CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Science

Master in International Security Studies

Master Thesis

2021 **Giampaolo La Rosa**

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Science

Master in International Security Studies

The 5G Technology Nexus: Assessing Threats and Risks of Implementation

Master Thesis

Giampaolo La Rosa

Prague 2021

Author: **Giampaolo La Rosa**

Supervisor: **Mgr. Petr Špelda, Ph.D.**

Year of the defence: 2021

Abstract

The new 5G technology, next generation of telecommunication and mobile network, is all around the world in course of inspection and inquiry for its astonishing novelty, from new services to functions and scalability. However, every technology brings alongside new possibilities and new threats scenarios, especially in this case where the impact on the present network is promised to be massive, with brand new features allowed by 5G, like Internet of Things, widespread virtualization and huge leap forward in rapidity and capability of the mobile transmission. An increase in the network surface, considered as more connections, more devices connected and more traffic load of data, will expand also the possible entry point and fault exploitable by a malevolent actor, raising common concern about the technology. The deployment of such a technology on European soil, especially in some states of the Union, caused uproar and critics primarily in the security field. Following a global trend, but also leading a best practice approach, the EU developed a series of mechanisms and agencies that are challenged to oversees the gradual shift from old 4G LTE to 5G. In this paper a Critical Information Infrastructure Protection (CIIP) framework is used to analyse the criticalities of the new technology. Definition of the critical sectors, Regulations and Organization predisposed to cybersecurity, cooperation mechanism will be covered to formulate the possible solution to adopt and thus, minimize the damages to the vital internet network.

Length of the work: 97.000 characters

Declaration

1. I hereby declare that I have compiled this thesis using the listed literature and resources only.
2. I hereby declare that my thesis has not been used to gain any other academic title.
3. I fully agree to my work being used for study and scientific purposes.

In Prague on 05/01/2021

Giampaolo La Rosa

Giampaolo La Rosa

Contents

Abbreviations 7

Introduction 8

Research target, research question 13

Literature review 14

Conceptual and theoretical framework, research hypothesis 16

Empirical data and analytical technique 18

First Part 19

- Historical Evolution 19
- The 5G in a Nutshell 24
- 5G Architecture 27

Second Part 31

- Structure of the Cases 31
- Threats to the Infrastructure 34
- Threats to IoT 38
- Threats to Core Network 39
- Threats to Access, Virtualization and Multi Edge Computing Technologies 40
- Recommendations 42

Considerations and Conclusion 44

Bibliography 49

Abbreviations

ARPANET	Advanced Research Projects Agency Network
CERT	
CIA	Confidentiality, Integrity, Availability
CIIP	Critical Information Infrastructure Protection
DARPA	Defense Advanced Research Projects Agency
DoS	Denial of Service
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DPM	Data Protection Manager
ENISA	European Union Agency for Cybersecurity
FTP	File Transport Protocol
ICT	Information Communication Technology
ISP	Internet Service Provider
IoT	Internet of Things
NFS	National Science Foundation
NR	New Radio
LAA	License Assisted Access
LAN	Local Area Network
LTE	Long Term Evolution
MANO	Management and Orchestration
MEC	Mobile Edge Computing
MIMO	Massive Input Massive Output
MNO	Mobile Network Operator
PPM	Password Protection Module
RAN	Radio Access Network
RAT	Radio Access Technology
SMTP	Simple Mail Transport Protocol
SDN	Software Defined Networking
SSL	Secure Sockets layer
TLS	Transport Layer Security
VIM	Virtualised Infrastructure Management
VPC	Virtual Private Cloud
VPN	Virtual Private Network

Introduction

The last decade has witnessed the rise and profound sedimentation of, a not completely new, but now fundamental field of International Security Studies: cybersecurity. Around the world, global powers, regional one and rogue states are increasingly concerned about their vulnerabilities in what is correctly considered the new perfect double-edged sword: the cyber domain. This domain and the vectors of offense and defence that live within it are those that David E. Sanger iconically named "Perfect Weapons" and that during the last thirty years challenged constantly academics, officers and politicians around the world with the puzzling experience of a unbelievable paradigm shift. Perfect weapon represented the right definition for a world that until the early 90s was frozen into a permanent nuclear confrontation between Superpowers locked in their own definition and theoretically capable of mutual assured destruction but practically unable to use those "imperfect weapons". Deterrence during the second half of 20th century pushed all relevant actors to inaction, or action with other means. However, the old paradigm gradually slid away after the steady progress of the internet and the so called new "information age".[1] Information age unfolded many new possibilities alongside many new threats, but the major characteristic of the new paradigm is that confrontation was no more a taboo, not like in the previous nuclear weapons, incredibly expensive but impossible to use without causing enormous consequences. On the opposite, cyber weapons are extremely powerful but potentially can cause no harm to humans, destroying assets and systems, are expendables and usable by different actors, the immediate result was to revive old confrontations.[2] As the reader will understand deeper in this work, however, cyber weapons are "perfect" only on paper and even if it is possible to use them without taking in account responsibility to the alleged attack is also possible inflict terrible damages and kill or harm people. They could be perfect in some ways, but they are not the final pacifist weapon capable of leaving the burden of casualties from the shoulders of governments and decision makers.[3]

Although the cyber domain is a theatre of confrontation, its fluidity is the most prominent feature that brings to our era. In fact, from one side, the cyber domain is characterized by the network positive overextension bringing alongside incredible economic and technological opportunities, but, from the other, more connections mean more accesses and possible

[1] Buchanan, B. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, London 2020, Harvard University press, pp.1-10.

[2] Sharma, A. *Cyber Wars: A Paradigm Shift from Means to Ends.* Institute for System Studies and Analysis (I.S.S.A9 Defence research and Development Organization (D.R.D.O), Ministry of Defence, India.

[3] Liang, Q.; Xiangsui, W. *Unrestricted Warfare*, Shadow Lawn Press 2017, pp.2-18.

vulnerabilities from all over the globe. This feature of double edged sword marked our recent times and raised suspicion for the so called hybrid threat scenario, where combat, non-combat, political, economic, financial, media and other fields are all mixed in a hybrid and ubiquitous field difficult to grasp and immunize against.[4] Since 1960 the first Computers, and afterwards LAN connections, proved that the net could present pitfalls in all three aspects of information security: confidentiality, integrity and availability (the so called CIA). Unfortunately, the sensibilization of Government and public opinion vis-à-vis the transformation and expansion of the cyberspace came only after the 90s and the commercialization and globalization of the internet.[5] From this historical point Cybersecurity was considered anew. Two different aspects emerged clearly from breaches in the perceived safe environment of the internet: the social and economic perspective focused on the assurances and guideline to protect against Cyber-crime and Data stealing and the birth of a new complex conflict scenario, hybrid or multi domain, where the point of connection for all the domains was the Cyberspace. The hybrid threat became of steady interest during the 2000s. In this decade, in fact, many glaring events were put under the spotlight of public opinion. First of all, in 2008, the Stuxnet hacking (also called operation "Olimpic Games") was gradually uncovered by a team of security experts and resulted in the opening of a Pandora box. US and Israel were under the formation of a task force that used a cyber weapon against Iranian enrichment facilities with the result of a complete halt of their nuclear program and the infection of millions of computers all around the word.[6] From that historic moment on was a continuous sequence of cyber espionage, election interference and military action taken as retaliation against cyber-attacks, like the Israeli bombing of an Hamas hackers hideout during last year (2019).[7] The escalation of relevance in the cyber domain is impossible to disprove together with the magnitude triggered by the ICT revolution in the decision making environment. This decade has the merit to have solidified a previously mild and naïve conception of the network into what now is perceived from the public opinion and especially from various Government as the new field capable of tip the scale to another level, as proven by the last most controversial cybersecurity breaches, the Snowden case, the

[4] Bachmann, S.D.; Gunneriusson, H. *Hybrid Wars: the 21st Century's new Threats to Global peace and Security*. Bournemouth University, UK.; Swedish Defence University.

[5] Becker, W. (2006). *The Dot.Com Revolution in Historical Perspective*. Entreprises Et Histoire. 43. 10.3917/eh.043.0034.

[6] Gates, G. *How a Secret Cyberwar Program Worked*, The New York Times, 2012. In https://archive.nytimes.com/www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html ;

[7] Peck, M. *Israel Bombed Cyber Hackers (That Is Historic, For Many Reasons*), The National Interest, May 12, 2019. In https://nationalinterest.org/blog/buzz/israel-bombed-cyber-hackers-historic-many-reasons-56987 ;

Russian backed intrusion in US Presidential elections and Korean network disruptions.[8] Possibly, in other words, the new environment took time and practical cases to be fully understood and perceived as it is, the next breakthrough in human history.

But how all these developments are connected with the advancements in the ICT field? The main concept to define at this point is what is 5G and why is it so important for the next generation of security experts. Considered in sheer data 5G is simply the logical next step in the ever-evolving technical scenario. Faster, better, stronger and indeed it is. Not taking it lightly is it possible to say that 5G will increase drastically the "power" of our wireless connections, however, is important to focus more on two factors enabled by the technology. First, the rapidity of the new connection is not a merely an increasing in multiply order (from 1GB per second to 20GB, 20 times faster) but is also a multiplier of time. The speed of communication since the beginning of the information age was a pivotal factor for development and unexpected threats. The time spent to deliver information in the entire human history was probably the main factor capable of change all the others, and now is it highly probable that the thing will not change.[9] More speed means more connections, more data transferred, bigger possibilities available and in the meantime less time to "manage" the grid. Humans are capable of manage only a limited number of things in fraction of time and this development will lead to an environment more and more automatic without a "man in the button room". The second factor to focus on is the new possibility of Internet of Things (IoT), that basically means every device connected to internet will be capable of establish autonomous connection with other device, without the intervention of humans. This is not a brand new world if we intend device as machines like servers and host but the novelty came from the magnitude and diffusion of what will be considered as a connected device, from a trimmer to a hoover, everything may communicate through internet thanks to sensors and software dedicated to the scope. Interfaces will be totally automated and this, even if already possible for many things, is not widespread and only a ubiquitous, stable and powerful new architecture based on 5G will be capable to sustain and implement on large scale. This new feature is also a big reason of concerns mainly for the same reason of speed, lack of human control in the process, but also an

[8] Garamone, J. Cybercom Chief Discusses Importance of Cyber Operations, US Department of Defence, 2015. In https://www.defense.gov/Newsroom/News/Article/Article/604453/cybercom-chief-discusses-importance-of-cyber-operations/ ;

[9] Singer, P.W.; Brooking, E.T. *Likewar*, Mariner Books, New York, 2019, p.47-55;

incredible augmentation in the attack surface, or better said, augmentation of the vulnerability surface (understood as vulnerable to cyber-attacks). [10]

Considering these features, speed and IoT, 5G could be the nexus which allow old and new technical exploits to be used by concerted strategies. Studying risks and threats will need a specific interest either in the technical aspect of technology (what can be done with such an infrastructure?) and strategic ways to employ 5G (how can be used the infrastructure?). One aspect without the other would result in a partial analysis and understanding of the matter and this has to be avoided specifically for the evolving nature of security, even more today revolving around the concept of hybrid, multi-domain security, as said before. The implementation of 5G networks will lead to a more connected, rapid, ubiquitous cyber domain, with a huge volume of data flowing in every possible direction. To cope with that means, understand the infrastructure and regulate it before any possible damage will be done.

That being said, however, is necessary also to specify that this paper is not intended to be a so wide and exhaustive display of all cybersecurity Threats for national security, or more widely, on a global scale. On the opposite, this work will revolve around narrower topic, in particular, the brand new 5G technology network implementation in Europe and how to protect the critical information infrastructure. As strategists will be inquired which new means are unleashed by 5G, what is needed to consider for right decision and policy making, besides, for this sake is much needed also a picture of possible strategic pitfalls and attention to implications, the beforementioned "How?" that represent the daily business of decision makers. For instance, analysing the installation of smaller and more numerous 5G repeater antennas in our cities will allow new kind of threats for the incoming traffic, possibly malicious and stemming from every kind of IoT devices, but also pose a root issue for the possible presence of backdoors (issued by the retailers and provider of the service).[11] This issue could unleash concerns about DDoS (Distributed Denial of Service), that practically speaking are Cyber-attacks that thanks to a high volume of data can overflow or suppress the capacity of the network infrastructure, causing complete paralysis and malfunction. In this example a technical specification makes a real escalation until a strategic problem for any organization (in the current example probably a State) that have to consider wisely the possibility of structural paralysis of the network in core

[10] Hill, M. *#ISC2Congress: How 5G is Expanding the Attack Surface*. Infosecurity Group. [Viewed date 17/11/2020]. Available from: https://www.infosecurity-magazine.com/news/isc2congress-5g-attack-surface/ .

[11] Nguyen-Duy, J. *Security Challenges Facing the Shift to 5G*. CSO, July 17, 2020. [Viewed the 3/12/2020]. Available from: https://www.csoonline.com/article/3567450/security-challenges-facing-the-shift-to-5g.html .

business or assets, and hence, has to act in advance to avoid a strategic impasse, or the possibility of being in checkmate by such and occurrence.

The possibility of a DDoS is only one possible vulnerability, and this one is not a novelty, but the How is indeed one. The new possibilities unfolded by 5G network are present in many aspects of the network, and they involve threats ranging from more “physical” ones like damage on infrastructures, to disinformation campaign and espionage made possible thanks to hijacking, spoofing and other exploits available for threat actors. It is indeed complicated to write of threat of such amplitude, but the modern trend is to devolve more attention on the broad picture and take in consideration every aspect of the Multi Domain reality but the main objective of a risk and threat assessment is to consider the possibilities and explore in extent the vulnerability of the system.[12]

As clearly shown by raw data, breaches and hackings are a threat of daily basis in the new global scenario dominated by the overarching presence of the network. Throughout 2020 almost 4000 confirmed data breaches caused an estimated 1 trillion dollars loss, half of those were the result of hacking (52%) the remaining phishing and malware.[13] It is a striking statistic because shows the huge cost for the market and also the vulnerability of the network. The trend is still in ascending phase, primarily because hacking is financially motivated and the business is becoming a slice of the pie for many threat actors (from criminal organization to foreign hackers), a 86% of those data breaches were financially motivated in fact but with a still good part of espionage and the prevalence of external actors.[14] It is clear that considering this an expanding surface of attack produced by the 5G technology will only cause more incidents, more vulnerabilities and more damages to the market, especially in the European case scenario. The criticality of this threat is the main reason that made the CIIP framework (Critical Information Infrastructure Protection) a valid tool to use in this research. The protection of a critical infrastructure, usually industrial or connected to energy and basic service providing, is expanded in the CIIP to information field, in this case ICT, that can be in this way be considered a centre of gravity for the stability of society and economy.[15] 5G will be an implementation of

[12] Zinzone, F.; M.Cagnazzo, M. *The art of war in the post-modern era*, self-produced, 2020. p.20-27.

