescent Trauma*, 15(3): 857–867, 2022.

[184] Martin Pawelczyk, Klaus Broelemann, and Gjergji Kasneci. Learning model-agnostic counterfactual explanations for tabular data. In *Proceedings of the web conference 2020*, pages 3126–3132, 2020.

[185] Marek Pawlicki, Aleksandra Pawlicka, Rafał Kozik, and Michał Choraś. The survey on the dual nature of xai challenges in intrusion detection and their potential for ai innovation. *Artificial Intelligence Review*, 57(12):1–32, 2024.

[186] Roy Pea. User centred system design-new perspectives on human/computer interaction. *J Educ Comput Res*, 3, 01 1987.

[187] Yifeng Peng, Xinyi Li, Jingda Yang, Sudhanshu Arya, and Ying Wang. Raft: A real-time framework for root cause analysis in 5g and beyond vulnerability detection. In *2024 IEEE 21st Consumer Communications & Networking Conference (CCNC)*, pages 446–454. IEEE, 2024.

[188] K. Phillips, J. C. Davidson, R. R. Farr, C. Burkhardt, and S. Caneppele. i aiken. *M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences*, 2(2):379–398, 2022.

[189] Hossein Pirayesh and Huacheng Zeng. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE communications surveys & tutorials*, 24(2):767–809, 2022.

[190] Alessandro Pollini, Tiziana C. Callari, Alessandra Tedeschi, Daniele Ruscio, Luca Save, Franco Chiarugi, and Davide Guerri. Leveraging human factors in cybersecurity: an integrated methodological approach. *Cogn. Technol. Work*, 24(2):371–390, May 2022. ISSN 1435-5558. doi:10.1007/s10111-021-00683-y. URL https://doi.org/10.1007/s10111-021-00683-y.

[191] Pawani Porambage, Johnson Okwuibe, Madhusanka Liyanage, Mika Ylianttila, and Tarik Taleb. The roadmap to 6g security and privacy. *IEEE Open Journal of the Communications Society*, 2: 1094–1122, 2021.

[192] Yuanhang Qi, M. Shamim Hossain, Jiangtian Nie, and Xuandi Li. Privacy-preserving blockchain-based federated learning for traffic flow prediction. *Future Generation Computer Systems*, 117: 328–337, 2021.

[193] Han Qiu, Tian Dong, Tianwei Zhang, Jialiang Lu, Gerard Memmi, and Meikang Qiu. Adversarial attacks against network intrusion detection in iot systems. *IEEE Internet of Things Journal*, 8 (13):10327–10335, 2020.

[194] Han Qiu, Tian Dong, Tianwei Zhang, Jialiang Lu, Gerard Memmi, and Meikang Qiu. Adversarial attacks against network intrusion detection in iot systems. *IEEE Internet of Things Journal*, 8 (13):10327–10335, 2021. doi:10.1109/JIOT.2020.3048038.

[195] Junwei Qu. A review of uwb indoor positioning. In *Journal of Physics: Conference Series*, volume 2669, page 012003. IOP Publishing, 2023.

[196] E. Quayle. Prevention, disruption and deterrence of online child sexual exploitation and abuse. *Era Forum*, 21:429–447, 2020.

[197] Paul Quinn and Gianclaudio Malgieri. The difficulty of defining sensitive data—the concept of sensitive data in the eu data protection framework. *German Law Journal*, 22(8):1583–1612, 2021.

[198] Pushpakumar R, Karun Sanjaya, S. Rathika, Ahmed Alawadi, Khamdamova Makhzuna, S. Venkatesh, and B. Rajalakshmi. Human-computer interaction: Enhancing user experience in interactive systems. *E3S Web of Conferences*, 399, 07 2023. doi:10.1051/e3sconf/202339904037.

