tworks:

Threats, Potential Vulnerabilities,

and Their Implications for National Security

ty and Privacy	
Type:	Article
URL:	https://knowledge.l

ancashire.ac.uk/id/eprint/5805
9/
doi:10.52

549/ijeei.v13i4.6573

Date	2025
Citation	Eghe Promise, Eh

igiator, Asantee, Georgee, Balisanee, Hewaa, Sa

lih, Abdulrahman, Aina, Folayo and Kuree, Ha

G

Networks: Threats, Potential Vulnerabilit

ies' and Their Implications for National Security

Security and Privacy. Indonesian Journal of E

International Journal of Electrical Engineering and Information Technics (IJEEE)

I), 13 (4). pp. 840-855. ISSN 2089-3272

Eg

Peter Smisek, Ehigiator, Asantee, Georgee, Balli

sanee,

Hewaa,

Salih,

Abdulrahmaan,

Aina,

Folay

Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 13, No. 4, December 2025, pp. 840~855
ISSN: 2089-3272, DOI: 10.52549/ijeei.v13i4.6573

Cybersecurity Implications of 5G Networks: Threats, Potential Vulnerabilities, and Their Implications for National Security and Privacy

Ehigiator Egho-Promise[1], George Asante[2], Hewa Balisane[3], Abdulrahman Salih[4], Folayo Aina[5], Halima Kure[6]
[1]Department of Computing, University College Birmingham, University Kingdom
[2]Department of Information Technology Education, Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development, Kumasi, Ashanti Region, Ghana.
[3]Business School, The University of Law, United Kingdom
[4]Northumbria University London, Department of Computer and Information Science, United Kingdom
[5]Department of Computing, School of Engineering and Computing, University of Central Lancashire, United Kingdom
[6]Department of Engineering & Computing, University of East London, United Kindom

Article Info

Article history:

Received Apr 16, 2025
Revised Sep 15, 2025
Accepted Nov 10, 2025

Keyword:

Cyber Security,
5G,
Threats,
Vulnerabilities,
National Security,
Privacy

ABSTRACT

The rapid expansion of Fifth Generation (5G) networks represents a revolutionary shift in telecommunications technology, offering increased speed, higher connection density, and enhanced network efficiency. Nevertheless, these benefits have also attracted various security risks that threaten the protection of national security and the privacy of private citizens. This research investigates the cybersecurity challenges associated with 5G networks by analysing emerging threats, assessing vulnerabilities in 5G infrastructure, and evaluating their impact on national security and individual privacy. The research approach includes a literature review of various sources of knowledge and regulations or policies, as well as a quantitative analysis of network vulnerabilities through penetration testing and threat modelling. The study's results indicate that network slicing introduces new risks to a network, as it provides potential attackers with easy access to weaknesses that exist within isolated network slices. Furthermore, the incorporation of Internet of Things (IoT) devices increases the overall risk, as they often lack proper security measures. Lastly, the multi-tenant characteristic of 5G networks poses a challenge in creating secure isolation between various operators and service providers. This makes it imperative for organisations and service providers to enhance their security measures, such as encryption and access control policies, as well as overall policies, to help rectify these issues. These findings concluded significant implications across national security and privacy fronts. The study re-emphasizes the importance of a multi-sectoral approach to cybersecurity by industries, policy-makers, and academic scholars. Measures and techniques that are relevant to implementing specific safety tactics and regulations were proposed. The results of this study serve as a reference for 5G cybersecurity. The results offer recommendations that are useful in developing security measures to counter threats and improve the security posture of future 5G networks.

Corresponding Author:

Ehigiator Egho-Promise,
Department of Computing,
University College Birmingham, University Kingdom
Email: Eegho-promise@ucb.ac.uk

1. INTRODUCTION

5G networks are already redefining telecommunications techniques. They are almost different from previous generations of wireless networks. 5G provides far higher data transfer rates and much lower latency, among other features. The fact that 5G technology enables nearly real-time communication and can

accommodate enormous amounts of data, positions 5G as an essential foundation for technological transformation. This extension involves the use of the Internet of Things (IoT). These advancements come with new and menacing cybersecurity threats that cannot be ignored. 5G brings new properties into the readings by depending on the software-defined architecture, employing virtualisation solutions and decentralising network management, which become new opportunities for threats [1]. Software Defined Networking (SDN) and Network Function Virtualization (NFV) make it easier to control the networks and make changes on the fly. However, they have also introduced a whole new way for a network to be hacked. Although 5 G's advanced features can significantly enhance network performance and functionality, these features also expand the concept of the attack surface and introduce new possibilities for exploitation [2]. Compared to hardware, the software is much more susceptible to intrusion, data alteration, and service unavailability [3]. The very structure of today's 5G networks is designed in layers and comprises numerous interconnected elements. These features make it significantly more challenging to protect such systems. Every layer in the existing layered network model, from the core network to the edge devices, presents a potential target for cyber threats. The connected nature, along with the distributed approach to processing data and storing it across the network of machines, multiplies the number of potential network attacks [4][5].

These weaknesses are not mere IT-related issues; they are directly related to the security of a nation's infrastructure. Core sectors, including electricity suppliers, transportation, and emergency services, currently rely heavily on 5G networks for their operations[6]. If the adversary manages to compromise these networks, then one would witness paralysis of critical services.

Network security in 5G is not concentrated around the core of the network as it is in the centralised networks. Thus, one may need a new approach in securing such a network. Security measures that are applicable in the centralised networks may not work for 5G's network. The risks are accentuated by the fact that cyber-attacks can affect most facets of the system simultaneously, unlike in the case of other systems, where multiple types of penetrations are required to sabotage it completely.

These cybersecurity adversities signify significant consequences, especially on the nation's security front. 5G networks have been identified to support major communication systems such as energy power systems, transport networks and public safety. An attacker can exploit these networks, and a successful cyberattack would have disastrous effects on these services. Additionally, several of these threats are no longer unique to a single nation, but rather transcend global boundaries [7]. Potentially, state-sponsored cyberattacks can readily harness 5G weaknesses to spy, sabotage, destabilise, or even subvert modern states. 'Adversarial' nation-states with highly developed cyber assets may use these operational weaknesses of 5G to deploy espionage, maintain instability in the geopolitical spectrum or compromise other nations' critical infrastructures. With the global progression of 5G technology, the impact of such attacks could spread beyond national borders, affecting global security and stability [8].

The high data transfer rate and network densification enable the transmission of a massive volume of data [9]. If data is intercepted or mishandled, it results in a serious violation of individuals' privacy. The combination of 5G with IoT increases these risks because a vast number of IoT devices are not constructed with high levels of security protection. Privacy violations, including unlawful surveillance, identity theft, data leakage, and similar threats, are among the privacy risks that can emerge as 5G becomes more widely deployed. Due to its broad application in modern society, the security issues associated with 5G can threaten almost every aspect of society, including personal privacy and national security [10]. Hence, 5G networks must be protected from a cybersecurity perspective, and such protection must also address the ethical issues associated with ubiquitous technology. There is therefore a need for a joint effort from governments, industry players and cybersecurity professionals to enhance strategies and policies that will ensure that, while reaping from the benefits of 5G technology, security risks and threats are minimised.

The purpose of this study, therefore, is to analyse the primary cybersecurity threats posed by 5G networks, identify and assess potential vulnerabilities in 5G infrastructure, explore the implications of these threats and vulnerabilities for national security and individual privacy, and propose strategic solutions and policy recommendations to mitigate these risks.

2. REVIEW OF LITERATURE

The advent of 5G technology brings transformative benefits across various industries, including high speed, ultra-low latency coefficients, and the opportunity to connect a large number of devices. Nevertheless, the advances are accompanied by a set of new cybersecurity threats peculiar to the 5G networks. These threats stem from the very aspects of 5G technology that are considered disruptive, such as network slicing, edge computing, and the increasing use of IoT devices.