[13] 35 Outrageous Hacking Statistics & Predictions. [Viewed date 21/11/2020]. Available from: https://review42.com/hacking-statistics/ .

[14] Verizon, Data Breach Investigation Report 2020. Available from: https://enterprise.verizon.com/resources/reports/dbir/ .

[15] Commission of the European Communities. *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*. Brussels 30/03/2009. {SEC(2009) 399}, {SEC(2009) 400}. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149 .

the current ICT architecture, expanding the mobile service providing and allowing more pervading feature to the connectivity (for example IoT), thus CIIP will greatly help in the formulation of a concrete structure of analysis. The framework is intended to work in accordance to regulations and political objective and engage risk assessments relative to 5G technology, with the final objective of a better understanding of the overall security environment for telecommunication. In order to accomplish this scope, a first part will be devoted to the general unfolding of history and aspects of 5G. First, the evolution of Internet and Communication Technology until the 5G last incoming footstep, converging particularly on the progress of risks and threats consequential to this evolution. Consequently, the technical aspects will be probed, trying to avoid too particular details not inherent to our field but trying to introduce in the best possible way to the thorny system functioning of a complex technology. Hence, network security, portable devices, wireless implication and data centres will be considered to formulate a clear and complete as possible assessment of risks for all these targets. The second part, on the other side, is divided in four major threat areas and cases that will ground the theory to practical cases. Examples will be unfolded and for each of them an author's suggestion of a possible remediation either technical and normative. The next and final part will be a general overview of the threats considered, a strategic consideration and personal suggestion of the European posture on the matter. The final objective of this paper is design a functioning analysis tool that consider higher stakes and technical implications in order to proceed on a solid basis to the following objective of assessing the European situation vis-à-vis the critical information infrastructure, and formulate some best practices and recommendations.

Research target, research question

The main objective of this paper is to use the CIIP framework for critical points individuation and evaluation, thus formulating most prominent threat cases in which the infrastructure can be put in jeopardy. Once defined the limits and structure of the 5G network will be possible to centre practical cases of attacks and risks, in this way helping also to formulate counter measures and prevention of threats. European Union will be considered as a whole for the same structure of the infrastructure and the political entity considered, in fact, every country has its own peculiarities but only thanks to the orchestration and management of the Union is it possible to achieve the result of a safe 5G environment. Governments, Internet Service Providers (ISP), organizations and companies are all together forming the ground of a huge network of different infrastructures and devices connected and potentially all cause for a breach for the entire system. The research question turns around this topic and can be resumed in: What kind of threats is facing the EU Critical Information Infrastructure, considering the incoming implementation of 5G technology? What can be done to mitigate and shield against them?

Literature review

With the objective in mind to acquire a broad but consistent literature base, the research work on such a phenomenon (the introduction in the ICT field of a critical new technology) was directed through three main directions. First, a general literature about cybersecurity, historical evolution of security, perception of threat (with elements of environment shaping) and perception of the security inside the network. A second part about the technical aspect of the 5G technology and finally, a third on regulations and recommendation made by key actors of decision-making stage. Conceptual/theoretical framework is demarked thanks to the contribution on cybersecurity by Bayuk's "Cyber Security Policy Guidebook" and Cavelties' "*Power and Security in the Information Age*" and especially with the Isabelle Abele-Wigert and Myriam Dunn's "*International CIIP Handbook*". These works solidified the groundwork of Cyberspace and cybersecurity, proceeding with the re-evolution of ICT and relative uncertainty disclosed by the new media. Although, "*Cyber Security Policy Guidebook*" has a defined scope to set a useful framework to apply in policy making, from the cybersecurity management cycle to direct recommendations and approaches, while "*Power and Security in the Information Age*" is a compelling critic of cybersecurity threats, our perception of those (based on a Constructivist view) and a consequent proposal for a better understanding of the field. The "*International CIIP Handbook*" was fundamental, on the other side, to introduce the methodology of the framework and helps with national cases and procedures. In a more general way was taken in consideration also works coming from Artificial Intelligence and cybersecurity from expert of their fields and with compelling opinion on the transforming landscape. Kai Fu-Lee's "*AI Superpowers*" deals with the Chinese perspective in AI and technology in general, revealing the internal Chinese market, economic dynamics and political ambition. On the other hand, Sanger's "*The Perfect Weapon*" is a great overview of all majors hacking of the last decade, with a strong accent on the incredible relevance of Cyber Domain in our era, underlining in that way the importance of the incoming network implementation. Alongside Sanger other important contribution to this field are Kaplan's "*Dark Territory*" and Buchanan's "*The Hacker and the State*". Both revolving around major hackings and the shaping of the cybersecurity field from the wake of internet to nowadays. A different view on the topic is also given by Maurer's "*Cyber*

Mercenaries" and Singer's "*Likewar*". Their contribution is especially focused on the willingness of a malicious actor to act against something/someone and not in the fragility of the grid that support the Internet and on the new social media environment that greatly deformed our perception and reality of conflict/security. Vulnerabilities for them, are inherently at any system in our times. Thus, both greatly contribute on the understanding of threat actors and the changing shift happening in the last decades regarding cybersecurity. Kurlantzick's and Ding's works (*Charm offensive* and *The Dragon's Hidden Wings*) are mostly used to understand the pivotal Chinese perspective over the global politics, and their perception of "soft power" and "peaceful rise", both themes interconnected to the 5G challenge for the perceived challenge/menace of the possible ZTE/Huawei installation of 5G platform over strategic states and allies of the US.

Another literature contribution in which is embedded the thesis is rounded in the more technical aspects of the topic, either if impossible to ground a technical dissertation in this project was assumed that a limited review was fundamental to understand the challenges posed by 5G networks. Two important manuals were reviewed: Osseiran, Monserrat, Marsch, Queseth and Rodriguez (*Fundamentals of 5G Mobile Networks*), both deeply involved in technical critical aspect of this technology and how overcome the major damaging edges. Moreover, they were supported by other short essays on specific topics as Ubiquitous connectivity and technology-policy. Another important part of literature in this part was centred on cybersecurity aspects, like Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short's "*Cybersecurity Essentials*", Johnson's "*Cybersecurity: Protecting Critical Infrastructures from Cyber Attacks and Cyber Warfare*" and finally Clark's "*Cyber Physical Security: Protecting Critical Infrastructure at the State and local Leve*l". The last two works are very focused on the Critical Infrastructure Protection framework and greatly help to formulate a better analysis of 5G infrastructure and how address the threats introduced in this paper.

The final section of literature was based on direct white papers, directive of governments and policy advice, all effort to thwart or control the phenomenon. The most relevant are: Clark's "*Critical Infrastructure Protection in Homeland Security*", the National Cyber Strategy of the United States of America, the Huawei Cybersecurity Evaluation Centre (HSEC) Annual Report 2019, but also private contribution to the discussion as Guide to Developing a National Cybersecurity Strategy, Strategic Engagement in Cybersecurity and 5G Mobile Broadband Technology - America's Legal Strategy to Facilitate Its Continuing Global Superiority of Wireless Technology. Very important contributions are also the CISCO and MERICS private study of the

5G phenomenon together with all the paper on 5G threat landscape, Cybersecurity of 5G Networks, EU coordinated risk assessment of the cybersecurity of 5G Networks, IoT Security Standards Gap Analysis. All of those produced by ENISA (European Union Agency for Cybersecurity), that all together greatly helped to construct the present work.

Conceptual and theoretical framework, research hypothesis

Taking in consideration that the main objective of the paper is to assess major threats inherently brought together by the 5G network revolution, the framework proposed is the Critical Information Infrastructure Protection (CIIP), different from the Critical Infrastructure Protection (CIP). CIIP has the added value that bridges the gaps between cybersecurity and CIP with a connected approach between these two before separated fields. The focus is on Information Infrastructure because the same subject of the analysis is the network itself and its correct functioning. Thus, taking together means (communication) and place (the network) is it possible to view the subject and object of the research. It is indeed critical to protect 5G network because will became soon completely intertwined with the other cabled and mobile networks and furthermore will enable the communication of an entire new set of mobile devices with the rest of the already connected world. The very structure of the network, for its nature without boundaries and clear limits of jurisdiction, was put under stress during the 2000s and consequently emerged the common need of a framework under which be able to analyse and prevent threats coming from the network. After 9/11 and the fight against terror, in first place the US but afterwards all countries, defined more up to date framework that considered the vast spectrum of threats able to damage and put in jeopardy critical infrastructure for the functioning of any state. CIPs were the result of these normative efforts and broadly considered many different threats, from natural disaster to terrorism, and in our case, cyber threats that can became an issue for the different core sectors like communications, banking and finance, energy, physical distribution and so on. [16]

[16] ENISA Quarterly N°4 Jun 2006, p. 4-5.

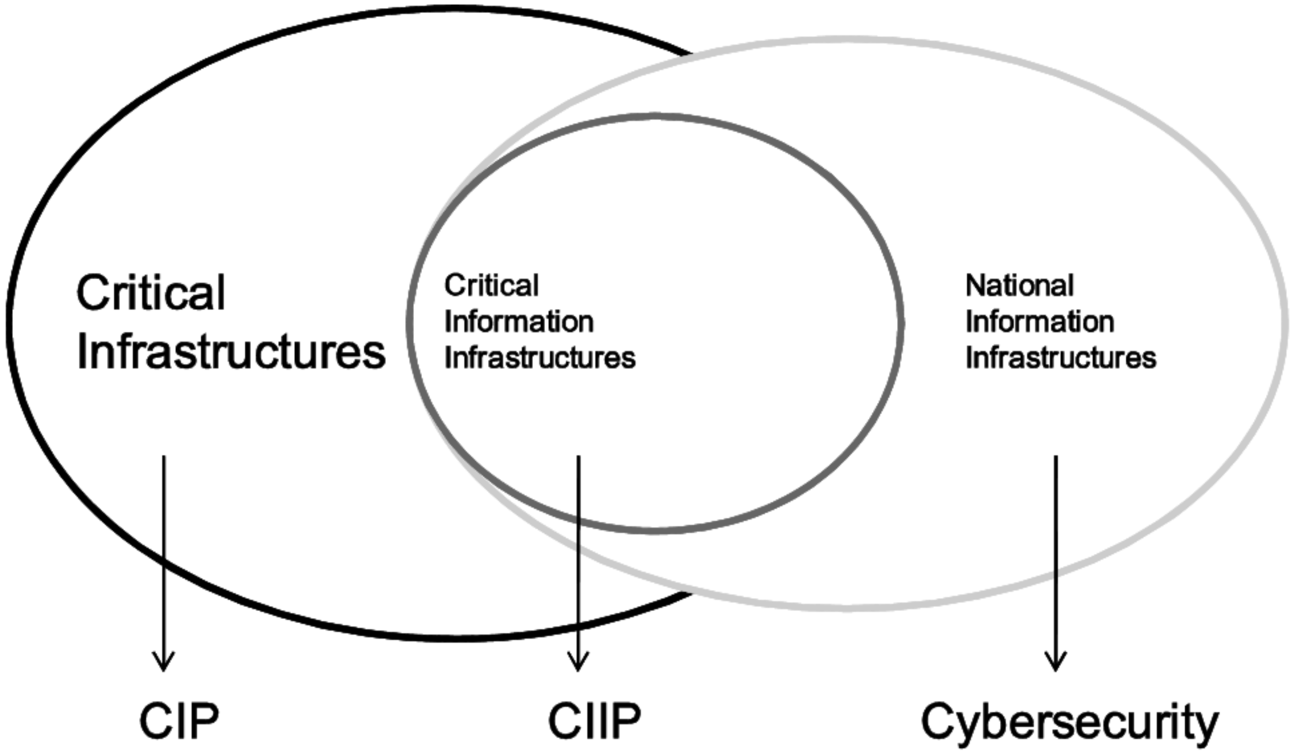
Critical Infrastructures
Critical Information Infrastructures
National Information Infrastructures
CIP
CIIP
Cybersecurity

Figure 1: CIIP Framework Scheme from The Art of CIIP Strategy (Cavelty, M.D), 2012

The emerging approach to Critical Infrastructure Protection, contextualized by the five-consecutive point of identify, protect, detect, respond, recover[17] was translated afterwards in a more common framework in many countries. Among the most important initiatives was the European Union's "*Policy on Critical Information Infrastructure Protection*" of 2009 that set five pillars very similar to the general framework but more cogent to the European environment: Preparedness and prevention; Detection and response; Mitigation and Recovery; International cooperation; Criteria for European Critical Infrastructures in the field of ICT.[18] In the following year the Union pushed forward the initiative endorsing a more stringent cooperation between member state and established after a resolution (2012) and two conferences (2009 and 2011) a European Forum for a Public-Private partnership for Resilience, many policy recommendations for National Computer Emergency Response Teams (CERTs) and giving the ENISA the possibility to coordinate those activities to form a cohesive response to cyber threats in order to ensure Infrastructure protection.[19] Finally in 2015 the OECD (Organization of

[17] Johnson, T.A.; *Cybersecurity Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, Taylor & Francis Group 2015, p. 27-28.

[18] European Commission. *Policy on Critical Information Infrastructure Protection (CIIP).* Law 7 February 2013. [Viewed the 4/11/2020]. Available from: https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip ;

[19] ENISA Baseline Capabilities of National/Governmental CERTs, 2012

Economic Cooperation and Development) collected and produced a recommendation paper on best practices that gathered together all the EU initiatives regarding the CIIP framework.[20]

In this paper the security of a critical infrastructure (the network) considered as hardware assets (data centres, cable backbone, antennas/cells, mobiles and other structures) and software assets (software, Cloud, protocols) involved in the correct functioning of 5G technology are all together viewed as a critical infrastructure to be shielded from any incoming possible threat. Bearing in mind the core of the analysis will be unfolded the same structure of the technology and how it works, the stakeholders involved in the workflow of the service providing and afterwards main threat will be proposed. Identification of the threat/risk, how to protect against it and how to detect it, followed by a brief proposal of response and recovery actions to undergo in order to minimize and limit damages to the critical infrastructure.

Empirical data and analytical technique

Data will be drawn from the selected texts or assumed accordingly to the evidences formulated in an in deep case study revolving around the phenomenon of 5G implementation in Europe. The study of the sources is aimed at acquiring in first place all the relevant problematics in the practical application (Internet of Things, Deep Learning and Artificial Intelligence, privacy of data and ubiquitous accessibility) and from those scaling the issue up across the normative and political aspects. The analysis of the existing studies on the matter in a so poorly inquired topic, and with incoming potentialities as a study subject, is probably the only way to frame the 5G nexus, homogenise the material and produce a valid assessment that take in consideration all the factors that were stated. An important part will be played by the construction of a model, or a threats/risks landscape, resuming all the development of ICT in the past years and applying it to the modern challenge of 5G.

[20] OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en .

