SECURITY OF 5G NETWORKS – A COMPLEX ISSUE –

Colonel Valentin-Gabriel GEORGESCU

Radio Frequency Management Agency, Defence Staff

DOI: 10.55535/RMT.2022.1.08

The history of mobile telecommunications is not very old. It has been a bit more than 40 years since the first generation of cellular communications (1G) was launched on the market, offering the possibility of making and receiving phone calls while on the go, even accompanied by a number of technological limitations, including network and system security. Each new generation of technologies that followed this stage brought significant diversification and improvements in services. Today, there is more and more talk of the fifth generation of mobile communications technologies (5G). The security aspects of 5G networks are a hot topic worldwide, both among major state and non-state actors. This article highlights the main characteristics of 5G technologies and why security of 5G networks is essential and complex.

Keywords: mobile communications; 5G networks; network architecture; 5G security; 5G threat landscape;

"5G is a big step forward on several fronts, but won't actually provide a full security upgrade until we see pure 5G networks with no legacy tech – so not for another 10 years or more."

Karsten Nohl,
founder of Security Research Labs GmbH (SRLabs)

RESEARCH METHODOLOGY

The aim of this article is to analyse the threats and risks of 5G-based networks as currently identified, in order to highlight whether the concerns about the security aspects associated with 5G, which have been released into the public space, are really supported or are mere speculations hiding issues of a completely different nature (e.g., interests in banning Chinese manufacturers/suppliers of 5G equipment and infrastructure from the market).

The current 5G services in the portfolio of Romanian communication operators are mainly based on existing 4G/LTE infrastructures.

It would not be appropriate to address the security of 5G networks without a study of previous generations and the specific aspects of each of them at the time of their launch. To this end, the longitudinal method, combined with the comparative analysis method, have examined the characteristics of each generation and the main differences between them.

The comparative analysis method and the descriptive method have been used to present the communication networks based on 5G technologies and the types of network architectures, given that the current 5G services in the portfolio of Romanian communication operators are mainly based on existing 4G/LTE infrastructures.

In order to identify and highlight the security aspects of 5G networks, i.e., the threats and risks associated with them, the comparative analysis method and the bibliographic research method have been combined, in particular the study of documents developed at EU level on cybersecurity of 5G networks, the EU toolbox on risk mitigating measures and the report on the EU coordinated risk

assessment on the cybersecurity of 5G networks. The bibliography studied has also included the United States' national strategy to secure 5G, as a strategic partner of Romania and the European Union, for the analysis of the United States; vision on the security aspects of new 5G technologies.

FROM 1G TO 5G – A HISTORY OF 40 YEARS

The telecommunications industry is undoubtedly one of the areas that has known a significant and high-impact progress in a relatively short period of time. In the early 1980s the first generation of mobile communications technologies (1G) was launched. Although a limited technology in terms of the offered services (analogue voice communications only), it paved the way for the follow-on developments. It did not have the power to replace traditional fixed telephony, but offered the possibility to make phone calls while being in motion outside the buildings, although the size of equipment used was quite large (in fact not a problem at that time, since there were no other similar terminals to compare with).

In the early 1980s the first generation of mobile communications technologies (1G) was launched. Although a limited technology in terms of the offered services (analogue voice communications only), it paved the way for the follow-on developments.

About 10 years later, a second generation of mobile communications (2G) technologies, also known as GSM (Global System for Mobile Communications), appeared on the market, offering superior voice quality by switching from analogue to digital, and also providing a new service, known as SMS (Short Message Service). They are still in use today. The first call in GSM technology was made in the Finnish network Radiolinja, in 1991[1].