According to Dangi et al. [11], network slicing attacks are among the most prominent cybersecurity threats associated with 5G networks. Network slicing is one of the critical features of 5G that allows operators to set up as many completely separate virtual networks or 'slices' on a single physical base. Each slice can be

customized to address different Operations Support Systems (OSS) usage requirements [12]. Although this capability enhances network optimisation and specific customer solutions, it also introduces new security risks. As per Wong and Schotten [13], one of the major concerns is the isolation between specific slices. If one slice is compromised, an attacker could potentially gain access to other slices, leading to widespread disruptions across the network. For instance, an attacker focuses on a particular slice of the critical infrastructure. Once they breach the perimeter, they exploit the lack of isolation and move to other slices for consumer services, leading to a domino effect [14].

Moreover, Edge Computing Vulnerabilities are another significant concern in the context of 5G networks. Edge computing is a key component of 5G, bringing computational power closer to the data source to reduce latency and enhance data processing efficiency [15]. Unlike controlling data to the central cloud, the new 5G networks can perform this control at the edge, that is, from the network they emerged from. According to Khan et al. [10], this decentralisation is most desirable for applications that require processing to take place virtually simultaneously or with very low latency, such as self-driving cars and smart cities. The distributed nature of edge computing introduces multiple new points of vulnerability.

The IoT-related risks contribute more to the cybersecurity challenges experienced in 5G networks [16]. One of the most touted features of 5G is the ability to support a massive number of IoT devices. This capability is fundamental for enabling the next generation of smart homes, cities, and industries, where numerous interconnected devices collaborate to automate processes and enhance efficiency. Nonetheless, the sheer volume of IoT devices linked to 5G can also dramatically expand the potential attack surface. Anand et al. [1]. found that many IoT devices, particularly those designed for consumer use, possess limited computational power and, consequently, often lack robust security features. Such devices can be the most accessible in terms of availability, allowing attackers to launch large-scale Distributed Denial of Service (DDoS) attacks. Typically, in a DDoS attack, several compromised devices, also known as botnets, are used with the primary intention of flooding the target with traffic, thereby causing disruption to services [17]. The risk posed by IoT devices in 5G networks is not limited to DDoS attacks. IoT devices can also work as a gateway to a larger network for the attackers. Once an attacker gains control of a poorly secured IoT device, they could use it to access the network it is connected to, potentially compromising other devices and systems on the same network. This threat is perilous insofar as IoT devices are connected to essential infrastructures, such as smart grids or ICSs. An attacker who manages to penetrate IoT devices in such environments could disrupt business operations, cause physical harm, or steal essential data [18]. However, the problem of IoT device security in 5G networks is complicated, as these devices are often numerous, installed evenly in various environments, and are difficult to control.

However, a comprehensive and multi-layered approach to security is necessary to mitigate the risks associated with network slicing, edge computing, and IoT devices in 5G networks. This approach incorporates robust encryption protocols to safeguard data in transit, robust authentication mechanisms to ensure that only authorised devices and users can access the network, and real-time monitoring and threat detection systems to identify and respond to attacks as they occur. Additionally, the security policy and its best practices should be implemented uniformly across slices, edges, and IoT devices to ensure the network remains resilient against attackers.

As 5G networks become increasingly critical to the functioning of contemporary societies, they are also driving new aspects of national security threats. These concerns primarily relate to the risks of cyber-attacks that could disrupt critical infrastructure, facilitate espionage, and compromise national sovereignty. 5G brings benefits on the economic and societal fronts, but it presents risks that experienced state and non-state actors can capitalise on. Thus, understanding and mitigating these risks is crucial for safeguarding national security in the era of 5G.

Critical infrastructure disruption is one of the most significant security threats associated with 5G networks [19]. The current world economy and society are sharply dependent on computers and the internet. This is evident in critical infrastructure, including electrical power systems, water supply systems, transportation networks, and medical services. According to Mourtzis et al [20], the high-speed, low-latency capabilities of 5G make it the backbone of smart infrastructure, enabling real-time monitoring, automated controls, and enhanced coordination across various sectors. However, this interconnectivity also means that a successful cyber-attack on 5G networks could have cascading effects, potentially leading to widespread disruptions of essential services. For instance, a cyber-attack targeting the 5G network supporting an electric grid could disrupt power distribution, leading to blackouts that affect millions of people and critical facilities, such as hospitals and emergency services [21]. Likewise, with the complexity of 5G transport systems, the transport system would be paralysed, logistics disrupted, and mayhem created in the cities. The scale and speed of such disruptions would likely be beyond the scope of disruptions possible in preceding generations of mobile networks, as 5G is deeply integrated into critical infrastructure.

Another critical national security issue related to 5G is espionage [22]. The large volumes of data transmitted over 5G networks, including sensitive government and corporate communications, make them prime targets for espionage by foreign actors. Jones and McCaslin [23] study found that state-sponsored actors could exploit vulnerabilities in 5G networks to intercept communications, steal sensitive data, and conduct surveillance on key individuals and organisations. The use of 5G for essential government communications and military operations further increases the risk of espionage. For example, through a point of presence in a 5G network, an attacker may be able to probe, listen to, and disrupt secure military communications, track the movements of military personnel and equipment, or exert influence over leadership and control mechanisms [24].

To address these national security concerns, various policies and regulatory controls have been established at both national and international levels. These frameworks aim to enhance the security of 5G networks, protect infrastructure, and mitigate the threat of espionage. The regulation expected to have the most significant impact on 5G network security is the General Data Protection Regulation (GDPR), mainly concerning data protection within the EU [25]. Generally, the GDPR demands high data protection standards, including secure processing of personal data, which is vital for preventing the theft of sensitive information transmitted over 5G networks. Compliance requires organisations to adopt robust encryption, access controls, and data breach notification procedures, all of which contribute to the overall security of 5G networks [26]. Like many other countries, the United States has implemented policies, guidelines, and frameworks to enhance cybersecurity through the National Institute of Standards and Technology (NIST) across various sectors, including telecommunications. The NIST Cybersecurity Framework, widely embraced by public and private organisations, offers a comprehensive approach to managing cybersecurity risks [27]. It highlights the importance of identifying critical assets, safeguarding them, monitoring cybersecurity, reporting incidents, and managing responses and recovery. Consequently, the framework is particularly pertinent to 5G networks, given their vital role in supporting essential services and the need for ongoing monitoring and adaptation to emerging threats.

National cybersecurity strategies also play a crucial role in addressing the security challenges posed by 5G networks. Nearly every country in the world has taken some preemptive measures regarding its firms or infrastructure. For instance, the US's 5G Strategy includes the requirement of creating a security-first 5G ecosystem, identifying the trusted vendors and supply chain security, and cooperating internationally in the sphere of cybersecurity [28]. The strategy also highlights the importance of maintaining the integrity of 5G networks to prevent espionage and protect sensitive data from foreign adversaries. Similarly, the European Union's Toolbox for 5G Security guides member states on mitigating security threats associated with 5G networks [29].

According to Patel et al.[30], the deployment of 5G networks, with their promise of faster speeds, lower latency, and the ability to connect a massive number of devices, marks a significant technological leap forward. Nevertheless, these advancements have also raised concerns about the potential violation of privacy, particularly regarding data acquisition and monitoring, as well as the possibility of building complex surveillance systems. As 5G becomes more integrated into everyday life, the amount of data generated and collected will increase exponentially, raising serious questions about how this data is used, who has access to it, and how individuals' privacy can be protected.