First Part

Historical Evolution

The evolution of ICT field strictly ties together cybersecurity and the very evolution of computers. Every step up in IT became sooner or later a new step for the entire cyber environment and so, to trace this movement, is necessary to go back to the first computers available. During the first computer era, when computers were big as a room and too expensive for any private company the security of these calculator was strictly speaking only physical. Guards and controls were put in place to deter damages to the hardware and in order to avoid stealing of data (still available only under the form of punched cards). There was no trinity of cybersecurity, availability, integrity and confidentiality, but on the opposite the only very important matter was preserve the functioning of the overpriced bare metal and besides grant the very functioning of the still unperfect technology, very keen to data loss and breakdowns.[21] However, after the diffusion of a primitive system of data sharing raised the first concerns in the confidentiality field. Especially for intelligence and secrecy matters the US government started to research and employ a primitive form of cryptography that in the 1974 became a NIST (National Institute of Standards and Technology) standard de facto and after a real US Computer Security Act. A first line of defence was set in a way common in human history, encrypting messages was an old way to preserve confidentiality of information, the DES was the first cipher approved by the NSA and NIST, developed by IBM (replaced in modern times by AES that with different enhancements is still in force).[22] For instance, in Europe either after the 2013 and 2014 study on Cryptographic Protocols there is no common framework in place for all countries and the matter is entrusted by foreign/industry standards.[23] In the 80s minicomputers became largely available and more affordable for companies either for personal

[21] Bayuk, J.L; Healey, J; Rohmeyer, P; Sachs, M.H; Schmidt, J; Weiss, J. *Cyber Security Policy Guidebook*; edited by John Wiley and Sons, Inc. USA 2012. Pp.15-21.

[22] National Research Council. 1996. *Cryptography's Role in Securing the Information Society*. Washington, DC: The National Academies Press. Pp.414-420. Available from: https://doi.org/10.17226/5131 .

[23] ENISA, Data Protection, Cryptographic protocols and tool. [Viewed the 21/11/2020]. Available from: https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/cryptographic-protocols-and-tools .

use and with the diffusion of LAN (Local Area Network) cable the first real connections break up in the market. The LAN connected computer environment created a new need of security, in fact there was no more certainty of users using a specific PC, new controls were needed to connect a user to a specific login and consecutive task (mainly because this intrackability resulted in many frauds and illicit). The issue was first approached with a password-based logic that ensured a minimum of access control, although this first LAN networks were protocol-free or better did not rely of safe protocols to ensure data integrity resulting in the clear reading of password during the transfer online (with the right knowledge any hacker could read passwords passing through LAN networks).

A decisive step forward was achieved with the ARPANET project, financed by American DARPA organization (Defence Advanced Research Project Agency), and consisting in a primitive network that connected core military and research infrastructure that have to be preserved in case of atomic confrontation with Soviet Union in a classic Cold War scenario. This network, connecting just few computer around USA demonstrated the viability of a distributed method of communication that allowed all interfaces of the net to be in contact and exchange data (in primitive form of FTP and Telnet protocols, for file transfer and remote login). A decisive advancement was made thanks to the first email protocol (SMTP) that allowed the real communication of entities around the network, resulting alas in an unexpected overflow of the network capabilities due to great usage and lack of hardware performance. This first network reunites a bunch of bases (at first only four bases) and thereafter was expanded to the peak of forty during the 70s. The growing demand of services and more connectivity, triggered by the common assumption of the potentiality of the new communication vector resulted in the further expansion of ARPANET and practical fusion with NSF (National Science Foundation) in a new NSFNET the ancestor of the modern internet that was not this time only for secret and military purposes but cantered around academic use and widespread knowledge sharing.[24]

Although this huge step represented a concrete new opportunity, brough together as always new vulnerabilities. This era was characterized by a common naivety and thus was easy to exploit for a young student of computer like Robert Morris. In the 1988 he launched the first known Worm (a Malware capable to self-replicate and infect more machines without external actions) that rapidly affected all the mail servers around USA, the NSFNET was completely overwhelmed by the infection that caused the utter paralysis of the network and huge economic

[24] National Science Foundation. *A Brief History of NSF and the Internet*. [Viewed the 05/10/2020]. Available from: https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050 .

impact on the new born system. Interesting in this matter is that the only unaffected laboratory was the AT&T (the main American telecommunication company) one that was involved during the crisis in an experiment of a new type of traffic and packets inspector called *Firewall*. The function of this new method of inspection worked, and still works in a certain simplified way, matching all incoming packets allowing network traffic only those whose source and destination matched with a previously authorized list of addresses. Firewall even if in an experimental stage reduced Morris's work impact to minimum and instituted a new security policy still valid nowadays.[25] The further effect of the work was the raising awareness for these kinds of malwares and consecutive damages, thus imposing in the best practices for network management Detection and Recovery in addition to Prevention for cybersecurity standards. At this point was clear that any modem with public access was vulnerable to the rising category of hackers, that with simple line of code could access any visible interface menacing phone companies and providers of the service. The age of innocence was over. During this pioneer age another fundamental threat was discovered. Viruses. Installed in floppy disk a virus can affect the machine where introduced and even penetrate in websites, ready to infect visitors' users. The consequent reaction was the development of Antivirus software, sold to companies and governments interested in an improved defence against these malicious codes. Antivirus vendors were from that moment busy with forensics and analysis of malware in order to keep track and archive all possible threats and sell a new type of service.

The 90s were the age of e-commerce, also described of any kind of commerce made through and into the internet. Many new vendors and companies were interested in spreading their services and goods online, the structure of the network began to be solid and ramified to sustain such a traffic. Computer started to be a constant presence also in the private life of people, allowing growing demands. The money poured into the new medium had a seismic effect to raise both hardware capabilities and boost volume of business to be made.[26] The new threats of the network (worms, viruses) imposed new standards based on firewall technology, like the DMZ (Demilitarized zones) capable to reduce incoming suspect traffic thanks to a combination of phone's firewalls and port's restrictions (the famous port 80 issue). However, hardware capabilities of the network were still strained, and the DoS and next DDoS attacks were widespread. These kinds of attacks relying on the poor bandwidth available at the time,

[25] Bayuk, J.L; Healey, J; Rohmeyer, P; Sachs, M.H; Schmidt, J; Weiss, J. *Cyber Security Policy Guidebook*; edited by John Wiley and Sons, Inc. USA 2012. Pp.20-25.

[26] Johnson, T.A. *Cybersecurity: Protecting Critical Infrastructures from Cyber Attacks and Cyber Warfare*. CRC Press, Taylor & Francis Group, 2015. Pp. 6-15.

submerged the target with an unbearable amount of traffic, either coming from a single point (DoS, Denial of Service) or from multiple sources (Distributed Denial of Service). No counter measure was available except to widen the available bandwidth at the time. The same time became evident to be a core aspect of security, time was necessary to deliver services but also fundamental to grant fluid access and stable connections, the disruption of the service became a thorn in the side of internet and is still a core aspect of *Availability* cybersecurity principle.

The new environment fertilized by the widespread diffusion of e-commerce during the 90s produced another important innovation. Growing concern about privacy and security of authorized connection pushed forward the effort to introduce a certified connection protocol, formalized during 1995 and called TLS (Transport Layer Security) that relied and still rely on SSL (Secure Socket Layer) communication protocol. SSL was new and innovative first and foremost for the embedded feature of certification required to finalize a connection between two interfaces, but one drawback was the necessity of long identification string that further engulfed the already busy network. Certificates work in the same way of the non-online ones, they need a certification authority of a "root" certifier that generate a chain of trust (a cascade effect of certification that entrust the upper level to the lower one). In such a way giving a certificate to a user became key to access and being acknowledged as a trusted entity. VPN (Virtual Private Network) was another solution adopted to resolve the problem of unwanted accesses.[27] A way to encrypt the entire remote access session and give the permission to an entire organization if needed in an easier and more intuitive way. However, all the new features introduced in internet during this fruitful decade have the consequence of deeply tie together commerce and technology, especially developer, technicians and all the workforce that maintained the network up and running. Crashes were frequent, malfunction same, and patch and update highly required. The need of a constant contact between investors, managers and developers became key to a core aspect of security, a security "by design" at first but also in continuous update and ready to intervene in case of troubles.

The early 2000 brough to the spotlight a new challenge, wireless technology. The network was already challenged by mobile computing and other portable devices, but in this case the change was seismic. The network was already enormous and tentacular, new and old actors emerged following the bait of easy money, the generic hacker became distinguished by many different labels, depending on their purpose. Cybercriminal, hacktivist, Cyberterrorist, State Sponsored.

[27] Cloudflare. *What is Encryption? | Types of Encryption*. [Viewed the 05/10/2020]. Available from: https://www.cloudflare.com/learning/ssl/what-is-encryption/ .

A number of new traps were refined and used, these times witnessed a huge increase in *phishing* techniques (intended as baits, usually email, sent to many users and containing malicious codes, usually links) or the widespread use of *spyware* (formally responsible for any type of spy technique like keylogging and other). The increased volume of violations caused by real groups or gangs, specialised in such trades, raised concerns for the defences to put in place in order to cope with the threat. Malware installed in USB (like the terrible STUXNET but also the "Buckshot Yankee" at the American DoD that almost crippled the army command and caused the formation of the Cyber Command to respond to this menace).[28] Data stealing and *ransomware* also sees his place under the spotlight, with many spectacular actions that resulted in data stolen and coded from big companies that consequently have to pay a ransom to have back their confidential data, and many times resulted in the leakage of data and image damage worth millions of dollars. Protection for data became rapidly the main concern of companies and organizations, backups, data storage and other measures were studied but notwithstanding the issue remain paramount.

From 2000 to nowadays other relevant novelties came out, the emergence of the Cloud and all relative branches connected to the use of the technology (all the IaaS, PaaS, SaaS where cloud computing provide the bedrock for Infrastructure, Platform or Software application and turn this capability in a service for companies and people), the VPC (Virtual Private Cloud) model of deployment that practically expanded the concept of VPN but also the ever expanding mobile network, culminated in IoT and 5G. If some pattern emerge from this historical overview is that from the first steps of the cyber space at an increasing faster pace all the aspects of our life were involved in a pervasive network where healthcare, power-grids, financial markets, weapons systems are virtually all connected. In this fluid environment the pattern is a recurrent action-reaction. New threats and new countermeasures alternate the pace of development, marking certain periods with overreliance on the solidity of the network and other with the delusion about the fragility of the system. Cybersecurity in a nutshell is all about these recurrent cycles, analyse new technologies, detect vulnerability, prevent malfunction and attacks and strengthen the overall architecture for the next evolution. Unfortunately, all cited threats are still there, no one was banished forever from the network and on the opposite, all are still in place and could be used to harm and damage in also new way and with new means. The countermeasure side then is the core of our defence, establish best practices and norms that promote a safer

[28] F. Kaplan, "*Dark Territory*" Simon & Schuster, New York 2016, p.78-82;

environment for everyone, 5G is, reduced to the essential, an incredible occasion either for new development but also (as history shows) for new threats and vulnerabilities.

The 5G in a Nutshell

The exponential spike in internet traffic that can be explained with two intertwined phenomena, growth of users and quality of service. The world internet users from the 90s to now skyrocketed from 2 to 50 users per 100 inhabitants (considering the large part of developing world, but the statistic has a way more impactful display for developed world, from 11 to 81), in the same way the services offered and necessity of more addresses brought back many times the topic of IPv4 limitations (the Internet Protocol version 4 has a limitation to 32bit address space, and hence "only" 4,294,967,296 possible unique addresses) and the necessity of implementation of the new IPv6 standard for internet communication (that allow 128bit addresses and an exponential increase in numbers, close to 3.4 x 10^{38}).[29] All the expanding businesses, companies and services needed more bandwidth, more datacentre, faster technologies to meet the client's needs. An impressive crowd in a couple of decades demanded accesso to ubiquitous video/content sharing, social media and other kind of services become integrated in their smartphones and in their same life. One data for everything can show the magnitude of the phenomenon. In 2019, 2.26 billion were subscribed on Facebook, with similar numbers to the following platform like YouTube, Instagram, WeChat and so on. It is difficult indeed to trace the share and volume of data exchanged in a whole year, but one thing is clear, the whole infrastructure needed a new way to transmit and receive mobile data, incredible possibilities of market were waiting and saturation was impossible.[30] Considering this 5G was only the natural evolution of a society that needed (or best wanted) ultra-high-definition video, super-fast connection and everything that can enhance their internet experience wherever they are. Interconnectivity could in all the ways improve the possibilities for revolutionary changes, allowing the development of smart cities, allowing IoT, vehicles communication, roadside infrastructures, waste management, all kind of sharing economy and so on.[31]

[29] Internet World Stats. *Internet Growth Statistics*. [Viewed the 07/10/2020]. Available from: https://www.internetworldstats.com/emarketing.htm .

[30] Roser, M.; Ritchie, H.; Ortiz-Ospina, E. (2015) - *Internet*. Published online at OurWorldInData.org. Available from: https://ourworldindata.org/internet.

[31] J. Rodriguez, "*Fundamentals of 5G Mobile Networks*", John Wiley & Sons, Ltd 2015, p. 29-54;

But what is exactly 5G? As said in the introduction 5G is all about speed, ubiquity, bandwidth and will allow IoT and advanced features for mobile communication. But in this instance is it possible to delve deeper in the details. 5G is of course the next step in the ICT evolution, a so far steep slope that with a decade recurrence made a step toward the next threshold.

- Before 1G (<1983): All wireless communications were only voice-centric;
- 1G (1983-): The US cellular system came out and was named AMPS (Advanced Mobile Phone Service), is commonly referred as the first generation of wireless communication;
- 2G (1990-): Migration from analogic system to the digital one, GSM technology (Global system for Mobile Communication) was born in 1991 and defined a new circuit-switched network that enable full duplex voice telephony (reference from Wiki). Major innovation of 2G included: Digital Signal, Encryption and data (Short Message Service SMS);
- 2.5G (1995-): High capacity voice and limited data service, this system allows 1.25 MHz bandwidth, in the US called CDMA and at the same time in Europe GSM was upgraded from GSM to GPRS and EDGE systems;
- 3G (1999-): Full data capability. 3G was the first international standard of the ITU (International Telecommunication Union). This generation use WCDMA (Wideband Code Division Multiple Access) technology using 5 MHz bandwidth. The first full-fledged data-centric system. Data driven communication brought to mobile phones GPS (Global Positioning System), location-based services and on-demand video, creating the first appetite for faster connections;
- 4G (2013-): high-speed data rate with voice function system. Enhanced with the LTE system (Long Term Evolution) grants a 20 MHz bandwidth and considerable licensing costs for the operator but is the only feasible way to shift to high velocity data rates and mobile video. Practically speaking 4G never met the requirement and was enhanced from the first stages with LTE, the same 5G technology can be considered the last step of this long-term evolution;
- 5G (2020-): has still to be officially defined and standardised but has the potential to be high-capacity, ultra-high-speed data and a designed low latency and operational expenditure system for operators. 5G aims to redraw a new ecosystem for wireless networks that connect many domains and assets.[32]

[32] Fransen, F. *5G Security: Can 5G secure IoT?* TNO, 2019. [Viewed the 12/11/2020]. Available from: https://www.surf.nl/files/2019-03/5G%20Groningen%205%20-%20Can%205G%20secure%20IOT.pdf .