[199] Keyvan Ramezanpour and Jithin Jagannath. Intelligent zero trust architecture for 5g/6g networks: Principles, challenges, and the role of machine learning in the context of o-ran. *Computer Networks*, 217:109358, 2022.

[200] Tebogo Motlatso Ramonyai, Noluntu Mpekoa, and Sheethal Tom. Cyber security skills development in south africa: Addressing the gender gap in the industry. In *2024 Conference on Information Communications Technology and Society (ICTAS)*, pages 144–149, 2024. doi:10.1109/ICTAS59620.2024.10507137.

[201] Karen Renaud and Lizzie Coles-Kemp. Accessible and inclusive cyber security: a nuanced and complex challenge. *SN Computer Science*, 3(5):346, 2022.

[202] Marcus K.. Rogers. *"THE DEVELOPMENT OF A MEANINGFUL HACKER TAXONOMY : A TWO DIMENSIONAL APPROACH by mkr.* 2005.

[203] Marcus K. ; Goldman Rogers, James; Mislan, Rick; Wedge, Timothy;, and Steve Debrota. Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law:*, 1, 2006.

[204] Ahmad-Reza Sadeghi, Christian Wachsmann, and Michael Waidner. Security and privacy challenges in industrial internet of things. In *Proceedings of the 52nd annual design automation conference*, pages 1–6, 2015.

[205] Amir Mahdi Sadeghzadeh, Saeed Shiravi, and Rasool Jalili. Adversarial network traffic: Towards evaluating the robustness of deep-learning-based network traffic classification. *IEEE Transactions on Network and Service Management*, 18(2):1962–1976, 2021.

[206] Sara Salim, Benjamin Turnbull, and Nour Moustafa. A blockchain-enabled explainable federated learning for securing internet-of-things-based social media 3.0 networks. *IEEE Transactions on Computational Social Systems*, 2021.

[207] Chamara Sandeepa, Bartlomiej Siniarski, Nicolas Kourtellis, Shen Wang, and Madhusanka Liyanage. A survey on privacy for b5g/6g: New privacy challenges, and research directions. *Journal of Industrial Information Integration*, 30:100405, 2022. ISSN 2452-414X. doi:https://doi.org/10.1016/j.jii.2022.100405. URL https://www.sciencedirect.com/science/article/pii/S2452414X22000723.

[208] Elizabeth Sanders and Pieter Jan Stappers. Co-creation and the new landscapes of design. *CoDesign*, 4:5–18, 03 2008. doi:10.1080/15710880701875068.

[209] HP Sanghvi and MS Dahiya. Cyber reconnaissance: an alarm before cyber attack. *International Journal of Computer Applications*, 63(6), 2013.

[210] R. Sarre, L. Y. C. Lau, and L. Y. C. Chang. Responding to cybercrime: current trends. *Police Practice and Research*, 19(6), 2018.

[211] Danish Sattar and Ashraf Matrawy. Towards secure slicing: Using slice isolation to mitigate ddos attacks on 5g core network slices. In *2019 IEEE Conference on Communications and Network Security (CNS)*, pages 82–90. IEEE, 2019.

[212] Paul Scalise, Matthew Boeding, Michael Hempel, Hamid Sharif, Joseph Delloiacovo, and John Reed. A systematic survey on 5g and 6g security considerations, challenges, trends, and research areas. *Future Internet*, 16:67, 02 2024. doi:10.3390/fi16030067.

[213] F. Schmidt, F. Varese, and S. Bucci. (2023). *Understanding the prolonged impact of online sexual abuse occurring in childhood. Frontiers in Psychology*, 14:1281996., 2023.

[214] K. C. Seigfried-Spellar and V. Soldino. *(2020).* The Palgrave handbook of international cybercrime and Cyberdeviance.

[215] Georgios Selimis, Rui Wang, Roel Maes, Geert-Jan Schrijen, Mario Münzer, Stefan Ilić, Frans MJ Willems, and Lieneke Kusters. Rescure: A security solution for iot life cycle. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pages 1–10, 2020.