Data collection is a privacy concern that is associated with 5G. 5G networks, therefore, make more opportunities available than ever before in relation to the generation and transfer of data of all types, and this could be done in real-time [31]. This involves not only the usual types of data, such as communications and web browsing activities, but also vast amounts of data from connected devices, such as smart homes, wearables, and industrial IoT sensors. Khan et al. [32] found that one of the most significant challenges arising from large amounts of data within a 5G ecosystem is that the privacy of the individual can no longer be guaranteed, as this opens the floodgates for hackers, cybercriminals, and identity thieves. Among the most severe problems, one of the most significant is that the data collected from the use of 5G-connected devices may be relatively private and intrusive [32]. For example, information obtained through health monitoring devices is most likely to provide insights into habits, physical health, and even emotional status. In addition, a significant privacy concern that goes under the 5G consideration is location tracking [33]. The data collected by 5G networks is far more accurate than that collected by previous versions of cellular networks, primarily due to the increased presence of 5G cell towers and the utilisation of advanced technologies such as beamforming and massive MIMO (Multiple Input Multiple Output). This enables the tracking of individuals' movements with a level of detail that was previously unattainable. Although it has been used on the positive side, as it enhances navigational assistance or fosters location-sensitive services, uncertainties surround the privacy area. The ability to track an individual's location with such accuracy opens the door to potential abuses, including unauthorised surveillance by both private entities and governments [34]. For instance, accurate location

information could be used to bring advertising that caters for a specific individual's location, thereby resulting in unsettling advertising.

Moreover, another privacy implication of 5G is the potential for mass surveillance [35]. The improvements demonstrated in 5G networks establish the infrastructure needed for comprehensive surveillance on an unprecedented scale [36]. In particular, governments might be tempted to use these capabilities to inquire more deeply into the activities of their citizens for reasons that can be alleged to be as diverse as national security protection from crime and so on. However, the introduction of such surveillance could quickly extend beyond these specified objectives, and as a result, the privacy and civil liberties of citizens would be comprehensively violated [37]. The potential for mass surveillance in a 5G world is not merely theoretical. Several governments have already explored or begun adopting surveillance systems that leverage 5G capabilities. For instance, in some states, 5G is utilised to upgrade security frameworks installed in numerous cities, towns, and even homes, incorporating facial recognition, real-time video analysis, and other advanced technologies used in tracking individuals and predicting their actions [38].

Thus, to mitigate these privacy risks, robust regulatory frameworks and technical safeguards are essential. According to Tamburri [39], regulations such as the General Data Protection Regulation (GDPR) in the European Union ensure the proper protection of people's privacy by establishing standards for data collection, processing, and sharing. However, as 5G technology evolves, these regulations will need to adapt to the complexities of location identification, as well as those associated with mass surveillance [40]. Additionally, technical measures such as encryption, anonymisation, and decentralisation of data processing must be used systematically and correctly.

3. RESEARCH METHODOLOGY

3.1. Research Design

This research employed a mixed-methods approach. Various research methodologies and approaches have been used. These include the Quantitative method, the Qualitative method, the Abductive research approach, and the Pragmatist research philosophy.

3.2. Data Collection

Primary data collection has been the foundation of this study, providing thorough insights through qualitative interviews and quantitative surveys. Using a random selection technique, a sample of 50 to 100 survey respondents was selected to represent the population. Well-structured interviews were used to gather expert comments, observations, and thoughts. Participants were asked open-ended questions about their thoughts, opinions, and experiences with the cybersecurity implications of 5G. A purposive sampling technique was used to select respondents, including experts in reports and cybersecurity representatives with relevant field experience. A sample size of 5 to 10 respondents was selected for interview using the purposive sampling technique.

3.3. Data Analysis

Quantitative data analysis was conducted using statistical techniques, including frequency distribution, descriptive statistics, correlation analysis, and regression analysis. Thematic analysis was used to analyse qualitative data to discover emergent themes, patterns, and differences. Interview outcomes were evaluated.

These analytical techniques have been crucial in assessing the cybersecurity risks and opportunities that exist in 5G networks. The occurrence levels and the effects of various threats were identified. Patterns and relationships between different security risks and their associated risks were examined. Simulations were used to define potential attacks and evaluate the efficiency of security measures [41]. Moreover, risk assessment tools have also been integrated. This has helped in rating the severity and probability of different threats, and hence has facilitated the correct prioritisation of threats. These methods have provided a more reliable analytical consideration of the 5G cybersecurity problem. Data were analysed through the use of the following tools: Statistical Package for Social Science (SPSS),

4. RESULTS AND DISCUSSION

This section presents the study's findings. The section outlines the data analysis for both qualitative and quantitative data, utilising thematic and regression analyses.

4.1. Theme One: Identification of Cybersecurity Threats

This is the first theme of the study in which the researcher asked the informants about the severity and impact of cybersecurity threats in terms of identification. Additionally, this particular theme was categorised into two sub-themes so that the viewpoints related to the concerned themes.

4.1.1. Sub-theme: Specific data for the severity of cybersecurity threats in 5G networks

When the researcher asked respondents about specific data on the severity of cybersecurity threats in 5G networks, several respondents provided valuable insights. One informant noted that their study uncovered significant issues, highlighting that the attack surface of 5G networks is much larger compared to previous network generations. The introduction of numerous new devices and services further increases the potential exposure points.

Another respondent emphasized that vulnerability rates are nearly 40% higher in 5G than in 4G. The greater number of connections and the new architectural design of 5G bring about new types of threats that were not previously encountered.

Furthermore, another respondent reported a 50% increase in reported security threats after the rollout of 5G compared to 4G. The complexity of the new technology, which features Network Slicing and Edge Computing, has widened the attack surface and resulted in more security incidents, including hacking attempts. Another finding indicated a 40% increase in threat levels explicitly related to network slicing and edge computing. One research group reported that 5G networks, capable of supporting at least a hundred times the data capacity of their 4G counterparts, present a larger attack surface.

It was also revealed that there is a 30% increase in cyber-attack attempts on 5G networks compared to earlier generations. Moreover, the number of disclosed vulnerabilities in 5G systems is reportedly 30% higher than in 4G systems, contributing to a more sensitive risk profile. Finally, findings from a particular industry study suggested that the extended use of IoT devices in 5G networks has created an increased attack surface, raising security concerns.

4.1.2. Sub-theme: Preventable cybersecurity threats of 5G in previous generations of mobile networks

In this particular theme, respondents discussed preventable cybersecurity threats associated with 5G compared to earlier mobile networks. One informant noted that the density and variety of connected devices in 5G, from appliances to industrial equipment, introduce new vulnerabilities not prevalent in 4G. Another highlighted that the expanded exposure area allows multiple simultaneous attacks, such as DDoS via IoT and network slicing vulnerabilities, where attackers exploit loopholes across slices. A third respondent pointed out that 5G's more complex and diverse mechanisms create unique threats.

During interviews, a key participant emphasized that the larger IoT ecosystem in 5G increases the risk of DDoS attacks via compromised devices. Another mentioned that network slicing vulnerabilities could lead to data leaks or service disruptions due to cross-slice interference. An additional interviewee observed that the complexity of the expanded infrastructure complicates control and security measures.

Further insights included concerns about risks introduced by SDN and NFV, such as software bugs and configuration errors. The increased IoT connectivity raises the likelihood of DDoS attacks previously less feasible, while new attack vectors like remote hijacking of IoT devices and exploitation of network slicing features also emerged as distinct threats in 5G.

4.2. Theme Two: Vulnerability Assessment

4.2.1. Sub-theme: technical features of 5G networks that contribute to cybersecurity threats

In this theme, respondents discussed the technical features of 5G that heighten cybersecurity risks. One informant noted that the increased topological complexity of 5G networks, while aiding management, also creates vulnerabilities, as a flaw in one slice can impact others. Another highlighted that features like network slicing, which constructs multiple logical networks on a single physical infrastructure, centralize the network but also pose the risk that a failure or attack on one slice could affect the entire system.

A respondent further explained that the integration of SDN and NFV introduces software vulnerabilities, making networks more susceptible to bugs and hacking. The growing number of connected IoT devices, many lacking robust security, amplifies this risk. Additionally, one participant pointed out that the virtualization and reliance on network slicing diminish the perceived independence of network segments, allowing potential interference and data exposure.

Another respondent emphasized that the complexity and interconnectedness of software-defined 5G networks create more opportunities for cyberattacks. The expansion of connected devices also broadens the attack surface by exploiting existing vulnerabilities. Lastly, one informant highlighted that the layered nature of 5G's virtualization and slicing could present multiple entry points for adversaries if proper separation protocols are not enforced.

