Forum: Disarmament and International Security Committee

Issue: Redefining cybersecurity in the midst of 5G development

Student Officer: Niki Ktistaki

Position: Chair

INTRODUCTION

Since the 1980s, when the first mobile phones were created, huge changes have been made in technology that have directly impacted and facilitated our everyday lives. We have had the opportunity to communicate by chat, call, or even video call, with people thousands of miles away, share information and data, transfer money, etc. We are privileged enough to have the whole world at our fingertips and we are able to access every corner of the globe with just one click. We have the chance to meet people from other countries without needing to meet in person, access thousands of sources to find information just for one topic etc.

It is unbelievable to imagine that video calling was made possible just over a decade ago and now we not only can video call our friends, but attend school classes and work online. We can now control our house security system, turn the lights on or off and close the windows or the blinds, just by using an app on our phones, and automated devices in our houses, like vacuums, are almost a given. Automated vehicles are starting to become a reality and artificial intelligence is at its peak. All that has happened in a period of only 30 years, and every minute that passes we are getting one step closer to completely changing the way we live.

Here is where the 5G development steps in. The 5G (fifth generation) development is already shaping the future of our lives and our world. It will not only offer faster networks for communicating and sharing information but it will establish a global wireless framework in which everyone and everything will be connected with each other. It is estimated that in the next 10 years, 5G will make groundbreaking changes in our everyday lives, building the bridge to the future of technology, innovation, and development. The introduction of 5G will shape our lives in a way that we cannot even imagine right now and offer opportunities to advance our way of life.

However, it should be taken into consideration that 5G has been developing only for the past few years and its introduction to the modern world is fairly new and fresh. Thus, the world is still working towards establishing a stable ground in which 5G could be developed and implemented. The increased connectivity that it offers comes with heightened cybersecurity threats and dangers. 5G connects the virtual and the physical world and its consequences will affect society as a whole. Legal frameworks are still being created to accommodate all the possible dangers and situations that 5G could cause so that violations of personal data and information and threats to cybersecurity are minimized. Governments, private and public companies should protect not only the 5G infrastructure and services but the applications and IoT devices that run across 5G rails. Ensuring cybersecurity is the first step towards the rightful implementation of 5G networks so that they can be used to their full potential.

DEFINITION OF KEY-TERMS

bps

The term stands for "bits per second" and it is a way to measure data transfer rates, like network connection and Internet download speeds. Internet connection speeds are often measured in Mbps (1,000,000 bps). Some networks, like 5G, support speeds over 1,000 Mbps and are measured in Gbps.

Modem

"Modem or else "Modulator-Demodulator" is a hardware component that allows a computer or another device, such as a router or switch, to connect to the Internet".[1]

Mobile phone penetration

"Mobile Phone Penetration refers to the number of SIM cards or mobile phone numbers in a certain country, it does not refer to the number of mobile phone devices".[2]

IoT devices

"IoT devices are pieces of hardware, such as sensors, actuators, gadgets, appliances, or machines, that are programmed for certain applications and can transmit data over the internet or other networks. They can be embedded into other mobile devices, industrial equipment, environmental sensors, medical devices, and more". [3]

Hardware

[1] "Modem Definition." Tech Terms, Tech Terms, 2 Sept. 2019, techterms.com/definition/modem

[2] "Mobile Phone Penetration." Infobip, www.infobip.com/glossary/mobile-phone-penetration.

[3] Arm Ltd. "What Are IoT Devices." Arm | The Architecture for the Digital World, www.arm.com/glossary/iot-devices. Accessed 19 May 2021.

“It refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners”[4]

Software

“Software comprises the entire set of programs, procedures, and routines associated with the operation of a computer system”. [5]

Choke-point

“A chokepoint is a single point through which all incoming and outgoing network traffic is funneled. As all traffic passes through a choke point it is the natural place to focus monitoring and control efforts such as Internet firewalls. It is also the natural place at which to break the connection with the external network if necessary”.[6]

Firewall

“A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules”. [7]

Vendor

“A commercial organization that acquires or develops software to sell to the end-user”.[8]

Research and development (R&D)

“Research and development (R&D) is the part of a company's operations that seeks knowledge to develop, design, and enhance its products, services, technologies, or processes”.[9]

BACKGROUND INFORMATION

What is 5G development?

[4] "Hardware Definition." Tech Terms Computer Dictionary, 5 Dec. 2006, techterms.com/definition/hardware. Accessed 22 May 2021.

[5] "Software | Definition, Types, & Facts." Encyclopedia Britannica, www.britannica.com/technology/software. Accessed 22 May 2021.

[6] "Chapter 4 - Network Security Policy." Black Sheep Networks Inc, www.blacksheepnetworks.com/security/info/fw/steph/policy.html.

[7] "What Is a Firewall?" Cisco, www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.

[8] "Definition of Software Vendor." PCMAG, www.pcmag.com/encyclopedia/term/software-vendor.

[9] Ross, Sean. "Why Should You Invest in Research and Development (R&D)?" Investopedia, 22 July 2019, www.investopedia.com/ask/answers/043015/what-are-benefits-research-and-development-company.asp.

