UDC 004.056.55 **doi:** https://doi.org/10.20998/3083-6298.2025.03.08

Oleksandr Pasko[1], Andrii Tkachov[1]

[1]National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine

6G SECURITY REQUIREMENTS THROUGH THE LENS OF THREAT EVOLUTION

Abstract. Topicality. The development of mobile networks from 4G to 6G was accompanied by fundamental architectural changes, such as the transition to software, cloud and AI-oriented solutions, which radically expand the attack surface and complicate the organization of security. The experience of 4G (where problems with secure data transmission, signal vulnerability and confidentiality were revealed) and 5G (where risks of violating the isolation of network slices and compromising open APIs arose) showed that for 6G it is necessary to implement the "security-by-design" model. However, there is still a lack of a systematic approach to defining architectural requirements that would cover both legacy and new threats. **The subject of study** in the article is the security architecture of sixth-generation networks. **The purpose of the** article is to create a structured list of security requirements for 6G networks, formed on the basis of an analysis of evolutionary threats and the specifics of a new, multi-domain architecture. **The following results** were obtained. The analysis of 4G and 5G identified key legacy risks (DoS/DDoS, MitM, attacks on cores and slices of networks). Considering these risks, as well as specific threats of 6G (attacks on the AI lifecycle, post-quantum risks, THz/RIS/VLC and DLT/Blockchain vulnerabilities), a comprehensive list of general security requirements for 6G networks was formed, such as the implementation of a zero-trust architecture, post-quantum cryptography, AI/ML lifecycle protection, privacy by default, physical security for new spectra/technologies, AIOps-based resilience principles for autonomous self-healing and unification of global standards. **Conclusion.** The formed requirements provide the basis for implementing the "security by default" paradigm in a multi-domain, AI-oriented 6G architecture.

Keywords: 4G, 5G, 6G, cybersecurity, mobile networks, security threats.

Introduction

Problem relevance. The development of mobile networks from 4G to 6G brings not only higher speeds and lower latency, but also a transition from hardware to software-implemented solutions, open interfaces and distributed computing, which completely changes the approaches to security [1-2]. 4G has already the transition to “all-IP” and the separation of the control and user planes, although it had performance advantages, but expanded the possibilities for attacks. These vulnerabilities appeared in signaling processes, data transmission between the station and the core and in user privacy [3]. In 5G, the service-based architecture (SBA), together with software-defined networking (SDN) and network functions virtualization (NFV), Multi-Access Edge Computing (MEC) and end-to-end network separation, turned it into a “cloud data center” with strict quality requirements, while adding risks of isolation violations and complexity in management [4-5]. 6G is expected to be a platform built from the ground up on AI and cloud technologies, with intent-based control, digital twins and the fusion of terrestrial and non-terrestrial networks (SAGIN), requiring built-in security by default and an end-to-end trust model [6-8].

Literature review. Research on 4G points to typical threats to all-IP networks – eavesdropping, man-in-the-middle attacks, jamming, rogue base stations, signaling storms and risks to the network core that may be inherited by subsequent generations [3]. Research on 5G points to weaknesses in the SDN/NFV stack, open APIs, MEC and risks of breaking isolation between network slices [4, 9-10]. For 6G, the NGMN/SOLIDS concepts describe a three-layer model and four cross-cutting planes (data/AI/security/collaboration), a single resource space from device to cloud and the integration of terrestrial networks. Also, the scientific part focuses on the need to implement zero trust, post-quantum encryption, privacy by default and artificial intelligence (AI) lifecycle security, as well as physical security for new technologies [1-2, 6-8]. Additional reviews systematize both old threats (DoS/DDoS, MitM) and new ones (AI supply chain attacks, post-quantum cryptography (PQC) transition, attacks on new technologies, cross-domain trust issues), emphasizing the need for unified standards [5, 9]. However, despite the extensive number of review and vision papers focusing on prospective 6G threats, a comprehensive and systematic approach to defining security requirements is currently lacking. Existing studies either focus too broadly on the security of future technologies (AI, PQC, reconfigurable intelligent surface (RIS)) or limit themselves to cataloging 6G risks without offering a structured, actionable set of requirements

The purpose of the research is to create requirements for the security of 6G networks, taking into account the experience of previous generations (4G and 5G). To achieve this purpose, it is necessary to identify architectural features and typical threats for 4G and 5G networks. It is also necessary to identify potential threats to the 6G network by analyzing legacy vulnerabilities and the specifics of the new architecture. Based on this, a list of 6G security requirements will be formed, consistent with the principles of leading industry documents, which is the basis for implementing "built-in" security as an integral feature of the 6G architecture.

1. 4G

The 4G LTE system is built on a new “all-IP” model with a “flat” structure. It combines only three main parts that work as a single mechanism: User Equipment (UE), E-UTRAN radio network (consisting of eNodeB base stations) and EPC packet network core. UE devices communicate with eNodeB using special access protocols and E-UTRAN is connected directly to

evolved packet core (EPC) – a powerful IP system that connects to external provider networks. This simple organization was the key to reducing delays and unifying data and voice transmission, which opened the way to the massive mobile Internet [3].

Inside the packet network core, advanced elements operate, which are the intelligence center of the network. Among them, the access gateway node (AGW) stands out, which combines very critical functions, in particular the role of Mobility Management Entity (MME). MME is responsible for user equipment (UE) identification, its authentication and mobility. To ensure reliability and performance, the architecture supports a "mesh" topology, where each base station (eNodeB) can connect to multiple AGWs. In addition, its full compatibility with the TCP/IP stack greatly simplifies connectivity to any external IP devices, such as routers and servers [3].