Continuing the series of developments in the field of mobile communications, the 3rd generation (3G) appeared in 2000, adding to the already existing services the possibility of data and (even at low speed) internet access. That was the moment opening the way to future high-speed networks and smartphones. Unlike previous technologies, 3G have had a significant lifecycle and are still used today. They were followed in 2009 by the fourth generation (4G LTE, and 4G+ later on),

[1] On 1 July 1991, the world's first GSM call on a commercial network was made between Finland's former prime minister Harri Holkeri and vice mayor of the city of Tampere Kaarina Suonio, https://www.fonearena.com, retrieved on 8 May 2021.

when speed and stability of the connections became a constant in the needs of any user of smart devices. In retrospect, it can be seen that each generation of technologies has meant a *"revolutionary"* moment in the evolution of mobile communications at the time when they were launched on the market.

But a *"really true"* revolution is announced today by the fifth generation of mobile communications (5G), which goes beyond the individual communication needs, moving towards the connectivity of a wide variety of smart devices and concepts such as the Internet of Things (IoT), Artificial Intelligence (AI), Virtual/Augmented Reality (VR/AR) or Big Data *(figure no. 1)*.

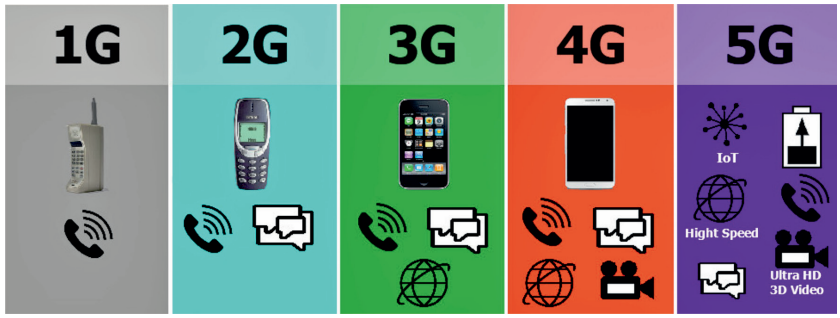

Figure no. 1: The evolution of mobile communications (5G_Technology_the_Fourth_Gen_Technology, 2020)

A "really true" revolution is announced today by the fifth generation of mobile communications (5G), which goes beyond the individual communication needs, moving towards the connectivity of a wide variety of smart devices and concepts such as the Internet of Things (IoT), Artificial Intelligence (AI), Virtual/Augmented Reality (VR/AR) or Big Data.

Consequently, the telecommunications industry will join other industries and sectors such as automotive, agriculture, energy and utilities, emergency services, health, security, education, smart homes and cities, that will benefit from the advantages of the new generation of technologies of mobile communications.

5G NETWORKS IN A NUTSHELL

The mobile communications networks based on 5G technologies can be briefly characterised by a variety of new features, such as: instant connectivity (1 million devices per km^2), huge speeds (over 10 Gbps), extremely low latency (1 millisecond), scalability (possibility to extend the network), energy efficiency (hardware components switch off when not in active use).

The standards have been developed by the *3rd Generation Partnership Project* (3GPP)[2], and named *"5G NR"* (New Radio). They have been continuously developed under *"releases"*. For example, the first standard started in 2018 with Release 15. It was updated and followed by Release 16 that was published at the end of 2019. Release 17 completion date was initially planned for 2021, but because of COVID-19 global pandemic, the 3GPP postponed it for 2022, assuming the meetings in-person will be possible again.

Basically, a mobile communications network comprises two main components: *the radio access network (RAN) and the core network (CN)*. The role of the *radio access network* is to connect mobile users to the main core network; it consists of physical infrastructure elements, such as towers/pillars/masts, small network cells, connection devices and dedicated systems installed inside the buildings (indoor equipment).

A requirement of 5G networks is that, in order to be able to provide specific features and services according to the standards (e.g., support of large number of users, high speeds and data capacities), as well as an adequate coverage, a sufficient amount radio spectrum distributed in several frequency bands is necessary.