4.2.2. Sub-theme: technical features of 5G networks that contribute to cybersecurity threats

In this particular theme, the researcher asked the respondents about the most vulnerable components in the 5G network architecture. One informant highlighted that "The most threatened part of this network is

the data routing and management part of the core network because it is most important as well as complex in its functionality."

The second informant highlighted that "The end-user devices, as most of the time have a different level of security, can be leveraged to gain access to the network or to conduct an attack on the other device. The security breaches in end-user devices demonstrate that the extensive use of various connected devices can raise problems that are difficult to address. All these cases show that the much-needed security involves structures and the devices that are in the rooms."

According to the third respondent, "In 5G architecture, some of the components are important points of contact and can be exploited to interrupt or eavesdrop on a connection. Data route and management, another core component, is also a significant target since this component constitutes the core network."

According to a key respondent, "end-user devices are also at risk because of the variance of the security level of the gadgets connected to the network. Intruders easily use them for launching attacks or unauthorised access to the network resources."

During the interview session, one of the key interviewees highlighted that "Base stations and the core network are the most exposed components." Another informant revealed that "Mobile switching centres and base stations are highly susceptible to attacks because they handle a large amount of traffic and organise the data transfer. Sacrificing these can potentially degrade large groups of the network."

In addition, another interviewee reported, "Base stations are even more susceptible to such hacks because they are 'command central' for the transmission of data and are also open to both physical and remote assaults." The eighth informant highlighted that "Base stations and the core network are some of the most sensitive to DDoS attacks because they control and direct all the traffic." Likewise, the last informant highlighted that "Due to their importance in controlling and directing traffic flows, base stations and core networks remain at the highest risk because of them."

4.3. Theme Three: Implications for National Security

4.3.1. Sub-theme: potential risks and challenges of securing 5G networks

In this theme, the researcher explored the potential risks and challenges of securing 5G networks by interviewing respondents. One informant noted that specific cases, such as events involving base stations in Nassir, Tel Aviv, and Khobar Towers, illustrate how attacks on critical facilities can disrupt multiple services. Another respondent emphasized that targeting critical network links demonstrates how central data processing functions can be compromised, leading to severe data breaches.A key informant highlighted the complexity of protecting 5G networks, explaining that attacks on base stations can disrupt the entire network, while vulnerabilities in applications expose central points of data management to significant threats. Another respondent pointed out that end-user device vulnerabilities remain a major concern due to the varied security levels across interconnected devices, stressing the need for a comprehensive approach to securing the entire infrastructure.One participant emphasized the growing need for robust security measures, as attacks on base stations can impact entire network slices and millions of users. Another respondent discussed how the expanding network topology and intricate linkages create additional challenges for identifying and mitigating threats. They referenced recent attacks on base stations to demonstrate the vulnerability of this complex infrastructure.Several respondents also addressed breaches in telecommunication systems, highlighting issues related to integrity, confidentiality, and the decentralization of 5G infrastructure. One informant emphasized that attacks on base stations illustrate how a single compromised node can disrupt numerous services, showcasing the systemic nature of vulnerabilities. Another noted that 5G integration amplifies the risk, as a single vulnerability can threaten the entire network, reinforcing the importance of holistic security measures.

4.3.2. Sub-theme: How critical infrastructure of 5G could be targeted in a cyber-attack

In this particular theme, the researcher inquired about how the critical infrastructure of 5G could be targeted in a cyberattack. One informant highlighted that "Several worrying trends could evolve: For instance, if an attack is launched against the '5G-enabled smart grid', it has the potential to cause major blackouts to homes, businesses, and critical facilities such as hospitals. Another scenario deals with the infiltration of the transportation systems that employ 5G broadband for tracking and managing processes in real time."

The second informant highlighted that "Perturbations here may cause the occurrence of an accident or traffic congestion. Likewise, targeting the healthcare sector, which employs 5G for telemedicine and patient supervision, puts the lives of patients and the inviolability of their data at risk. In other words, any threat towards any of these crucial factors exposes the whole country's social, political and even economic stability to the all-important element – risk."

According to the third respondent, "Multiplied by bad actors' access to 5G networks, several worrying outcomes can arise after an attack on critical infrastructure. For instance, when an attack focuses on 5G-connected traffic management systems, its consequences may include massive traffic congestion, incidents, or

even fatal injuries. 5G-targeted attacks might jeopardise patients' records and affect the quality of delivered remote care."

During the interview session, one of the key interviewees highlighted that "Interference with smart grids incorporating 5G technology can disrupt electricity supply, disrupting living, working, and even emergency services. They demonstrate the extent to which 5G technology is integrated into our everyday lives and the potential harm that can result from breaches.

Another informant revealed that "Some examples are inability to power homes and offices, interruptions in transportation services that can result in quantitative and qualitative ramifications." In addition, another interviewee reported that "It might cause more serious damages to services that are essential for the population and the economy of a country, for example, blackout or lost connections."

Another key informant emphasised that "An attack on certain strategic assets would result in social inconvenience, economic losses, and the threat to lives— such reasons make the protection of such assets necessary." The last informant reported that "Non-functionality of the common emergency response system as well as failure of safety systems and precautionary measures can cause extreme public safety and economic impacts."

4.4. Theme Four: Privacy Risks and Surveillance Implications

4.4.1. Sub-theme: Primary privacy risks associated with 5G network

In this theme, the researcher explored the primary privacy risks associated with 5G networks through respondents' insights. One informant pointed out that the major threats stem from the vast amounts of data handled by 5G networks, often without explicit user consent. They highlighted that 5G enhances control over data from IoT devices, which can track user activities, locations, and health records, raising concerns about data storage, ownership, and usage.

Another respondent emphasized that identity compromises through hacking or intrusion are significant risks. They also noted that users are often only partially aware of data collection and may not explicitly agree to data sharing, increasing the potential for privacy violations. A key informant added that the handling of vast amounts of personal and sensitive data by billions of smart devices poses dual risks: data interception due to security loopholes and unauthorized access by unintended individuals. Concerns were also raised about the lack of transparency regarding user consent.

One respondent highlighted that users may not fully understand how their data is circulated or utilized across numerous devices, leading to issues of unclear ownership and control, which exacerbate privacy challenges. Another respondent identified data leakage as a growing risk, driven by increased data collection and insufficient mechanisms for obtaining user consent for various types of personal information.

4.4.2. Sub-theme: How 5G networks enable surveillance and the implications for user privacy

In this particular theme, the researcher asked the respondents about how 5G networks enable surveillance and the implications for user privacy. As an outcome, one informant highlighted that "5G networks might improve extreme surveillance because the technology offers increased density of the connected devices and large data handling capacity. For example, the increased use of sensors and cameras associated with smart cities can result in even more surveillance of individuals' movements and actions. This kind of surveillance could be used for several objectives, from traffic control to crime fighting; however, the potential for negative uses exists."

The second informant highlighted that "The implications for user privacy are important because people may be observed in ways they are not aware of, or perhaps do not want, which gives rise to questions about personal liberty." According to the third respondent, "Through the opportunity of high density of connected devices and sensors, it can be stated that 5G networks can dramatically augment surveillance potential. For example, visionary intelligent urban projects based on 5G may install many television cameras and sensors in public areas."

During the interview session, one of the key interviewees highlighted that "it can benefit public safety or operations, at the cost of being worried about always monitoring and privacy. One of the disadvantages of tracking people's movement and activities in real-time is that it can be abused and lead to violating people's right to privacy." The fifth respondent reported that "Due to the increased reliability of connections, 5G also raises the potential of mass surveillance of individuals and thus compromises privacy."

Another informant revealed that "With the higher data definition and node connection chance of 5G, there may be more profound monitoring of personal details by authorities. This is an area that has great potential in provoking privacy concerns if it is not well managed." In addition, another interviewee reported that "The higher connectivity of 5G networks means that the connection between the user and the network can be monitored at a more detailed level, which is a clear advantage for surveillance, and a clear danger to their privacy."