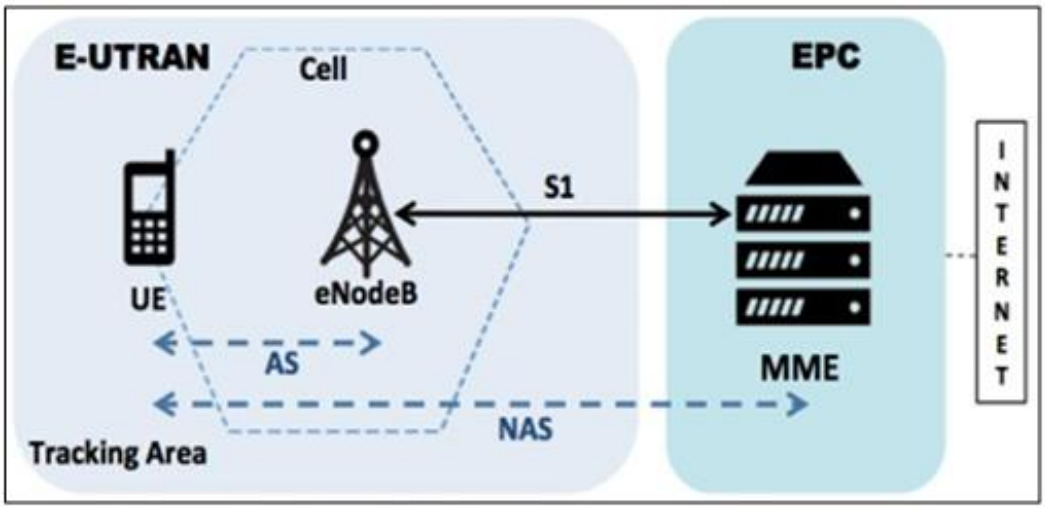

Fig. 1. 4G LTE System Architecture [3]

In summary, the 4G architecture achieved a unique combination. It simplified both the control plane (CP), which handles the signals, and the user plane (UP), which carries the data itself. This separation of functions, together with the idea of "all-IP" integration, was the basis for the further development towards 5G networks. However, at the same time, this change in architecture also expanded the "attack surface", creating new possible weaknesses in the signaling and the data transmission system [3].

The LTE security model is purposefully focused on two key areas: protecting unique user identifiers and strengthening the integrity of signals between the user equipment (UE) and the network core. To protect user data, SIM cards and UEs use temporary identifiers, which reduces the risk of leakage of permanent IDs. The security of signaling exchanges between the UE and MME is also significantly strengthened, and special protocols for encryption key management and authentication are used for secure transitions between 4G and non-4G networks [3].

In the LTE core (EPC), the critical elements are the Serving Gateway (SGW) and Packet Data Network Gateway (PGW) gateways, through which user traffic passes and the exit/entry points to external networks, so the security model provides for mutual authentication at the interfaces and protection of inter-network communication channels. The foundation of this model is a developed key hierarchy that provides session key generation and encryption/integrity for the control plane (RRC/NAS) and secure transport connections between eNodeB and AGW (IPsec), while user plane encryption is performed on the UE–eNodeB link in PDCP [3].

Although LTE has advanced security mechanisms (including mutual authentication, encryption, and the use of temporary identifiers), practical experience has revealed a persistent set of threats: from passive eavesdropping and man-in-the-middle (MitM) attacks to active jamming and signal "storms" [3].

Let's consider the ***main threats inherent in 4G networks***:

Eavesdropping and Data Interception. An attacker can carry out unauthorized interception of communications. This is done using flaws in protocols or incorrect settings of security mechanisms (such as IPsec/TLS). The result is an uncontrolled leak of highly sensitive information [3].

Man-in-the-Middle (MitM). This type of attack allows an attacker to intercept and modify traffic between a subscriber and the network by exploiting weak authentication mechanisms or by substituting legitimate network elements – in particular, through the use of rogue base stations (rogue eNodeBs) [3].

Jamming and Denial of Service (DoS/DDoS). Jamming creates noise or false signals that overload communication channels, making the network unusable by normal users who physically disrupt the communication channel. Denial of Service (DoS/DDoS) attacks overload the network with excessive traffic, which degrades the quality of the network or makes it unavailable [3].

Fake Base Stations (IMSI-Catchers). These malicious base stations skillfully imitate the operator's

real communication towers, forcing user devices (UEs) to connect to them. This allows attackers to intercept and manipulate traffic, and force devices to downgrade to a less secure standard [3].

Signaling Storms. This type of attack occurs when too many RRC/NAS messages are sent. They overload the network's signaling system, causing long delays and connection failures [3].

Replay Attacks. The attacker intercepts valid signaling or data messages and then retransmits them to another user or network in order to bypass security checks or interrupt an active communication session [3].

Redirection Attacks. The essence of this threat is to change the routing or authentication systems in order to direct traffic from the user's device to malicious networks or websites. This attack is carried out by intercepting and altering signaling messages or exploiting vulnerabilities in the network's routing and authentication processes [3].

Threats to Core Elements (SGW/PGW). As previously mentioned, SGW and PGW gateways are critical components of the LTE architecture, attacks targeting them can disrupt the entire network, causing major system failures and uncontrolled data leaks [3].

