Proceedings of the International Conference on Engineering, Technology and Applied Science Innovations pp. 53–59
DOI: 10.15439/2025I28
ISSN 2300-5963 ACSIS, Vol. 46

Regulatory and Governance Aspects of 5G and Beyond

Dionysia Varvarigou
University of Patras
Patras, Greece
dvarvarigou@upatras.gr

Kostas Lampropoulos
University of Patras
Patras, Greece
klamprop@ece.upatras.gr

Spyros Denazis
University of Patras
Patras, Greece
sdena@upatras.gr

Paris Kitsos
University of Patras,
University of Peloponnese
Patras, Greece
pkitsos@ieee.org

***Abstract*—The rapid deployment of 5G networks introduces new opportunities for digital transformation while exposing critical vulnerabilities across technical and regulatory domains. This paper offers a comprehensive exploration of the European cybersecurity landscape for 5G and beyond, analyzing how legislative frameworks such as GDPR, the EECC, and NIS2 shape telecom security practices. It examines the roles of key actors including ENISA, national regulatory authorities, and international bodies, and discusses how telecom operators can implement and operationalize these frameworks. The paper further presents a practical use case demonstrating how the SAND5G platform supports compliance and incident response through contextualized risk assessment and real-time threat mitigation. Looking ahead, it outlines future governance challenges and emerging technologies—such as quantum cryptography, zero trust architectures, and AI-driven security—required to secure next-generation networks like 6G. The study underscores the need for dynamic, multi-layered, and forward-looking cybersecurity strategies that balance innovation with resilience.**

***Index Terms*—SAND5G Platform, 5G Security, Cybersecurity Regulations.**

I. Introduction

THE SAND5G project is a European research initiative dedicated to advancing the security analysis of 5G and beyond networks. This paper builds upon the comprehensive findings of SAND5G, particularly those presented in Deliverable D2.1 "Security analysis for 5G and beyond networks," to provide a critical overview of the multifaceted evolution of 5G technology, its associated security implications, regulatory frameworks, and strategic perspectives for future telecommunications.

The project underscores a dual strategy that leverages both technical advancements and regulatory policies to fortify network security. It highlights the pioneering roles of standardization bodies such as 3GPP, ETSI, and ITU-T, alongside collaborative projects and initiatives focused on securing 5G infrastructures. The analysis addresses emerging security challenges introduced by 5G adoption, including vulnerabilities linked to IoT proliferation, the convergence of IT and telecom infrastructures, and complexities arising from software-defined networking and virtualization.

The global deployment of 5G networks marks a critical milestone in telecommunications, enabling unprecedented speeds, massive device connectivity, and ultra-low latency that power innovative applications from smart cities to Industry 4.0. However, these advancements bring new complexities in security and privacy that require comprehensive governance frameworks. Europe's approach emphasizes harmonizing rapid technological progress with robust protection of data and infrastructure resilience. The SAND5G project contributes to this endeavor by integrating technical innovation with regulatory insight, ensuring that security is embedded not only in network design but also in policy and operational practices. This paper examines the European regulatory environment alongside emerging security strategies, highlighting the challenges and opportunities of securing 5G and paving the way for future generations such as 6G.

This work advocates a holistic approach that integrates technical solutions, governance frameworks, and international collaboration to navigate the evolving security landscape of 5G and beyond. The subsequent sections provide an in-depth background on standardization and innovations in 5G, explore the intricate security landscape shaped by novel architectures and extensive connectivity, examine regulatory compliance and data protection considerations, and review existing security mechanisms. The paper further presents the European Union's strategic response through initiatives such as the 5G toolbox and concludes with insights into future telecommunications innovations including 6G and beyond.

To ensure the secure and resilient deployment of 5G networks, regulatory frameworks play a pivotal role alongside technical safeguards. Within the European Union, the security and privacy of telecommunications infrastructure are guided by a complex yet comprehensive set of regulations and directives. These legal instruments not only define the responsibilities of operators and service providers but also establish mechanisms for oversight, coordination, and enforcement. Understanding this evolving regulatory landscape is essential for aligning technical innovation with legal compliance and public trust. The following section outlines

This article describes work undertaken in the context of the SAND5G project, "Security Assessments for Networks anD services in 5G" which has received funding from the European Union's Digital Europe programme under grant agreement No 101127979 and is supported by European Cybersecurity Competence Center. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them

the most relevant EU legislation shaping the 5G cybersecurity domain.