The eighth informant highlighted that "The surfeit of data that 5G networks can gather has the potential to produce more accurate surveillance, violating some personal rights and raising the likelihood of state misuse." The ninth informant stated that " 5G makes surveillance possible, thus violating people's privacy and making them vulnerable to government or corporate domination." Likewise, the last informant highlighted that "There is a problem with the enhanced connectivity provided by 5G."

4.5. Theme Five: Mitigation Strategies and Technological Developments

4.5.1. Sub-theme: strategies to address and mitigate vulnerabilities in 5G networks

In this theme, the researcher explored strategies to address and mitigate vulnerabilities in 5G networks, drawing on insights from respondents. One informant emphasized the use of enhanced protection layers and improved security measures for network slicing as key strategies. Another respondent highlighted the adoption of advanced encryption methods, both within and beyond the system, as well as ongoing advancements in network slicing security to protect virtual networks.

A key informant noted the growing efficiency of identity and access management solutions in controlling access to networking resources. They also mentioned the integration of artificial intelligence (AI) and machine learning to monitor threats in real time, alongside efforts to develop common security architectures that provide a roadmap for the secure implementation of 5G services.

Another respondent highlighted the recent development of stronger encryption techniques and the use of AI-based systems to counter attacks in real-time. They emphasized measures such as advanced encryption, real-time threat scanning, and improved network slicing isolation to protect data and identify risks effectively.

Further insights revealed the use of deep learning algorithms and new machine learning applications for threat identification, alongside the rollout of more secure encryption techniques to enhance 5G security and reliability. Several respondents also highlighted the ongoing development of AI-driven anomaly detection and stronger encryption protocols as critical methods to safeguard 5G networks. Additionally, measures such as advanced coding and AI technologies were cited as essential for creating extra layers of security to prevent known vulnerabilities.

4.6. Quantitative Analysis

In addition to the interviews, data were also collected through a survey. The results of the survey are discussed in the preceding sections.

4.6.1. Reliability Statistics

Table 1. Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.671	.701	33

Table 1 presents the reliability statistics to confirm the internal consistency of the scale using Cronbach's alpha. The value of 0.671 is sufficient to elaborate on the consistency of the scaled items. This value suggests that the internal consistency of the 33 items is moderate.

Distribution of General Questions

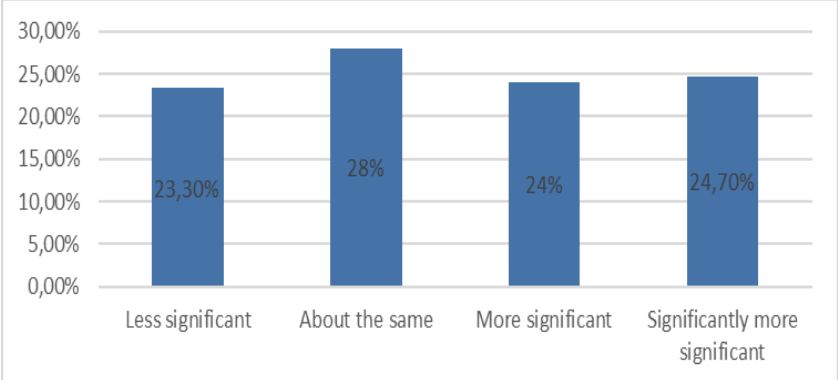

Figure 1. Perceived Significance of Cybersecurity Threats Posed by 5G Networks

The data presented in Figure 1 reflects the perceptions of respondents regarding cybersecurity threats in the context of 5G networks compared to previous wireless technologies. The distribution of responses is as follows:

24.7%: "Significantly more significant"
24.0%: "More significant"
28.0%: "About the same"
23.3%: "Less significant"

This distribution provides insights into how professionals and stakeholders in the field perceive the evolution of cybersecurity risks with the advent of 5G technology.

Nearly a quarter of respondents believe that cybersecurity threats in 5G networks are significantly more pronounced than in previous generations. This may reflect concerns about the increased complexity and interconnectedness of devices in 5G systems, as well as the anticipated rise in attack surfaces due to the proliferation of Internet of Things (IoT) devices.

This perception underscores the need for robust security measures and frameworks to mitigate potential vulnerabilities that may arise from the deployment of 5G technology.

Another substantial portion of respondents perceives the threats as more significant, but not to the extent of the previous category. This suggests that, despite improvements in technology, the perception of increased risk remains high due to the evolving nature of cyber threats. Organizations may need to prioritize cybersecurity investments and strategies as they transition to 5G to mitigate perceived risks effectively.

A significant majority (28.0%) feel that the cybersecurity threats are comparable to those faced in earlier networks. This could suggest that, despite technological advancements, the fundamental nature of the threats may not have undergone significant changes. This perspective may lead to complacency in security practices, as organizations might underestimate the unique threats posed by 5G technology.

The smallest segment of respondents views the cybersecurity threats as less significant, suggesting an optimistic outlook that advances in security measures accompany the rollout of 5G technology. Reliance on this perspective could be risky, as it may lead to insufficient preparedness for potential cyber threats that are unique to 5G environments.

The combined percentages of those who view threats as "Significantly more significant" and "More significant" (48.7%) indicate a prevailing concern among stakeholders regarding the cybersecurity risks associated with 5G technology.The fact that 51.3% of respondents view the threats as either "About the same" or "Less significant" suggests a divide in perception. This disparity could stem from varying levels of understanding of cybersecurity risks, operational contexts, or experiences with previous network technologies.

4.6.2. Correlation Analysis

Table 2. Correlation Matrix

		Dependent Variable	Threats	Potential Vulnerabilities	Cybersecurity Implications of 5G Networks
Pearson Correlation	Dependent Variable	1.000	.318	.464	.709
	Threats	.318	1.000	.277	.155
	Potential Vulnerabilities	.464	.277	1.000	.366
	Cybersecurity Implications of 5G Networks	.709	.155	.366	1.000
Sig. (1-tailed)	Dependent Variable	.	.000	.000	.000
	Threats	.000	.	.000	.029
	Potential Vulnerabilities	.000	.000	.	.000
	Cybersecurity Implications of 5G Networks	.000	.029	.000	.
N	Dependent Variable	150	150	150	150
	Threats	150	150	150	150
	Potential Vulnerabilities	150	150	150	150
	Cybersecurity Implications of 5G Networks	150	150	150	150

Table 2 reveals the relationships between the dependent variable and the independent variables—Threats, Potential Vulnerabilities, and Cybersecurity Implications of 5G Networks. The dependent variable exhibits a strong positive correlation with the Cybersecurity Implications of 5G Networks ($r = .709$, $p < .001$), indicating that as the perceived implications of 5G networks increase, the dependent variable also increases significantly.

There is a moderate positive correlation between the dependent variable and Potential Vulnerabilities ($r = .464$, $p < .001$), suggesting that as potential vulnerabilities in 5G networks rise, the dependent variable also

tends to increase. The correlation with Threats is weaker but still positive (r = .318, p < .001), indicating a lesser but statistically significant relationship between perceived threats and the dependent variable.

Among the independent variables, Cybersecurity Implications of 5G Networks exhibits a weak positive correlation with Potential Vulnerabilities (r = 0.366, p < 0.001) and a very weak correlation with Threats (r = 0.155, p = 0.029). Threats and Potential Vulnerabilities are weakly correlated (r = .277, p < .001), indicating that they are somewhat related, but each still contributes uniquely to the dependent variable.

The data in Table 4,2 shows that the "Cybersecurity Implications of 5G Networks" is the most critical factor related to the Dependent Variable in this study. The low correlations between the independent variables (Threats, Vulnerabilities, 5G Implications) are a positive sign. It means they are likely measuring different, non-overlapping aspects of the cybersecurity landscape. This increases our confidence that each one contributes unique explanatory power to the model. With a sample size of 150 (N = 150) and highly significant p-values (p < 0.000), the findings are statistically robust.