2. 5G

The development of the fifth generation of mobile communications (5G) is not just about increasing speed, but a fundamental change in the way networks are built. Instead of a single approach, 5G offers two main strategies. The first, Non-Standalone (NSA), is the most common initial solution: 5G New Radio (NR) works together with the previous generation EPC core from 4G. The second, Standalone (SA), involves a complete architecture with the new 5G Core (5GC). In practice, operators often start with NSA for a quick increase in speed, and then gradually move to SA. This “hybrid” phase is why real-world latency and speed figures in commercial networks can vary greatly, as they depend on which architecture (NSA or SA) the operator uses [10].

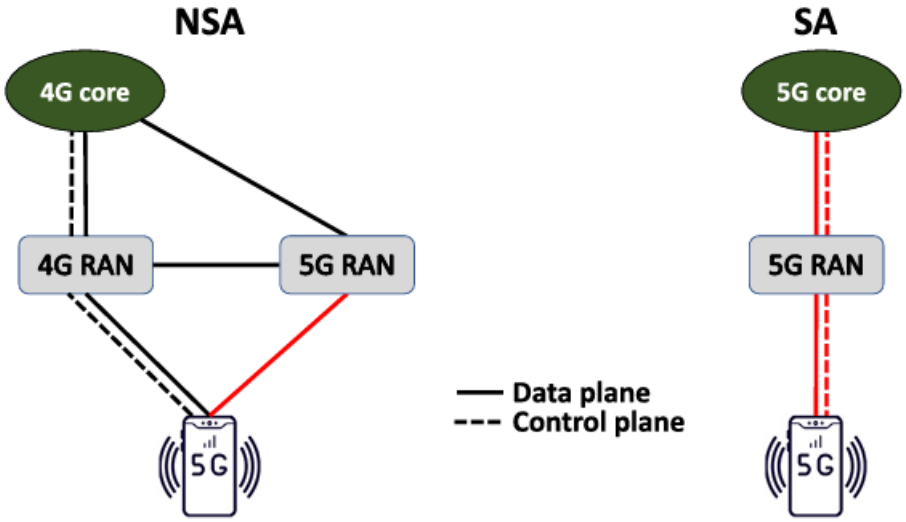

Fig. 2. A schematic diagram of 5G NSA and 5G SA architectures. [10]

The key architectural innovation of 5G Core (5GC) is the Service-based Architecture (SBA). Instead of large, indivisible systems, core functions (such as AMF, SMF, UPF) are implemented as independent microservices. These services do not communicate with each other via internal protocols, but interact via open, standardized application programming interfaces (APIs) using protocols such as HTTP/2 and OpenAPI. This, together with software-defined networking and network functions virtualization, allows the network to dynamically scale, place functions closer to the user (MEC), and implement network slicing. At the radio access layer (RAN), gNB nodes are also logically divided into blocks, and their integration occurs via high-speed xHaul transport channels (fronthaul/midhaul/backhaul). This enables end-to-end management, ensuring that the slices are truly end-to-end, with a single QoS policy [4]. Operationally, this shift to SBA means that telecom networks are becoming more like cloud data centers, running on a software-configurable data plane with active service level monitoring. This single physical environment can simultaneously guarantee different requirements (for example, high speed, ultra-low latency, or a large number of connections). At the same time, this flexibility also brings management complexity. Ensuring traffic isolation, adhering to quality rules, collecting detailed information, and supporting automated management are becoming daily necessities [4].

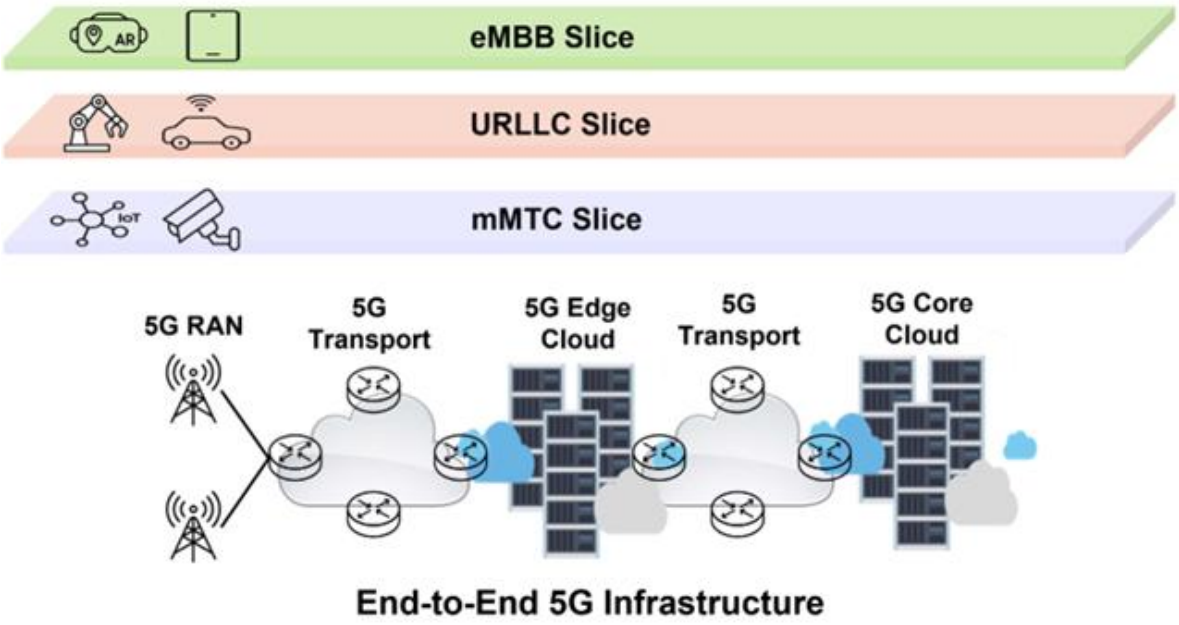

Fig. 3. The concept of network slicing [4]