Summarizing 5G has three main objectives to achieve in order to be a concrete leap forward:

- Speed (ultra-high-speed radio access): Download speed of up to 20 Gbps, this will allow to download 40 GB of data in less than a minute. Speed as was said is crucial either for core functions or new developments;
- Responsiveness (ultra-low latency): essential to control autonomous cars and high precision devices in real time. Reliability and availability in any given time is core in this use cases. End-to-end latency for this sake as to be reduced below the threshold of human reflex. In theory 5G network will have a latency of less than 1 ms;
- Scale (Massive connectivity): by 2020, there are 12 billion of IoT devices and endpoints globally.[33] Not including smartphones, laptop and tablets. All these devices will need real-time communication for their functions and to achieve this point massive scale is needed for all the devices, sensors and applications.

Considering the three features expected from 5G is it possible to summarize five pieces that together will grant the success of this leap:

- Speeds and Feeds. Speeds of up to 20 Gbps will be achieved using a combination of innovations such as carrier aggregation (CA), massive multiple input multiple output (MIMO) and quadrature amplitude modulation (QAM);
- Unlicensed spectrum: MNOs (Mobile Network Operators) are increasingly using unlicensed spectrum in the 2.4-5 GHz frequency bands. 5G has the potential to tap into a vast amount of spectrum available in these unlicensed bands to offload traffic in heavy congested areas and provide connectivity for billions of IoT devices. Advancements in Wi-Fi, LTE in Unlicensed spectrum (LTE-U), License Assisted Access (LAA), and MultFire provide better quality and regulated access to unlicensed spectrum;
- Internet of Things (IoT): IoT devices pose a diverse set f requirements and challenges for 5G networks. It's only fair that IoT should likewise pose a diverse set of solutions as well;
- Virtualization: Network functions virtualization (NFV) enables the massive scale and rapid elasticity that MNOs will require in their 5G networks. Virtualization enables a virtual evolved packet core (vEPC), centralized radio access network (C-RAN), mobile edge computing (MEC), and network slicing.

[33] Lueth, K.L. *State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time*. IoT Analytics, November 19, 2020. [Viewed the 3/12/2020].Available from: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/ .

- New Radio (NR): Although the other 5G innovations introduced in this section all have strong starting points in LTE Advanced Pro, 5G NR is a true 5G native technology that has yet to be standardized. 5G NR address the need for a new radio access technology that will enable access speeds up to 20 Gbps. [34]

That being said, finally to reduce the topic that can be expanded in many direction 5G has the three main scope (speed, responsiveness and scale) that defines why the technology is needed and what is expected to do to represent a solid next step in the ICT field. And is it possible also to pinpoint five fields that represent opportunities for industries and the how of 5G can became pivotal for evolution of our society. Speeds and Feeds, Unlicensed Spectrum, IoT, Virtualization and New Radio are all factors that can really tip the balance and open new opportunities either for the services provided and for the user experience.

5G Architecture

There are mainly two areas to cover in order to understand the functioning of 5G and the best-case scenario of a roll out: the physical infrastructure and the network one, or in other words the hardware and software of the technology.

[34] Lee, H. *Concept and Characteristics of 5G Mobile Communication Systems*. Hankyuon National university, January 15, 2015. [Viewed the 4/11/2020]. Available from: https://www.netmanias.com/en/post/blog/7109/5g-iot/concept-and-characteristics-of-5g-mobile-communication-systems-1 .

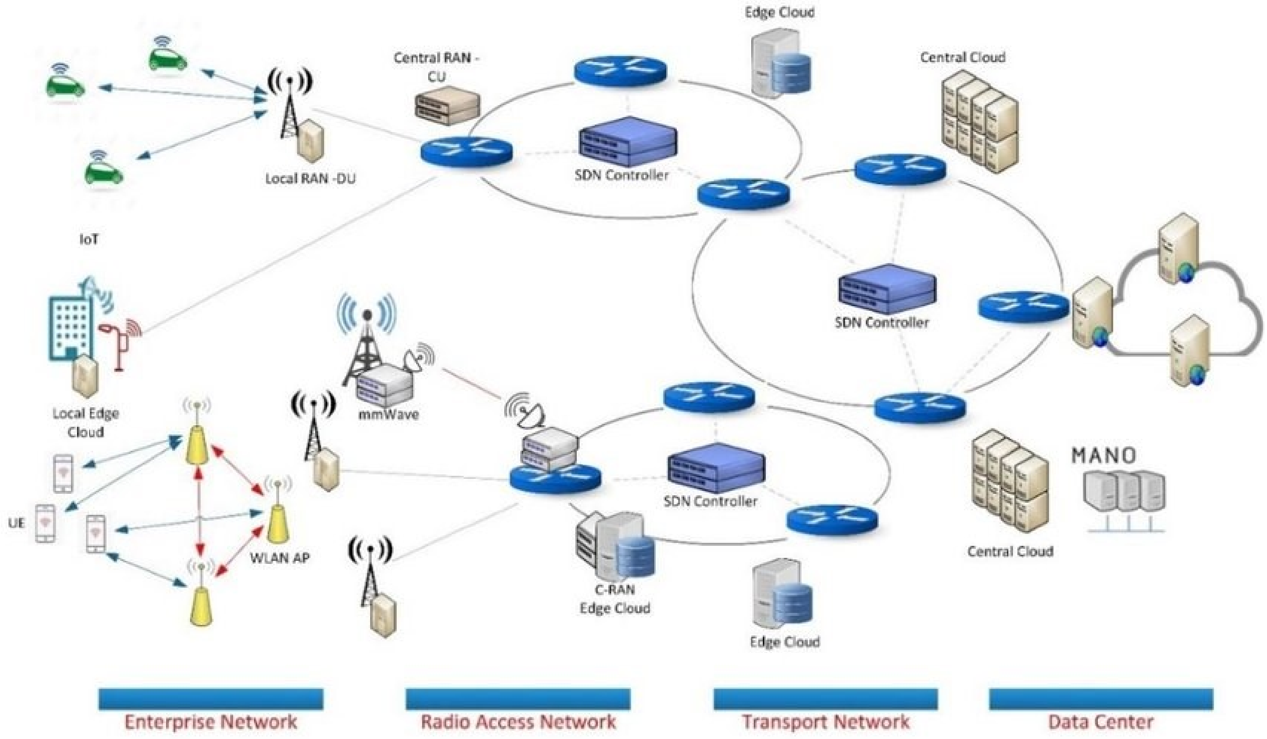

Figure 2: 5G Architecture from ENISA Threat landscape for 5G Networks, November 2019

Hardware: the entire ecosystem will rely of four areas, Data Center, Transport Network, Radio Access Network and Enterprise Network. Starting from the head the Data Center rely, as for previous and other uses, on Cloud Computing. Central Cloud are the core of any further development and represent the resource allocation storage and often the computational power of any process run on the network. Central Cloud is linked to the network and orchestrated by SDN (Software Defined Networking) controllers that enable the allocation of resources through Transport Network and until Edge Cloud interfaces and antennas. All the traffic so far is still by cable. SDN controller are key for the transport layer of the technology and are the connecting ring between central Cloud and Radio Access Network (RAN) that is the fundamental part of mobile network. RAN is assigned to two kind of cells, the 4G and 5G with different purposes. In fact, 4G technology either if surpassed still plays a role in the deployment of early 5G systems and maybe will continue to have a role in the overall architecture. 4G macro cells are necessary for continuous connection and ulterior insurance against data loss and connection errors but also to manage long communication thanks to 4G Sector antennas. In other words, 4G infrastructure will continue to hold the funnel of data flowing from micro and local 5G antennas and the RAN controller.[35] On the other side 5G cells will provide the already mentioned connection speed and coverture, micro cells will be needed in a pervasive way for the same

[35] EMF Explained 2.0. *5G Explained – How 5G Works*. [Viewed the 11/11/2020]. Available from: http://www.emfexplained.info/?ID=25916 .

nature of bandwidth used by the technology (in fact 5G uses micro-waves of the 24-100 MHz spectrum that are way more powerful but of short length and needed more repeaters). All these micro cells capturing and sending data will bounce to 5G Massive MIMO (Multiple Inputs Multiple Outputs) that are a new piece to introduce in the framework. MIMO is a technology designed to scale connection possibilities for end users and process a massive amount of data at the same time. Many micro elements are placed in a any physical case of the antenna allowing more people to connect to the device and on the same time connect to the network and maintain a high throughput. Finally, all these cells are the connection to Enterprise Networks relying either on Local Edge Cloud, WLAN or Local RAN (in this case especially for IoT functions).[36]

Software: the software architecture is way more complex and for sake of understanding was explained beforehand the hardware structure. Network Slicing, MANO, RAN, NFV, SDN, MEC. The prominent feature of 5G network is the complete virtualization of the core network, especially in the software side of the technology that is treated here is it possible to prove the edge that provides this function.

Virtualising means practically raise flexibility and portability for any networking system and service, build upon the already mentioned Central Cloud this feature relies heavily on Software Defined Network (SND) for a simpler management and Network Function Virtualization (NFV) to enable the communication technology to allocate network functions on different network components based on various necessities and standards (quote literally the paper pag.20). 5G's key feature is the possibility of network slicing. Network slicing is the possibility of use a single physical network as bedrock for multiple ones in accordance with particular cases. In this way thanks to 5G a user would be able to deploy a specific function only according to necessities and not requiring the entire infrastructure but relying only on one segment of the network. For instance, communication between autonomous cars requires minimal lag time but not high throughput (amount of data for the process), using slicing will be possible accommodate other services in the free zone of the network operated by this task.

Another important component of 5G infrastructure is Management and Network Orchestrator (MANO), all the NFV and Virtualised Infrastructure Management (VIM), Virtualised Network Functions (VNF) pass through MANO. Even if not a complete novelty in the sector, in 5G plays a key role for the weight and extension that virtualization has in the overall technology worth.

[36] 5G PPP Architecture Working Group. *View on 5G Architecture*. 2019. [Viewed the 11/11/2020]. Available from: https://5g-ppp.eu/5g-ppp-5g-architecture-wg-white-paper-rev-3-0-for-public-consultation/ .

Radio Access Network (RAN) is the protocol defined by 3GPP specifically for 5G functioning and describe how centralized unit and distribute unit will communicate. Besides RAN has the role to provide small-cell coverage for multiple operators "as a service" in two-tier architecture.

Software Defined Networks (SDN), while NFV focuses on optimising the network services SDN separates the control and forwarding planes of the software managing functions. SDN relies on multiplying controls over packet forwarding functionality inside the network, this function usually is united under a physical device but for the same nature of 5G a control divided in data plane and control plane have had implemented. In this way the difficulty of configuration and alteration of the control function of the network is reduced (no more under responsibility of the sole operating system) and also enables the implementation of more consistent control policies through fewer and uniformly accessible controllers.

Multi Access Edge Computing (MEC) is the provision of cloud computing capabilities at the edge of the network, in particular to end user application that thanks to high bandwidth and low latency will benefit of all the possibilities of the cloud wherever they are. MEC will allow users to have a possibility previously available only in run-time from their end user device.

Summarizing the overall 5G infrastructure put in place and to be deployed is it notable the hardware peculiarity of the new MIMO antennas and a more needed pervasive presence of repeaters (with shorter range but higher throughput and bandwidth) that will allow the wanted coverage for mobile devices. On the back end of the process the ever-present Cloud (central or edge) will be joined by SDN controller to maintain the backbone of the service and allow a optimized management of every process. The entire hardware of physical layer of 5G can be divided in Storage, Computing and Networking. On the other side, the software is way more complicate to sum up with a strong virtualization infrastructure orchestrated by MANO and composed by NFV and SDN that allow network slicing and better allocation of network resources while RAN, RAT and MEC are involved in the management of sessions, connections, communication and proper functioning of the protocols. 5G is the nexus of all these components and the results are the starting premises and performance granted. [37]

[37] ENISA, "*ENISA Threat landscape for 5G Networks*", November 2019, p. 16-45;

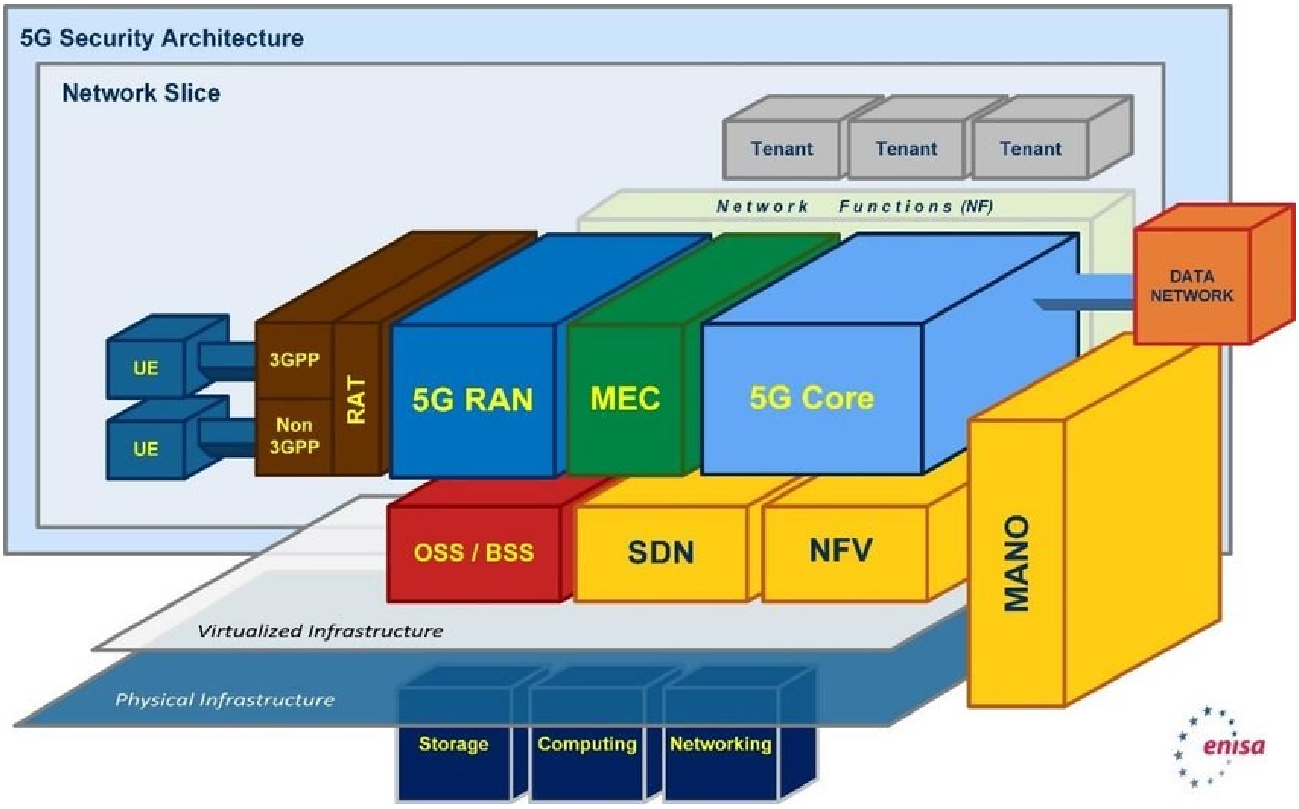

Figure 3: 5G Security Architecture from 5G Architecture from ENISA Threat landscape for 5G Networks, November 2019

