THE IMPACT OF 5G TECHNOLOGY ON CYBERSECURITY ENVIRONMENT

Benedictos Iorga

Spiru Haret University, Faculty of Engineering and Computer Science,
Bucharest, Romania
E-mail: iorga.ben.mi@spiruharet.ro; iorgaben@yahoo.com

Abstract:

The sustained evolution in the field of information technology, the ascending social necessity for permanent digital connection and worldwide accelerated information consumption determined the rapid development and operationalization need of a 5th generation digital communication technology, generically named 5G. The new technology which promises to revolutionize all digital technology, communications, data transmission and Internet access signify, will generate, in addition to immeasurable benefits and advantages (economic, industrial, technical, social, cultural), a profound impact on global cybersecurity.

I hereby set out to briefly determine and analyze the impact of the 5G communication technology implementation on current cyber environment, starting from the technical transformations induced by the new technology and using the current patterns of known, tested and documented cyber threats in the global network environment.

While apparently 5G technology promises to ensure a high level of security within the cellular communication environment by implementing the logical network segmentation (Network Slicing), adopting new dynamic end-to-end encryption tools (IMISI encryption) and operationalizing software-defined networks (SDN), I consider there is a high probability that the current cyber threats will benefit from a new developing environment and expansion at a global, insufficiently anticipated and known level.

Keywords: technology, 5G, cyber risk, internet, security threat, cyber vulnerability.

Introduction

It is for the first time in the modern history of the states when a mobile communications technology has determined the rethinking of strategic relations between the greatest technological powers, respectively the USA and CHINA, with chain effects on global security. In such a context, the question naturally arises: *What are the fundamentals of the dispute?* Certainly one of the main divergent elements is the subsequent economic and financial effect of the development and implementation of a new cutting-edge digital technology which promises a significant impact on the society transformation over the next 30 years.

Apparently, we deal with an economic conflict in order to take over the global communications market of the 5th generation with long term effects on the multi-spectrum evolution of society, on a global level. Although the economic element of the divergences cannot be neglected, any strategic dispute caused by the emergence of disruptive technology also has the security component, especially in the cybersecurity field and associated emerging risks.

Therefore, we witness the emergence of a new revolutionary technology whose initial development is apparently gained by the Asian profile industry (China) with two emerging effects represented by the economical impact (which imposes the standard, develops the systems and monopolizes the market of profile and subsequently creates technical dependency) and which controls the large volumes of data (global access to broadband communications systems, operational dependency, indirect control of critical communications infrastructure security of technology consuming states).

The 5th or 5G mobile communication technology theoretically represents a stage of the digital natural development by moving to the next level in mobile communications after the successful operation of 3G (2000-2010) and 4G (2010-present) technologies. Practically, however, from a technical point of view, there is a fundamental change in the philosophy, architecture and communication capabilities in mobile networks, compared to previous 3G/4G technologies (figure no. 1), as follows:

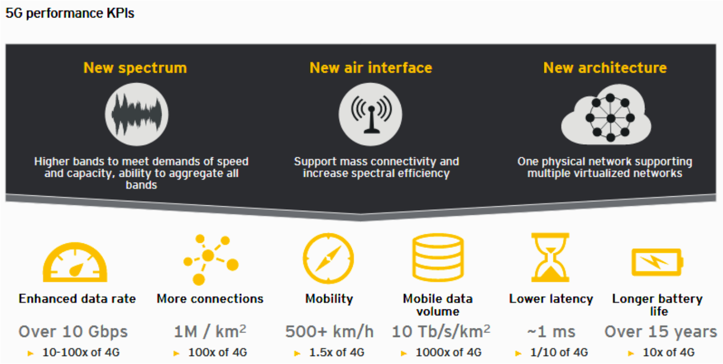

Figure no. 1 - *5G performance*
Source: **[1]** *https://www.ey.com/Publication/vwLUAssets/ey-china-is-poised-to-win-the-5g-race-en/$FILE/ey-china-is-poised-to-win-the-5g-race-en.pdf, pp.16*

a. Users’ traffic speed. It is the main technical gain generated by 5G technology, along with bandwidth capacity. 5G will allow 10-20 Gbps traffic speed, with a real user experience of 100 Mbps (wide area, outdoor) and 1 Gbps (indoor) respectively, about 100 times higher than 4G technology. This feature will facilitate the Internet of Things, Machine to Machine Communication and Connection everywhere concept development.

b. Bandwidth. A 5G communications network will ensure a minimum bandwidth of 10 times greater than 4G, and the traffic capacity for a given geographical area is estimated to be at least 10Mb/s/m^2;

c. Communication latency. 5G networks promise to ensure communications between devices, with an optimal latency of 1 millisecond, compared to 4G networks that provide latencies of approximately 50 milliseconds**;**

d. Coverage level. 5G architecture aims at total urban coverage with an estimated connection density of 10^6 devices/km^2 by the use of „Massive MIMO” micro antennas, which utilize millimetric (very short) waves with low energy consumption and the use of a very high frequency spectrum (Ghz), which allows reducing radio interference.

e. Used frequencies. The used frequency bands will migrate to the higher spectrum (Ghz) being used depending on the operational scenario, as follows: 700 MHz band (690-790 MHz) for long distance coverage in rural/urban areas, 3400-3800 MHz band for urban clusters area coverage and the 26 GHz band (24.25-28 GHz) for densely crowded urban areas coverage in order to meet the broadband needs.

f. Security. 5G technology will implement 5 new concepts, theoretically aiming at developing the current security level, as follows: implementing a new network authentication system [16, 5G-AKA, EAP-AKA, EAP-TLS, pp.5-9], operationalization of „*software defined networks*” concept, implementation of network segmentation systems into dedicated sub-networks (*Network Slicing*), migration to network virtualization (NVF) and native cloud systems.