A requirement of 5G networks is that, in order to be able to provide specific features and services according to the standards (e.g., support of large number of users, high speeds and data capacities), as well as an adequate coverage, a sufficient amount radio spectrum distributed in several frequency bands is necessary. While frequency bands below 1 GHz are suitable for coverage, including indoor or rural areas coverage, the millimetre waves at 26 GHz and above will be able to provide large data transport capacities, but over short distances, since the short millimetre waves have limited propagation through obstacles. This explains the presence of small network cells (femtocells, picocells, microcells) within the architecture of future 5G networks. It has to be mentioned that this higher part of radio spectrum has not been used in the networks based on the previous generations of technologies.

The antenna is one of the key components of a radio access network, and play a major role within the small cells. The 5G networks will use *"massive MIMO"* (Multiple-Input and Multiple-Output) antennas, consisting of hundreds of elements, able to transmit and receive data from a large number of users connected simultaneously to the network.

[2] The 3rd Generation Partnership Project (3GPP) unites 7 telecommunications standard development organisations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as *"Organisational Partners"* and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies, https://www.3gpp.org/about-3gpp/about-3gpp, retrieved on 10 May 2021.

The core network must support devices and applications with different traffic profiles. It ensures the management of mobile connections, respectively voice transfers, data, internet. It is designed to manage network functions such as virtualisation and network slicing, with cloud integration and in internet-based services, thus minimising latency/response time. Software applications and software-defined networking are key to ensure the flexibility for an efficient use of the 5G network.

One of the 5G characteristics is that 5G Radio Access Network can connect both to 5G and 4G (LTE) Core Networks, thus defining the type of network architecture *(figure no. 2)*.

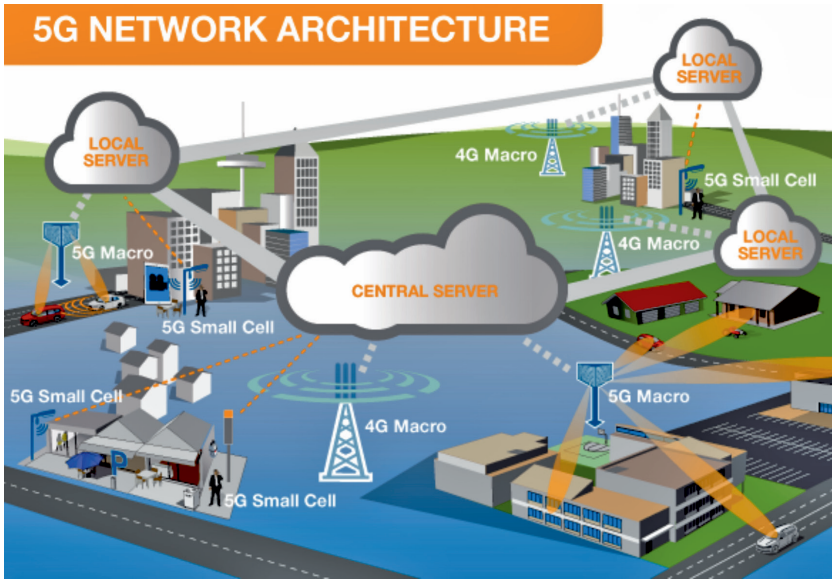

Figure no. 2: 5G and 4G working together (5G Explained – How 5G Works)

The core network must support devices and applications with different traffic profiles. It ensures the management of mobile connections, respectively voice transfers, data, internet. It is designed to manage network functions such as virtualisation and network slicing, with cloud integration and in internet-based services, thus minimising latency/response time.

The case of 5G RAN connected to 4G (LTE) CN is known as *"non-standalone architecture"*. It allows mobile network operators to provide 5G services without replacing the existing network, but limited to high-speed connectivity and lower latency to those users having 5G-enabled devices. The integration of 5G with existing 4G networks is what the majority of mobile network operators offering *"5G"* has done or will do as a first step of 5G deployment, since the option minimises costs on infrastructure.