Second Part

Structure of the Cases

This part will be characterised by the display of particularly significative threat posed by the adoption of the new technology in the European Union case. The framework used will be as previously said the CIIP, that follow five main points in its assessment. First, the definition of critical sector. This part was already explained in length in the previous chapter (5G architecture) where all the critical part of the infrastructure was analysed and overviewed. The following threat analysis will be based upon the consideration of only those assets and components. Every single part of the architecture is critical on its own and can cause massive damage to the whole, hence, the protection has to be considered indistinctly for any components and asset of 5G technology. The second point has to introduce CIIP initiatives in the selected structure (in this case the EU) and what was done to handle the and prevent any harm to the critical information infrastructure. The European Union since 2009 demonstrated a steady interest for the CIIP framework and the potentialities that can demonstrate for management and prevention. In 2009 the Commission of European Communities released a communication to set the stage for further enhancements of the European coordination in cybersecurity and protection of critical information infrastructures.[38] In 2015 these recommendations where formalised by the OECD in a paper for digital economy best practices[39] with the clear scope of widening the security environment with a bottom-up approach that solidify companies and rise resilience of the network. In 2016 two other papers were disseminated by ENISA, the first with a comprehensive state of the work of all European state members. With all leading authorities, organization in place, management structures and roles and responsibilities for the CIIP governance.[40] And the second with a set of good practices, findings and CIIP governance profiles especially designed for policy making purposes and building a better knowledge of the criticalities of cybersecurity.[41] The third, fourth and fifth points of the CIIP framework can be all dealt together in this case because are all regarding the activity of ENISA organization that is practically the only authority entrusted of the cybersecurity of the union, hence, also its organizational structure, early warning mechanism and law and legislation. ENISA with the 2019 Cybersecurity Act of the European Union was confirmed in the role of cybersecurity authority, with more resources and more task also, especially the formulation of a certification scheme for network components and services but also the new task of secretariat of the national CSIRTs (Computer Security Incidents Response Teams).[42] The CSIRTs were introduced with the NIS directive (Security of Network and Information Systems),[43] the first legally binding policy about cybersecurity in Europe. CSIRTs were specifically designed and activated to respond to cyber threats and attacks with risk management, incident responding and work alongside CERTs (Computer Emergency Response

[38] Commission of the European Communities. *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*. Brussels 30/03/2009. {SEC(2009) 399}, {SEC(2009) 400}. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149 .

[39] OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en .

[40] ENISA. *CIIP Governance in the European Union Member States*. 2016. [Viewed the 23/11/2020]. Available from: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/ciip-governance-in-the-eu-annex .

[41] ENISA. *Stocktaking, Analysis and Recommendations on the Protection of CIIs*. 2016. [Viewed the 23/11/2020]. Available from: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis .

[42] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). [Viewed the 11/11/2020]. Available from: https://eur-lex.europa.eu/eli/reg/2019/881/oj .

[43] European Commission. *The Directive on security of network and information systems (NIS Directive)*. [Viewed the 11/11/2020]. Available from: https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive .

Teams).[44] Pivotal is, in fact, to coordinate all these actors in this way building a trusted and solid environment capable to face cyber threats and counter or react to attacks, shortages and malfunctions.[45] Another important actor in this organization are ISACs (Information Sharing and Analysis Centers) that work more on collection of information about cyber threats and critical infrastructures and is fundamental for knowledge sharing and analysis capabilities among union members and different organizations.[46] Finally, regarding the last point of the CIIP framework, law and legislation in place, the EU was particularly attentive toward cyber threats and the new challenges of the network and in 2019 adopted the Cyber Security Act that poses a new milestone for cooperation and clarify roles and responsibilities of members and concretize the role of ENISA and a certification authority.[47] Another important policy paper, in the end, was the recommendation for 5G network security of 2019 May.[48]

That being said, in the following continuation of the second part of the paper four main threat will be probed and analysed, with a final part in which will be summarized conclusions, some limited recommendations and challenges for the future of the 5G technology. Every case will be introduced and contextualized with practical applications, enriched with an inspection of criticalities posed by the threat in our framework and finally discussed for a proposed mitigation and possible remediation to apply. It is central to state in this instance that any threat will not be delved too deep in technical details, because as said in the introduction this is not the scope of the paper, but on the contrary will be presented with a large scope that aim to give a grasp of the situation and can be a useful tool for reducing the gaps of knowledge at high level, pointing out the fields that need more attention at governmental and organization level. A final specification has to be made upon the definition of assets. The following threats affecting the critical information infrastructure are not aimed at the whole network, but usually try to compromise a certain asset, that can be described as ICT component like: hardware, software

[44] ENISA. *ENISA's contribution to the Critical Information Infrastructure protection (CIIP)*. 2017. [Viewed the 11/11/2020]. Available from: https://www.enisa.europa.eu/publications/ed-speeches/enisas-contribution-to-ciip .

[45] ENISA. *Baseline Capabilities of National/Governmental CERTs*. 2012. [Viewed the 11/11/2020]. Available from: https://www.enisa.europa.eu/publications/updated-recommendations-2012/at_download/fullReport .

[46] ENISA*. Information Sharing and Analysis Centers* (ISACs). [Viewed the 11/11/2020]. Available from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing .

[47] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). [Viewed the 12/11/2020]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC .

[48] Raccomandazione (UE) 2019/534 della Commissione, del 26 marzo 2019, Cibersicurezza delle reti 5G. [Viewed the 12/11/2020]. Available from: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32019H0534 .

and communication components; communication links between them; data responsible for the system functioning, consumed or produced by it; physical infrastructure used by the 5G system; the human agents interacting with the system.[49] The four cases analysed are:

1. Threats to the infrastructure;
2. Threats to IoT;
3. Threats to the Core Network;
4. Threats to access, virtualization and multi-edge computing technologies.

Threats to the Infrastructure

The first threat that comes in mind when discussing networks is the security of its own infrastructure, the backbone of the technology. It is natural because is the basis of the service and still and probably will always be a weak point. Physical disruption of the service can't be managed in different ways as the present common best practices suggest, but in the 5G case a more granular and specific focus has to be devoted toward, for instance, the MIMO cell towers and the presence of repeaters in a wide and large area that has to be covered by the service. However, risks envisaged by the infrastructure are not only barely physical, like damages to the grid, to antennas or other shortages, but can be understood also as flaws of the general design and other faults that can be avoided with careful planning and management. In this category is worth to consider sabotage of network infrastructure, like the ones to radio access, edge servers and jamming (all aspects incredibly sensible for the extensive desired coverage of the service), but also is fundamental to bring into the spotlights the aspects of design faults, cardinal for the Huawei quarrel for example,[50] that heavily involves the suspect of backdoors and other design gaps that can cripple the entire security frame of the network.[51]

Starting from the most remote threat, in terms of distance and time can be the best approach. Thus, a possible compromised supply chain, vendor or service provider. This specific threat is considered as an intentional tampering or specific design of hidden systems into hardware

[49] ENISA. *ENISA Threat Landscape for 5G Networks: Threat assessment for the fifth generation of mobile telecommunications networks (5G)*. 2019. Available from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks .

[50] Reichert, C. *US finds Huawei has backdoor access to mobile networks globally, report says*. CNET. Feb. 12, 2020. [Viewed the 21/11/2020]. Available from: https://www.cnet.com/news/us-finds-huawei-has-backdoor-access-to-mobile-networks-globally-report-says/#:~:text=Chinese%20tech%20giant%20Huawei%20can,reported%20Tuesday%2C%20citing%20US%20officials.

[51] Bartock, M.; Cichonski, J.; Souppaya, M. *5G Cybersecurity: Preparing a Secure Evolution to 5G*. National Institute of Standards and Technology. April 2020. Pp. 5-12.

material used for 5G deployment and functioning. Usually referred as a "backdoor" this type of manipulation aims at acquiring control or have privileged entry point or control mode in a specific device or software.[52] Are extremely dangerous because if not previously noticed can be used as a way to bypass controls, authentication and encryption, practically disarming any security measure in place. Backdoors have the specific purpose to neutralize security measures and have a ready to use way to act on the asset without permissions. In the 5G case the device that will be interested by a vendor or provider are. From the MIMO antennas, to the micro cells and the RAN controller, a backdoor in any of these devices will impact massively the security of the network, putting in jeopardy the entire ecosystem. For instance, a backdoor in a MIMO antenna could be used either to syphon data outside the network without permission, but also transmitting malicious code to mobile devices, infecting a huge number of those. Backdoors have impact on all three field of cybersecurity, affecting availability, confidentiality and integrity. Considering another example, IoT and domotics will be and are widely available in homes, offices and industries. With the threat of backdoor in any of those devices, like a smart plug, a camera, a stereo or anything else, and with the connection granted by 5G will be practically possible to have a breach in any place and a malicious insertion tunnel everywhere.[53]

Backdoors can be used as main container of many different threats stemming from manipulation of hardware equipment, to exploitation of existing vulnerabilities and exploitation of flaws in security, management and operational procedure or also user equipment already compromised. The threat of concealed hardware or software components in a product provided for the functioning of the 5G network, either in an initial stage or during maintenance or updates/features, can have a terrible impact on the security of the overall architecture and give the consequent opportunity of exploitation. For instance, a well-placed and hidden vulnerability in a micro-cell can enable the remote use or control of the device by an unauthorized actor with administration privileges. The incorrect distribution of privileges is a big issue for security and can result in cascade effect damages, with the compromising of any guarantee of availability, confidentiality and integrity. Exploitation of a backdoor can happen either thanks to software and hardware vulnerabilities, unknown to the vendor and user, or even a well-known flaw by the attacker. In such cases the attacker can use flaws like

[52] Malwarebytes. *Backdoor computing attacks*. [Viewed the 21/11/2020]. Available from: https://www.malwarebytes.com/backdoor/ .

[53] Lewis, T.G. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Third Edition 2020 John Wiley & Sons, inc. Hoboken, USA. Pp.110-121.

meltdown, spectre and buffer overflow or also use old pieces, technologies or protocols embedded to leverage against new components working in the same device.[54]

Flaws in security, management and operational procedures are not specifically related to the 5G network but can be well connected to a backdoor or infrastructural breach. In this case, in fact, is it assumed the management of a complex scenario with many components and organization working together to grant the service. Configuration, update and patch management of the software can be utilized by a threat actor and leveraged to undermine operational and security procedures useful to the functioning of the system, compromising the integrity and availability of the network.

For this reason, an accurate inspection and evaluation of providers and vendors is highly recommended. 5G will have the characteristic to multiply the possible weak points of insertion and hugely widen the surface of attack. The Huawei case was particularly discussed in the last years mainly for the low level of trust internationally put on the Chinese government and its connection with the private sector (in this case the tech giant LTE Huawei that tried to dissociate from the government in order to abide to international standards and promote a security framework said to be particularly strict).[55] Moving on this international case that have many strategical aspects but also more cogent and technical is important to state for sake of justice that any government and organization have the interest to have an edge on new technology and surveillance in general. As deeply studied by Shoshana Zuboff data and in general telecommunication will be the field on present and future international competition, and considering this is only natural to be concerned by foreign interests but also try to maintain the actual structure of the global market based on regulation and standards.[56] To be completely fair, in the global power competition the edge over surveillance and "capabilities" over homeland assets is already a long story and the USA were the first to implement backdoor measures and a "Golden Power" rule over its own ISP. A pivotal example is the sanction imposed over Iran in 2012 under Obama administration that required the favourable vote of many "untapped" members of Security Council of UN. In that case the NSA (National Security Agency) used for the first time the "Homeland Act" (Control the source and name) to wiretap AT&T internet hub and spy over Gabon, and other countries that were necessary to win the vote and

[54] ENISA. *ENISA Threat Landscape for 5G Networks: Threat assessment for the fifth generation of mobile telecommunications networks (5G*). 2019. Pp. 61-63.
[55] Huawei. *Huawei's Security Standards and Certification*. Huawei technologies Co., Ltd. 2020. [Viewed the 21/11/2020]. Available from: https://www.huawei.com/it/trust-center/transparency/standard-certification .
[56] Zuboff, S. *The Age of Surveillance Capitalism*. Profile Books LTD, London 2019. Pp. 3-21;

bypass a possible veto. The operation was so successful because all the traffic interceptor through the embassies in US soil was analysed and transformed in reports for the white house, reports capable of shift the countries opinion over the matter.[57] That is to be said for a more objective and realistic perception of what is at stakes when it comes to 5G competition in European soil, in this case any possible foreign retailer, vendor or provider has to be carefully inspected if a strategic and national sovereignty has to be maintained.

The other aspect considered here about threat on physical/infrastructure security is the material disruption of signal (radio wave) either by antennas sabotage or signal sabotage. It is not meant to be discussed further possible disruption at the infrastructure, specially cabled or core because will be outside the scope of the paper and the possible cases are multiple; from terrorism to vandalism and any physical damage to the upper grid that are present in our networks by the onset of ICT technology. In 5G networks the same new structure of microwave communication will bring on the scene new threats. The main assets in microwave and short length transmission are MIMO and Micro cells. The first will be responsible of Massive Input of data and Massive Output connecting all the micro cells and IoT/mobile devices to the backbone of the service. The least will grant with their ubiquitous presence in the urban fabric a short and powerful means that can support 20 Gbps of speed over a bandwidth between 24 to 100 GHz.[58] But while a damage to one of the many Micro cells needed is probably not detrimental of the entire service, but will pose only a decreasing in performances, a damage to MIMO cells, will pose a critical risk for its beamforming properties.[59]

DoS (Denial of Service) is probably the main culprit to possible signal problem to the infrastructure of 5G technology but considering the overwhelmingly majority of mobile devices connected and for which the system is designed this threat will be considered further on in the IoT chapter, altogether the more specific DDoS (Distributed Denial of Service) that is may more dangerous for the critical information infrastructure.

[57] Buchanan, B. *The Hacker and the State*. Harvard University Press, London 2020, p. 2-20;

[58] Boccardi, F.; Heath, R.; Lozano, A.; Marzetta, T.; Popovski, P. *Five Disruptive Technology Directions for 5G*. 2013. Communications Magazine, IEEE. 52. 10.1109/MCOM.2014.6736746.