II. Existing European Regulatory Framework

Regulatory compliance, particularly in the context of European legislation, plays a significant role in shaping user-centric security considerations for 5G networks. In the European Union (EU), several key regulations and directives govern cybersecurity and data protection, impacting how 5G networks are deployed, managed, and secured. Here are some important aspects of regulatory compliance in the EU [1].

GDPR [2] is one of the most comprehensive data protection regulations globally and significantly impacts the security and privacy of user data in 5G networks. GDPR applies to the processing of personal data by organizations operating within the EU or offering goods and services to individuals in the EU. It imposes strict requirements on data controllers and processors, including obligations related to data protection principles, lawful processing, data subject rights, data breach notification, and privacy by design and by default. Compliance with GDPR is essential for safeguarding user privacy and avoiding hefty fines and penalties for non-compliance.

The ePrivacy Directive [3] governs the processing of personal data and the protection of privacy in the electronic communications sector. While not specifically tailored to 5G networks, it applies to the collection and use of data transmitted over these networks, including metadata generated by communication services. The forthcoming ePrivacy Regulation, intended to replace the current directive, aims to modernize and strengthen privacy rules for electronic communications, further impacting the security and privacy of 5G networks.

The European Electronic Communications Code (EECC) [4] is the main EU policy framework for the telecom sector. Adopted in 2018, these rules apply to all electronic communications services and networks in the EU. Currently, the EECC has been transposed by most EU countries, with the Commission supporting Member States in the implementation process.

Security requirements for the telecom sector are contained in Article 40 of the EECC (which replaces Article 13a of the Framework Directive). Article 40 asks Member States to ensure that operators take “appropriate” cybersecurity measures and report significant incidents to the national authorities; Article 41 asks Member States to ensure that the national competent authority, for instance a telecom national regulatory agency (NRA) or a cybersecurity agency, depending on the national setting, has the powers to audit telecom operators and to enforce measures in case of cybersecurity deficiencies.

In terms of supervision of these security requirements, Member States have taken diverse approaches. For instance, where binding rules apply to mobile network operators, they may cover different types of technical and organizational measures. In Member States where security measures are further clarified in more technical and practical detail (often via secondary legislation), they often refer to the ENISA framework of detailed technical telecom security measures, which was developed with all Member States to implement the EECC and contains a detailed list of relevant telecom security measures.

The NIS1 [5] establishes cybersecurity standards for operators of essential services (OES) and digital service providers (DSPs) within the EU. It requires member states to adopt national cybersecurity strategies, designate competent authorities, and establish incident reporting mechanisms for significant cyber incidents. Compliance with the NIS Directive involves implementing appropriate security measures, conducting risk assessments, and reporting cybersecurity incidents to national authorities.

The revised NIS Directive, referred to as NIS2 [6], will repeal and replace Articles 40 and 41 of the EECC, with effect from 18 October 2024, streamlining the cybersecurity policy framework, adding providers of public electronic communications networks and providers of publicly available electronic communications services to the ‘digital infrastructure’ sector. The NIS2 Directive establishes: (a) obligations requiring Member States to adopt national cyber security strategies and to designate or set up competent authorities, cyber crisis management authorities, cyber security single points of contact and computer security incident response teams (CSIRTs), (b) cybersecurity risk management measures and reporting obligations for entities of the type referred to in Annexes I and II of the NIS2 Directive, (c) rules and obligations regarding the exchange of cybersecurity information and (d) Member States' obligations regarding supervision and enforcement. Under the NIS2 Directive, the Commission has to issue implementing acts on security measures and incident reporting, for several entities under the NIS2 digital infrastructure sector, including TLDs, DNS, and content delivery networks (CDNs). The NIS Cooperation Group already published detailed technical security measures for TLD registries [7] and is drafting a guideline on security measures for the DNS providers. In addition, the NIS2 allows the NIS Cooperation Group, together with the Commission and ENISA, to conduct EU-wide risk assessments in critical supply chains.