The case of 5G RAN connected to 5G CN is known as *"standalone architecture"* and requires a new fully virtualised network. It is a cloud-based solution, separated from any existing 4G network, and suitable for those mobile operators who plan to deliver new enterprise services (e.g., smart cities) and vertical market solutions. This type of architecture will actually be the one supporting the car-to-car communications/self-driving cars, remote imagery and surgery, real-time monitoring and control etc.

SECURITY ASPECTS OF 5G NETWORKS – THE THREAT LANDSCAPE

The network architectures of previous *"G"s* have not presented significant issues of concern from a security perspective, therefore the question *"why things look different in the case of 5G?"* might be justified.

The 2G and 3G networks have been basically focused on people connectivity through voice and text messages, while 4G has added high-speed internet connectivity to the previous services.

The 2G and 3G networks have been basically focused on people connectivity through voice and text messages, while 4G has added high-speed internet connectivity to the previous services. As it has already been shown, 5G networks comes now with the feature of mass connectivity: connectivity of things to things, services, people, …to everything. It means designing new infrastructures able to use the network functions virtualisation (NFV) for new services, the software defined networking (SDN) for adaptability, and cloud-native architectures for the scalability of resources. The real 5G networks will be based on a standalone architecture and will use a producer-services model instead of fixed functional entities.

The security of 5G networks has multiple dimensions. There are three main types of risk that make 5G a security complex issue.

A *first type of risk* is represented by the larger attack surface and attack opportunities *(figure no. 3)*. Considering that the new architecture of 5G networks (mainly the standalone networks) is different from the previous ones, new risks would target a larger physical surface, especially on the RAN. It happens due to the large number of (poorly secured) IoT devices connected to the 5G network, new endpoints, frequent software patching, therefore more opportunities for the hackers and various ways to penetrate the networks. The less secured

IoT devices, especially the cheapest ones, could introduce weak points into home networks, thus making possible ransomware attacks, sabotage, theft of data etc. Or they could be introduced in botnets and distribute malware across the networks, launch DDoS (Distributed Denial of Service) attacks to shutdown websites, or get fraudulent data and information (credit cards, passwords etc.) by tricking people through *phishing* attacks[3].

The widespread use of network configuration software will be able to open up opportunities to attack networks and take control of them by malicious state or non-state actors.

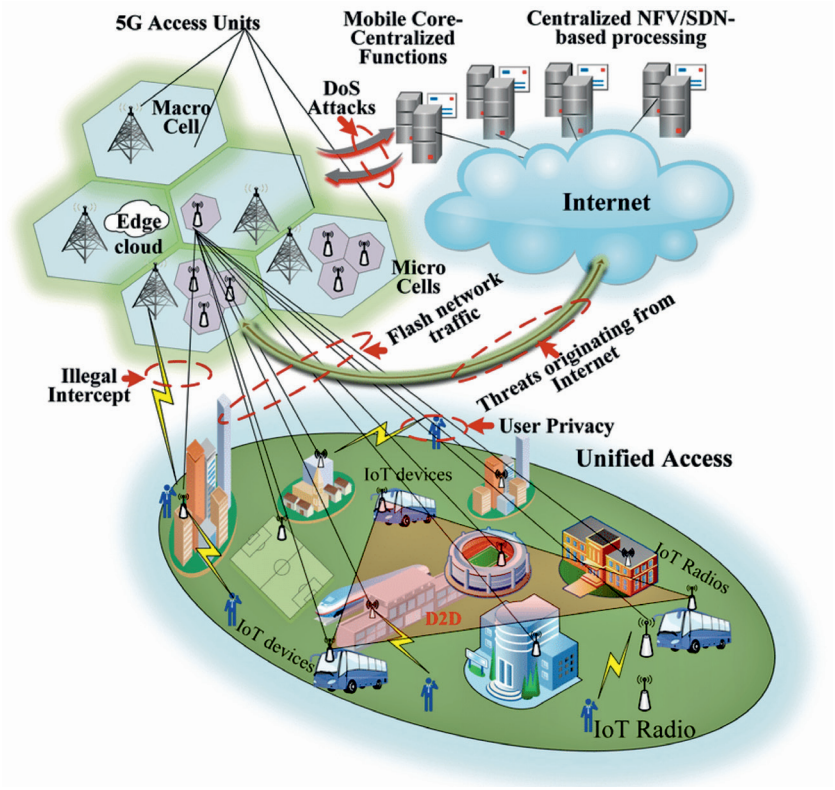

Figure no. 3: Threats in 5G networks
(5G Security: Analysis of Threats and Solutions, 2017)