The term 5G stands for the 5th generation and it is a new mobile network. It is designed to connect virtually everyone and everything, including not only mobile devices but machines and objects as well. It is a network really different from the four previous ones, 1G, 2G, 3G, and 4G. It is meant to make great technological changes as it will provide higher multi-Gbps data speeds, low latency, more reliability, massive network capacity, and increased availability.

However, in order to fully understand the 5th generation and the changes that it will make, we need to firstly explore the previous four networks.

1st Generation (1G)

1G was first introduced to the public in Japan, in 1979 by Nippon Telegraph and Telephone (NTT). It is the first generation for wireless cellular technology or else called mobile telecommunications and the audio it transmitted was analog.

2nd Generation (2G)

2G was firstly launched in Finland, in 1991 by Radiolinja and replaced 1G. 2G will have far more benefits than 1G. 2G systems are more efficient as they allow greater mobile phone penetration levels, they introduced data services for mobile devices, the SMS (Short Message Service) and they made phone conversations digitally encrypted. Later on, other than text messages, it also provided picture messages and MMS (Multimedia Message Service).

3rd Generation (3G)

The 3rd generation provided a faster information rate than the other two networks. Later releases of 3G – 3.5G and 3.75G – provided mobile broadband access to smartphones and mobile modems in laptop computers. Thus, it could be applied to wireless voice telephony, mobile Internet access, and video calls of a low quality.

4th Generation (4G)

The 4th generation has been the latest and most advanced network of all and it is the one we still use today. It was first provided to the public in Norway and Stockholm, in 2009 and in the United States in 2011. Except for the standard voice, text, and image services, 4G offered mobile broadband internet access to smartphones and laptops. Some other applications include gaming services, hid-definition TV, video conferencing, 3D television, etc.

After having a better and general idea about the previous networks, we can better realize what changes are to be made with the introduction of 5G.

Advantages of the 5G Technology

1. Faster speed

4G which is the fastest current network that we use offers about 45Mbps on average. However, 5G could achieve 10- or 20-times faster speeds. This will allow faster browsing and downloading. It is estimated that downloading a 3D movie will take only a minute or so, while using 4G could take about seven minutes.

2. Low latency

Latency specifies the end-to-end communication delay, measuring the time between the sending of a given piece of information and the corresponding response. Efforts to improve latency have started since the development of 4G. Latency has now been an integral part of 5G development since the beginning. Low latency is important for a variety of different applications today and the low delays that could be achieved open the way to more experiences. Some opportunities of low-latency include automated cars, multiplayer online gaming, virtual reality, factory robots, etc. It will also make possible high-speed virtual and augmented reality video without delays.

3. Higher bandwidths

Higher bandwidths will contribute to higher and faster transmission of data, images, and videos and 5G will allow more data to travel faster over wider coverage areas. It is estimated that 5G bandwidths are 10 times higher than the 4G ones.

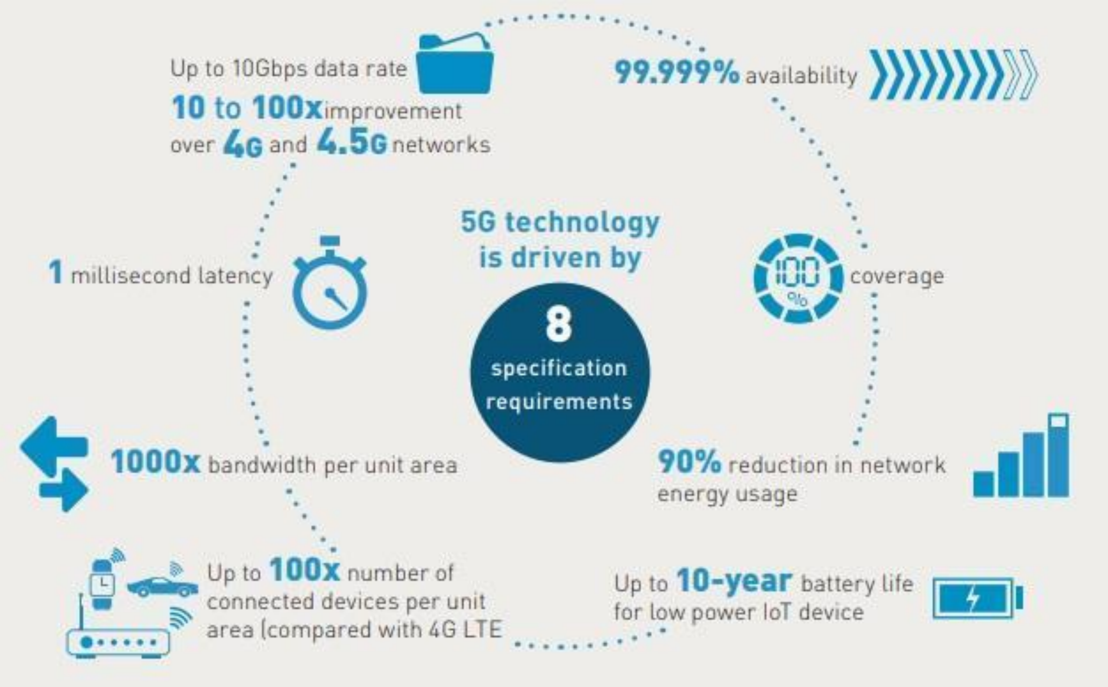
Up to 10Gbps data rate
10 to 100x improvement over 4G and 4.5G networks
99.999% availability
5G technology is driven by
8 specification requirements
1 millisecond latency
100%
coverage
1000x bandwidth per unit area
90% reduction in network energy usage
Up to 100x number of connected devices per unit area (compared with 4G LTE
Up to 10-year battery life for low power IoT device