The above-mentioned capabilities generate a broad spectrum of applicability in the industrial, economic, technological and security environment, both in the area of technology producing and service consuming states. In this study, we start from the hypothesis that 5G technology, though it generates a new paradigm of the digital society equivalent to the period of Internet emergence, will most likely not cause an „apocalypse” in the cybersecurity field.

I consider that 5G networks transformations, induce in the network environment (figure no. 2) will require a new model of cybersecurity „business” and, at the same time, a rethinking of security strategies and policies in the online environment, especially at the level of critical communication infrastructures in each state. The size of security policies and technical measures adaptation and 5G implementation impact on the cyber environment will be determined primarily by the correct identification and extended analysis of security risks induced in the network environment and broadband communications infrastructures of the states on the way to the new era of global connection and artificial intelligence.

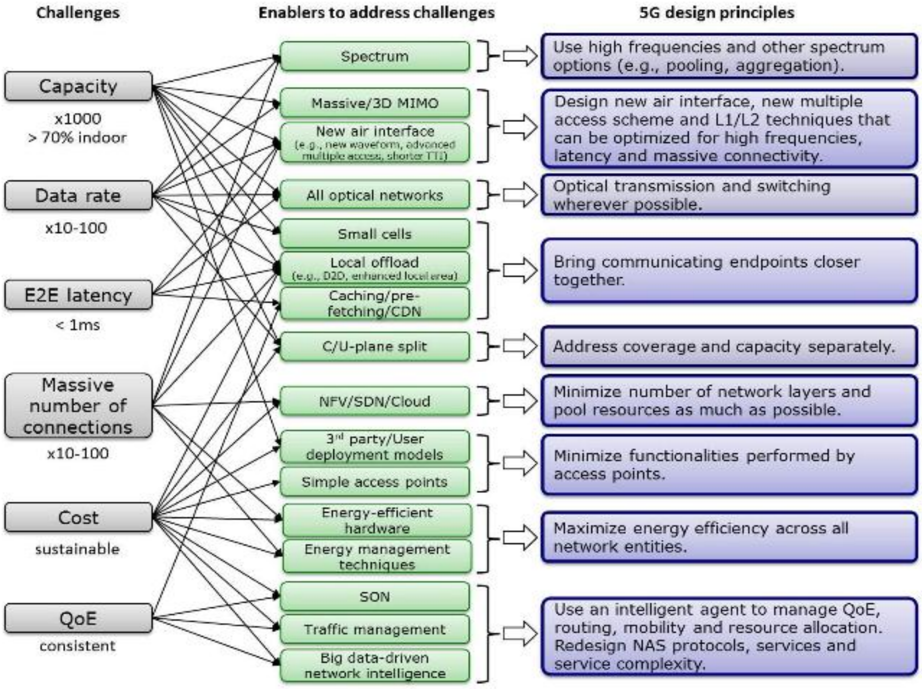
Challenges
Enablers to address challenges
5G design principles
Capacity
x1000
> 70% indoor
Data rate
x10-100
E2E latency
< 1ms
Massive number of connections
x10-100
Cost
sustainable
QoE
consistent
Spectrum
Massive/3D MIMO
New air interface (e.g., new waveform, advanced multiple access, shorter TTI)
All optical networks
Small cells
Local offload (e.g., D2D, enhanced local area)
Caching/pre-fetching/CDN
C/U-plane split
NFV/SDN/Cloud
3rd party/User deployment models
Simple access points
Energy-efficient hardware
Energy management techniques
SON
Traffic management
Big data-driven network intelligence
Use high frequencies and other spectrum options (e.g., pooling, aggregation).
Design new air interface, new multiple access scheme and L1/L2 techniques that can be optimized for high frequencies, latency and massive connectivity.
Optical transmission and switching wherever possible.
Bring communicating endpoints closer together.
Address coverage and capacity separately.
Minimize number of network layers and pool resources as much as possible.
Minimize functionalities performed by access points.
Maximize energy efficiency across all network entities.
Use an intelligent agent to manage QoE, routing, mobility and resource allocation. Redesign NAS protocols, services and service complexity.

Figure no. 2 - 5G challenges

Source: **[2]** P. Agyapong, M. Iwamura, D. Staehle, W. Kiess, A. Benjebbour, *"Design considerations for a 5G network architecture"*, IEEE Commun. Mag., vol. 52, no. 11, pp. 65-75, 2014.

The cybersecurity environment in 5G technology.

Although the standard specific to 5G communication systems has not been completed yet (*IMT-2020, the name used in ITU for the standards of 5G, is expected to continue to be developed from 2020, according to ITU press release*), under the report on cybersecurity impact, numerous experts in the field of information technology have founded two divergent evaluations **[3].**

The first, mainly supported by the promoters of technological developments in the Asian space but also by a part of the European research area, stipulates that 5G technology is the safest communication technology ever developed and will not have a significant impact on the global cybersecurity environment. The induced insecurity risks are evaluated as being strict of technical nature and will be managed through "security by design" approaches and security policies adapted to each environment/network segment. Thus, they evaluate that the new emerging risks or the level of cyber insecurity risk induced by the operation of 5G mobile networks will be absorbed and limited by the innovative technical protection measures such as implementation of „Software Define Networks” systems, „end2end encryption solutions”, securing the authentication process at the infrastructure level and implementing the virtualization tools and subnets logical segmentation - networks slicing. For example, the leader of Silverfort cybersecurity company, Hed Kovetz, declares that “*The 5G system incorporates secure identity management for identifying and authenticating users to ensure that only the genuine user can access services. Its new authentication framework enables mobile operators to choose authentication credentials, identifier formats and authentication methods for users and IoT devices*.”