[216] Mehdi Setayesh, Shahab Bahrami, and Vincent W.S. Wong. Resource slicing for embb and urllc services in radio access network using hierarchical deep learning. *IEEE Transactions on Wireless Communications*, 21(11):8950–8966, 2022. doi:10.1109/TWC.2022.3171264.

[217] Bora Bugra Sezer, Hasret Turkmen, and Urfat Nuriyev. Ppfchain: A novel framework privacy-preserving blockchain-based federated learning method for sensor networks. *Internet of Things*, 22:100781, 2023.

[218] Hitali Shah. Millimeter-wave mobile communication for 5g. *International Journal of Transcontinental Discoveries, ISSN*, pages 68–74.

[219] E. D. Shaw, K. G. Ruby, and J. M. Post. *The Insider Threat to Information Systems.* 1998.

[220] Cong Shi, Jian Liu, Hongbo Liu, and Yingying Chen. Wifi-enabled user authentication through deep learning in daily activities. *ACM Trans. Internet Things*, 2(2), May 2021. doi:10.1145/3448738. URL https://doi.org/10.1145/3448738.

[221] Weiping Shi, Xinyi Jiang, Jinsong Hu, Yin Teng, Yang Wang, Hangjia He, Rongen Dong, Feng Shu, and Jiangzhou Wang. Physical layer security techniques for future wireless networks. *arXiv preprint arXiv:2112.14469*, 2021.

[222] Yi Shi, Kemal Davaslioglu, and Yalin E. Sagduyu. Generative adversarial network in the air: Deep adversarial learning for wireless signal spoofing. *IEEE Transactions on Cognitive Communications and Networking*, 7(1):294–303, 2021. doi:10.1109/TCCN.2020.3010330.

[223] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-bit blockcipher clefia. In *Fast Software Encryption: 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers 14*, pages 181–195. Springer, 2007.

[224] Reza Shokri and Vitaly Shmatikov. Privacy-preserving deep learning. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 1310–1321, 2015. doi:10.1145/2810103.2813687.

[225] Usmonov Botir Shukurillaevich, Radjabov Ozod Sattorivich, and Rustamov Umedjon Amrillojonovich. 5g technology evolution. In *2019 International Conference on Information Science and Communications Technologies (ICISCT)*, pages 1–5. IEEE, 2019.

[226] S. Smallbone and R. Wortley. Preventing child sexual abuse online. In J. Brown, editor, *Online Risk to Children*, pages 143–162. 2017.

[227] M. R. J. Soudijn and B. C. H. T. Zegers. Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, 15(2):111–129, 2012.

[228] S Sullivan, Alessandro Brighente, Sathish AP Kumar, and Mauro Conti. 5g security challenges and solutions: a review by osi layers. *Ieee Access*, 9:116294–116314, 2021.

[229] G. Sykes and D. Matza. Techniques of Neutralization: A theory of Delinquency. *In: American Sociological Review*, 22:664–670, 1958.

[230] ELANOR TAYLOR. Explanation and the right to explanation. *Journal of the American Philosophical Association*, 10(3):467–482, 2024. doi:10.1017/apa.2023.7.

[231] Vishal A Thakor, Mohammad Abdur Razzaque, and Muhammad RA Khandaker. Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities. *IEEE Access*, 9:28177–28193, 2021.

[232] Manesh Thankappan, Helena Rifà-Pous, and Carles Garrigues. Multi-channel man-in-the-middle attacks against protected wi-fi networks: A state of the art review. *Expert Systems with Applications*, 210:118401, 2022.

[233] Manesh Thankappan, Helena Rifà-Pous, and Carles Garrigues. A distributed and cooperative signature-based intrusion detection system framework for multi-channel man-in-the-middle attacks against protected wi-fi networks. *International Journal of Information Security*, pages 1–20, 2024.