Figure 1: Key Requirements Of 5G[10]

Engagement of the 5G Technology on Societal Sectors

5G, by having all the above characteristics, will create many social and economic opportunities as it will be applied in many sectors, some of them being health care, transportation, education, agriculture and entertainment. Because of its use in these sectors, it is important that the applications and IoT devices operate as anticipated without fail or delays, as to minimize any possible risks.

Countless are the benefits the 5G technology may provide in the daily life of the individual, some of which are the following: when we are in need of medical assistance, instead of going to the hospital, we could be diagnosed and receive the necessary care from the comfort of our homes, via a video call. This will be especially necessary for people living in rural or distant areas and they need to travel hours to visit a hospital. In the transportation sector, except for the automated vehicles that are now being developed, vehicles could communicate with each other by relaying signals and thus minimizing the risks of car accidents, and they could also communicate with sensors on the bridges or roads and traffic lights. Technology in the area of education is quite familiar to all of us after the COVID-19 pandemic hit. However, by using 5G in the educational procedure, virtual reality could be introduced in the classrooms, allowing

[10] Thales Group. "Key requirements of 5G." Photograph.
www.thalesgroup.com/sites/default/files/gemalto/Image002.jpg.

students and teachers to dig deeper into knowledge. In the entertainment sector, many opportunities will arise for online concerts as the musicians could play together with no response time and thus with no sound delays.

Implications of the 5G Technology on Cybersecurity

5G has already started a revolution in the technology sector, by being able to support a wide range of applications and thus creating new opportunities for a developed world. 5G networks also play a key role in achieving digital transformation of the economy and that's why the cybersecurity of 5G is vital for the protection of the global economy and our societies. However, 5G can create many vulnerabilities that will pose new threats and dangers in cybersecurity.

A new feature that 5G is introducing, is that it permanently replaces hardware with software and now all future upgrades will no longer involve building and physically installing new network infrastructure but will require digitally installing the latest software. This feature creates new challenges as there is more software being used in the network core compared to hardware that hostile agents can hack. Previous networks contained "choke-points", that could stop possible cyber-attacks, but now with the software replacement, many of them have been removed, leaving the system unprotected.

According to the European Union (EU), there are many security challenges that may appear, which are linked to:

a. Security concerns related to the availability and integrity of the networks

b. Key innovations in the 5G technology and the crucial role of software and the plethora of services and applications enabled by 5G

c. The complexity of interlinkages between suppliers and operators and the building and operation of 5G networks

Some of the risks that may arise include:

1. Data compromise

Data compromise is one of the most significant problems that may arise. Third parties could unlawfully access a device that is connected to a 5G network and thus have access to all data and information that are stored or are being collected by that device. This data could be stolen or even destroyed. Hence, violations of human rights when it comes to personal data and limited protection in the digital space is the first risk that should be minimized when talking about the introduction and implementation of 5G networks.

Tech-company Huawei and social media platforms have been accused of human rights violations and theft of personal data and information.

Huawei

Huawei was founded in 1987 by Ren Zhengfei, a former army officer and member of the Chinese Communist Party, and it is now the world's second largest smartphone supplier after Samsung. Over the last few years, many concerns have been raised on whether or not Huawei is a technological threat or not. Even though it is a private firm, the Chinese Law states that organizations must "support, cooperate with and collaborate in national intelligence work". This means that Huawei, by having this control, could have the ability to spy or disrupt communications, steal data and information and hack networks. Many foreign policy professionals have also warned about the threat that Huawei poses to national and international security and economic integrity, as it can also be a huge risk to commercial activities as well.

With the introduction of 5G networks, breaches of privacy and violations of data protection are more likely to happen as state-sponsored hackers could use the devices that are connected to 5G networks, which often have weaker security features, as back doors into strategically vital networks. Many countries like the US, the UK, Australia and New Zealand, have restricted the actions of Huawei and the roll out of services and devices. In order to monitor the company, the United Kingdom also created the National Cyber Security Centre (NCSC). In the UK, Boris Johnson ordered for all Huawei technology to be removed from the UK's 5G network by 2027.

TikTok

TikTok is a mobile app, owned by the Chinese company ByteDance, that has exploded in the past two years. As of January 2021, it is the 7th most used social network in the world, with more than 689 million active users. TikTok was alleged for stealing children's personal information, including phone numbers, videos, location and biometric data, without any warning, transparency or the consent that is required by the law and without the children or parents knowing where the information is sent or why is this information going to be used in.

This settlement claimed that the company engaged in "The theft of private and personally identifiable TikTok user data" for the data of more than 89 million children, some as young as six years old. The data was tracked and sold to advertisers, violating state and federal law. This violation is on the radar of US authorities, as there are concerns it has links to the Chinese government through the Chinese company ByteDance.