In 5G, security is no longer a separate layer added on top. It is built into the SBA microservice model itself. Protection is built on the principles of authentication and authorization between each individual network function, the use of access tokens, encryption of interactions between services, and strict control of trust policies. Since the 5GC core is based on cloud technologies, familiar security concepts such as "zero trust" are transferred to the level of individual APIs and microservices, but at the same time classic cloud risks associated with interfaces and isolation arise [5].

Network Slicing imposes special security requirements. For network slicing to function effectively, strict isolation between slices, consistent enforcement of quality rules, and end-to-end telemetry from radio access to the core are required. Security in this context is not just encryption, but a whole set of measures that includes slicing rules, speed/latency guarantees, and automated anomaly detection. Therefore, protection must be implemented not only in 5GC, but also in the transport network and on the radio interface [4].

In addition, an edge component is emerging - MEC technology, where computing and network functions are transferred to peripheral data centers closer to the user. This extends the "trust boundary" of the network beyond the traditional core, requiring critical access control, API protection and clear policies between different domains. Therefore, the overall threat landscape in 5G is not about finding fundamentally new types of attacks, but rather rethinking known cloud risks (SDN, API, isolation) on a telecommunications scale [1, 5].

Despite the built-in security mechanisms, the 5G architecture, focused on SDN/NFV, microservice APIs, end-to-end partitioning and MEC, significantly expands the attack surface. Most of the risks are similar to typical problems of cloud environments (unprotected interfaces, sharing issues, DoS attacks), but their impact in 5G is greater due to centralized control. The consequences of even partial degradation of one function can have a cascading effect [4-5]. Let's consider the ***main threats inherent in 5G networks***:

Attacks on the SDN controller and its interfaces. Centralization of control makes the SDN controller a critical point of failure. Its compromise or manipulation through North/Southbound interfaces allows an attacker to change routing, QoS and segmentation policies throughout the network [9].

Vulnerabilities in the NFV stack. Virtual network function (VNF/VM) isolation issues, hypervisor vulnerabilities, or access to the NFV orchestrator threaten both confidentiality (data leakage from neighboring VNFs) and availability of critical services [9].

Isolation violation between network slices. If segmentation policies on RAN/Transport are configured incorrectly or proper SLA control is lacking, cross-slice interference or even traffic leakage between slices can occur, which directly violates uRLLC or eMBB guarantees [4].

Compromise of open APIs (SBA, OSS/BSS, edge). Standard cloud threats such as weak authentication, token leakage, or injection vulnerabilities can enable unauthorized calls or modifications of core network functions [5].

MEC/edge – physical and local attacks. Co-locating functions at edge sites, often in collaboration with third parties, adds risks of physical access, local DDoS and MitM attacks in weakly protected segments [9].

DDoS and signaling storms. Even with cloud resilience, uncontrolled avalanche traffic (e.g. from IoT

botnets) or signaling plane congestion can exhaust critical SBA services (e.g. AMF) or transport segments [9].

NSA→SA transition risks. In NSA mode, the mixed traffic and control path between the legacy EPC and the new 5GC creates an increased likelihood of integration errors and points of mistrust at the interfaces between eNB/gNB/UPF components [10].

3. 6G

The sixth generation of mobile communications (6G) is expected to hit the market in 2030. It is not just an evolutionary step from 5G, but a radical rethinking of the architecture. The main task of 6G is to create a single, highly intelligent infrastructure that will be a connecting link between the physical, digital and biological worlds, embodying the idea of the Internet of Everything (IoE) [1].

The need for 6G arises from the obvious gap between the capabilities of 5G networks and the ambitious requirements of the new scenarios described in IMT-2030 [11]. These future scenarios require not only massive speed increases (up to Terabits per second (Tbps)), but also ubiquitous intelligence (where AI/ML is a native function of the network and is "present everywhere": from user devices (UE) and RAN/transport to edge centers and the cloud), integrated sensing and connectivity (ISAC), the implementation of digital twins and the creation of environments that connect the human, digital and physical worlds. That is why 6G must provide not just better performance, but a fundamentally new quality of service: sustainable energy efficiency, global coverage and intent-driven design [1].