[234] Vrizlynn L. L. Thing. Ieee 802.11 network anomaly detection and attack classification: A deep learning approach. In *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6, 2017. doi:10.1109/WCNC.2017.7925567.

[235] Florian Tramèr, Alexey Kurakin, Nicolas Papernot, Ian Goodfellow, Dan Boneh, and Patrick McDaniel. Ensemble adversarial training: Attacks and defenses, 2020.

[236] G. Tziakouris, R. Bahsoon, and M. A. Babar. A survey on self-adaptive security for large-scale open environments. *ACM Computing Surveys (CSUR)*, 51(5):1–42, 2018.

[237] Michael Veale and Lilian Edwards. Clarity, surprises, and further questions in the article 29 working party draft guidance on automated decision-making and profiling. *Computer Law Security Review*, 34(2):398–404, 2018. ISSN 0267-3649. doi:https://doi.org/10.1016/j.clsr.2017.12.002. URL https://www.sciencedirect.com/science/article/pii/S026736491730376X.

[238] Sandra Wachter and Brent Mittelstadt. A right to reasonable inferences: Re-thinking data protection law in the age of big data and ai. 2019, 04 2019.

[239] D. S. Wall. *Cybercrime: The transformation of crime in the information age*. Cambridge, UK: Polity Press, 2007.

[240] Yichen Wan, Youyang Qu, Longxiang Gao, and Yong Xiang. Privacy-preserving blockchain-enabled federated learning for b5g-driven edge computing. *Computer Networks*, 204:108671, 2022.

[241] Cheng-Xiang Wang, Xiaohu You, Xiqi Gao, Xiuming Zhu, Zixin Li, Chuan Zhang, Haiming Wang, Yongming Huang, Yunfei Chen, Harald Haas, et al. On the road to 6g: Visions, requirements, key technologies, and testbeds. *IEEE Communications Surveys & Tutorials*, 25(2):905–974, 2023.

[242] Dan Wang, Hao Qin, Bin Song, Xiaojiang Du, and Mohsen Guizani. Resource allocation in information-centric wireless networking with d2d-enabled mec: A deep reinforcement learning approach. *IEEE Access*, 7:114935–114944, 2019. doi:10.1109/ACCESS.2019.2935545.

[243] Dingding Wang, Muhui Jiang, Rui Chang, Yajin Zhou, Baolei Hou, Xiapu Luo, Lei Wu, and Kui Ren. A measurement study on the (in) security of end-of-life (eol) embedded devices. *arXiv preprint arXiv:2105.14298*, 2021.

[244] Minghao Wang, Tianqing Zhu, Tao Zhang, Jun Zhang, Shui Yu, and Wanlei Zhou. Security and privacy in 6g networks: New areas and new challenges. *Digital Communications and Networks*, 6 (3):281–291, 2020. ISSN 2352-8648. doi:https://doi.org/10.1016/j.dcan.2020.07.003. URL https://www.sciencedirect.com/science/article/pii/S2352864820302431.

[245] Naiyu Wang, Wenti Yang, Xiaodong Wang, Longfei Wu, Zhitao Guan, Xiaojiang Du, and Mohsen Guizani. A blockchain based privacy-preserving federated learning scheme for internet of vehicles. *Digital Communications and Networks*, 2022.

[246] Ying Wang, Peilong Li, Lei Jiao, Zhou Su, Nan Cheng, Xuemin Sherman Shen, and Ping Zhang. A data-driven architecture for personalized qoe management in 5g wireless networks. *IEEE Wireless Communications*, 24(1):102–110, 2017. doi:10.1109/MWC.2016.1500184WC.

[247] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. Testing metrics for password creation policies by attacking large sets of revealed passwords. pages 162–175, 10 2010. doi:10.1145/1866307.1866327.

[248] H. C. Whittle, C. E. Hamilton-Giachritsis, and A. R. Beech. A comparison of victim and offender perspectives of grooming and sexual abuse. *Deviant Behavior*, 36(7):539–564, 2014.