TikTok agreed to pay out the 92 million settlement but it states that it doesn’t agree with the assertions of the lawsuit but believes that settling the case is the best path forward. The company has also faced allegations from both the public and the Trump administration that it had been stealing user data. The latter even argued that TikTok was a threat to national security, and had attempted to instate a country-wide ban.

2. Availability compromise

Availability compromise is a main area of risk, where an attack takes a network offline and results in lost connectivity. It also poses a threat to national security, as it can target key energy and/or defense infrastructure. In order to protect against this, we have to use multiple vendors, different 5G networks, and non-overlapping technologies.

3. Speed

Even though speed is one of the greatest advantages of 5G development, it can also cause many problems. 5G networks are extremely fast and this means that stealing personal data and information is fairly easy and fast, even for someone with limited hacking knowledge. In previous networks, high network traffic is a sign that a violation has happened. However, in a high-speed network, like 5G this will be difficult to notice and the third party can have access to data before any monitoring system notices it.

4. Increased connectivity

In a 5G network, millions of users, devices, and applications could be connected at the same time with each other and this increased connectivity maximizes the cybersecurity risks. By increasing the number of online devices, the potential vulnerabilities are increased as well. As a result, unauthorized users and third parties will have more points of potential entry into the network, steal data and commit human rights violations. Some “less-sophisticated” objects, like smart bulbs or wireless charging points, even if they are fully integrated into the network, can give fewer indicators when a cyber-attack is happening, compared to a PC, that could impact the responsiveness of those responsible for securing the network.

In conclusion, many things should be taken into consideration when talking about the development and implementation of 5G. We understand now that even though 5G development will offer opportunities that we have never thought of, these opportunities are quite vulnerable and hide potential risks for cybersecurity.

It creates vulnerabilities for businesses and organizations, which have to change their mindset and strategies in order to adapt and survive in a changing world. They need to redefine their strategy to ensure cybersecurity and protect their data and information. Only then, they can maximize the utility of 5G and use it to their advantage. However, this is not only a problem for business owners, but for civilians as well. From now on, mobile phones will also need the extra protection that wasn't needed before, like firewalls, as they have to be treated as if they were devices on the public internet.

VIDEO: HOW 5G WORKS[11]

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

Czech Republic

The Czech Republic is one of the countries that have taken important action towards installing 5G networks and ensuring cybersecurity. In September 2020, Czech Republic organized the second Prague 5G Security Conference 2020. In 2019, Prague also published "The Prague Proposals: The Chairman Statement on cybersecurity of communication networks in a globally digitalized world"[12], in which it focuses on four main areas: policy, technology, economy, and privacy. Having these in mind, in the proposal, Prague presents the main risks of 5G development in cyberspace and the importance of "ensuring security while supporting innovation". Last but not least, it proposes a set of steps that should be taken in these four areas that were mentioned, in order to ensure the cross-border safe use of 5G.

[11] CNET. "How 5G Works and What It Delivers." 4 Oct. 2019, *YouTube*, youtu.be/iQeaK0NGMnA.
[12] https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf

China

China is one of the leaders in 5G development, as it has built the world's largest 5G high-speed mobile network with more than 260 million 5G mobile connections. China's 5G network coverage and number of users have increased significantly in the past year. Huawei, a Chinese tech company, has made further progress, saying it will launch its 6G networks in 2030, which is 50 times faster than 5G. The company has also taken the lead in 6G research and development. However, many have claimed, including US officials, that Huawei is an extension of the Chinese Communist Party. Under China's 2017 National Intelligence Law, Huawei, appears that it can legally conduct intelligence work on behalf of the Chinese government. This means that, the Chinese government has the ability to use Huawei's 5G networks to collect information and steal intellectual property and personal data. There are also worries that the company might use its powers to disable networks to exert coercive pressure on a country.

South Korea

Cybersecurity is South Korea's first priority, when it comes to developing 5G networks. Its cyberspace is really at risk as the country doesn't have a well-developed defense cyber system to be able to protect personal data and information, as it has been a victim of many cyber-attacks in the past years. Over the years, South Korea has made many attempts to adapt to the changes and challenges that arise in the area of cybersecurity, by increasing its investments in this field and upgrading the complicacy of measures and response capabilities to confront various sources, types, and intensities of cyberattacks.

USA

US officials have already started to examine the challenges and opportunities to a successful and prosperous 5G future and decided on a number of tools and guidelines to make sure that this could be achieved. The United States are also thinking of establishing a coordinated national strategy for 5G that consists of a range of policy measures both in the short-term and in the long-term. In the short term, priority will be given to reforming the deployment of 5G networks, making additional spectrum available and helping to lead adoption and demand for advanced wireless systems. In the long-term, supporting future technological and market competitiveness, by creating the conditions for Research and Development (R&D) investment, technology transfer and early-stage research, is vital. Last but not least, the US have acknowledged how big of a threat Huawei is to cybersecurity and data protection and thus the government does what it can to limit Huawei in the United States, or even restrict its rise altogether.

Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security

In GA resolution 73/266, the Secretary-General was requested to establish a Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security. The UN Group of Governmental Experts (GGE) on Advancing responsible State behavior in cyberspace in the context of international security (formerly: on Developments in the Field of Information and Telecommunications in the Context of International Security) is an UN-mandated working group in the field of information security. It consists of experts from 25 States working in their personal capacity.

On November 11, 2020, the Secretary General published a statement on the proposed program budget for 2021 for the developments in the field of information and telecommunications in the context of international security. The statement recalled the resolutions 73/266 of 22 December 2018 and 74/28 of 12 December 2019.

European Union (EU)

The EU has taken a plethora of actions and measures to establish cybersecurity and provide Member States with guidance and measures to handle the 5G development. Firstly, it uses a range of instruments to protect electronic communications networks. Some of them are EU telecommunications framework[13], the NIS Directive (Directive on Security of Network & Information Systems)[14] and the Cybersecurity Act[15]. The EU has also proposed the Network and Information Security (NIS) Directive, which has established the NIS Cooperation Group. It has also created the “EU Cybersecurity plan to protect open internet and online freedom and opportunity”[16], which was released on February 7, 2013 in Brussels.

Royal United Services Institute (RUSI)

The Royal United Services Institute (RUSI), which was founded in 1831, is the world’s oldest and the UK’s leading defense and security “think tank”. Its goals are to inform, influence and enhance public debate on a safer and more stable world. In February 2020, it published a

[13] 5 Directive 2002/21/EC as last amended by Directive 2009/140/EC of 25 November, 2009 on a common regulatory framework for electronic communications networks and services, and Directive 2018/1972 of 11 December, 2018 establishing the European Electronic Communications Code.

[14] Directive (EU) 2016/1148 of 6 July, 2016 concerning measures for a high common level of security of network and information systems across the Union.

[15] Regulation (EU) 2019/881 of 17 April, 2019 on ENISA (the European Agency for Cybersecurity) and on information and communications technology cybersecurity certification.

[16] "EU Cybersecurity plan to protect open internet and online freedom and opportunity." European Commission - European Commission, 7 Feb. 2013, ec.europa.eu/commission/presscorner/detail/en/IP_13_94.

report on “5G Cyber Security: A Risk-Management Approach”[17]. The paper studies in depth the high-level risks that are related to 5G networks and assesses risk-management approaches that could mitigate them.

TIMELINE OF EVENTS

DATE	DESCRIPTION OF EVENT
1979	1G was introduced, which established seamless mobile connectivity and introduced mobile voice services
1991	2G wireless technologies were introduced, which increased voice capacity delivering
1988	3G was introduced and optimized mobile for data enabling mobile broadband services and provided better and faster connection
2011	4G made its appearance and delivers more capacity for faster and better broadband experiences and is expanding to new frontiers.
2013	Mobile companies Samsung and Huawei announced plans to invest in 5G development
7 February 2013	The “EU Cybersecurity plan to protect open internet and online freedom and

[17] Sullivan, James, and Rebecca Lucas. 5G Cyber Security: A Risk-Management Approach. Royal United Services Institute for Defence and Security Studies, 2020. rusi.org/sites/default/files/20200602_5g_cyber_security_final_web_copy.pdf.

	opportunity” was released
2016	Google started planning the development of a 5G network
February 2017	Ericsson created the first 5G platform that offered end-to-end support for the fifth-generation wireless network.
February 2017	Samsung announced new 5G home router
October 2017	London was preparing to carry out large scale trials of 5G
April 2019	UK authorised Huawei to help build 5G network
May 2019	Jeremy Wright, culture secretary general, warned that the rollout of 5G could be delayed due to security concerns that arised.
12th December 2019	Resolution A/RES/74/28 on advancing responsible state behavior in cyberspace in the context of international security was adopted by the General Assembly
March 2020	Samsung launched the first 5G smartphone

23rd-24th September 2020	The 2nd Prague 5G Security Conference took place

RELEVANT UN RESOLUTIONS, TREATIES, AND EVENTS

A/RES/74/28[18]

Resolution adopted by the General Assembly on 12 December 2019, on advancing responsible state behavior in cyberspace in the context of international security. The resolution stresses the importance of technology for the creation of new opportunities for the Member States and the development of the civilizations. However, it expresses its concerns that technology can be used for negative purposes and threaten international stability and security. Thus, it urges all Member States to establish a framework of cooperation and to be guided by the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

PRAGUE 5G SECURITY CONFERENCE 2020

The Prague 5G Security Conference was organized for the second time on Wednesday 23 and Thursday 24 September 2020 and it was conducted virtually due to the COVID-19 pandemic. It is the world's leading forum for discussing the risks associated with the development of 5G infrastructure. In this two-day conference, a wide range of topics was covered, like the nation’s approach to ensuring cybersecurity and the new opportunities and risks of 5G through research and development in the past year.

[18] United Nations General Assembly, Res on Advancing responsible State behavior in cyberspace in the context of international security, 18 December 2019, A/RES/74/28, https://undocs.org/en/A/RES/74/28.