The second category of experts, especially from the US area but also from certain European states, estimates that 5G technology will generate a series of new technological threats **[4, William Chalk, CSO]** and will alter the actual level of cybersecurity within the network environment, mainly due to the domination and technological monopoly of Chinese companies (Huawei and ZTE) serving the strategic interests of Beijing authorities.

As an example, the American artificial intelligence and security expert at Brookings Institution, Chris Meserole, states that *“The fear ultimately is that China monitors the traffic that’s passing through American networks, Western networks, and it’s recording it and sending it back to China, and China has this gold mine of data. The bigger fear from a military perspective is that China builds in a back door and they selectively use it. The scale and scope of 5G technology make the threat exponentially greater. Just as 3G networks ushered in the smartphone and 4G revolutionized society by facilitating apps such as Uber, 5G will connect users like never before and bring about the fastest, most reliable wireless services in history*”.

However, the two divergent positions are not transparently supported by scientifically based technical risk analyses or by concrete evidence available to the general public and academic environment.

Nevertheless, based on the historical experience generated by the implementation of 4G/4G LTE technology, together with the evolution of the society access to the Internet, we can recognize that there has been a significant global expansion of cyber risks and a transformation of the digital security environment. In this context, if we comparatively analyze the results of Deloitte's research **[5]** with regard to the evolution of cyber threats since 1990 *(figure no. 3)* and the result of 3GPP standardization organization study **[6** - 3rd Generation Partnership Project], as regards the evolution of mobile communication systems standards *(figure no. 4)* we can conclude that:

✓ Cybersecurity risks have evolved, along with the development of mobile communications systems;

✓ Risk explosion on cybersecurity and diversification of threats spectrum have been determined by the emergence and facilitation of the almost global access to the Internet network, using mobile data communication infrastructures (3G, 4G, 4G LTE networks, since 2010);

✓ The increase in the speed of access and capacity of data traffic in the mobile network environment has led to an increase of the users’ interconnection level within the online environment and in the same time, to an increase of the cyber attack surface area within the digital society.

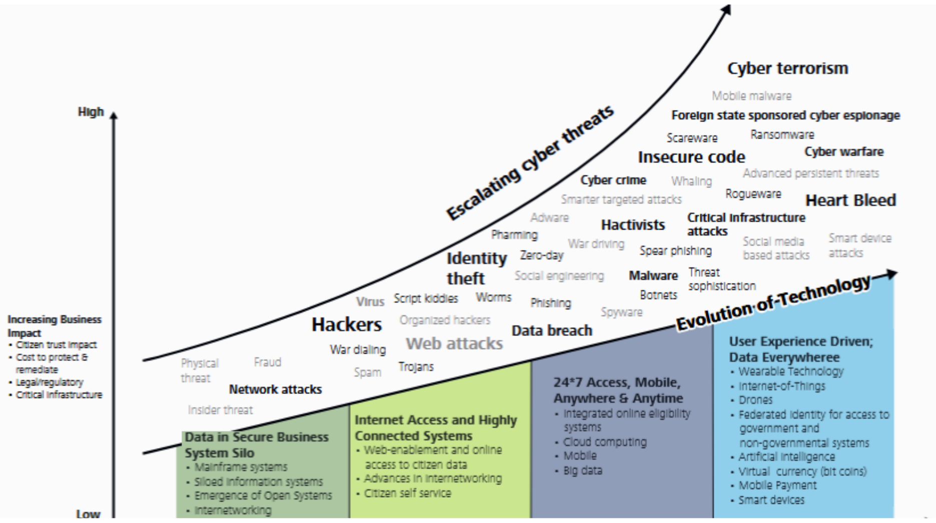

Figure no. 3 - *Evolving technology and cyber threats escalating*
Source:**[5]**
https://www.nascio.org/dnn/portals/17/2014Presentations/2014_Deloitte-NASCIO_Cybersecurity_Study_Overview _10_1.pdf