The Resilience of Critical Entities (CER) Directive [8] covers the physical resilience of critical entities against man-made and natural hazards, in coherence with the NIS2 Directive which covers cybersecurity risks. This Directive focuses on all relevant non-cyber natural and man-made risks, including cross-sectoral or cross-border, that may affect the provision of essential services, such as natural disasters, accidents, public health emergencies and antagonistic threats, including terrorist offences, sabotage and hybrid threats. It covers eleven sectors, including digital infrastructure.

The EU Cybersecurity Act [9] introduces a certification framework for cybersecurity products, services, and processes, including those related to 5G networks. The frame-

work enables the voluntary certification of ICT products, ICT processes, and ICT services based on common cybersecurity standards and schemes recognized across the EU. A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services and ICT processes: 'basic', 'substantial' or 'high'. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident. Compliance with cybersecurity certification requirements can enhance the trustworthiness and security of 5G products and services, fostering consumer confidence and market competitiveness.

The Cyber Resilience Act (CRA) [10], for which a provisional political agreement has been reached in December 2023, requires manufacturers of connectable software and hardware products intended for the EU market to ensure that such products are developed in line with security-by-default and security-by-design principles and that their security is maintained throughout their lifetime, for instance through testing and security updates. The CRA covers a wide range of products deployed by network operators, such as routers and switches. It has the potential to increase transparency on the security of such products and facilitate supply chain security management for critical infrastructure covered by the NIS2 Directive, including operators of public electronic communications networks and core Internet infrastructure. The agreement reached is, as of February 2024, subject to formal approval by both the European Parliament and the Council.

While the European regulatory framework sets the foundation for securing 5G networks, its effective implementation and coordination depend on the efforts of specialized institutions. Among them, the European Union Agency for Cybersecurity (ENISA) plays a pivotal role in translating policy into practice. As the EU's dedicated cybersecurity body, ENISA supports member states and stakeholders by developing technical guidelines, facilitating collaboration, and strengthening collective preparedness. The following section explores ENISA's multifaceted contributions to securing 5G and beyond.

III. European Union Agency for Cybersecurity (ENISA)

ENISA [11] plays a key role in enhancing cybersecurity and resilience across the EU, particularly within the telecommunications sector. It provides guidance, best practices, and recommendations to strengthen the security of telecom networks and infrastructure.

ENISA collaborates with telecom stakeholders to collect threat intelligence, analyze emerging risks, and share actionable information to improve situational awareness. It works closely with EU institutions, national cybersecurity agencies, industry groups, and international partners to coordinate efforts and address common cybersecurity challenges. This includes participation in working groups, joint initiatives, and information-sharing frameworks to bolster collective resilience.

The agency publishes security guidelines and technical standards covering network security, incident response, risk management, and security-by-design. ENISA also supports the telecom sector in developing incident response and crisis management capabilities through guidance, exercises, and simulations to improve preparedness.

Furthermore, ENISA contributes to cybersecurity certification schemes for telecom products and services, promoting common evaluation criteria and mutual recognition of certifications across EU member states.

To build capacity, ENISA organizes training, workshops, and awareness programs for telecom professionals, regulators, and policymakers, fostering knowledge sharing and improving the sector's overall cybersecurity posture.

ENISA's role extends beyond guidance and standard-setting. The agency actively coordinates large-scale cybersecurity exercises such as the annual European Cybersecurity Challenge, fostering readiness and collaboration among Member States. Through its Threat Landscape reports, ENISA provides up-to-date intelligence on evolving cyber threats, including those targeting 5G infrastructures. The agency also supports the implementation of the EU 5G Toolbox, assisting countries in adopting consistent risk mitigation measures. ENISA's collaboration with CERTs (Computer Emergency Response Teams) across Europe enhances rapid incident response and information sharing, critical for managing the complex threat environment in telecommunications.

While ENISA primarily operates within the EU context, its activities also intersect with broader international efforts aimed at securing global telecommunications infrastructure. As 5G networks are inherently cross-border in nature, threats targeting them often span jurisdictions. Consequently, cooperation with international organizations and standardization bodies becomes essential to ensure cohesive and interoperable security practices. Building on ENISA's regional contributions, the following section explores the EU's role in fostering global partnerships for 5G security and resilience.