Regression Analysis

Table 3. Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.760[a]	.577	.568	.65709866	.577	66.361	3	146	.000	1.891

a. Predictors: (Constant), Cybersecurity Implications of 5G Networks, Threats, Potential Vulnerabilities
b. Dependent Variable: Dependent Variable

Table 3 indicates that the predictors—Cybersecurity Implications of 5G Networks, Threats, and Potential Vulnerabilities—explain 57.7% of the variance in the dependent variable (R^2 = .577). The model is statistically significant, as shown by the F-change (66.361, p < .001), with a Durbin-Watson value of 1.891, suggesting no significant autocorrelation in the residuals.

Table 4. ANOVA Estimates

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	85.960	3	28.653	66.361	.000[b]
	Residual	63.040	146	.432		
	Total	149.000	149			

a. Dependent Variable: Dependent Variable

b. Predictors: (Constant), Cybersecurity Implications of 5G Networks, Threats, Potential Vulnerabilities

The ANOVA Estimates (Table 4) further support the model's significance (F = 66.361, p < .001). The regression model explains a substantial portion of the variance compared to the residual variance.

The Table 4 confirms that the regression model is highly statistically significant. The p-value (.000) is less than .001, meaning there is an extremely low probability that the relationships observed between the predictors and the Dependent Variable occurred by chance. In short, the combination of "Threats," "Potential Vulnerabilities," and "Cybersecurity Implications of 5G Networks" does a significantly better job of predicting the Dependent Variable than simply using the mean of the Dependent Variable.

Table 5. Coefficient Estimates

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	-9.295E-17	.054		.000	1.000	-.106	.106
	Threats	.170	.056	.170	3.021	.003	.059	.280
	Potential Vulnerabilities	.193	.060	.193	3.237	.001	.075	.311
	Cybersecurity Implications of 5G Networks	.612	.058	.612	10.559	.000	.497	.726

a. Dependent Variable: Dependent Variable

Table 5 presents the coefficient estimates for the independent variables (Threats, Potential Vulnerabilities, and Cybersecurity Implications of 5G Networks) that jointly offer crucial insights into their influence on the dependent variable. The unstandardized coefficient (B) for Threats is 0.170, indicating that for every one-unit increase in Threats, the dependent variable increases by 0.170 units, assuming other factors are constant. The p-value is 0.003, which is below the 0.05 threshold, indicating that this effect is statistically significant. The coefficient for Potential Vulnerabilities is 0.193, suggesting that a one-unit increase in Potential

Vulnerabilities leads to a 0.193-unit increase in the dependent variable. The p-value is 0.001, confirming that this relationship is statistically significant. Referring to the cybersecurity implications of 5G Networks, the coefficient value is 0.612, indicating a substantial impact on the dependent variable. The standardised Beta of 0.612 reflects the strongest influence among the variables considered. The p-value is <0.001, highlighting the significance of this variable in predicting the dependent variable.

Thus, the findings of the regression analysis confirmed that all independent variables have a positive and statistically significant effect on the dependent variable, with the Cybersecurity Implications of 5G Networks showing the most substantial impact.

4.7. Interpretation of Findings

The information obtained from this study provides fundamental insights into the changes in cybersecurity in 5G networks, where, on the one hand, they are more secure compared to their previous versions, and on the other hand, they open new avenues for attackers. The data gathered from different sources presents a rather diverse and multifaceted picture of how 5G technology increases existing cybersecurity threats while also complicating their nature in various ways.

4.7.1. Cybersecurity Threats in 5G Networks

The study reveals that 5G networks result in greater exposure to attacks compared to 4G networks. Vulnerability rates were reported to have increased by as much as 50% compared to 4G networks, following the growth of the attack surface due to the increased number of products connected to the network, as well as the addition of new network functions such as network slicing and edge computing. This aligns with the current literature, which asserts that, due to 5G's superior features and the overall larger number of connected devices, there is a likelihood of security violations. Other works have reported that the attack surface is larger and the vulnerability rates are higher than those of conventional 6LoWPAN, due to a more extensive architectural framework and the inclusion of additional IoT devices.

This is due to the added complexity introduced by network slicing. The SDN is separated from the hardware, and the NFV is related to the software layer. As we can clearly see, these technologies are somewhat helpful for managing the network and optimising connections, but at the same time, they also open up new possibilities for attacks. Based on the results, although Network Slicing offers operational advantages by running multiple virtual networks on a single physical infrastructure, it also involves risks. A problem in one slice may cause problems for other slices, and this is not a common problem in earlier network architectures. This aligns with the understanding of market trends regarding cyber threats and vulnerabilities, which are related to the possibilities of software and virtualisation [42].

4.7.2. Preventable Cybersecurity Threats

The study also notes several risks that are exclusive to the 5G network. However, many of them are avoidable in terms of IoT device density and risks arising from network slicing. For example, the likelihood of using the targeted IoT devices for DDoS is real. This is in concordance with past studies, which show that with the sheer number of connected devices in 5G networks, such attacks hold a significant chance (Scalise et al., 2024). In addition, the introduction of new threat vectors due to network slicing, including cross-slice attacks, means that more security mechanisms must be implemented to secure 5G, considering that it is designed with a different architecture compared to previous generations of technologies.

4.7.3. Implications for National Security and Privacy

The results of these studies are quite disturbing, particularly in the context of a country's security and privacy. This study highlights that the increasing complexity of 5G networks poses a significant threat to national security. Given that every major city may face large-scale disruptions from cyberattacks on smart grids and transportation systems, which are becoming increasingly integrated, it is evident that there is a serious need for a robust security strategy in place to address these emerging threats. This is in line with the claims made in the literature regarding the susceptibility of critical infrastructures to cyberattacks enabled by enhanced network technologies, as noted by Carlo and Obergfaell. in 2024.

Privacy risks are also seen as another interesting factor that breaks into the scene. Based on the findings, one can conclude that 5G networks possess an excellent capacity for data collection, but also raise numerous privacy concerns. With the growth in the amount and specificity of information received from IoT devices and sensors, there is an increased risk of privacy infringement, as clients are unlikely to be aware of the extent of data being collected and used. This aligns with research revealing that 5G networks enable enhanced data handling, which consequently raises privacy concerns [43]. The strong signal that 5G networks provide for surveillance and monitoring exacerbates this problem, as the technology's capabilities can be used to infringe on individuals' right to privacy.

4.7.4. Contribution to Understanding Cybersecurity in 5G Networks

This study contributes to the literature on cybersecurity in 5G networks by providing real-life experiences and evidence of the risks associated with the use of this technology. The awareness of emergent threats and attack vectors, as well as the risks associated with incorporating new technological attributes and the potential for privacy violations, can prove beneficial for both academic and industrial communities. Based on the study's findings, it is concluded that there is an urgent need to introduce stronger guarantees and implement higher levels of privacy for the 5G system.

Therefore, the results of this research establish the necessity of implementing adequate security and privacy measures to address the emerging risks and hazards associated with 5G networks. With the further introduction of 5G technology, it is crucial to address these challenges to ensure that the country's security and the people's privacy are not compromised. Lasting solutions and future research on 5G technology, as well as its industry applicability, must address the mentioned risks and ensure that the advancement does not compromise security and privacy.

4.8. Theoretical Contributions

In this study, several theoretical contributions have emerged, expanding the knowledge of cybersecurity in 5G networks. These contributions refine current theories and provide fresh insight into how it is possible to mitigate 5G-specific difficulties.

One of the conceptual theoretical contributions of this study is the creation of an improved attack surface model for 5G networks. Previous modes focused mainly on protecting previous generations of network technology and do not quite fit for the complications offered by the 5G security. The new framework incorporates characteristics of networking, including network slicing and edge computing, as well as the widespread adoption of IoT. Furthermore, by incorporating these additional dimensions into the framework, a more comprehensive understanding of how the attack surface evolves in 5G scenarios is achieved. Furthermore, unlike existing approaches that focus solely on newly discovered vulnerabilities, this approach also provides a more detailed view of potential threats, which significantly enhances the theoretical contribution in the domain of network protection.