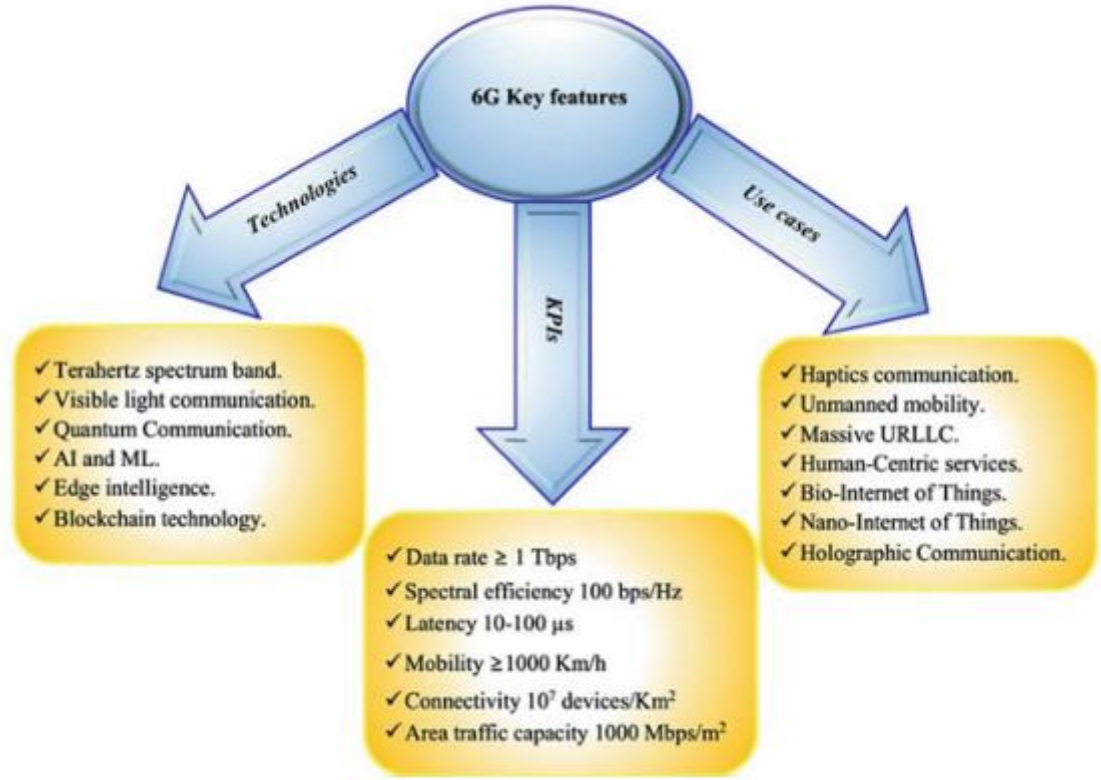

Fig. 4. Major milestones of 6G wireless [13]

The architectural core of 6G is a cloud-native and AI-based service platform that integrates computing power directly at the network edge, enhances end-to-end network slicing (E2E-slicing) and uses digital twins of the network for management. Unlike 5G, where the transition to cloud infrastructure (cloudification) was concentrated mainly in the core, 6G involves much broader decentralization: functions and computations are dynamically redistributed in a single resource space – from end devices to a centralized cloud. At the same time, a key feature is the establishment of sustainability requirements "by design", which creates fundamental advantages over 5G: providing more flexible services for vertical industries, ensuring better determinism of delays and energy consumption, as well as native support for different types of access (terrestrial, Wi-Fi, satellite) [1].

A specific functional model is offered by SOLIDS: a three-layer topology with a resource layer, a network function layer and a service layer, which permeate four end-to-end planes – data collection, AI, security and sharing and cooperation. The resource layer combines basic resources (radio, computation, storage) into a single pool. The network function layer composes individual functions or combines them to meet service requirements. The service layer is responsible for supporting services and customizing them to meet specific requirements. The data acquisition plane provides telemetry collection and processing. The AI plane provides the AI engine. The security plane builds

"native security" by providing end-to-end protections. Finally, the collaboration plane provides secure data, models, and resources exchange [6].

Another feature of the architecture is the native integration of the non-terrestrial component (NTN) in the form of SAGIN – a single space-air-ground network. Unlike 5G approaches, where the network core is often located on the ground, 6G-SAGIN aims to create a "flat" service network with unified interfaces and the ability to place selected CN functions in orbit (e.g., on LEO satellites) to reduce Round Trip Time (RTT) and ensure seamless mobility. This reveals another crucial advantage over 5G: truly ubiquitous global coverage and better support for latency-sensitive services on a global scale, which is critical for applications such as digital twins [7].

Parallel to the evolution of the architecture, 6G is experiencing physical innovations: the use of reconfigurable intelligent surfaces (RIS), optical channels (VLC), the development of the terahertz (THz) band, the introduction of Cell-free MIMO and integrated sensing and communication (ISAC). These technologies lay the technical foundation for deploying ultra-dense networks, achieving terabit speeds and ultra-precise positioning [5].

Finally, the 6G architecture directly addresses the operational challenges of 5G - high power consumption, O&M complexity and orchestration between different domains. In the SOLIDS model, this is transformed into AI-driven automation of operations (AIOps), integration of energy conservation policies, simplification of the protocol stack, and further separation of signaling and data (CP/UP). Thus, "consistency and simplicity" become design requirements [6].

Given the key architectural principles of 6G (AI-native management, softwarization, integration of a huge number of IoT devices and non-terrestrial networks (NTN/SAGIN), use of new spectrums/technologies such as THz/RIS/VLC) and the ambitious goals of building a "trusted network", it is important to understand that 6G not only inherits the risks of 5G, but also scales them proportionally to the growth of the number of connections and the autonomy of solutions. Therefore, let's consider the ***potential threats to 6G networks***:

Attacks on the life cycle of AI systems. As 6G is built with an AI-native architecture (where AI is the "nervous system" for managing policies, analytics, intrusion detection systems and orchestration), a new class of threats emerges. Attacks aim to compromise data, models or decisions made by AI, for example, "poisoning" training data or manipulating input data (adversarial evasion) [4, 7].

Post-quantum risk or Harvest-Now-Decrypt-Later. The potential creation of a quantum computer threatens to break most current asymmetric cryptographic algorithms. Critical, long-lived 6G data (such as telemetry or permanent trust keys) can be intercepted today and stored for future decryption [4, 5].