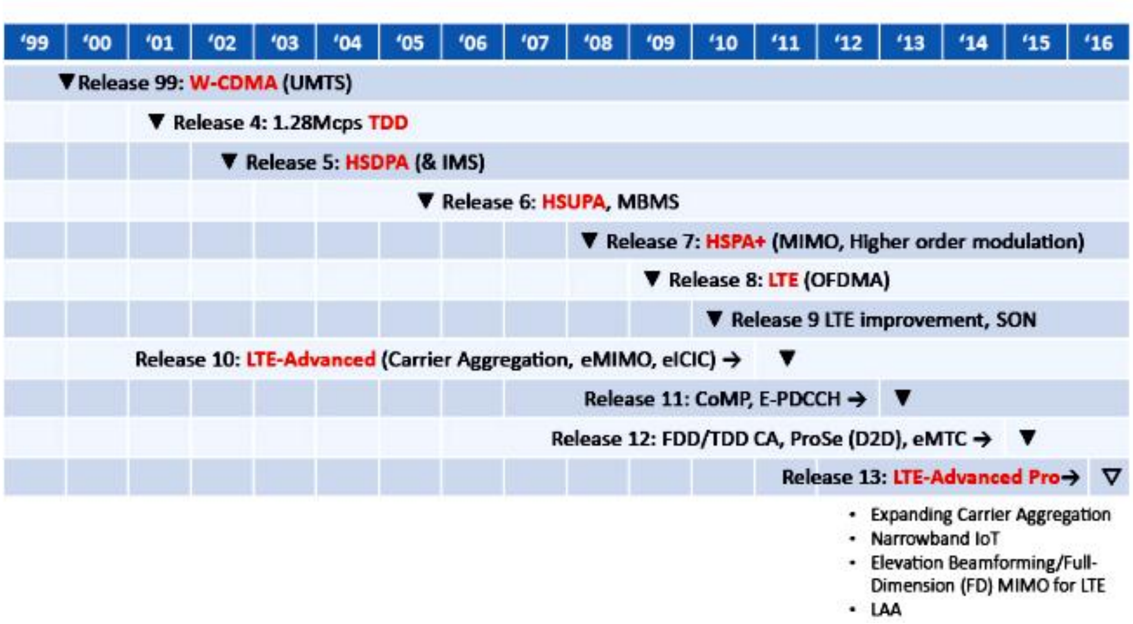
'99
'00
'01
'02
'03
'04
'05
'06
'07
'08
'09
'10
'11
'12
'13
'14
'15
'16
▼Release 99: W-CDMA (UMTS)
▼ Release 4: 1.28Mcps TDD
▼ Release 5: HSDPA (& IMS)
▼ Release 6: HSUPA, MBMS
▼ Release 7: HSPA+ (MIMO, Higher order modulation)
▼ Release 8: LTE (OFDMA)
▼ Release 9 LTE improvement, SON
Release 10: LTE-Advanced (Carrier Aggregation, eMIMO, eICIC) → ▼
Release 11: CoMP, E-PDCCH → ▼
Release 12: FDD/TDD CA, ProSe (D2D), eMTC → ▼
Release 13: LTE-Advanced Pro→ ▽
• Expanding Carrier Aggregation
• Narrowband IoT
• Elevation Beamforming/Full-Dimension (FD) MIMO for LTE
• LAA

Figure no. 4 – *Networks Communication Standards evolution,*
Source: **[6]** 3GPP, *http://www.aec.mk/irc2018/irc2018_s3_02_1.pdf,* p.13

Thus, the diversification of cyber-attack tools and the attacks complexity are directly proportional with the users' capacity of access to the network environment and with the number of interconnected equipment. In the same time, the equation of threats in the digital environment depends on the capabilities offered by the communication channels. Therefore, the impact of 5G technology on the digital security environment will be a significant one, similar to a paradigm shift in the way of securing the network environment, argued by the persistence and enhancement of the vulnerabilities specific to the current 3G, 4G, 4G LTE networks that will continue to function, as well as by the emergence of new vectors threatening the global digital society.

In the new technological context, defined by a massive agglomeration of users, the lack of the systems interconnection boundaries, the critical infrastructures dependence of the mobile data, society dependence to the critical infrastructure networks and by the „Internet of Things" concept materialization, not only does the cyber threats taxonomy, but also the area they are generated from (Asia, USA, Europe, etc) gains significance. The importance of cybersecurity in the context of 5G networks operationalization derives mainly from the increased possibility of discharging relatively easy the critical communication services and infrastructures, using precisely the advantages of technological evolution, such as the possession of equipment production patent (firmware, zero-days errors, backdoors), the traffic speed, broadband transport capacity, mobility of network access, as well as the lack of centralized control and visibility of network environment.

Also, in the expected context of the increased number of connections to the Internet network from 7 billion hardware in 2019 to 21.5 billion in 2025, according to the analyses conducted by IoT Analytics **[7],** along with the „smart objects" and „IoT" technology implementation, the effects of the destructive actions to disrupt critical communications services will be rapidly visible and exponentially amplified.

5G technology implementation in the actual context of accelerated social and industrial processes digitization together with the emergence of a real technological cold war between mainly USA and CHINA but also Europe ((buffer zone or test area) will determine 6 (six) categories of effects on the digital security environment, with an impact on social security, as follows:

1. Increasing the dependence of states critical infrastructures on the major global technology producers:

From the beginning, 5G technology has been supported and promoted by Chinese multinational companies, such as ZTE and Huawei, that have strategically surprised the technology field by successfully developing and testing the 5G equipment since 2017, exceeding the efforts of the American profile industry. If in the situation of 3G and 4G networks there were about 10 major global manufacturers of technology (equipment, infrastructure, software) among which Siemens, Lucent, Ericsson, Alcatel, NEC, Nokia, Panasonic Marconi and Huawei, currently the development of 5G systems (complete cycle of operationalization and production) is mainly carried out by 4 major manufacturers, namely Nokia, Ericsson, Huawei and ZTE.

In terms of the primary components, chipsets and controllers required in 5G equipment (mobile terminals, smart equipment, servers), the technology is dominated by 4 global manufacturers, namely Qualcomm (USA), MediaTek (Taiwan), Samsung Electronics (South Korea) and HiSilicon (China, a subsidiary of Huawei).