IV. International Cooperation in 5G Security

Securing 5G networks is a global challenge that transcends regional boundaries. The European Union actively cooperates with international bodies such as the International Telecommunication Union (ITU), the Global System for Mobile Communications Association (GSMA), the 3rd Generation Partnership Project (3GPP), and other regional cybersecurity agencies to harmonize standards, develop secure-by-design architectures, and share threat intelligence. These collaborations facilitate the alignment of security frameworks, promote technical interoperability, and support coordinated responses to transnational cyber threats and large-scale incidents. Joint efforts—such as coordinated threat reporting, the development of shared risk assessment

methodologies, and participation in cross-border cybersecurity exercises—help enhance collective preparedness and resilience.

On the policy level, such cooperation also reinforces global consensus around key principles like transparency, accountability, and proportionality in cyber risk management. It further supports the development of trusted ICT supply chains through common evaluation schemes and coordinated vendor risk assessments, aiming to mitigate dependencies on untrusted suppliers and ensure strategic autonomy. These international efforts are crucial for sustaining long-term cybersecurity in a rapidly evolving technological landscape.

While international cooperation provides a broad framework for harmonizing 5G security practices across borders, effective implementation depends heavily on the actions of national regulatory authorities. These authorities serve as the operational arms of policy enforcement, translating international and regional strategies into concrete technical and organizational requirements. The next section examines the pivotal role played by national regulators in overseeing compliance, coordinating incident response, and fostering resilience at the member state level.

V. Regulatory Authorities

National regulatory authorities oversee 5G network security and enforce compliance with applicable laws and standards. While specific requirements vary by jurisdiction, authorities typically set security standards and guidelines that telecom operators must follow, covering areas such as authentication, encryption, access control, incident response, and risk management.

Operators are often required to conduct risk assessments, implement risk management processes, and promptly report significant cybersecurity incidents to authorities. Regulatory bodies monitor compliance through audits, inspections, and reporting, imposing penalties for non-compliance when necessary.

Authorities also promote collaboration and information sharing among operators, government agencies, and other stakeholders to address common cybersecurity threats. A key example of such international cooperation is ENISA's European Competent Authorities for Secure Electronic Communications (ECASEC) expert group [11]. This group plays a central role in aligning national efforts by agreeing on technical and organizational measures for the implementation of Articles 40 and 41 of the European Electronic Communications Code (EECC) and the provisions of the NIS2 Directive concerning telecom security and incident reporting. Furthermore, ECASEC facilitates the voluntary exchange of information among national experts on threats, cybersecurity incidents, lessons learned, applicable standards, and practical tools. The group also contributes to the development of ENISA's policy and technical outputs by reviewing and providing input on key documents, thereby reinforcing a coordinated and resilient approach across Member States.

While national authorities are responsible for setting and enforcing regulatory standards, the responsibility for practical implementation lies primarily with telecom operators. These operators act as the frontline of network security, translating legal and policy requirements into actionable security practices within their infrastructures. The following section explores how telecom providers operationalize compliance, establish robust governance structures, and deploy security controls to protect 5G networks against evolving cyber threats.

VI. Telecom Operators

For telecom operators, adhering to regulatory frameworks such as the EECC, the NIS Directive, and the GDPR is vital for maintaining secure and resilient 5G networks. To ensure compliance and mitigate risks, operators must begin by conducting comprehensive assessments to determine which regulatory requirements apply to their operations, enabling them to formulate an effective compliance strategy. Establishing robust governance frameworks is equally important, with clearly defined roles and the appointment of dedicated compliance officers to oversee implementation. Strong security and privacy controls should be deployed, including mechanisms for encryption, access management, intrusion detection, and data loss prevention. Operators are also expected to develop and communicate formalized policies and procedures that cover key areas such as data protection, incident response, risk management, and staff training.