Physical layer vulnerabilities in new spectra (THz/VLC/RIS). The use of new technologies offers new attack vectors. Despite the high directivity of the beams, which increases security, jamming, targeted eavesdropping and spoofing remain relevant. In particular, malicious configuration of RIS (reflection manipulation) or exploitation of data leaks through VLC light channels create new opportunities for compromise [8, 12].

Expansion of the attack surface through Softwarization (software), SBA and open APIs. The shift to software-defined networking, service-based architecture (SBA), and multi-cloud environments significantly increases the potential attack surface. The core of the network, managed through open APIs, becomes vulnerable to supply chain attacks (via containers, microservices) and credential compromise [8].

Risks of network slice isolation. While network slices provide logical isolation of services, they create new vulnerabilities at the interfaces. Improper configuration of isolation policies or errors in network functions can violate the isolation boundaries. This can allow an attacker to escalate privileges from a less secure slice to a critical one [5, 12].

Security in the integrated space-air-ground network (NTN/SAGIN). The integration of ground, air, and space segments significantly expands the domain of trust and its perimeter. This creates vulnerabilities at the interfaces, particularly at the gateways between the ground and space segments [5, 7-8].

Risks of Distributed Ledger Technologies (DLT/Blockchain). While the use of DLT is proposed to increase transparency, the technology itself introduces new vulnerabilities. These include logical errors or "bugs" in smart contracts, attacks on the consensus mechanism, and the risk of personal data exposure through metadata leaks in public ledgers [8, 12].

Privacy threats from digital twins. With the proliferation of applications that create digital twins, the 6G network will collect unprecedented amounts of data. This massive collection of information increases the risk of re-identification and deep profiling of users [8, 12].

Vulnerability due to the scale of the Internet of Everything (IoE). The projected tenfold increase in the number of connected devices is turning the 6G network into a massive "attack front." This means that "old" vulnerabilities are now being exploited on an unprecedented scale, and the sheer number of devices makes it difficult to continuously monitor and manage incidents in real time [8].

Legacy threats. 6G threat analysis indicates that not all problems of previous generations have been solved by the introduction of new technologies. Threats such as classic DoS/DDoS attacks, Man-in-the-Middle (MitM) and spoofing are still relevant for 6G networks [9].

The difficulty of harmonizing standards. The 6G architecture involves the interaction of protocols and standards from numerous organizations (3GPP, ETSI, IETF, IEEE). The evolution of security standards for software-defined networking (SDN), network functions virtualization (NFV) and other mechanisms (SACM) makes verification difficult. The lack of agreed security

requirements at the domain boundary creates “gray zones” that are ideal for attacks [5].

Given the above potential threats to 6G networks, let’s look at the ***main requirements for 6G*** cybersecurity that should help mitigate the impact of these threats.

Total implementation of a “zero trust” architecture and continuous attestation. Since the 6G network consists of multiple domains and open APIs, which destroys the outdated perimeter security model and complicates trust between devices (UE), the edge and the cloud, it is necessary to implement access policies based on identity and context, as well as perform continuous trust verification [5, 13].

Post-quantum cryptography (PQC-by-design). Addresses the future vulnerability of modern cryptography to quantum computers. To do this, 6G networks should support hybrid schemes (combination of classical cryptography and PQC) and have a clear key migration plan [5, 13].

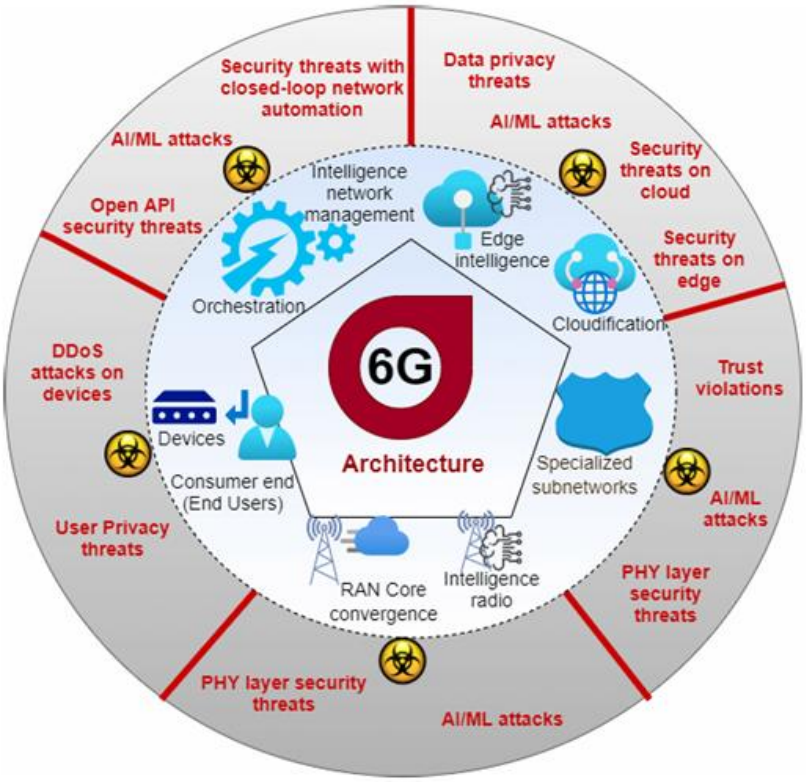

Fig. 5. 6G Security Threat Landscape [5]

Full AI/ML lifecycle security. It is very important to protect against AI/ML attacks such as training data/model poisoning, inference, or model inversion/extraction via open APIs. This requires data origin verification [5].