Therefore, the next 5G infrastructure will depend on one of these equipment and technology providers. Thus, there is a reduction in the number of companies in the field of advanced technology capable of producing 5G communications systems and equipment, practically, the market is currently divided between the US, China and partly Europe (on certain network segments).

In the future context, „after 5G implementation", the critical communication infrastructures in each state will be significantly dependent on one of the 4 manufacturers of 5G systems as well as one of the chipset manufacturers, given the advanced level of technology and the existing discrepancy between them and the other communications companies in the profile industry.

Technically, the 5 facilities offered by 5G networks (traffic speeds between 1 - 10Gbps with 1 millisecond latency, minimum download speeds of 50 Mbps, the urban coverage level through MIMO antennas of approximately 10 times better than 4G networks, network interference discharge by customizing Beamforming, and implementing future full-duplex mobile communications in the future) will determine the gradual migration of the critical communications infrastructure of each state (government authorities, companies, medical systems, systems energy, banking systems) to the 5G network environment.

In addition, the increasing need for communications bandwidth, the limitations of 4G networks but also the fixed infrastructure to ensure mobile access and cloud-based real-time access to data and information will indirectly require the migration of applications, critical services and data traffic associated with the 5G mobile infrastructures. The two elements, corroborated with the complexity of high technology, will generate, as a consequence, the direct functional critical infrastructure dependence on the availability of 5G equipment and systems and on the capability and credibility of the system's manufacturer. Under the security and continuity of critical services, most technology-consuming states will have to choose between the dependence on the Asian technology and American technology, in the context where cybersecurity is no longer an exclusively technical issue.

From the perspective of induced security risks, besides the significant dependence on 5G systems and equipment manufacturers, the lack of transparency in the level of infrastructure, equipment production and maintenance cycle determined the European states (+ the USA) at the issuance, in a technical summit in Prague (May 5, 2019), of two recommendations indirectly intended upon high-tech developers.

As a future target, securing the critical communication infrastructure will inclusively imply the traceability growth of developing, implementing and operational processes of 5G technology communications infrastructure through:

- *„Shared responsibility of all stakeholders should drive supply chain security. Operators of communication infrastructure often depend on technology from other suppliers. Major security risks emanate from the cross-border complexities of an increasingly global supply chain which provides ICT equipment. These risks should be considered as part of the risk assessment based on relevant infor-*

mation and should seek to prevent the proliferation of compromised devices and the use of malicious code and functions”.

- *Customer – whether the government, operator, or manufacturer -- must be able to be informed about the origin and pedigree of components and software that affect the security level of the product or service, according to state of art and relevant commercial and technical practices, including transparency of maintenance, updates, and remediation of the products and services”***[8]**

In the 5G technology generated context, cybersecurity acquires a new dimension represented by the transparency of the equipment (hardware) manufacturing processes, software products development, materialization of firmware updates and maintenance activities.

2. The need to adapt current cybersecurity technologies to the new network infrastructure and architecture framework - the emergence of a „*dynamic cybersecurity policy*” concept.

5G networks or „next generation of radio networks” in the network architecture level would mainly involve 4 innovative elements which require changing the current cybersecurity paradigm, based on standard security policies, as follows:

- *Facilitate the implementation of „software-defined network” networks and „software-defined radio”* to the detriment of traditional ISO/OSI networks. The security policy applicable to an ISO/OSI model network architecture will have to be redefined as **a dynamic security policy** adapted to a software network infrastructure (SDN - *Open Wireless Architecture*), which will work by alternatively modifying the traffic capabilities and the communication routes between users through fast dynamic allocations/deliveries of IP addresses, much more frequently than the traditional routine. For example, in the 5G infrastructure traffic situation, the number of nodal gateway equipment will increase by a factor of 20 to 30 times the original amount and the volume of distributed gateway equipment will decrease considerably **[9].**

- *The 5G network environment segmentation in 3 logically individualized networks,* as follows: radio access network (*radio access network - RAN*), *core network* (data centers networks) and „*transport network*” respectively. The principle will determine the change of a single technical infrastructure cyber protection concept and will ensure extended cybersecurity for the protection of a *network* function virtualization (***Network functions virtualization - NFV***), aimed at the simultaneous facilitation of several different functionalities, using the virtualization principles type IaaS. Thus, the perimeter cyber protection actions of the network environment will no longer be sufficient for traffic control and limitation of external threats, as it is necessary to combine active and passive protection measures.

- *Operationalizing the concept of network segmentation -* ***Network slicing*** into different segments of logical networks dedicated to a single set of functionalities. The high traffic speed estimated at 100Mbps/download/user and respective 50Mbps/Upload/user, the maximum latency estimated at 4 ms and the high level of coverage respectively, facilitates the segmentation of a common network platform into several subnets dedicated to different functionalities such as: networks dedicated to mobile communications (Mobile broadband network), networks dedicated to "machine to machine" communications, networks dedicated to government authorities (gov - networks), networks dedicated to the medical system (medical - networks), etc.

From the security point of view, these dedicated subnetworks (logically separated at the level of a single platform) will generate a high-security level, yet carrying significant resource consumption since different protection layers can be applied according to the importance and sensitivity of processed data, the network critical availability level or the subnetwork importance to the critical infrastructure. Although the cybersecurity level will significantly increase and will be adjusted based on the operational requirement, the complexity of measures and the personnel’s knowledge level will become determinant.