To address privacy risks in particular, telecom companies should perform Data Protection Impact Assessments (DPIAs), ensuring that GDPR obligations are met throughout their service delivery. Incident response capabilities must be in place to allow for prompt reporting of cybersecurity events to both the relevant authorities and affected individuals. Additionally, third-party suppliers must be subject to rigorous security and compliance oversight, as they are often integral to the telecom ecosystem. Building a resilient security culture requires ongoing training and awareness programs for both employees and contractors. Finally, operators must implement continuous monitoring and regular audits to evaluate the effectiveness of security controls and update them as necessary to adapt to evolving threats and regulatory requirements. Through this proactive and structured approach, telecom operators can safeguard their infrastructure, meet legal obligations, and foster trust among users and regulators alike.

While telecom operators are expected to adopt comprehensive security and compliance strategies, the complexity of modern 5G infrastructures demands the support of advanced platforms that enable rapid detection, contextual analysis, and coordinated response. To demonstrate how such support is operationalized in practice, the following section presents a realistic scenario in which the SAND5G platform is employed to manage a security breach. This use

case illustrates how integrated tools and compliance workflows—aligned with both GDPR and NIS2—empower telecom actors to respond effectively and maintain regulatory assurance in the face of cyber incidents.

VII. Use Case: Security Breach Mitigation using the SAND5G Platform under GDPR/NIS2

In this illustrative scenario (see Figure 1), we demonstrate how the SAND5G platform supports a telecom operator in managing a security breach under GDPR and NIS2. When a potential intrusion is detected via integrated IDS (e.g., Snort3), SAND5G enriches the alert with contextual asset data and calculates impact scores. This enables the security analyst and Data Protection Officer (DPO) to quickly assess the situation, fulfill notification obligations within 72 hours (GDPR), and notify the NIS authority as required. If needed, users are informed and further steps are taken. The platform also logs mitigation activities and helps ensure post-incident compliance and policy updates.

While the SAND5G platform exemplifies how advanced tooling can support compliance and incident management under today's regulatory frameworks, it also establishes a solid foundation for the cybersecurity solutions of tomorrow. As networks transition toward 6G, platforms like SAND5G are expected to evolve, embracing increased complexity and integrating emerging technologies such as quantum security, zero-trust models, and AI-driven governance. The following section explores future governance models and security innovations that will be essential to support this next leap in telecommunications.

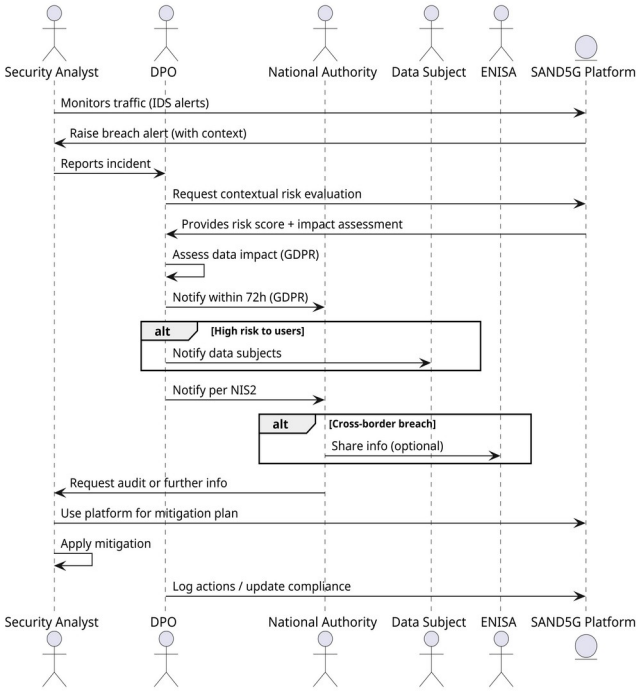

Figure 1: Security breach mitigation process using the SAND5G platform under GDPR and NIS2 directives.

VIII. Future Governance for 6G Security

The complexity and ubiquity of 6G networks introduce new security and resilience challenges. Adversaries are becoming more sophisticated, employing advanced AI techniques to launch novel attacks. To address these threats, 6G networks must achieve significantly higher levels of trustworthiness, dependability, and security, requiring advancements across multiple domains. Key approaches include the following subsections.