The study presents a new concept of the vulnerability model in line with network slicing, which is a core aspect of 5G. The model illustrates how weaknesses in one slice impact the others and how previous theoretical models did not fully address this issue. This model continues to add value to academic discussions by presenting a well-articulated framework for understanding and preventing cross-slice vulnerabilities. For this reason, the paper is quite helpful in filling a gap.

Additionally, the primary contribution of this study is a theoretical model for privacy in 5G networks. The framework aims to examine the consequences mentioned by 5G technology, which entails collecting large volumes of data, and how these capacities infringe on user privacy. Consequently, the present framework of data granularity and user consent, with the possibility of linking surveillance, provides a heightened view of privacy issues concerning 5G networks. It builds upon previous privacy models and designs with the features of 5G in handling and processing respective data, and enriches the discussion on privacy in the context of new access network technologies. Even though NIST, 3rd Generation Partnership Project (3GPP) and International Telecommunication Union (ITU) frameworks exist, there are a few gaps. NIST and ITU's recommendations are not legally binding. Countries can make independent decisions. 3GPP, on the other hand, standards are highly complex and offer numerous configuration options. This can lead to misconfigurations and inconsistent security postures across different operators. 3GPP provides the 'what' and not the 'how', providing inconsistent and insecure implementation [44].

4.9. Practical Implications

4.9.1. Recommendations for Industry Practitioners

4.9.1.1. Enhanced Security Protocols

5G security is an important issue, and industry practitioners should focus more on enhancing and deploying sophisticated mechanisms for the protection of new networks. This entails implementing protective measures for data in transit and data at rest, establishing robust authentication procedures, and integrating general security features into every network component with regular updates.

4.9.1.2. Strengthening Network Slicing Security

Since network slicing enables the creation of multiple logical networks on the same physical infrastructure, there is a need for the practitioner to come up with and implement security features that guarantee that the slices are isolated and protected from each other. This is done to control and prevent any form of cross-slice risk, and this requires setting up strict access controls and monitoring to establish any risk.

4.9.2. Recommendations for Policymakers

4.9.2.1. Regulatory Framework

The existing known weaknesses and threats in smart devices, pose the need to offer enhanced protection for the IoT devices that will be working using the 5G link. This current talent recommendation defines that practitioners should always practice Secure Codes and Systems Security Checks and ensure that IoT devices are SEC-complaint.

4.9.2.2. Promoting Collaborations

It is recommended that Intelligence-Driven Authentication (IDA) works with the government ministries, industries and academic institutions to exchange information on new threats and methods that are most effective. In fostering strategies and technologies towards the protection of 5G networks this collaborative methodology will be of great help.

Figure 4.2 summarises the 5G threats and how these threats could be mitigated.

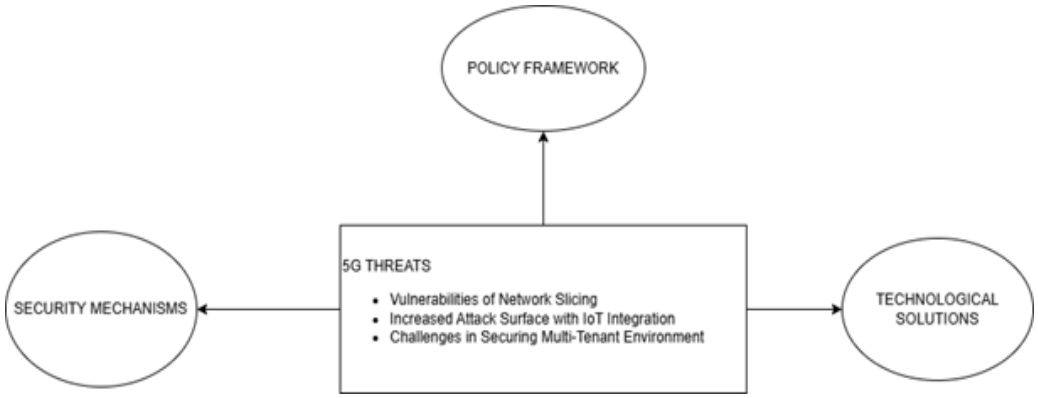

Figure 2. Mitigating 5G threats

5. CONCLUSION

Summary of Key Findings

Network slicing in 5G is efficient in the management of resources and has facilitated the differentiation of services, however, the issue poses significant security threats. That is because every slice can become a potential threat if they are not isolated and protected. These findings suggest that enhanced security is required to counter security challenges in the 5G architecture.

Key findings include:

Vulnerability of Network Slicing: The integration of 5G technology with IoT devices increases the exposure to attacks at a faster pace. Many IoT devices come with few security features, which can easily be manipulated to conduct an attack that compromises the integrity of the network. This highlights the need for effective security measures and proper management of IoT devices operating in a 5G environment.

Increased Attack Surface with IoT Integration: Another security concern related to 5G networks is that multiple operators often rely on shared infrastructure. Hypertext Transfer Protocol (HTTP)- based services installation must guarantee the absence of breaches in client isolation among different tenants.

Challenges in Securing Multi-Tenant Environments: One can conclude that the security of 5G is not only about technologies, but also about regulations. The work emphasises the need for detailed research on security and privacy policies for 5G networks, as they differ from those of current networks.

CONCLUSION

It has been established that the protection of 5G networks is crucial due to the disruptions they will bring to various industries. The study reveals that 5G indeed presents significant opportunities; however, these new opportunities also introduce new threats that need to be mitigated. The consequences in the areas of national security and privacy can be imagined, as every leakage or violation has immediate consequences for communities. End-user devices are considered the most vulnerable component in the 5G network architecture, since these devices have different security levels.

In this respect, the research contributes value to the existing literature on threats to the 5G connectivity infrastructure and proposes specific solutions for addressing these issues. The research results suggest that a combination of technological solutions, security mechanisms, and policies is necessary to develop efficient security models. This paradigm is necessary for building robust 5G networks that can respond to these evolving threat landscapes.

REFERENCES

[1] P. Anand, A. K. Tripathi, P. K. Sharma, and I. Gupta, "IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges," IEEE Access, vol. 8, pp. 168825-168853, 2020, doi: 10.1109/ACCESS.2020.3022342.

[2] J. Cook, S. U. Rehman, and M. A. Khan, "Security and privacy for low power IoT devices on 5G and beyond networks: Challenges and future directions," IEEE Access, vol. 11, pp. 39295–39317, 2023.

[3] R. R. Asaad and V. A. Saeed, "A cyber security threats, vulnerability, challenges and proposed solution," Applied Computing Journal, pp. 227–244, 2022. [Online]. Available: https://doi.org/10.52098/acj.202260

[4] J. A. Khan and M. M. Chowdhury, "Security analysis of 5G network," in Proc. EIT, 2021. [Online]. Available: https://doi.org/10.1109/EIT51626.2021.9491923

[5] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, "5G Security Challenges and Solutions: A Review by OSI Layers," IEEE Access, vol. 9, pp. 122426-122445, 2021, doi.org/10.1109/ACCESS.2021.3105396.

[6] M. Jinsong and M. Yamin, "5G network and security," in Proc. INDIACom, 2020. [Online]. Available: https://doi.org/10.23919/INDIACom49435.2020.9083731

[7] K. Ramezanpour, J. Jagannath, and A. Jagannath, "Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective," Computer Networks, vol. 221, p. 109515, 2023. [Online]. Available: https://doi.org/10.1016/j.comnet.2022.109515

[8] U. Gorrepati, P. Zavarsky, and R. Ruhl, "Privacy protection in LTE and 5G networks," in Proc. ICSCCC, 2021. [Online]. Available: https://doi.org/10.1109/ICSCCC51823.2021.9478109

[9] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, M. Ylianttila, "The roadmap to 6G security and privacy," IEEE Open Journal of the Communications Society, vol. 2, pp. 1094-1122, 2021, doi.org/10.1109/OJCOMS.2021.3078081

[10] L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang, and C. S. Hong, "Edge-computing-enabled smart cities: A comprehensive survey," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10200–10232, Oct. 2020, doi: 10.1109/JIOT.2020.2987070.