[249] S. K. Wurtele. Preventing cyber sexual solicitation of adolescents. In R. Alexander, editor, *Research and practices in child maltreatment prevention (Vol*, volume 1, pages 361–393. 2017.

[250] Saiqin Xu, Alessandro Brighente, Baixiao Chen, Mauro Conti, Xiancheng Cheng, and Dongchen Zhu. Deep neural networks for direction of arrival estimation of multiple targets with sparse prior for line-of-sight scenarios. *IEEE Transactions on Vehicular Technology*, 72(4):4683–4696, 2023. doi:10.1109/TVT.2022.3224586.

[251] Wenyuan Xu. Jamming attack defense. In *Encyclopedia of Cryptography, Security and Privacy*, pages 1–8. Springer, 2021.

[252] Yang Xu, Jia Liu, Yulong Shen, Jun Liu, Xiaohong Jiang, and Tarik Taleb. Incentive jamming-based secure routing in decentralized internet of things. *IEEE Internet of Things Journal*, 8(4): 3000–3013, 2020.

[253] Yang Xu, Jia Liu, Yulong Shen, Xiaohong Jiang, Yusheng Ji, and Norio Shiratori. Qos-aware secure routing design for wireless networks with selfish jammers. *IEEE Transactions on Wireless Communications*, 20(8):4902–4916, 2021.

[254] Ricardo Yaben, Niels Lundsgaard, Jacob August, and Emmanouil Vasilomanolakis. Towards identifying neglected, obsolete, and abandoned iot and ot devices. In *8th Network Traffic Measurement and Analysis Conference*. IFIP, 2024.

[255] M. Yar. Cybercrime and society. *SAGE publications, Bandura, A. (1976). Self-Reinforcement: Theoretical and Methodological Considerations. Behaviorism*, 4(2):135–155, 1976. URL http://www.jstor.org/stable/27758862.

[256] Sze Ling Yeo, Duc-Phong Le, and Khoongming Khoo. Improved algebraic attacks on lightweight block ciphers. *Journal of cryptographic Engineering*, 11:1–19, 2021.

[257] Mika Ylianttila, Raimo Kantola, Andrei Gurtov, Lorenzo Mucchi, Ian Oppermann, and Robert Abbas. 6g white paper: Research challenges for trust, security and privacy. 09, 06 2020.

[258] Jun Zhang, Chao Chen, Yang Xiang, Wanlei Zhou, and Athanasios V. Vasilakos. An effective network traffic classification method with unknown flow detection. *IEEE Transactions on Network and Service Management*, 10(2):133–147, 2013.

[259] Jun Zhang, Xiao Chen, Yang Xiang, Wanlei Zhou, and Jie Wu. Robust network traffic classification. *IEEE/ACM Transactions on Networking*, 23(4):1257–1270, 2014.

[260] Rui Zhang and Quanyan Zhu. Flipin: A game-theoretic cyber insurance framework for incentive-compatible cyber risk management of internet of things. *IEEE Transactions on Information Forensics and Security*, 15:2026–2041, 2020.

[261] Wuyang Zhang, Russell Ford, Joonyoung Cho, Charlie Jianzhong Zhang, Yanyong Zhang, and Dipankar Raychaudhuri. Self-organizing cellular radio access network with deep learning. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 429–434. IEEE, 2019.

[262] Zhou Zhou, Youliang Tian, Jinbo Xiong, Jianfeng Ma, and Changgen Peng. Blockchain-enabled secure and trusted federated data sharing in iiot. *IEEE Transactions on Industrial Informatics*, 2022.

[263] James Zou and Londa Schiebinger. Ai can be sexist and racist — it's time to make it fair. *Nature*, 559:324 – 326, 2018. URL `https://api.semanticscholar.org/CorpusID:51677390`.