A. Physical Layer Security

Physical Layer Security (PLS) ([12],[13]) harnesses the physical characteristics of wireless channels to establish security, employing methods such as spread spectrum, frequency hopping, and directional antennas. It also emerges as a promising security technology for 6G due to its immunity to traditional cryptography vulnerabilities. Leveraging the physical attributes of wireless channels, PLS renders eavesdropping or interference by attackers exceedingly challenging.

B. Quantum Cryptography

Quantum cryptography ([14]) utilizes the principles of quantum mechanics to forge unbreakable encryption, offering a promising avenue for 6G security by evading vulnerabilities present in traditional cryptography. In addition, it stands out as a highly promising security solution for 6G networks, leveraging the distinct principles of quantum mechanics, which starkly contrast classical physics. This inherent distinction makes quantum cryptography resilient against attacks, even from formidable adversaries.

C. Zero Trust Security

Zero Trust Security ([15],[16]) operates under the assumption that no user or device is inherently trustworthy, necessitating comprehensive traffic inspection regardless of origin or destination. Zero Trust architecture provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. It emphasizes continuous authentication, authorization, and validation, alongside granular access control and continuous monitoring. It presents a robust security paradigm that operates under the assumption that no user or device holds inherent trustworthiness. Consequently, all network traffic undergoes scrutiny, regardless of its origin or destination, offering potent defense mechanisms against attacks on 6G networks.

D. Artificial Intelligence and Machine Learning

AI and ML technologies [17],[18]) are poised to bolster 6G network security by swiftly identifying and mitigating intrusions, discerning malicious traffic patterns, and predicting potential attacks. They offer multifaceted avenues to bolster the security of 6G networks. These technologies can adeptly identify and mitigate intrusions, discern malicious traffic patterns, and forecast potential threats. While still

evolving, AI and ML hold considerable promise in revolutionizing the security landscape of 6G networks.

E. Enhanced Authentication and Authorization

6G will adopt advanced authentication and authorization methods [19],[20], including multi-factor authentication and biometric verification, strengthening identity and access management to protect networks.

F. Secure Network Slicing

Secure network slicing [21],[22] aims to create isolated virtual networks tailored to specific services or user groups, ensuring protection and resource separation across 6G infrastructures.

G. Quantum Key Distribution

Quantum Key Distribution (QKD) [23], based on quantum mechanics, enables secure key exchange between parties, safeguarding against eavesdropping and interception in 6G channels.

As 6G technology approaches realization, governance models must evolve to accommodate unprecedented technological complexity and agility. Future governance will likely incorporate adaptive regulatory frameworks enabled by real-time monitoring and AI-powered compliance tools, allowing for rapid responses to emerging threats. Moreover, ethical considerations surrounding AI deployment, user privacy, and digital sovereignty will demand multi-stakeholder engagement including industry, governments, academia, and civil society. Transparent mechanisms for accountability, certification, and cross-border cooperation will become critical. This dynamic governance approach aims to balance innovation acceleration with security assurance, fostering trust and sustainability in next-generation networks.

In light of these anticipated advancements, it becomes imperative to reflect on the regulatory foundations that must evolve in parallel. The following conclusion synthesizes the insights presented and outlines the key priorities for securing future networks.

IX. Conclusion

As 5G networks become the backbone of modern digital infrastructure, regulatory oversight remains essential to ensuring their security and resilience. The European Union's frameworks—GDPR, EECC, and the NIS Directives—provide a solid foundation for data protection, risk mitigation, and incident response. Institutions like ENISA, along with national authorities and international partners, play a vital role in guiding and enforcing these regulations.

This paper has illustrated how telecom operators can align with evolving compliance demands and has demonstrated the practical value of platforms like SAND5G in navigating real-world breaches. These tools enable actionable, risk-based decision-making and help bridge the gap between regulatory requirements and operational response.

However, as we move toward 6G, new threats and technological paradigms demand a shift in cybersecurity governance. Adaptive regulatory models, AI-enhanced security mechanisms, and quantum-safe solutions will be key to protecting next-generation networks. Moving forward, a holistic, collaborative, and proactive governance strategy will be essential—not only to safeguard infrastructure, but also to foster trust and innovation across the digital ecosystem.