The widespread use of network configuration software will be able to open up opportunities to attack networks and take control of them by malicious state or non-state actors.

[3] *Phishing* attacks are a means to persuade potential victims into divulging sensitive information such as credentials, or bank and credit card details. They involve a combination of social engineering and deception, https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing, retrieved on 10 May 2021.

Another sensitive aspect is related to the 5G antenna. In high frequency spectrum, the propagation of microwaves is on short distance, allowing a higher data capacity. That means comparing with 4G, on the same geographic area there will be a larger number of 5G antennae. Through radio jamming the mobile user access to network services in a specific area could be easily blocked. *Spoofing*[4] and *sniffing*[5] are other potential threats that should worry.

In March 2020, the US Administration issued the *"National Strategy to Secure 5G of the United States of America",* as President Trump's vision for America "*to lead the development, deployment, and management of secure and reliable 5G communications infrastructure worldwide*" together with US allied and partner nations (National Strategy to Secure 5G of the USA, 2020). According to the strategy, *"5G infrastructure will be an attractive target for criminals and foreign adversaries due to the large volume of data it transmits and processes as well as the support that 5G will provide to critical infrastructure"* (Ib., p. 1)

In March 2020, the US Administration issued the "National Strategy to Secure 5G of the United States of America", as President Trump's vision for America "to lead the development, deployment, and management of secure and reliable 5G communications infrastructure worldwide" together with US allied and partner nations.

The analysis of the US strategy reveals two major types of threats to 5G infrastructure:

1. theft of data transited through 5G networks, for the purpose of obtaining financial gains, gathering information and monitoring;
2. the interruption of public and private services based on or causing malfunctions in communications infrastructures.

Therefore, 5G infrastructures will need to ensure an adequate level of information security and address the risks to critical infrastructure, public safety and health, and economic and national security.

The concerns in respect with the 5G security are not related to the White House only. The European Commission pays an utmost attention to the security aspects of the future 5G networks, recognising that this new generation of technologies will play a key role to the development of the Digital Single Market within the EU.

---

[4] *Spoofing* is the act of disguising a communication from an unknown source as being from a known, trusted source, https://www.forcepoint.com/cyber-edu/spoofing, retrieved on 10 May 2021.

[5] *Sniffing* is a process of monitoring and capturing all data packets passing through given network, https://www.greycampus.com/opencampus/ethical-hacking/sniffing-and-its-types, retrieved on 10 May 2021.

As a result of the preliminary study on 5G security, in November 2019 the European Union Cybersecurity Agency (ENISA) published a first edition of the *"ENISA Threat Landscape for 5G Networks"* Report, as an overview of the security challenges in 5G networks. It was reviewed by ENISA, NIS Cooperation Group and European Commission, and updated in December 2020. The document presents an overview on 5G threats as result of the comprehensive studies based on public information available, coming from the 5G standardisation groups (3GPP, ETSI etc.) and 5G stakeholders (mobile network operators, vendors, national and international bodies, institutes etc.).

According to the Commission Recommendation on Cybersecurity of 5G networks, "*the dependence of many critical services on 5G networks would make the consequences of systemic and widespread disruption particularly serious. As a result, ensuring the cybersecurity of 5G networks is an issue of strategic importance for the Union, at a time when cyber-attacks are on the rise and more sophisticated than ever*" (Commission Recommendation, 2019, p. 1).