[59] Masterson, C. *Massive MIMO and Beamformin: The Signal processing Behind the 5G Buzzwords*. AnalogDialogue, vol.51. June 2017. [Viewed the 21/11/2020]. Available from: https://www.analog.com/en/analog-dialogue/articles/massive-mimo-and-beamforming-the-signal-processing-behind-the-5g-buzzwords.html# .

Threats to IoT

The risks behind Internet of Things are probably the most commonly addressed while focusing on the dangerous environment of 5G nexus. For instance, usually the ubiquitous connectivity of IoT devices capable of autonomous communication is portrayed as a major challenge for daily security in modern cities, and indeed it is in some ways. Autonomous vehicles with interconnected traffic lights and other road signals, the presence of a number of devices in homes and offices capable of recording video, audio and other signals, and a range of other interconnected services that the 5G network will allow raised widespread preoccupations. All the threats connected to IoT are in some ways connected also to the devices which will benefit and use the wireless services and thus is better to say that in our service-line from the Data centre to the user (end-to-end) this category of threats is related to the last and more close to the user aspects. Exactly for this reason is it possible to enumerate a series of threat related to confidentiality field, like: (Abuse of lawful interception function, abuse of user authentication/authorization data, fraud scenarios, lateral movement, fraudulent usage of shared resources, traffic sniffing). Unfortunately, the major flaw in all the IoT environment is the limited nature of the devices (except for larger device like cars that can depend on a large hardware) and especially all relative to domotics that usually suffer of limited hardware and computational ability, various kind of transmission technology and lack of basic components security often. In this regard it is possible to consider all this range of device vulnerable to malicious activity and for the sake of critical infrastructure safety will be necessary prevent an upstream mechanism. Devices could be victims of IoT botnets (for instance the 2016 Mirai malware)[60] capable of corrupt many systems to use as "bots" and act simultaneously thanks to the presence of a Command and Control (C2) resource to coordinate a wide range of malicious activity and especially a DDoS attack. In other words, a threat actor could slit between the weak security mechanism in place among the domotic devices and spread laterally thanks to the connectivity. Once formed a network of IoT devices corrupted the same actor responsible for the infection could use this botnet to launch a number of attacks and of course a distributed denial of service, leveraging on the number of devices flooding the network with requests.[61]

[60] Cloudflare. *Inside the infamous Mirai IoT Botnet: A Retrospective Analysis*. [Viewed the 21/11/2020]. Available from: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ .

[61] Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. *5G security: Analysis of threats and solutions*. 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, 2017, pp. 193-199, doi: 10.1109/CSCN.2017.8088621.

A DDoS is probably the main concern regarding IoT in the present case, a flooding attack, can slow down and paralyze the receiving cells/antennas and interrupt the service either for a long time or only in order to open up a breach for further exploitation. As a definition DoS can be categorized as a actively damaging activity aimed at interrupting a communication service in the 5G case a network service.[62] The type of attack is simple and for this reason still lethal in many ways, saturation of the bandwidth with a massive number of requests of with huge traffic that overwhelm the capabilities of the infrastructure. This flooding makes unavailable the service for users or can cause a disruption of performance. Considering the threat field under the scope, Infrastructure and physical security, DoS can be affecting the more fragile nodes of the network, for instance the already mentioned MIMO and broadband or Microcells that compose the backbone of the wireless service. The DoS threat for those assets has to be regarded as collection or interception of signals (passive stance) from the antennas that in a certain amount can be detrimental for the correct functioning of the system. The flooding of the target with illegitimate service request, usually made with the use of false IP address, prevent the user identification, when the server processing all the information is overwhelmed, the service start to slow down and crash. In this case is it safe to consider the service disrupted and the DoS attack successful.[63]

Threats to Core Network

In this section is considered a wide range of threats that could affect the core network of the critical information infrastructure and compromise the overall integrity, availability and confidentiality of the 5G network. First of all, it is necessary to introduce Application Programming Interface (API) that are a core function of the system and help to manage the various software and defines interactions between them. As is expected without APIs is impossible to operate such a rich and heterogeneous environment as the 5G one and in fact many functions are entrusted to open-source APIs. The possible threat of having a one compromised API in the 5G core can pose a serious risk and jeopardize the communication and logic connection between components. A threat actor can exploit this vulnerability targeting API responsible for network function, internetworking interfaces, roaming interfaces and so

[62] Future Learn. *DoS and DDoS attacks*. [Viewed the 21/11/2020]. Available from: https://www.futurelearn.com/info/courses/teaching-cybersecurity/0/steps/57188 .

[63] Crowdstrike. *What are Denial-of-Service (DOS) Attacks*? November 12, 2020. [Viewed the 3/11/2020]. Available from: https://www.crowdstrike.com/epp-101/denial-of-service-dos-attacks/?utm_campaign=dsa&utm_content=seu&utm_medium=sem&utm_source=goog&utm_term=&gclid=CjwKCAiA_Kz-BRAJEiwAhJNY7yZriA-QxP4QD6wx0IZ2R8KBHWEPB560oLdZt4uhGy81HL1MKAZf8xoC_VEQAvD_BwE .

on, exposing different layers of the network.[64] Another consistent threat to consider is "Memory Scraping" that is particularly dangerous for SDN controller, an already mentioned critical part of 5G functioning. Usually, a memory scaring malware is designed to collect sensible information from a software component, besides was noted that mainly affect SDN application servers. A core dump of an SDN controller can be a real damage for the system because can be exploited furthermore to trigger a reboot procedure and affect with a coordinated effort the boot procedure of the software.[65] The result can be the extraction of sensible SDN data, particularly important for many API rules. Many different layers of the network also can be interested by an unauthorized "traffic sniffing" that is one of the most common and used method to extract information from a network. Sniffing is the translation of eavesdropping, and like it is the method used to intercept valuable data from a network element. In 5G networks there are many entry points for such an activity, from the SDN controller, to network function, edge node, virtualization orchestrator, possibly any component is vulnerable to interception of some kind of information transmitted or passing through it. Data such as, confidential information, system time, subscriber location and many subscriber/user/organisation data can be tracked and extracted by a malicious actor.[66]

Threats to Access, Virtualization and Multi Edge Computing Technologies

These types of threats are related more to the internal structure of the network and pose a concrete challenge for the incoming implementations into the already working 4G LTE system. Virtualization is one of the most important components of the technology, forming the backbone of slicing and a huge amount of service types. The same nature of virtualization, relying on cloud can be a vector of threat for the infrastructure, in fact, if compromised even a small part of the cloud or the sliced resource can become a risk for the whole.[67] It comes logical to assume that a network used by different tenants has to be secured by illicit traffic that ingress and egress from the slice or part of the cloud. On the other side Multi Edge Computing (MEC) is

[64] ENISA. *ENISA Threat Landscape for 5G Networks: Threat assessment for the fifth generation of mobile telecommunications networks (5G*). 2019. Pp. 55-57.

[65] API Crazy. *Security Best Practice for Protecting Against Memory Scraping Malware in Target & Home Depot*. September 25, 2014. [Viewed the 22/11/2020]. Available from: https://apicrazy.com/2014/09/25/security-best-practice-for-protecting-against-memory-scraping-malware-in-target-home-depot/ .

[66] Lichtman, M.; Rao, R.; Marojevic, V.; Reed, J.; Piqueras J. R. (2018). *5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation*. 1-6. 10.1109/ICCW.2018.8403769.

[67] Ivezic, M. *Unlocking the Future – Why Virtualization Is the Key to 5G*. 5g.security, March 21, 2020. [Viewed the 24/11/2020]. Available from: https://5g.security/5g/virtualization-key-5g/#:~:text=5G%20network%20virtualization%20will%20permit,network%20functions%20virtualization%20(NFV).&text=This%20architecture%20introduces%20the%20possibility,top%20of%20shared%20physical%20infrastructure. .

a novel approach of 5G technology that try to bridge the gap of services for mobile user experience. Doing this is achieved with the provision of Cloud computing capabilities directly at the edge of the network, basing this service on third parties offering their processing and storage capabilities to use for the overall network. MEC will grant high bandwidth and low latency for end user application and is one of the cardinal tenets of the 5G technology. However, these "hotspots" are also a possible entry point for edge node overload or man-in-the-middle attack that base their activity on this hardware. Access network threats are all related to the faculty for the attacker to penetrate a determined component of the network and compromise a "ring" of the chain. The most common and dangerous for 5G networks are: ARP poisoning; IMSI catching attacks; MAC spoofing.

Starting from ARP poisoning that is a common technique used since the dawn of internet era and that consist in an interception of a MAC address and the association with a different user's IP. Switching IP address cause the diversion of the traffic from the legitimate user to another one and then a communication hijacking. Considering the number of devices operating in 5G environment this threat based on an essential protocol (the ARP, Address Resolution Protocol) is particularly pressing.[68] Association of IP addresses has to be maintained scrupulously in order to preserve the integrity of the network. On a similar page but with different connotation is IMSI catching attacks. Capturing traffic between a mobile device and its paging protocols a malicious actor can associate with the victim's identity and gain sensible information about it.[69] Finally the MAC spoofing attack has the similar pattern to rely on a MAC address vulnerability and practically mask or change a target MAC address with another (or also a NIC Network Interface Controller). However, change a MAC address is usually impossible because embedded into the driver, hence, the favourite technique is the masking, the real "spoofing". The result of such an attack is that the identity is stolen and can be used to perform a various array of attacks into the network. All these techniques can be considered as hijacking in various forms, of session and identity for the most and are problematic in a highly connected environment that entails IoT elements, edge computing, Cloud and various ICT components.[70]

[68] Rahman, F.M.A.; Kamal, P. *A Holistic Approach to ARP Poisoning and Countermeasures by Using Practical Examples and Paradigm.* International Journal of Advancements in Technology. ISSN 0976-4860.

[69] Fong, M. *Protecting High-Level Personnel from IMSI Catchers*. Security magazine, February 21, 2020. [Viewed the 2/12/2020]. Available from: https://www.securitymagazine.com/articles/91767-protecting-high-level-personnel-from-imsi-catchers .

[70] ENISA. *ENISA Threat Landscape for 5G Networks: Threat assessment for the fifth generation of mobile telecommunications networks (5G*). 2019. Pp. 59-62.

Recommendations

This brief chapter is devoted to recommendations and possible mitigation or prevention for the threats that were unfolded before. There are plenty of singular solutions, techniques and best practices that are constantly formulated and updated for this common issue, old problems sometimes have old solutions and other times none, it is a very murky field where interconnections could be discovered years after the inquiry of a vulnerability or specific malware. Anyway, for the four threat areas that were probed here will be proposed some limited solution available in the large ocean of possible.

The infrastructure of 5G could be greatly affected by backdoors, signal disruption alongside DoS (and DDoS with the contribution of IoT devices). Starting from the DoS threat it is not an easy task to formalize prevention of such a widespread and old but stubborn vulnerability in common networks, however here is proposed a general line that can be helpful in order to avoid massive damage and service disruption for 5G network. It was identified the target of such a threat, made of basically antennas and repeaters that intercept wireless traffic and tether it through the network till the servers. The overload of incoming traffic is the main cause of this type of attack, hence, a first defence should be interposed between source of the traffic and destination. Looking at the structure of the 5G system, heavily relying on Cloud and virtualization, the first line of defence should be Attack Detection granted by Cloud Service.[71] Once reduced the surface of attack, other measures can be IP's filters that automatically blocks a certain serial numbers and rate limiting (problematic for the same nature of the network). Limiting the rate, in fact, is a common measure that reduce the available traffic for a Network Interface Controller (NIC) and can be implemented either in hardware or software but the main issue in the 5G case is the same necessity to have a continuous and not reduced constant traffic in and out of the cells. All the cells involved in the wireless network should work on their specific scale (microcells on hundreds of requests while MIMO antennas on thousands/hundreds of thousands "search for available data") and for this reason a thorough analysis of the traffic can help to avoid massive or not normal amount of traffic but on the other hand this measure limit also the possibility of scaling the available services and general possibilities of the technology. Other measures to counter DoS are those provided by Cloud

[71] Weiss, A. *How to Prevent DoS Attacks*. eSecurityPlanet, July 3, 2012. [Viewed the 2/12/2020]. Available from: https://www.esecurityplanet.com/networks/how-to-prevent-dos-attacks/ .

services (like *Amazon Shield* or *Cloudflare*) that offer a DMZ or "mitigation centers" that filter the incoming traffic, detecting the legitimate.[72]

On the backdoor issue side, the solution or mitigation is way more complex. In case of embedded backdoor, either hardware or software the maybe obvious solution is an accurate evaluation of every device and asset that will compose the system network infrastructure. Scrupulous scrutiny has to be undertaken in order to avoid the more manifest and predictable vulnerabilities. A "zero thrust" model can be useful to approach any implementation and grant the best outcome during the rolling out.[73] Zero thrust is meant as a way of analysing everything that concerns the system as possibly malicious or damaging, nothing and no one can be trusted and, in this way, the best standard of security can be implemented. After the implementation of devices of pieces of software monitoring should also be considered. In fact, monitoring a given piece of the system and all the processes that are done by it is a common way to find breaches and backdoors. General best practices involves also using multiple vendors and providers of piece of equipment, installing open source software that can be analysed by the community and often prevent many threats (knowledge sharing), scanning for known backdoors, checking software integrity signatures and monitoring suspicious traffic passing through the piece of equipment. [74]

Prevent threat from IoT without taking into account the safety of the devices is possible only raising the ladder and blocking any possible flooding at the first dam available, in our critical infrastructure framework, micro-cells and MIMO antennas. Thus, the DoS remediation remain a good point of resilience, underpinned by DMZ (Demilitarized zones), reduction of traffic and IP firewall. However in general terms is possible to minimize the surface of vulnerability thanks to few recommendations like: inspection and classification of the private network, in terms of all devices attached to that; virtually separate all IoT devices, either from the rest of the network

[72] Okta. *How to mitigate DoS attacks*. [Viewed the 5/11/2020] Available from: https://developer.okta.com/books/api-security/dos/how/ ;

[73] Carder, J. *What is the Zero Trust Model of Cybersecurity, Really?* LogRhythm, October 1, 2020. [Viewed the 13/12/2020]. Available from: https://logrhythm.com/blog/what-is-the-zero-trust-model-for-cybersecurity/ .