CYBERSECURITY STANDARDISATION CONFERENCE 2021[19]

IN FEBRUARY 2-4 2021, THE CYBERSECURITY STANDARDISATION CONFERENCE WAS ORGANIZED VIRTUALLY BY THE EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA), WHICH PRESENTED THE DEVELOPMENTS AND UPCOMING CHALLENGES IN EUROPEAN STANDARDISATION UNDER THE CYBERSECURITY ACT. THE CONFERENCE ATTRACTED OVER 2000 PARTICIPANTS FROM THE EU AND FROM AROUND THE WORLD AND IT ADDRESSED STANDARDISATION IN RELATION TO THE RADIO EQUIPMENT DIRECTIVE (RED) AND CERTIFICATION UNDER THE PROVISIONS OF THE CYBERSECURITY ACT (CSA). THE CONFERENCE HAD TWO OBJECTIVES: TO PROVIDE THE GROUND FOR DIALOGUE BETWEEN POLICYMAKERS, INDUSTRY, RESEARCH, STANDARDISATION AND CERTIFICATION ORGANISATIONS AND THE IMPLEMENTATION OF THE CYBERSECURITY ACT IN THE MOST EFFECTIVE WAY.

African Union Convention on Cybersecurity and Personal Data Protection[20]

The “African Union Convention on Cybersecurity and Personal Data Protection” was adopted on June 27, 2014, by the 23rd ordinary session of the Assembly, which was held in Malabo, Equatorial Guinea. Out of 55 countries, 14 have signed the Convention and 8 have ratified it. The Convention is guided by the Constitutive Act of the African Union, which was adopted in 2000. It states that all Member States must establish a legal framework with the goal of strengthening fundamental human rights and freedoms, like personal data protection. It also states that data processing must be done in a way that is not likely to constitute a breach of privacy or freedoms.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

Cybersecurity of 5G networks: EU Toolbox of risk-mitigating measures

The EU toolbox was published in January 2020 by the Network and Information Systems (NIS) Cooperation Group, under the supervision of the European Union. It has two main objectives: a. Identifying a set of common measures to mitigate the cybersecurity risks that arise from 5G development and b. Providing guidance to the Member States for the selection of plans to be

[19] "Highlights of the Cybersecurity Standardisation Conference." ENISA, European Union Agency for Cybersecurity, 5 Feb. 2021, www.enisa.europa.eu/news/enisa-news/highlights-of-the-cybersecurity-standardisation-conference.

[20] African Union Convention on Cybersecurity and Personal Data Protection. African Union, 2014. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

taken to mitigate these risks. It clearly explains the risks of the 5G development and it proposes both strategic and technical measures that should be taken.

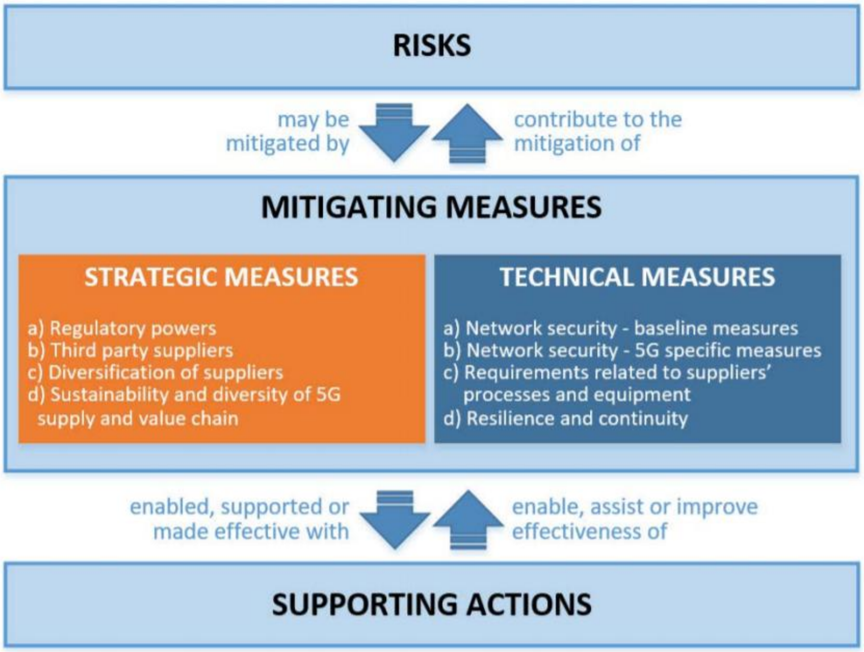
RISKS
may be mitigated by
contribute to the mitigation of
MITIGATING MEASURES
STRATEGIC MEASURES
a) Regulatory powers
b) Third party suppliers
c) Diversification of suppliers
d) Sustainability and diversity of 5G supply and value chain
TECHNICAL MEASURES
a) Network security - baseline measures
b) Network security - 5G specific measures
c) Requirements related to suppliers' processes and equipment
d) Resilience and continuity
enabled, supported or made effective with
enable, assist or improve effectiveness of
SUPPORTING ACTIONS

Image 1: Toolbox measures and supporting actions[21]

EU Network and Information Security Directive[22]

The NIS Directive was proposed by the EU as part of the EU Cybersecurity Strategy[23] and it is the first piece of an EU-wide cybersecurity application. It was adopted in 2016 and since then every EU Member State has started to adopt national legislation in accordance with the directive. Its main goal is to enhance cybersecurity across the EU and develop the cross-border collaboration of the Member States.

Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks

[21] "Toolbox Measures and Supporting Actions." Table. European Commission, 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[22] Official Journal of the European Union. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. European Commission, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[23] European Commission. "EU Cybersecurity plan to protect open internet and online freedom and opportunity." *European Commission*, 7 Feb. 2013, https://ec.europa.eu/commission/presscorner/detail/en/IP_13_94

This recommendation was published on March 26, 2019 by the European Commission. It recognizes 5G as “a major enabler for future digital services” and at the same time the threats that come with its development. It mentions that “a high level of data protection and privacy is an important element in ensuring the security of 5G networks”.

Report on Security Controls in Third Generation Partnership Project (3GPP)[24]

THE EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA) RELEASED A REPORT ON SECURITY CONTROLS IN 3GPP, WHICH WAS PUBLISHED IN FEBRUARY 24, 2021 UNDER THE SUPERVISION OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY. IT PROVIDES A HIGH-LEVEL OVERVIEW OF THE STANDARDS THAT ARE NEED TO BE MET FOR THE SECURITY OF 5G NETWORKS, AN EXPLANATION OF THE TECHNICAL SPECIFICATIONS DEVELOPED BY 3GPP FOR THE SECURITY OF 5G NETWORKS AND A SYNOPSIS OF THE KEY FINDINGS AND SOME GOOD SECURITY PRACTICES.

POSSIBLE SOLUTIONS

COMMUNICATION AND COLLABORATION BETWEEN MEMBER STATES

The first and most important thing that should be done is to achieve collaboration and communication between Member States, as it is important to share knowledge and information when it comes to developing 5G. It is vital for countries to understand how 5G works, the dangers and threats that may arise, and why it is necessary for the modern world to adapt to the new challenges and conditions. Only then, a cross-border legislation could be formed and implemented to ensure cybersecurity while developing 5G technologies.

The creation and implementation of a cross-border legal framework

A cross-border legal framework is not only essential but important in order to achieve security in the web space while creating and implementing the 5G technologies. 5G is a new network and most countries haven’t created a legislation yet that covers most aspects of the issue. In order to safely approach the development and implementation of 5G all Member States should find a common ground so as to agree what guidelines need to be set to achieve cybersecurity, minimize the possible risks and use the 5G network to its full potential.

Establishing global common cybersecurity standards

[24] SECURITY IN 5G SPECIFICATIONS: Controls in 3GPP Security Specifications (5G SA). European Union Agency for Cybersecurity (ENISA), 2021. https://www.enisa.europa.eu/publications/security-in-5g-specifications.

Not having coordinated cybersecurity standards, guidelines and regulations from various entities across the globe makes aligning global IIoT system-level cybersecurity requirements for manufacturers difficult. Many countries and governments develop their own cybersecurity standards that are most of the times very different and conflict in many ways. This creates challenges for manufacturers and system integrators when attempting to build and deploy services for a global market. Thus, is it crucial to create a set of common cybersecurity standards so as to minimize the risks of security threats and theft of data.

Achieving resilience

In order to achieve resilience, strong and flexible 5G networks should be created. A resilient 5G network should always be available, reliable and perform as expected and recover quickly in case of cyber-attacks. Using multiple vendors and non-overlapping technologies, could help in creating a stronger and more reliable 5G network. To achieve resilience, frequent testing and monitoring are necessary as well. Tech companies and governments should carry out regular tests to ensure that there are no signs of cyber-attacks and that firewalls and security systems are operating well.

Education and Training

Education and training are vital when it comes to introducing and implementing 5G technologies and networks that are really different from the previous ones. Humans are the weakest link when it comes to security and protection of information. Citizens, governments and manufacturers, all need to be sufficiently informed about the dangers, the advantages and disadvantages and how they can protect themselves from possible attacks (ex. creating strong passwords, finding the right vendor to trust, avoiding potentially dangerous applications etc.). That’s why training, workshops and seminars should be regularly offered by the government to the users and by the company to the employees.

Adopting resolutions and conventions

Until a specific cross-border legislation is created, Member States and manufacturers should all comply with the UN resolutions that have been adopted on cybersecurity and the development of 5G. EU countries should implement the EU toolbox, as it offers states with guidance and a safe path to follow while implementing and creating 5G networks. Only if Member States, companies and users have in mind national and international conventions and treaties, the risks could be reduced and a higher level of security could be achieved.

BIBLIOGRAPHY

Williams, Hannah. “A Timeline of 5G Development: From 1979 to Now.” Tech Advisor, *Tech Advisor*, 13 Nov. 2020, www.techadvisor.com/feature/small-business/timeline-of-5g-development-3788816.

Gurnani, C. P. "5G Technology: Driving the Cybersecurity Evolution." *Infosecurity Magazine*, 22 Jan. 2021, www.infosecurity-magazine.com/opinions/5g-driving-cybersecurity-evolution/.

Knowles, Gregg. "The Cybersecurity Risks Associated with 5G Networks and How to Manage Them." *ITProPortal*, 17 Mar. 2021, www.itproportal.com/features/the-cybersecurity-risks-associated-with-5g-networks-and-how-to-manage-them/.