Privacy-by-default. Various network services such as XR and digital twins process huge amounts of sensitive data. Therefore, it is necessary to minimize the amount of data processed, use TEE, and apply privacy-preserving technologies [13].

Network slice isolation. It prevents information leakage between slices and privilege escalation that can occur due to failures or errors in policies or network functions [12].

PhySec for THz/RIS/VLC. Physical Security (PhySec) for new environments (THz/RIS/VLC) should prevent the escalation of physical layer attacks (e.g., through jamming and spoofing) and compromise of Reconfigurable Intelligent Surfaces (RIS) configurations. This requires the implementation of RIS authentication schemes, pilot contamination detection, and the use of physical layer coding techniques [13].

Resilience-by-design and AIOps. Address the fact that the scale of 6G and the criticality of its services require autonomous detection, incident localization, and network self-healing without human intervention. This is achieved through closed loop protection, resilience testing, and the multipath principle [5, 13].

DLT for privacy. The use of distributed ledger technology is promising, but poses risks of deanonymization of users. Therefore, it is necessary to implement smart contract verification and disclose data only on necessary attributes instead of issuing full certificate information [13].

Digital Twin Integrity. Ensuring the integrity of digital twins is essential to prevent erroneous decisions in network management. This requires digital signature of simulation data and policies for reproducibility of results.

Standards Unification. As the scope of 6G architecture encompasses a large number of

organizations with different standards, it is necessary to develop consistent security requirements that close gray areas.

Discussion of Results

The results of the study demonstrate that the formation of 6G security requirements cannot be approached as an isolated task, but must be viewed through the accumulated experience of 4G and 5G threat evolution. The comparison of legacy risks with projected 6G vulnerabilities shows that the fundamental issues of data interception, signaling manipulation and DoS/DDoS attacks remain relevant, yet they manifest on a much larger scale in 6G due to the massive growth of devices, the deep integration of AI and the expansion of non-terrestrial domains. The identified threats to new 6G technologies – such as the manipulation of RIS surfaces, exposure through VLC channels, or AI lifecycle attacks – highlight that traditional perimeter-based protection becomes ineffective. This supports the necessity of adopting zero-trust principles and continuous attestation as baseline mechanisms rather than additional controls.

Another important observation is the increasing interdependence between architectural domains. While in 4G and 5G the majority of critical risks were concentrated in the core, the transition to a unified resource space in 6G shifts vulnerabilities across all layers of the network – from user equipment and edge platforms to satellite and orbital components. This multidomain exposure emphasizes the need for strong end-to-end isolation, secure cooperation mechanisms and unified standards, as fragmentation between different organizations (3GPP, ITU-R, ETSI, IETF) can create exploitable gaps. The results also show that the native integration of AI and digital twins, although necessary for automation and optimization, introduces a new class of systemic risks: poisoning or manipulating training data may lead to cascade failures across the network, affecting service orchestration and trust management.

Conclusions

The research results have formed requirements for the protection of sixth-generation (6G) mobile networks. The requirements should be implemented according to the principles of Security-by-design and Resilience-by-design, which requires the total implementation of the Zero Trust architecture, post-quantum cryptography (PQC-by-design) and ensuring resilience based on AIOps. It is critical to protect sensitive data through privacy-by-default and guarantee the integrity of all components, including AI/ML systems and digital twins, through the isolation of network slices and physical security (PhySec). The successful implementation of these comprehensive measures requires the mandatory unification of global security standards to eliminate gaps. This system of requirements is based on a detailed analysis of both the architectural features of 6G and the vulnerabilities that can potentially be inherited from previous generations of 4G and 5G networks. Thus, the proposed list provides a basis for implementing the "security by design" paradigm in the 6G architecture, which is critical for ensuring resilience and trust in a multi-domain environment.