[11] R. Dangi, G. Kaddoum, S. Garg, G. P. J. N. K. K. G. and D. N. K. , "ML-based 5G network slicing security: A comprehensive survey," Future Internet, vol. 14, no. 4, p. 116, Apr. 2022, doi: 10.3390/fi14040116.

[12] L. Bonati, M. Polese, S. D'Oro, S. Basagni, and T. Melodia, "Open, programmable, and virtualized 5G networks: State-of-the-art and the road ahead," Computer Networks, vol. 182, p. 107516, Dec. 2020, doi: 10.1016/j.comnet.2020.107516.

[13] V. -L. Wong and H. D. Schotten, "A Survey on 6G Security: Technology, Challenges, and Future Directions," in IEEE Open Journal of the Communications Society, vol. 3, pp. 2310-2332, 2022, doi: 10.1109/OJCOMS.2022.3223377.

[14] A. S. George, "5G-enabled digital transformation: Mapping the landscape of possibilities and problems," Partners Universal Innovative Research Publication, vol. 2, no. 3, pp. 01–37, 2024. [Online]. Available: https://doi.org/10.5281/zenodo.11583365

[15] P. Zhou, X. Wang, K. Wang, Y. Zhang, and S. Mao, "Communication-Efficient Offloading for Mobile-Edge Computing in 5G Heterogeneous Networks," IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10237–10247, Jul. 1, 2021, doi: 10.1109/JIOT.2020.3028207.

[16] M. Umaselvi, E. Menaka, V. Chandrasekar, and D. Saravanapriya, "5G and IoT networks risk management," in Secure Communication for 5G and IoT Networks. Springer, 2022, pp. 47–71.

[17] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," Telecommunication Systems, vol. 73, no. 1, pp. 3–25, 2020.

[18] M. Shafiq, H. Tian, A. K. Bashir, X. Du, and M. Guizani, "The Rise of 'Internet of Things': Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks," Wireless Communications and Mobile Computing, vol. 2022, p. 8669348, 2022, doi: 10.1155/2022/8669348.

[19] J. P. Mohan, N. Sugunaraj, and P. Ranganathan, "Cyber security threats for 5G networks," in 2022 IEEE International Conference on Electro Information Technology (eIT), 2022, pp. 446–454.

[20] D. Mourtzis, J. Angelopoulos, and N. Panopoulos, "Smart manufacturing and tactile internet based on 5G in industry 4.0: Challenges, applications and new trends," Electronics, vol. 10, no. 24, p. 3175, 2021.

[21] L. F. Ribas Monteiro, Y. R. Rodrigues, and A. C. Zambroni de Souza, "Cybersecurity in cyber–physical power systems," Energies, vol. 16, no. 12, p. 4556, 2023.

[22] G. Paul, J. Irvine, R. Johnson, and A. Craig, "The security of 5G: Written evidence submitted by the University of Strathclyde," University of Strathclyde, Glasgow, UK, Tech. Rep., 2020.

[23] M. P. Jones and E. L. McCaslin, "Special operations in a 5G world: Can we still hide in the shadows?" M.S. thesis, Naval Postgraduate School, Monterey, CA, USA, 2020.

[24] M. Anisetti, C. Ardagna1, M. Cremonini1, E. Damiani1, J. Sessa1, and L. Costa, "Security threat landscape," White Paper Security Threats, 2020.

[25] J. Ortiz, R. Sanchez-Iborra, M.-V. Lopez, J. J. Alcaraz, D. Garcia-Roger, and J. F. Monserrat, "Enforcing GDPR Regulation to Vehicular 5G Communications Using Edge Virtual Counterparts," in 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 2020, pp. 121-126, doi: 10.1109/5GWF49715.2020.9221332.

[26] H. Jahankhani, S. Kendzierskyj, and O. Hussien, "Approaches and methods for regulation of security risks in 5G and 6G," in Wireless Networks: Cyber Security Threats and Countermeasures. Cham: Springer, 2023, pp. 43–70.

[27] D. P. Möller, "NIST cybersecurity framework and MITRE cybersecurity criteria," in Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. Cham: Springer, 2023, pp. 231–271.
[28] V. Rajasekar, J. Premalatha, and M. Saracevic, "Cybersecurity in 5G and IoT networks," in Secure Communication for 5G and IoT Networks. Springer, 2022, pp. 29–46.
[29] M. Robles-Carrillo, "European Union policy on 5G: Context, scope and limits," Telecommunications Policy, vol. 45, no. 8, p. 102216, 2021.
[30] B. Patel, V. K. Yarlagadda, N. Dhameliya, K. Mullangi, and S. C. R. Vennapusa, "Advancements in 5G Technology: Enhancing Connectivity and Performance in Communication Engineering," Engineering International, vol. 10, no. 2, pp. 117–130, 2022, doi: 10.18034/ei.v10i2.715.
[31] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5G in the internet of things era: An overview on security and privacy challenges," Computer Networks, vol. 179, p. 107345, 2020.
[32] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 196–248, 2019.
[33] M. Koivisto, A. Hakkarainen, M. Costa, P. Kela, K. Leppänen, and M. Valkama, "High-efficiency device positioning and location-aware communications in dense 5G networks," IEEE Communications Magazine, vol. 55, no. 8, pp. 188-195, Aug. 2017, doi: 10.1109/MCOM.2017.1600655.
[34] M. Pugh, "Privacy? What privacy?: Reforming the state secrets privilege to protect individual privacy rights from expansive government surveillance," Belmont Law Review, vol. 9, p. 265, 2021.
[35] S. Ribeiro-Navarrete, J. R. Saura, and D. Palacios-Marqués, "Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy," Technological Forecasting and Social Change, vol. 167, p. 120681, 2021.
[36] B. Patel, V. K. Yarlagadda, N. Dhameliya, K. Mullangi, and S. C. R. Vennapusa, "Advancements in 5G Technology: Enhancing Connectivity and Performance in Communication Engineering," Engineering International, vol. 10, no. 2, pp. 117–130, 2022, doi: 10.18034/ei.v10i2.715.
[37] V. Rusinova, "Privacy and the legalisation of mass surveillance: in search of a second wind for international human rights law," The International Journal of Human Rights, vol. 26, no. 4, pp. 740–756, 2022.
[38] M. Shehab, I. Kassem, A. A. Kutty, M. Kucukvar, N. Onat, and T. Khattab, "5G Networks Towards Smart and Sustainable Cities: A Review of Recent Developments, Applications and Future Perspectives," IEEE Access, vol. 9, pp. 2987-3006, 2021, doi: 10.1109/ACCESS.2021.3139436.
[39] D. A. Tamburri, "Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation," Information Systems, vol. 91, p. 101469, 2020.
[40] M. K. Banafaa, O. Pepeoglu, I. Shayea, A. Alhammadi, Z. A. Shamsan, M. A. Razaz, M. Alsagabi, and S. Al-Sowayan, "A Comprehensive Survey on 5G-and-Beyond Networks With UAVs: Applications, Emerging Technologies, Regulatory Aspects, Research Trends and Challenges," IEEE Access, vol. 12, pp. 7786-7826, 2024, doi: 10.1109/ACCESS.2024.3386393
[41] K. Kaska, H. Beckvard, and T. Minárik, "Huawei, 5G and China as a security threat," NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, Estonia, Tech. Rep., 2019.
[42] T. Li, J. Wang, Z. Cheng, and J. Chen, "Fifth-Generation Mobile Communication Technology Network Attack Defense Based on Software-Defined Network Technology in Power Internet of Things," Frontiers in Energy Research, vol. 10, p. 950611, 2022, doi: 10.3389/fenrg.2022.950611.
[43] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," Digital Communications and Networks, vol. 6, no. 3, pp. 281-291, Aug. 2020, doi: 10.1016/j.dcan.2020.07.003.
[44] Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2019). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials*, *22*(1), 196-248.