Otterspeer, Wouter. "In a 5G World, Cybersecurity is a Problem. Here’s What You Can Do About It." *PwC*, 13 Feb. 2020, www.pwc.nl/en/topics/blogs/cybersecurity-in-a-5g-world.html.

"Prague 5G Security Conference Announced Series of Recommendations: The Prague Proposals." *Government of the Czech Republic*, 3 May 2019, www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

"23 - 24 September 2020: The Second Year of the Prague 5G Security Conference." *Government of Czech Republic*, 23 Sept. 2020, www.vlada.cz/en/media-centrum/ocekavane-udalosti/23---24-september-2020-the-second-year-of-the-prague-5g-security-conference-183728/.

"COSMOTE 5G - The First 5G Network." *COSMOTE*, www.cosmote.gr/cs/cosmote/en/5g.html.

"When Was 5G Introduced?" *Verizon*, 6 Dec. 2019, www.verizon.com/about/our-company/5g/when-was-5g-introduced.

The Evolution of Mobile Technologies:1G, 2G, 3G, 4G LTE. *Qualcomm*, 2014, www.qualcomm.com/media/documents/files/download-the-evolution-of-mobile-technologies-1g-to-2g-to-3g-to-4g-lte-qualcomm.pdf.

NIS COOPERATION GROUP. *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures*. *European Commission*, 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

European Commission. EU TOOLBOX FOR 5G SECURITY: A set of robust and comprehensive measures for an EU coordinated approach to secure 5G networks. *European Commission*, 2020, https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.

Brake, Doug. "A U.S. National Strategy for 5G and Future Wireless Innovation." *ITIF | Information Technology and Innovation Foundation*, 27 Apr. 2020, https://itif.org/publications/2020/04/27/us-national-strategy-5g-and-future-wireless-innovation.

"China Rolls out the World's Largest 5G Network: MIIT." *Global Times*, 19 Apr. 2021, https://www.globaltimes.cn/page/202104/1221466.shtml.

"South Korea’s 5G Cybersecurity Strategy." *Institute for Security and Development Policy*, 22 Mar. 2021, https://isdp.eu/event/south-koreas-5g-cybersecurity-strategy/.

Bowler, Tim. "What is Huawei and Why is It Being Banned?" BBC News, 14 July 2020, https://www.bbc.com/news/newsbeat-47041341.

Lee, Doowan, and Shannon Brandao. "Huawei Is Bad for Business." *Foreign Policy*, 30 Apr. 2021, https://foreignpolicy.com/2021/04/30/huawei-china-business-risk/.

Martin, Alexander. "Huawei: The Company and the Security Risks Explained." *Sky News*, 28 Jan. 2019, https://news.sky.com/story/huawei-the-company-and-the-security-risks-explained-11620232.

"Privacy Groups: TikTok App Violating Children's Privacy." *ETCISO.in*, 15 May 2020, https://ciso.economictimes.indiatimes.com/news/privacy-groups-tiktok-app-violating-childrens-privacy/75750050.

"TikTok Sued for Billions over Use of Children's Data." *BBC News*, 21 Apr. 2021, https://www.bbc.com/news/technology-56815480.

Neely, Amber. "TikTok Agrees to Pay $92 Million to Settle Data Breach Lawsuits." *AppleInsider*, 26 Feb. 2021, https://appleinsider.com/articles/21/02/26/tiktok-agrees-to-pay-92-million-to-settle-data-breach-lawsuits.

Waring, Joseph. "TikTok Fined for Privacy Breach." *Mobile World Live*, 15 July 2020, https://www.mobileworldlive.com/apps/news-apps/tiktok-fined-for-privacy-breach.

Irwin, Luke. "TikTok Sued over Its Use of Children’s Personal Data." *IT Governance UK Blog*, 22 Apr. 2021, https://www.itgovernance.co.uk/blog/tiktok-sued-over-its-use-of-childrens-personal-data.

"Network Security in the 5G Era." *Reply: Digital Services, Technology and Consulting*, 30 July 2020, https://www.reply.com/en/industries/telco-and-media/5g-security-for-mobile-networks.

"11 Cybersecurity Best Practices You Should Apply in 2020." *Blog | MetroStar*, http://blog.metrostar.com/cyber-security/13-cybersecurity-best-practices-apply-2020.

"Low Latency - The Specific Feature of 5G | Reply." *REPLY*, 23 June 2020, https://www.reply.com/en/industries/telco-and-media/low-latency-what-makes-5g-different.

Linge, Nigel. "5G: What Will It Offer and Why Does It Matter?" *The Conversation*, 24 Jan. 2019, https://theconversation.com/5g-what-will-it-offer-and-why-does-it-matter-109010.

AT&T Business Editorial Team. "How 5G Will Impact the Transportation Industry." *AT&T Business*, https://www.business.att.com/learn/tech-advice/how-5g-will-impact-the-transportation-industry.html.

"New Guidelines for Telecom and 5G Security." *ENISA*, 10 Dec. 2020, www.enisa.europa.eu/news/enisa-news/new-guidelines-for-telecom-and-5g-security.