REFERENCES

1. NGMN Alliance (2025), "Network Architecture Evolution Towards 6G", https://www.ngmn.org/wp-content/uploads/250218_Network_Architecture_Evolution_towards_6G_V1.0.pdf
2. Loscri, V., Chiaraviglio, L. and Vegni, A. M. (Eds.) (2024), "The Road towards 6G: Opportunities, Challenges, and Applications. A Comprehensive View of the Enabling Technologies", *Springer,* pp. 185–196, doi: https://doi.org/10.1007/978-3-031-42567-7
3. Machora, L. M. (2024), "Cyber-security and performance Issues in 4G LTE network", *World Journal of Advanced Engineering Technology and Sciences,* vol. 12(02), pp. 622–662, doi: https://doi.org/10.30574/wjaets.2024.12.2.0328
4. Park, K., Sung, S., Kim, H. and Jung, J. (2023), "Technology trends and challenges in SDN and service assurance for end-to-end network slicing", *Computer Networks,* vol. 234, pp. 109908, doi: https://doi.org/10.1016/j.comnet.2023.109908
5. Porambage, P., Gürd, G., Moya Osorio, D. P., Liyanage, M., Gurtov, A. and Ylianttila, M. (2021), "The Roadmap to 6G Security and Privacy", *IEEE Open Journal of the Communications Society,* vol. 2, pp. 1109–1122, doi: https://doi.org/10.1109/OJCOMS.2021.3078081
6. Liu, G., Li, N., Deng, J., Wang, Y., Sun, J. and Huang, Y. (2022), "The SOLIDS 6G Mobile Network Architecture: Driving Forces, Features, and Functional Topology", *Engineering,* vol. 8, pp. 42–59, doi: https://doi.org/10.1016/j.eng.2021.09.006
7. Cui, H., Zhang, J., Geng, Y., Xiao, Z., Sun, T., Zhang, N., Liu, J., Wu, Q. and Cao, X. (2022), "Space-Air-Ground Integrated Network (SAGIN) for 6G: Requirements, Architecture and Challenges", China Communications, vol. 19(2), pp. 97–108, doi: https://doi.org/10.23919/JCC.2022.02.008
8. Ylianttila M., Kantola, R., Gurtov, A., Mucchi, L., & Oppermann I., (Eds.). (2020). "6G White Paper: Research Challenges For Trust, Security And Privacy", *6G Research Visions,* No. 9, pp. 15–19, http://urn.fi/urn:isbn:9789526226804
9. Ounza, J. E. (2023), "A taxonomical survey of 5G and 6G security and privacy issues", *Global Journal of Engineering and Technology Advances,* vol. 14(03), pp. 042–060, doi: https://doi.org/10.30574/gjeta.2023.14.3.0047
10. Kousias, K., Rajiullah, M., Caso, G., Alay, O., Brunstrom, A., Ali, U., De Nardis, L., Neri, M. and Di Benedetto, M. G. (2024), "Empirical performance analysis and ML-based modeling of 5G non-standalone networks", *Computer Networks,* vol. 241, pp. 110207, doi: https://doi.org/10.1016/j.comnet.2023.110207
11. ITU-R (2023), Recommendation ITU-R M.2160-0: Framework and overall objectives of the future development of IMT for 2030 and beyond, ITU-R, Geneva, https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2160-0-202311-I!!PDF-E.pdf
12. Tripi, G., Iacobelli, A., Rinieri, L. and Prandini, M. (2024), "Security and Trust in the 6G Era: Risks and Mitigations", *Electronics,* vol. 13(11), pp. 2162, doi: https://doi.org/10.3390/electronics13112162

13. Gururaj, H. L., Ravi, V., Shreyas, J. N. and Sapna, R. (Eds.) (2024), “6G Cyber Security Resilience: Trends and Challenges”, Springer, pp. 47–75, doi: https://doi.org/10.1007/978-3-031-85008-0

Received (Надійшла) 26.09.2025
Accepted for publication (Прийнята до друку) 16.10.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Пасько Олександр Ігорович – аспірант кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Oleksandr Pasko – PhD student of Cyber Security Department, National Technical University “Kharkiv polytechnic institute”, Kharkiv, Ukraine;
e-mail: sashapasko2000@gmail.com; ORCID Author ID: https://orcid.org/0009-0005-4732-1615.

Ткачов Андрій Михайлович – кандидат технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Andrii Tkachov – candidate of technical sciences, senior researcher, associate professor of Cyber Security Department, National Technical University “Kharkiv polytechnic institute”, Kharkiv, Ukraine;
e-mail: Andrii.Tkachov@khpi.edu.ua; ORCID Author ID: https://orcid.org/0000-0003-1428-0173.

ВИМОГИ БЕЗПЕКИ 6G КРІЗЬ ПРИЗМУ ЕВОЛЮЦІЇ ЗАГРОЗ

О. І. Пасько, А. М. Ткачов

Анотація. Актуальність. Розвиток мобільних мереж від 4G до 6G супроводжувався фундаментальними архітектурними змінами, такими як перехід до програмних, хмарних та ШІ-орієнтованих рішень, що кардинально розширюють поверхню атаки і ускладнюють організацію безпеки. Досвід 4G (де були виявлені проблеми з безпечною передачею даних, вразливістю сигналів та збереженням конфіденційності) та 5G (де виникли ризики порушення ізоляції зрізів мережі та компрометації відкритих API) показав, що для 6G необхідно впровадити модель "безпека за замовчуванням" (Security-by-design). Проте досі бракує систематизованого підходу до визначення архітектурних вимог, які б охоплювали як успадковані так і нові загрози. **Предметом дослідження** у статті є архітектура безпеки мереж шостого покоління (6G). **Метою статті** є створення структурованого переліку вимог до безпеки мереж 6G, сформованого на основі аналізу еволюційних загроз та специфіки нової, багатодоменної архітектури. **Були отримані наступні результати.** Проведений аналіз 4G і 5G ідентифікував ключові успадковані ризики (DoS/DDoS, MitM, атаки на ядра та зрізи мереж). Враховуючи ці ризики, а також специфічні загрози 6G (атаки на життєвий цикл ШІ, постквантові ризик, вразливості THz/RIS/VLC та DLT/Blockchain), сформовано комплексний перелік загальних вимог до безпеки мереж 6G таких як впровадження архітектури нульової довіри, постквантову криптографію, захист життєвого циклу AI/ML, конфіденційність за замовчуванням, фізичну безпеку для нових спектрів/технологій, принцип стійкості за замовчуванням на основі AIOps для автономного самовідновлення та уніфікації глобальних стандартів. **Висновок.** Сформовані вимоги забезпечують основу для реалізації парадигми "безпека за замовчуванням" у багатодоменній, ШІ-орієнтованій архітектурі 6G.

Ключові слова: 4G, 5G, 6G, кібербезпека, мобільні мережі, загрози безпеки