The concept of networks logical segmentation depending on the destination or served need will most likely require the emergence of new equally customized communication protocols, depending on the subnet to which they are addressed, such as machine to machine type communication (MTC), Ultra-Reliable MTC (UMTC) or Extreme Mobile Broadband (xMBB)

- *Use of cloud computing infrastructure as native access infrastructure to applications* *and data resources.* The notion of native cloud computing infrastructure is perhaps one of the greatest benefits of 5G technology. Migration to the cloud computing environment will not only become a necessity imposed by the need for instant data access but will also be a requirement to meet the standard levels of Quality of Service (QoS) and Quality of Experience (QoE) respectively. The new concept of "native cloud networks" will allow overcoming the current barriers regarding the migration of data and information in the cloud computing environment, but at the same time, it will require adapting cybersecurity processes to an "end to end security" approach, using especially the advanced software encryption and infrastructure resilience solutions through virtualization.

The impact on the security environment interpreted by the need to adapt actual cybersecurity policies and strategies indirectly generates a series of additional human, procedural and technical nature risks.

From the point of view of the personnel and security administrators who will manage the networks security in 5G technology, the need to adapt the training and constant education will increase substantially. Also, the complexity of actions and attacks on infrastructure will be permanently in an upward dynamic which will require not only the possession of highly specialized technical teams, but also the tools and resources of action in near real-time, to be able to cope speed of attacks. Although technology will allow online training execution through augmented reality platforms and innovative simulation techniques close to the real environment, security processes and defensive cyber actions will need the substantial support of cyber products controlled by artificial intelligence.

Whereas technology will allow online training forms execution by augmented reality platforms and innovative simulation technics close to the real environment, security processes and defensive cyber actions will need the substantial support of artificially controlled cyber products

Procedurally, the cybersecurity concept will become less standardized and will experience a permanent dynamic. Thus, cybersecurity static procedures, almost indispensable today, will be gradually replaced by experiences of good practices and knowledge bases operationally validated in simulation centers. The cybersecurity concept will migrate to a comprehensive cybersecurity approach.

3. Increasing and energizing the global platform for manifesting cyber attacks and the attack environment, by expanding IoT and M2M communications.

One of the most significant cybersecurity implications, generated by 5G operationalization, is evaluated as increasing the attack surface by facilitating mobile broadband connections to the Internet of all objects, equipment and systems that have an active network port, regardless of the environment provenance. The notion of „smart objects", an extension of algorithms and artificial intelligence almost anywhere (from industrial processes to household objects) but also the expansion of digital multimedia has created the need for permanent network connection and, implicitly, the concept of „Internet of Things". Each equipment connected to the network environment (IoT) will act as a user or consumer of connection services, but will also act as a sensor at the network level. The more the number of interconnected devices will increase, the greater the society dependence on the functioning of communication networks and the Internet environment will be.

In a 4G digital society, a harmful "botnet" network obtained by penetrating and taking control over a number of interconnected computers creates significant destructive effects on a digital infrastructure under attack, rendering services and access to data, information and applications unavailable. However, in the future 5G, hacking actions will be directed to the intelligent devices of a user in his social environment (TV, refrigerator, central heating, air conditioning, etc.), and these can be successfully used to mount large-scale DDOS attacks towards the critical communications infrastructures of the states. Moreover, in the future 5G world, most likely, the same network of penetrated and remote-controlled devices, which has become a botnet, will be used to shut down an entire network of vehicles or drones in a region, or to control the power supply processes of a city.

Technically, the existence of non-standard and hybrid operating systems at the level of various smart objects and equipment will make it almost impossible to detect malware software or virus tools stored and hidden in the software of IoT equipment. A large amount of data generated by the IoT environment in future 5G networks will make it much more difficult to identify anomalies in the behavior of hacking actions or traffic anomalies in the digital environment, especially since the architectures and software applications have not yet implemented, under the restrictive effect of the law, the "security by design "concept.

Target diversification, new communication protocols capable of supporting M2M communications, as well as increasing the number of targets through vertical and horizontal digitization - Internet of Everything (IoE) and Smart City/Smart Society operationalization will increase the dependence of critical connection of infrastructure and environment and the "Butterfly effect" will be much easier to feel in the future security environment.

Ever since 2015, the company Wind River Systems (USA) in research for the security of IoT equipment **[10]** has drawn attention to the need to resize the concept of cybersecurity in the context of developing the three essential levels of digital society, namely smart cities, connected industry and connected buildings. The company's research concluded that there is no real solution, ideal for mitigating the risks generated by IoT development and the need to develop security standards unanimously accepted by the manufacturers of smart equipment and technology it is almost mandatory.

The emergent security risks arising from the IoT development, accelerated by 5G facilities derive from the fact that the operating systems used on smart devices are mainly based on Linux distributions and Open Source customizations such as FreeRTOS, Contiki/Contiki- NG, MBed OS and RIOT OS and equipment manufacturers use non-standard hardware architectures with short life cycles, replaced new versions relatively quickly, insufficiently tested for vulnerabilities and with minimalist security technical support.

According to security company Gartner **[11]**, over 25% of the cyber attacks by 2025 will be addressed to the IoT equipment or will have these systems as an intermediate target which will lead to a revaluation of risk analyzes on the digital environment.

The emergence of new vulnerable targets in the IoT environment which have not been considered essential up to now and the definition of the „smart home" digital environment as a vulnerability area, derives from the studies of the company NETSCOUT, which in the security report of 2018 **[12] Threat Intelligence Report, pp.2]** emphasized that "*five minutes is the average amount of time it takes for an IoT device to be attacked once connected to the Internet"*.