REFERENCES

[1] Cybersecurity and resiliency of Europe's communications infrastructures and networks, Follow-up to the Nevers Call of 9 March 2022, NIS Cooperation Group, 21 February 2024.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[3] Directive (EU) 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[4] Directive (EU) 2018/1972 of the European Parliament and the Council establishing the European Electronic Communications Code.

[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS 1 Directive).

[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[7] NIS Cooperation Group, Technical Guideline: Security Measures for Top-Level-Domain Name Registries, 23 March 2022.

[8] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities.

[9] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification.

[10] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final.

[11] ENISA's ECASEC Expert Group portal, https://resilience.enisa.europa.eu/article-13.

[12] L. Mucchi et al., "Physical-Layer Security in 6G Networks," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1901-1914, 2021, doi: 10.1109/OJCOMS.2021.3103735.

[13] E. O. Frimpong, B.-H Oh, T. Kim, I. Bang, "Physical-Layer Security with Irregular Reconfigurable Intelligent Surfaces for 6G Networks", Sensors 2023, 23, 1881. https://doi.org/10.3390/s23041881.

[14] C. R. García et al., "Secure and Agile 6G Networking – Quantum and AI Enabling Technologies", 23rd International Conference on Transparent Optical Networks (ICTON), Bucharest, Romania, 2023, pp. 1-4, doi: 10.1109/ICTON59386.2023.10207418.

[15] H. Sedjelmaci, K. Tourki and N. Ansari, "Enabling 6G Security: The Synergy of Zero Trust Architecture and Artificial Intelligence", in IEEE Network, doi: 10.1109/MNET.2023.3326003.

[16] M. A. Enright, E. Hammad and A. Dutta, "A Learning-Based Zero-Trust Architecture for 6G and Future Networks", 2022 IEEE Future Networks World Forum (FNWF), Montreal, QC, Canada, 2022, pp. 64-71, doi: 10.1109/FNWF55208.2022.00020.

[17] Abdulrahman Yarali, "Artificial Intelligence and Machine Learning in the Era of 5G and 6G Technology", in From 5G to 6G: Technologies, Architecture, AI, and Security , IEEE, 2023, pp.65-72, doi: 10.1002/9781119883111.ch4.

[18] M. M. Saeed, R. A. Saeed,M. Abdelhaq, R. Alsaqour, M. K. Hasan, R. A. Mokhtar, "Anomaly Detection in 6G Networks Using Machine Learning Methods", Electronics 2023, 12, 3300. https://doi.org/10.3390/electronics12153300.

[19] Samuthira Pandi V, Anitha Juliette Albert, K. Naresh Kumar Thapa, R. Krishnaprasanna, "A novel enhanced security architecture for sixth

generation (6G) cellular networks using authentication and acknowledgement (AA) approach", Results in Engineering, Vol. 21, 2024, doi:https://doi.org/10.1016/j.rineng.2023.101669.

[20] I. Darman, M. K. Mahmood, S. A. Chaudhry, S. A. Khan and H. Lim, "Designing an Enhanced User Authenticated Key Management Scheme for 6G-Based Industrial Applications," in IEEE Access, vol. 10, pp. 92774-92787, 2022, doi: 10.1109/ACCESS.2022.3198642.

[21] Z. Ren, X. Li, Q. Jiang, Y. Wang, J. Ma and C. Miao, "Network Slicing in 6G: An Authentication Framework for Unattended Terminals", in IEEE Network, vol. 37, no. 1, pp. 78-86, January/February 2023, doi: 10.1109/MNET.112.2100738.

[22] I. H. Abdulqadder and S. Zhou, "SliceBlock: Context-Aware Authentication Handover and Secure Network Slicing Using DAG-Blockchain in Edge-Assisted SDN/NFV-6G Environment", in IEEE Internet of Things Journal, vol. 9, no. 18, pp. 18079-18097, 15 Sept.15, 2022, doi:10.1109/JIOT.2022.3161838.

[23] Muhammad Zulfiqar Ali, etal, "Quantum for 6G communication: A perspective", IET Quantum Communication, Vol. 4, Issue 3, 2023, doi: https://doi.org/10.1049/qtc2.12060.