[74] Lewis, N. *Locking the backdoor: Reducing the risk of unauthorized system access*. Searchsecurity. [Viewed the 22/11/2020]. Available from: https://searchsecurity.techtarget.com/tip/Locking-the-backdoor-Reducing-the-risk-of-unauthorized-system-access#:~:text=There%20are%20many%20steps%20IT,both%20known%20and%20unknown%20backdoors.&text=Using%20multiple%20vendors%20to%20limit,Installing%20open%20source%20software ;

and from the device to the application; and finally monitor constantly the network and search for compromised devices while implement quarantine policy enforcement.[75]

Core, access, virtualization and multi-edge computing threats are very much related to infrastructure and IoT security but is it possible to connect some more aspects of prevention to the discussion. Isolation of application is warmly suggested, especially relying on the major technology of slicing, there each application flow will get is own slide of the network and in such a way can be better protected. Also "Small Cells-as a- Service", could greatly improve the resilience of MEC, SDN, NFV technologies.[76] Application layer can be possibly secured thanks to the SSL/TLS session-aware user authentication or Delayed password Disclosure (DPD), Password Protection Module (PPM) and secure tunnelled authentication protocols.[77]

Considerations and Conclusion

The chapters of this paper followed a stream stemming from the historical root of the ICT field and the development of internet, to the structure and challenges of the 5G technology revolution and till the major threat that are possibly envisaged by the deployment of the new infrastructure. All the chapters were relevant to deploy a straightforward analysis based on the Critical Information Infrastructure Protection (CIIP) that put on the centre a core element that has to be defended from any kind of incoming and prospective menace.[78] The main object of the analysis was the 5G infrastructure, projected in a close future scenario where all the relevant elements of the deployed technology will have a pivotal importance for the European security. Thus, the entire 5G infrastructure was considered as a Critical Information Infrastructure to be protected and explored in all the relevant aspects. The five focal point of the CIIP framework were unfolded in the proper way following the definition of critical sectors, past and present CIIP initiatives and policy, organizational structures, early warning and public outreach and law

[75] Forescout. *Reducing Risks from IoT Devices in an Increasingly Connected World*. Forescout Technologies, Inc. 2020. Available from: https://www.forescout.com/company/resources/reducing-risks-from-iot-devices-in-an-increasingly-connected-world/ .

[76] Vassilakis, V.; Chochliouros, I.; Spiliopoulou, A.; Sfakianakis, E.; Belesioti, M.; Bompetsis, N.; Wilson, M.; Turyagyenda, C.; Dardamanis, A. (2016). *Security Analysis of Mobile Edge Computing in Virtualized Small Cell Networks*. 475. 653-665. 10.1007/978-3-319-44944-9_58.

[77] UKDiss.com. *Sniffing Attacks Prevention and Detection Techniques*. 12th December 2019. [Viewed the 21/11/2020]. Available from: https://ukdiss.com/examples/sniffing-attacks.php ;

[78] Brechbühl ,H.; Bruce ,R.; Dynes, S.; Johnson, M.E. (2010). *Protecting Critical Information Infrastructure: Developing Cybersecurity Policy*. Information Technology for Development
Vol. 16, No. 1, January 2010, 83–91. Taylor & Francis Group. 16:1, 83-91, DOI: 10.1002/itdj.20096 .

and legislation.[79] Even if the CIIP framework was not updated since 2012 the ENISA organization carried on a great work of standardization and production of paper regarding cybersecurity and defence of critical infrastructure. The relevance of the topic, and the criticality posed by the information infrastructure safety was underlined first by the historical evolution of the ICT field, where the twofold development of technologies (from the ARPANET network to LAN and so on) and threats and vectors of risks was functional for a better framing of the 5G environment and what is really at stake with the ever evolving threat scenario.

In order to achieve a better grasp of the 5G technology, the second chapter of the paper was devoted to the technical aspect of the network, the main components, hardware and software involved in the functioning of the technology and implication necessary to shed light over this sometime confusing matter. It is possible to say, in fact, that 5G was generally overrated and underrated on the same level during the past years and in the various general discussions about technology, communication and cybersecurity. Like on every technical breakthrough (because it is indeed out of discussion that 5G is a revolutionary step in the ICT but also for human society, from Industry 4.0 to Smart Cities and everyday life of people) pragmatists pledged their support in every aspect concerning this evolution, stressing all the pros of a faster and overall better network, capable to breach a previously technical gap and enable new features (like diffused IoT and Virtualization, new services and so on); while more doubtful parties were concerned about privacy, various security threats and baseless health possible problems (not to mention other conspiracy theories).[80] However, this is not the instance to debunk all possible doubt about 5G nor a paper focused on a strong position against or pro it. For sure it can be said that luddite positions are out of time and the only possible discussion in the present era can be built around the new cybersecurity threat and global competition raised from the rolling out of 5G. The disruption of information infrastructure in Europe was considered the main subject to protect and there is no need probably to further discuss why, hardly will came to mind another field where a disruption could be more fatal for economy and general conditions. The importance of the ICT sector for EU is underlined by the funding put at disposition for the members, counted in more than €20 billion for extending high-speed network coverage, developing ICT products and services and strengthening ICT application to all e-fields

[79] Abele-Wigert, I.; Dunn, M. *The International Critical Information Infrastructure Protection (CIIP) Handbook 2006*. Enisa Quarterly, June 2006. Pp. 4-5.

[80] Wheeler, T.; Simpson, D. *Why 5G requires new approaches to cybersecurity: Racing to protect the most important network of the 21st century*. Brookings. Tuesday, September 3, 2019. [Viewed the 21/12/2020]. Available from: https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/ .

(government, learning, health, culture).[81] Starting from this point of Critical Information Infrastructure Protection was unfolded a series of threats that could affect various components of the network and how those could result in damages of a more or less importance. Infrastructure, Core, IoT and Multi-Edge and Access threats were all channelled to explain the most prominent risk that emerged from the deployment of 5G networks, however this paper is far from exhaustive. The network and the ICT infrastructure are by themselves, nowadays, the most entangled and tentacular system ever designed by humankind, it is only possible to try to grasp the magnitude of the change that are inbound. Every day there are more threats, new malicious piece of code, new exploits, new vulnerabilities found and from government to organizations and firms all together struggle in this quicksand. As the last *SolarWinds* hack is showing us,[82] but following a long trail of destructive hacking like the *NotPetya* case in Ukraine and many other it is practically impossible to separate cyber threats from everyday life, and especially politics and infrastructures.[83] Looking at the European situation is impossible to avoid the confrontation with cyber vulnerabilities, from one side for the relevance of the region, and from the other for the same political framework (the Union) that enhance cooperation among members but allows also infiltrations and mismanagement (the most prominent concern is relative to the so called patchwork effect, where any country led a separate politics into security matters).[84] The CIIP framework is capable to bridge this gap and connect the policy needed field to the technical aspect of the information technology, the following recommendation will help to avoid fatal issues and build a better environment capable to sustain the development of ICT filed. Europe has to be considered a whole, with the same criticalities and as stressed by ENISA and many other organizations the main aspects to enhance are:

- Promote bridges between all stakeholders;
- Contribute to the knowledge collection/dissemination;
- Disseminate 5G material;

[81] European Commission*. Information and communication technologies*. [Viewed the 21/12/2020]. Available from: https://ec.europa.eu/regional_policy/en/policy/themes/ict/ .

[82] Zetter, K. *Solarwinds Hack Infected Critical Infrastructure, Including Power Industry*. The Intercept, December 24, 2020. [Viewed the 24/12/2020]. Available from: https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastructure/ .

[83] Greenberg, *A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired, Security, 08.22.2020. [Viewed the 21/12/2020]. Available from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ .

[84] Gstöhl, S. *'Patchwork Power' Europe? The EU's Representation in International Institutions*. Bruges Regional Integration & Global Governance Papers 2/2008. College of Europe, United Nations University. Pp. 4-10. Available from: https://cris.unu.edu/sites/cris.unu.edu/files/BRIGG_2-2008_Gstoehl.pdf .

While recommending also actions to take in order to tackle the incoming threats, more rounded one:

- An increasing exposure to attacks, a wider surface of attacks increasingly relying on software. Poor software design could result in enormous damages for the grid;
- The characteristics of some piece of equipment inside the 5G environment became way more sensible to attacks or generally more sensitive;
- A more wireless and mobile reliant network put in jeopardy the entire ecosystem and necessitate to scrutiny the sensitive supplier's sector, in this regard the suppliers became crucial, especially to avoid meddling of non-EU countries;
- Avoid reliance on a single supplier to avoid shortages and dependencies;
- The core network and its availability and integrity are already a major security concern. 5G is expected to become the backbone of many critical sectors and IT application. As said with the CIIP framework the integrity and availability of those networks is a already a major national security concerns.[85]

Starting from the CIIP European framework [86], already ten years old but still of great help for understand the proportion of interest in the matter and how the Union plans to tackle any possible shortage, attack or failure of the grid. The five pillars underlined by the recommendation are still applicable to this case, because the protection of the infrastructure is still the ICT one, but it is necessary to extend the meaning to all the devices and components that will entangle the 5G technology. New hardwares are needed and those have to be introduced in the defence grid, in order to maintain a safe network and achieve all the goals of a safe and reliable environment.

1. Preparedness and prevention;
2. Detection and Response, an efficient early warning mechanism;
3. Mitigation and Recovery, fundamental for the continuity of services and stability of the technology;
4. International Cooperation, promoting EU priorities and enlarging a secure network;
5. Criteria for the ICT sector, for the facilitation of the regulation of the sector, avoid problems and the reliance on untrusty suppliers.

[85] ENISA. *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*. NIS Cooperation Group. 01/2020. Pp. 40-46.

[86] CIIP European framework

It is clearly notable that in order to prevent the incoming 5G threats and protect the critical information infrastructure, all the previous points have to be in some ways covered and implemented in a concrete and regulated manner. The European agency for cybersecurity has a great role, but it is also needed a great stimulus from the single governments of the Union, a unique understanding of what is at stakes and the participation of all the stakeholders (firms, companies, organizations and governments). The critical infrastructure framework is useful to stress the core function of a certain element and the network (and especially mobile one) is and will be increasingly a key element of economy, services, healthcare and general security. Maintaining a leading role in innovation and technology passes for sure now to this ICT next step and ensuring a safe environment is a criticality for the European Union, without a safe network where payments could be done without worries of interception, data can be stored and sent without hijacking, spoofing or man-in-the-middle risks, where communication can be granted in a safe and fast way without DoS or backdoor issues. All these situations are necessary to lead innovation and prevent enormous damages that can thwart freedom, independence and basic rights of individuals. It is of capital importance ensure deployment plans for the infrastructure of 5G, impose a close scrutiny of vendors and providers of any core components of the network, rely on many different sources of material to differentiate and avoid the threat of dependence and blackmail, impose rules and laws for ISP that clarify how and why apply controls and checks. Finally ensure that Quick Reaction Forces are available centrally for any country and a chain of responsibility is in action in case of disruption, attacks and shortages. Regulation on best practices and standards will greatly help to enlarge the security bases, especially throughout the private sector that will find solid footholds in a proper documentation and regulation. As exhaustively expressed by M.D. Cavelty [87] responding to cyber threats is easier thanks to the CIIP framework and the focus that pose to public-private partnership, better coordination and integration, awareness campaigns and promotion of education, international cooperation. But also, the nature of the system has the great advantage to clarify strategy making, with the definition of protection goals and top-down/ bottom-up interactions in the ICT field. The 5G nexus is not something that can be resolved with a single measure but on the opposite require strict cooperation of all the parties and of many different part of a big and intricate field, and in the present days the effort to ensure a safe network for everyone, where communication and transfer of data is granted and enshrined through the

[87] Cavelty, M.D. *The Art of CIIP Strategy: Tacking Stock of Content and Processes*. Center for Security Studies, ETH Zurich. January 2012. DOI: 10.1007/978-3-642-28920-0_2 .

principles of availability, confidentiality and integrity is probably the biggest challenge of the decade and will be the arena of bigger incoming discussions.

Bibliography

35 Outrageous Hacking Statistics & Predictions. [Viewed date 21/11/2020]. Available from: https://review42.com/hacking-statistics/ .

5G PPP Architecture Working Group. *View on 5G Architecture*. 2019. [Viewed the 11/11/2020]. Available from: https://5g-ppp.eu/5g-ppp-5g-architecture-wg-white-paper-rev-3-0-for-public-consultation/ .

Abele-Wigert, I.; Dunn, M. *The International Critical Information Infrastructure Protection*

(CIIP) Handbook 2006. Enisa Quarterly, June 2006.

Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. *5G security: Analysis of threats and solutions*. 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, 2017, pp. 193-199, doi: 10.1109/CSCN.2017.8088621.

API Crazy*. Security Best Practice for Protecting Against Memory Scraping Malware in Target & Home Depot*. September 25, 2014. [Viewed the 22/11/2020]. Available from: https://apicrazy.com/2014/09/25/security-best-practice-for-protecting-against-memory-scraping-malware-in-target-home-depot/ .

Bachmann, S.D.; Gunneriusson, H. Hybrid Wars: the 21st Century's new Threats to Global peace and Security. Bournemouth University, UK.; Swedish Defence University.

Bartock, M.; Cichonski, J.; Souppaya, M. *5G Cybersecurity: Preparing a Secure Evolution to 5G*. National Institute of Standards and Technology. April 2020.

Bayuk, J.L; Healey, J; Rohmeyer, P; Sachs, M.H; Schmidt, J; Weiss, J. *Cyber Security Policy Guidebook*; edited by John Wiley and Sons, Inc. USA 2012.

Becker, W. (2006). *The Dot.Com Revolution in Historical Perspective*. Entreprises Et Histoire. 43. 10.3917/eh.043.0034.

Brechbühl ,H.; Bruce ,R.; Dynes, S.; Johnson, M.E. (2010). *Protecting Critical Information Infrastructure: Developing Cybersecurity Policy*. Information Technology for Development Vol. 16, No. 1, January 2010, 83–91. Taylor & Francis Group. 16:1, 83-91, DOI: 10.1002/itdj.20096 .

Bayuk, J.L.; Healey, J.; Rohmeyer, P.; Sachs, M.H.; Schmidt, J.; Weiss, J. *Cyber Security Policy Guidebook*; edited by John Wiley and Sons, Inc. USA 2012.

Buchanan, B. *The Hacker and the State.* Harvard University Press, London 2020.

Boccardi, F.; Heath, R.; Lozano, A.; Marzetta, T.; Popovski, P. *Five Disruptive Technology Directions for 5G*. 2013. Communications Magazine, IEEE. 52. 10.1109/MCOM.2014.6736746.

Carder, J. *What is the Zero Trust Model of Cybersecurity, Really?* LogRhythm, October 1, 2020. [Viewed the 13/12/2020]. Available from: https://logrhythm.com/blog/what-is-the-zero-trust-model-for-cybersecurity/ .

Cavelty, M.D. *The Art of CIIP Strategy: Tacking Stock of Content and Processes*. Center for Security Studies, ETH Zurich. January 2012. DOI: 10.1007/978-3-642-28920-0_2 .

Cloudflare. *Inside the infamous Mirai IoT Botnet: A Retrospective Analysis*. [Viewed the 21/11/2020]. Available from: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ .

Cloudflare. *What is Encryption? | Types of Encryption*. [Viewed the 05/10/2020]. Available from: https://www.cloudflare.com/learning/ssl/what-is-encryption/ .