4. Enhancing cyber attack capabilities for current vectors by increasing bandwidth and attack surface and decreasing latency of communication channels.

The report from 2018 elaborated by the European Networks Information Security Agency for (ENISA) **[13],** highlighted that, during the period 2017-2018, the number of "Denial-of-Service" (DOS), "Distributed Denial-of -Service "(DDOS)" cyber attacks, web-based "attacks and „botnet"cyber-tools has increased, becoming the main threat vector in the future.

Implementing 5G technology and facilitating broadband data transmissions with traffic capabilities estimated at an approximate potential level of 10 Gbps - 50 Gbps and a latency value of between 4ms-1ms will increase the success rate for DDOS cyber attacks, starting from the real premise that data exfiltration from the network environment will become inefficient as compared to the unavailability of the services of an entire network and critical infrastructures of a state. Improvement of DDOS attack tools and their operational testing in recent military conflicts (Estonia, Georgia, Ukraine) will determine that, in the context of increasing the cyber attack surface (IoT/smart society environment) and improving the speed of online traffic, they will be *the main cyber risk vector for the communication infrastructures of states.*

If actual DDOS attacks can be almost randomly performed at any OSI architectural level, in the context of 5G systems implementation, the volumetric and protocol DDOS attacks dedicated to level 3 and 4 of the OSI model but also those of the ones specialized in flow concentrators and nodal gateway equipment will be chosen, in order to discharge as many segments of the network as possible.

Although blocking legitimate data traffic on a 5G network becomes difficult in the context of existing connections diversity, this can be accomplished by diversifying attack vectors and combining DDOS techniques with other vectors such as web-based attacks on data management systems of 5G services of mobile operators or malware vectors, similar to the case law "*Mirai malware*" from 2016.

In 2016, „Mirai” generically named malware has successfully penetrated the networks of IoT-type devices that used the Linux operating system. On September 20, 2016, the Mirai malware was used in the largest ever Distributed Denial of Service (DDoS) attack, targeting French cloud computing site OVH and, later in the same year, the United States DNS provider „Dyn” **[13].**

Practically, the network facilities effect generated by the 5G technology on the DOS/DDOS/Botnet attack vectors will be a trampoline, enhancing in the event of such a successful attack, the future effects on the continuity of the access services to the critical digital applications. The solution, in the new digital context, can be represented by the division and sharing of security risk between technology/service consumers, equipment manufacturers and 5G service provider respectively, by implementing the concept of "security as a service" as part of the service contract (SLA - service level agreement).

5. The emergence of new attack vectors and new cyber attack opportunities in the global digital environment.

The 5G environment and the increased dependence on the advanced technology at society level, as well as on the producer’s patents and technological standards offers reasonable indications about the possibility that, at one point, a technology producer could dismisses the communications infrastructure of a state, using constructive vulnerabilities specially designed or software elements gradually introduced in network architecture (exp: in SDN networks, as part of a firmware upgrade or as part of a legitimate maintenance process). In addition, large traffic capabilities through the 5G transport network nodes will create the real possibility of masking the exfiltration of confidential data from the network environment to the control servers of third parties or producers serving divergent security interests, without these exfiltrations to be quickly known and eliminated.

Therefore, the concept of cyber espionage, the possibility of data exfiltration from the network environment and the massive direct dependence on the technology of a certain developer may be the main new threats, not necessarily innovative in content, but in the form of manifestation and in the value of harm and destructive effects.

Another element of risk may be the accelerated development of online hacking platforms specialized for attacking GSM networks and infrastructure. A good example that can prove the effects of such a threat is the attack carried out by the online hacking platform „REGIN”, which allowed in 2014 the penetration of critical communication infrastructures in countries such as Algeria, Afghanistan, Belgium, Brazil, Fiji, Germany, Iran, India, Indonesia, Kiribati, Malaysia, Pakistan, Syria and Russia. According to the Kaspersky Lab analysis „*A REGIN module was able to monitor the control systems of the GSM cells, collecting data on the GSM cells and network infrastructure and subsequently penetrating any GSM target cell. According to the information logged on the GSM cell control system obtained by Kaspersky experts during the investigation, the attackers were able to access data that allowed them to control the GSM cells inside the network of the respective penetrated telecommunications operator. The attackers had access to data about the calls processed by a particular cell and could facilitate the redirection of the calls to other cells or the activation of neighboring cells”***[15].**

In addition to the mentioned threats, most likely 5G facilities will also diversify the applicability of ransomware threats as well as advanced and persistent attacks (APT) customized for communication systems, the motivation being provided on the one hand by the impact on the network environment but, on the other hand, by the successful procurement of illicit funds that will fuel the future development of new cybercrime tools.

Certainly, the assessment of emerging cybersecurity risks from the 5G operationalization will be subject to the analysis of each technology consumer state but also of cyber analysis environments considering that, the technical maturity of the 5th generation of mobile networks will be reached only between 2025-2030.

6. Migration of the cross-border organized cyber crime interest towards digital identities and personal data theft.

The 5G technology will boost the possibility of human communication in the social networking spectrum through the excessive use of virtual reality and, above all, of multimedia virtual communication, using augmented reality products. Although it may be considered futuristic, I evaluate that, in the near future, each individual, will be able to communicate in the social networking environment using one or more associated virtual identities. Thus we will find a parallel accelerated development of a new virtual human ecosystem associated with the social-terrestrial, similar to a new parallel world.