The supply chain and its complexity represent a *second type of risk*. On the one hand, it refers to the location of subcontractors – they may be located in several countries, so that the identification of the country of origin of a component is quite difficult (if not impossible) to achieve. In addition, the number of entry points in 5G supply chain could allow malicious threat actors to access the supply chain directly, or by compromising vendors. For example, the EU coordinated risk assessment report on cybersecurity states that *"While a threat actor's direct access to or influence on the telecom supply chain may significantly facilitate its exploitation for malicious actions and make the impact of such actions significantly more severe, it should also be noted that actors with a high level of intent and capabilities, such as State actor, would seek to exploit vulnerabilities at any stage of the product lifecycle provided by any supplier"* (NIS Cooperation Group, 2019, p. 22).

The supply chain and its complexity represent a second type of risk. On the one hand, it refers to the location of subcontractors – they may be located in several countries, so that the identification of the country of origin of a component is quite difficult (if not impossible) to achieve. In addition, the number of entry points in 5G supply chain could allow malicious threat actors to access the supply chain directly, or by compromising vendors.

On the other hand, the supply chain refers to the component quality control – at the beginning of a component's lifecycle, the quality control is low, while the impact of possible sabotage actions in the supply chain is high. In order to mitigate the risk, it is crucial

that the primary vendor and its companies should have an effective quality control process able to identify any vulnerability on security (mainly in software products). The trust in employees and common security measures to protect any illegal access to the vendor's production activity are also essential.

The software used in 5G networks contains millions of lines of code written in different locations, many errors in turn generating vulnerabilities. The EU coordinated risk assessment report concluded that unidentified vulnerabilities are *"a leading cause of potentially undetected, long-lasting intrusions into networks"* (Ib., p. 26). Regular software updates or patches are good occasions for insertion of backdoors or new vulnerabilities in the source code, since 5G networks will heavily rely on it.

The software used in 5G networks contains millions of lines of code written in different locations, many errors in turn generating vulnerabilities. The EU coordinated risk assessment report concluded that unidentified vulnerabilities are "a leading cause of potentially undetected, long-lasting intrusions into networks".

Even though most of the nations banned Huawei as a 5G vendor, this will not prevent the Chinese companies to influence the future supply chains. For example, Cisco, Nokia and Ericsson have factories in China; in addition, Nokia and Ericsson operate their Chinese subsidiaries mainly through joint ventures with local firms, although Nokia has moved part of its production out of China because of a possible ban, and also to demonstrate alignment with the security measures, especially the US ones.

The *third type of risk* refers to a limited diversity of 5G vendors. Nowadays, the 5G vendors worldwide able to provide 5G networks are not too many. The *"traditional"* providers of RAN equipment are Nokia and Ericsson in Europe and Huawei and ZTE in China, so the choices are not too diverse; this is another challenge for 5G because of the risk of systemic failures or hostile exploitation of the networks.

On the other hand, apart from a limited vendor competition, banning the Chinese companies and reliance on just one or two vendors (e.g., Nokia and Ericsson, in case the Chinese vendors are banned) would reduce competition and open new risks in case of problems. It is the same situation with the Chinese operators relying exclusively on Huawei and ZTE in case of banning the European manufacturers in return of international sanctions.

The controversial technological war between the USA and China on 5G has also repercussions at European level, its dimensions

being both political and economic. Politically, it is worth mentioning the signing, on 13 August 2018, by US President Donald Trump of a document (National Defense Authorization Act, 2018) by which one of the provisions on telecommunications equipment and services refers to the ban on the US government and their contractors to use equipment and technology produced by Huawei and ZTE or its subsidiaries or affiliates.

The intention to exclude the two major Chinese telecommunications equipment and services companies was extended by the USA and its allies worldwide aiming to remove Huawei from any critical infrastructure tender, based on the argument that this company presents high security risks.