Commission of the European Communities. *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*. Brussels 30/03/2009. {SEC(2009) 399}, {SEC(2009) 400}. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149 .

Crowdstrike. *What are Denial-of-Service (DOS) Attacks?* November 12, 2020. [Viewed the 3/11/2020]. Available from: https://www.crowdstrike.com/epp-101/denial-of-service-dos-attacks/?utm_campaign=dsa&utm_content=seu&utm_medium=sem&utm_source=goog&utm_term=&gclid=CjwKCAiA_Kz-BRAJEiwAhJNY7yZriA-QxP4QD6wx0IZ2R8KBHWEPB560oLdZt4uhGy81HL1MKAZf8xoC_VEQAvD_BwE .

Crowther, G.A. *National Defense and the Cyber Domain*; edited by The Heritage Foundation, 2018 Index of US Military Strength.

Ding, S. *The Dragon's Hidden Wings, how China rises with Its soft power*; edited by Lexington Books, Plymouth, UK 2008.

Dunn Cavelty, M. *Cyber-Security*; edited by Alan Collis, Contemporary Security Studies, Oxford University Press 2012.

Dunn Cavelty, M; Mauer, V; Krishna-Hensel, S. *Power and Security in the Information Age*; edited by Myriam Dunn Cavelty, Victor Mauer and Sai Felicia Krishna-Hensel 2007, published Ashgate Publishing Limited, UK 2007. 182 p. ISBN 978 0 7546 7088 9 .

ENISA. *Baseline Capabilities of National/Governmental CERTs. 2012*. [Viewed the 11/11/2020]. Available from: https://www.enisa.europa.eu/publications/updated-recommendations-2012/at_download/fullReport .

ENISA. *Data Protection, Cryptographic protocols and tool*. [Viewed the 21/11/2020]. Available from: https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/cryptographic-protocols-and-tools .

ENISA. *ENISA's contribution to the Critical Information Infrastructure protection (CIIP*). 2017. [Viewed the 11/11/2020]. Available from: https://www.enisa.europa.eu/publications/ed-speeches/enisas-contribution-to-ciip .

ENISA. *Information Sharing and Analysis Centers (ISACs)*. [Viewed the 11/11/2020]. Available from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing .

ENISA. *ENISA Threat Landscape for 5G Networks: Threat assessment for the fifth generation of mobile telecommunications networks (5G)*. 2019.

ENISA. *CIIP Governance in the European Union Member States. 2016.* [Viewed the 23/11/2020]. Available from: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/ciip-governance-in-the-eu-annex .

ENISA. *Stocktaking, Analysis and Recommendations on the Protection of CIIs. 2016*. [Viewed the 23/11/2020]. Available from: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis .

ENISA. *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*. NIS Cooperation Group. 01/2020.

EMF Explained 2.0. *5G Explained – How 5G Works*. [Viewed the 11/11/2020]. Available from: http://www.emfexplained.info/?ID=25916 .

European Commission. *Policy on Critical Information Infrastructure Protection (CIIP).* Law 7 February 2013. [Viewed the 4/11/2020]. Available from: https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip ;

European Commission. *The Directive on security of network and information systems (NIS Directive)*. [Viewed the 11/11/2020]. Available from: https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive .

European Commission. *Information and communication technologies*. [Viewed the 21/12/2020]. Available from: https://ec.europa.eu/regional_policy/en/policy/themes/ict/ .

Frias, Z & Martinez, J.P. 5G networks: *Will technology and policy collide?* Edited by Telecommunication Policy, journal number 42, Universidad Politecnica de Madrid, Spain 2018.

Fong, M. *Protecting High-Level Personnel from IMSI Catchers*. Security magazine, February 21, 2020. [Viewed the 2/12/2020]. Available from: https://www.securitymagazine.com/articles/91767-protecting-high-level-personnel-from-imsi-catchers .

Forescout. *Reducing Risks from IoT Devices in an Increasingly Connected World*. Forescout Technologies, Inc. 2020. Available from: https://www.forescout.com/company/resources/reducing-risks-from-iot-devices-in-an-increasingly-connected-world/ .

Fransen, F. *5G Security: Can 5G secure IoT?* TNO, 2019. [Viewed the 12/11/2020]. Available from: https://www.surf.nl/files/2019-03/5G%20Groningen%205%20-%20Can%205G%20secure%20IOT.pdf .

Future Learn. *DoS and DDoS attacks*. [Viewed the 21/11/2020]. Available from: https://www.futurelearn.com/info/courses/teaching-cybersecurity/0/steps/57188 .

Garamone, J. *Cybercom Chief Discusses Importance of Cyber Operations*, US Department of Defence, 2015. In https://www.defense.gov/Newsroom/News/Article/Article/604453/cybercom-chief-discusses-importance-of-cyber-operations/ ;

Gates, G. *How a Secret Cyberwar Program Worked*. The New York Times, 2012. In https://archive.nytimes.com/www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html .

Greenberg, A. *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired, Security, 08.22.2020. [Viewed the 21/12/2020]. Available from:

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ .

Gstöhl, S. *'Patchwork Power' Europe? The EU's Representation in International Institutions*. Bruges Regional Integration & Global Governance Papers 2/2008. College of Europe, United Nations University. Pp. 4-10. Available from: https://cris.unu.edu/sites/cris.unu.edu/files/BRIGG_2-2008_Gstoehl.pdf .

Germano, P. *In Europa si combatte la Proxy War digitale*; Edited by Limes April 2019; Italian Montly Geopolitical Review.

Geller, M & Nair, P. *5G Security Innovation with CISCO*; edited by Cisco Public, Whitepaper US 2018.

Hill, M. *#ISC2Congress: How 5G is Expanding the Attack Surface*. Infosecurity Group. [Viewed date 17/11/2020]. Available from: https://www.infosecurity-magazine.com/news/isc2congress-5g-attack-surface/ .

Huawei. *Huawei's Security Standards and Certification*. Huawei technologies Co., Ltd. 2020. [Viewed the 21/11/2020]. Available from: https://www.huawei.com/it/trust-center/transparency/standard-certification .

Huawei Cybersecurity Evaluation Centre (HSEC) *Annual Report 2019*, a report to the National Security Adviser of the United Kingdom March 2019.

National Cyber Strategy of the United States of America; The White House, Washington DC, September 2018.

Nguyen-Duy, J. *Security Challenges Facing the Shift to 5G*. CSO, July 17, 2020. [Viewed the 3/12/2020]. Available from: https://www.csoonline.com/article/3567450/security-challenges-facing-the-shift-to-5g.html .

Ijaz Ahmad; Tanesh Kumar; Madhusanka Liyanage; Jude Okwuibe; Mika Ylianttila; Andrei Gurtovk. *5G Security, Analysis of Threats and Solutions*; edited by Department of Computer and Information Science, Linkoping University, SE-581 83 Linkoping, Sweden 2018.

International Telecommunication Union (ITU). *Guide to Developing a National Cybersecurity Strategy, Strategic Engagement in Cybersecurity*; edited by International Telecommunication Union (ITU), Geneva, Switzerland 2018.

Internet World Stats. *Internet Growth Statistics*. [Viewed the 07/10/2020]. Available from: https://www.internetworldstats.com/emarketing.htm .

Ivezic, M. *Unlocking the Future – Why Virtualization Is the Key to 5G*. 5g.security, March 21, 2020. [Viewed the 24/11/2020]. Available from: https://5g.security/5g/virtualization-key-5g/#:~:text=5G%20network%20virtualization%20will%20permit,network%20functions%20virtualization%20(NFV).&text=This%20architecture%20introduces%20the%20possibility,top%20of%20shared%20physical%20infrastructure .

Johnson, T.A. *Cybersecurity: Protecting Critical Infrastructures from Cyber Attacks and Cyber Warfare*. CRC Press, Taylor & Francis Group, 2015.

Kaplan, F. *Dark Territory*. Simon & Schuster, New York 2016.

Khanna, P. *Connectography, mapping the future of global civilization*; edited by A Random House International Edition, New York 2016.

Kurlantzick, J. *Charm Offensive*; edited by A Caravan Book, New York 2008.

Lawrence W. & Barnes M.W. *5G Mobile Broadband Technology - America's Legal Strategy to Facilitate Its Continuing Global Superiority of Wireless Technology*; edited by Intellectual Property & Technology Law Journal Volume 31, Number 5, May 2019.

Lee, K.F. *AI Superpowers, China, Silicon Valley and the New World Order*; edited by Houghton Mifflin Harcourt Publishing Company, New York 2018.

Lee, H. Concept and Characteristics of 5G Mobile Communication Systems. Hankyuon National university, January 15, 2015. [Viewed the 4/11/2020]. Available from: https://www.netmanias.com/en/post/blog/7109/5g-iot/concept-and-characteristics-of-5g-mobile-communication-systems-1 .

Lewis, T.G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Third Edition 2020 John Wiley & Sons, inc. Hoboken, USA.

Lewis, N. *Locking the backdoor: Reducing the risk of unauthorized system access*. Searchsecurity. [Viewed the 22/11/2020]. Available from: https://searchsecurity.techtarget.com/tip/Locking-the-backdoor-Reducing-the-risk-of-unauthorized-system-access#:~:text=There%20are%20many%20steps%20IT,both%20known%20and%20unkno wn%20backdoors.&text=Using%20multiple%20vendors%20to%20limit,Installing%20open%20source%20software .

Lichtman, M.; Rao, R.; Marojevic, V.; Reed, J.; Piqueras J. R. (2018). *5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation*. 1-6. 10.1109/ICCW.2018.8403769.

Liang, Q.; Xiangsui, W. *Unrestricted Warfare*, Shadow Lawn Press 2017.

Lueth, K.L. *State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time*. IoT Analytics, November 19, 2020. [Viewed the 3/12/2020].Available from: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/ .

Malwarebytes. Backdoor computing attacks. [Viewed the 21/11/2020]. Available from: https://www.malwarebytes.com/backdoor/ .

Masterson, C. *Massive MIMO and Beamformin: The Signal processing Behind the 5G Buzzwords*. AnalogDialogue, vol.51. June 2017. [Viewed the 21/11/2020]. Available from: https://www.analog.com/en/analog-dialogue/articles/massive-mimo-and-beamforming-the-signal-processing-behind-the-5g-buzzwords.html# .

Maurer, T. *Cyber Mercenaries, the State, Hackers, and the Power;* edited by Cambridge University Press, New York 2018.

National Research Council. 1996. Cryptography's Role in Securing the Information Society. Washington, DC: The National Academies Press. Pp.414-420. Available from: https://doi.org/10.17226/5131 .

National Science Foundation. *A Brief History of NSF and the Internet*. [Viewed the 05/10/2020]. Available from: https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050 .

Okta. *How to mitigate DoS attacks*. [Viewed the 5/11/2020] Available from: https://developer.okta.com/books/api-security/dos/how/ .

OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en .

Peck, M. *Israel Bombed Cyber Hackers (That Is Historic, For Many Reasons*), The National Interest, May 12, 2019. In https://nationalinterest.org/blog/buzz/israel-bombed-cyber-hackers-historic-many-reasons-56987 ;

Roser, M.; Ritchie, H.; Ortiz-Ospina, E. (2015) - *Internet*. Published online at OurWorldInData.org. Available from: https://ourworldindata.org/internet.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). [Viewed the 12/11/2020]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC .

Raccomandazione (UE) 2019/534 della Commissione, del 26 marzo 2019, Cibersicurezza delle reti 5G. [Viewed the 12/11/2020]. Available from: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32019H0534 .

Reichert, C. *US finds Huawei has backdoor access to mobile networks globally, report says*. CNET. Feb. 12, 2020. [Viewed the 21/11/2020]. Available from: https://www.cnet.com/news/us-finds-huawei-has-backdoor-access-to-mobile-networks-globally-report-says/#:~:text=Chinese%20tech%20giant%20Huawei%20can,reported%20Tuesday%2C%20citing%20US%20officials .

Rodriguez, J. *Fundamentals of 5G Mobile Networks*; edited by John Wiley & Sons, Ltd, Chichester, United Kingdom 2015. 336 p. ISBN: 9781118867525.

Rahman, F.M.A.; Kamal, P. *A Holistic Approach to ARP Poisoning and Countermeasures by Using Practical Examples and Paradigm*. International Journal of Advancements in Technology. ISSN 0976-4860.

Sanger, D. *The Perfect Weapon;* edited by Scribe Publications Pty Ltd, London 2018. 313 p.

Singer, P.W.; Brooking, E.T. *Likewar*, Mariner Books, New York, 2019.

Sharma, A. *Cyber Wars: A Paradigm Shift from Means to Ends.* Institute for System Studies and Analysis (I.S.S.A9 Defence research and Development Organization (D.R.D.O), Ministry of Defence, India.

Shi-Kupfer, K & Ohlberg, M. *China's Digital Rise, Challenges for Europe;* edited by Mercator Institute for China Studies (MERICS), papers on China N°7, April 2019.

UKDiss.com. *Sniffing Attacks Prevention and Detection Techniques*. 12th December 2019. [Viewed the 21/11/2020]. Available from: https://ukdiss.com/examples/sniffing-attacks.php .

Vassilakis, V.; Chochliouros, I.; Spiliopoulou, A.; Sfakianakis, E.; Belesioti, M.; Bompetsis, N.; Wilson, M.; Turyagyenda, C.; Dardamanis, A. (2016). *Security Analysis of Mobile Edge Computing in Virtualized Small Cell Network*s. 475. 653-665. 10.1007/978-3-319-44944-9_58.

Verizon. *Data Breach Investigation Report 2020*. Available from: https://enterprise.verizon.com/resources/reports/dbir/ .

Weiss, A. *How to Prevent DoS Attacks*. eSecurityPlanet, July 3, 2012. [Viewed the 2/12/2020]. Available from: https://www.esecurityplanet.com/networks/how-to-prevent-dos-attacks/ .

Wong, V; Schober, W; Wang, L; *Overview of new technologies for 5G system*, Cambridge University Press, 1-24 p. DOI: https://doi.org/10.1017/9781316771655.002.

Wheeler, T.; Simpson, D. *Why 5G requires new approaches to cybersecurity: Racing to protect the most important network of the 21st century*. Brookings. Tuesday, September 3, 2019. [Viewed the 21/12/2020]. Available from: https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/ .

Yarali A. *5G mobile: Technologies, applications and Ubiquitous Connectivity*; edited by Nova Science Publisher Inc. Telecommunications Systems Management, Instituite of Engineering, Murray State University, Murray, US, 2017. 13p. ISBN: 978-1-53610-941-2.

Zetter, K. *Solarwinds Hack Infected Critical Infrastructure, Including Power Industry*. The Intercept, December 24, 2020. [Viewed the 24/12/2020]. Available from: https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastructure/ .

Zinzone, F.; M.Cagnazzo, M. *The art of war in the post-modern era*, self-produced, 2020.

Zuboff, S. *The Age of Surveillance Capitalism*. Profile Books LTD, London 2019.