The limitations regarding these concepts development are due so far to the lack of band capacity, the slow/inconsistent traffic speeds and the limitations of mobile connectivity. The 5G infrastructure, as discussed above, will discharge these limits. In the new context of virtual human society, the importance and necessity of security of virtual identity/identities will become at least as significant as that granted to the protection of personal data or biometric data. In this respect, cybercrime will intensify the actions of illicit exploitation of virtual identities in the online environment in order to obtain illicit material benefits and resources in an innovative way, exploiting precisely the social evolutions generated by the technology. Most likely, the value of the fingerprint and virtual identity of each user will become a tradable resource, so that the protection of virtual personal data in terms of cybersecurity of the population and users will become a new field of activity.

Conclusions

The 5G technology alongside the artificial intelligence systems will redefine the society we know nowadays and implicitly, the cybersecurity environment. Even if the transformation will not be abrupt, the technological revolution will impose the following major directions of the transformation of the current cyber environment:

- The level of threats will be a permanent ascending one dictated by overly rapid implementation of certain insufficiently tested and documented technologies (5G) as well as by the developed criminal capacity of the cybercrime structures. **The effect:** cybersecurity of infrastructures can be ensured through governmental – private or consumer – technology producer cooperation.
- Dependence of critical communication infrastructure functioning on the major technology and equipment producers will increase significantly. **The effect:** on a short term, states will be faced with the dilemma of choosing between American and Asian technologies.
- Risks of losing sovereignty and freedom to choose the cybersecurity tools for new communications technologies and network systems will increase and responsibilities will gradually be transferred to equipment manufacturers. **The effect:** the concepts of *„security as a service”* and *„security by design”* will be operationalized, as part of the service contracts (SLA);
- Critical communications infrastructures of states will gradually migrate from the private/government data communication networks to the public 5G communications infrastructures. **The effect:** the spectrum of vulnerabilities will increase being dictated by the capacity of operators and the resilience of public telecom infrastructure.
- Cybersecurity field will no longer be exclusively technical, but it will represent a „cross” type domain on the border between technology - security strategy - artificial intelligence - governance. **The effect:** cooperation between states within the cybersecurity field becomes mandatory.

5G technology impact on the security environment, at the current state of knowledge, can be the most estimated, but a precise determination of possible effects and actions to limit them must become the subject of national security strategies for both European and other states that will define technology implementation in the first wave.

The level of risk assumed along with 5G technology implementation must be balanced with strategic advantages resultant from the operationalization of the 5th generation network in the pioneering period, as compared to implementation during its maturity period.

In conclusion, though it is premature to carry out a comprehensive risk analysis on a 5G communications infrastructure, for objective reasons related to the lack of technological knowledge, anticipating the main risks and assessing the likely impact on cybersecurity environment, it will facilitate network environment securing processes in the short and medium term.

References

[1] *,** *China is poised to win the 5G raceKey steps extending global leadership***,** *https://www.ey.com/Publication/vwLUAssets/ey-china-is-poised-to-win-the-5g-race-en/$FILE/ey-china-is-poised-to-win-the-5g-race-en.pdf*, p.12, 2018

[2] P. Agyapong, M. Iwamura, D. Staehle, W. Kiess, A. Benjebbour, *"Design considerations for a 5G network architecture"*, IEEE Commun. Mag., vol. 52, no. 11, pp. 65-75, Nov. 2014.

[3] Colin Lecher, Russell Brandom, Is Huawei a security threat? available at *https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g*

[4] William Chalk, Privacy by design: *Cybersecurity and the future of 5G*, CSO, available at *https://www.idginsiderpro.com/article/3399000/privacy-by-design-cybersecurity-and-the-future-of-5g.html*

[5] ***, Deloitte-NASCIO *Cybersecurity Study "State governments at risk: Time to move forward"*, 2014, p.20, *https://www.nascio.org/dnn/portals/17/2014Presentations/2014_Deloitte-NASCIO_Cybersecurity_Study_ Overview_10_1.pdf*

[6] 3GPP, *http://www.aec.mk/irc2018/irc2018_s3_02_1.pdf*, p.13

[7] Knud Lasse Lueth, State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating, 2018, *https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/*

[8] *,** Prague 5G Security Conference: The Prague Proposals, Press release, *https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/*

[9]*** Huawei, 5G Network Architecture *,https://www.huawei.com/minisite/hwmbbf16/insights/5G-Nework-Architecture-Whitepaper-en.pdf,.p.12, 2018*

[10] ***, *Security in the Internet of Things- Lessons from the Past for the Connected Future, 2015, California, SUA*

[11] *https://www.computerweekly.com/news/450288414/IoT-to-play-a-part-in-more-than-a-quarter-of-cyber-attacks-by-2020-says-Gartner*

[12] ***, *NETSCOUT Threat Intelligence Report, Dawn of the terrorbit Era-https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901%20-%20NETSCOUT%20Threat%20Intelligence%20Report%202H%202018.pdf, pp.2*

[13] *,** *http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment /enisa-threat-landscape/enisathreat-landscape-2018*

[14] *https://www.allot.com/blog/iot_cybersecurity_challenges_and_solutions/*

[15] *https://securelist.com/regin-nation-state-ownage-of-gsm-networks/67741/*

[16] ***, *CableLabs, A Comparative Introduction to 4G and 5G Authentication*, pp.5-9, 2019, *www.cablelabs.com*