CONCLUSIONS

From the aspects presented, it can be concluded that most of the devices in 5G networks will not be mobile phones, but IoT devices. This is one of the main reasons of concern with respect to the level of security and protection that have to be offered by the future 5G networks.

The transition and deployment of 5G networks will be gradual. Although more and more mobile operators have introduced 5G in their commercial offers, the services provided are based on the current 4G network infrastructures, and are not *"pure 5G"* ecosystems yet. Because of the COVID-19 pandemic as well as of the lack of national legislation on 5G networks' security, spectrum auctions have been postponed and the 5G deployment process delayed.

Analysing the US and EU statements, it can be noticed that potential vulnerabilities of the new 5G networks are common worries. 5G networks can offer great flexibility through multiple configuration possibilities. At the same time, the network configuration may be accompanied by errors, opening door to new vulnerabilities.

Considering the threat landscape and the large variety of potential risks, it seems the goal of getting full security of 5G networks is unreachable, however measures for 5G mitigation of risks will have to be adopted. The new networks will be included in the national critical infrastructures, so any disruption could have a bad impact on national

The transition and deployment of 5G networks will be gradual. Although more and more mobile operators have introduced 5G in their commercial offers, the services provided are based on the current 4G network infrastructures, and are not "pure 5G" ecosystems yet. Because of the COVID-19 pandemic as well as of the lack of national legislation on 5G networks' security, spectrum auctions have been postponed and the 5G deployment process delayed.

security. Consequently, mitigating 5G risks and keeping the security of 5G networks under (state) control will be essential, no matter the controversies on vendors are.

It can be easily anticipated that once 5G will be deployed and operational, people and organisations will become dependent on the new services offered, for running their business and living the daily life. It happened the same with each of the previous generations…

BIBLIOGRAPHY:

1. Ahmad, I., Kumar, T., Liyanage, M., Gurtov, A. (2017). *5G Security: Analysis of Threats and Solutions*, https://www.researchgate.net/figure/5G-network-and-the-threat-landscape_fig1_318223878, retrieved on 17 September 2021.
2. Khan, S. (2020). *The Backbone of 5G Networks: A Guide to Small Cell Technology*, Telit.
3. Lake, J. (2020). *5G and Security: How Does 5G Work and What Are the Risks?* Comparitech.
4. Sathyanarayan, S. (2020). *Standalone (SA) and Non-Standalone (NSA) 5G Architectures: the Various Paths to 5G Revenues and Profitability*. Affirmed Networks.
5. Sullivan, J., Lucas, R. (2020). *5G Cyber Security. A Risk Management Approach*. Royal United Services Institute for Defence and Security Studies.
6. Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks C(2019) 2335 final (2019). *Official Journal of the European Union*.
7. *EU Coordinated Risk Assessment on the Cyber Security of 5G Networks* (October 2019). NIS Cooperation Group.
8. *The Federal Acquisition Supply Chain Security Act* S. 3085/2018.
9. *National Strategy to Secure 5G of the United States of America* (2020).
10. NIS Cooperation Group (2020). *Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures*. *CG Publication*, no. 1.
11. NIS Cooperation Group (2019). *EU Coordinated Risk Assessment of the Cybersecurity of 5G Network*s, Report.
12. Public Law No: 115-232 (August 2018). National Defense Authorization Act, https://www.congress.gov, retrieved on 21 July 2021.
13. *5G Explained – How 5G Works*, http://www.emfexplained.info, retrieved on 21 July 2021.
14. *5G Security Issues* (2019). GSMA.

15. 5G_Technology_The_Fourth_Gen_Technology (2020), http://hindustannext.com/5g_technology_the_fourth_gen_technology/, retrieved on 21 July 2021.
16. https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf, retrieved on 21 July 2021.
17. https://www.hsdl.org/?view&did=835776, retrieved on 21 July 2021.
18. https://www.researchgate.net/figure/5G-network-and-the-threat-landscape_fig1_318223878, retrieved on 21 July 2021.