„Ante Portas – Security Studies”
2021, No 1(16)
DOI: 10.33674/120216

Alika GUCHUA[1]
Georgia
Thornike ZEDELASHVILI[2]
Georgia

EU CYBER SECURITY STRATEGY AND ECONOMIC THREATS

Abstract:
Cyber-attacks have become one of the major problems in the modern world. Cyber-attacks can cause immeasurable damages to a company. They can cause tangible damages such as stopping services; they can ruin the public's trust in a company, and they can lead to leaks of important information that may affect corporate survival. For example, the EU cyber security market is estimated at 20.1 billion euros, which meets the established norms. However, the situation is being exploited by cyber-spies, hackers, posing a threat through various fraudulent and cyber-attacks, contributing to the collapse of the world economy. They also pose a great threat to the economies of different countries. Large European companies are more concerned with cybersecurity risks than the rest of the world. The rapid development of new technologies has shown that traditional approaches to cybersecurity are insufficient. The Council of the European Union announced today that it has officially adopted a new cybersecurity strategy. The strategy, which looks ahead to the next decade, was presented to the council in December 2020 by the European Commission and the high representative for foreign affairs. It contains a framework for how to defend businesses, organizations, and EU citizens from cyber-attacks and promote secure information systems. The strategy also outlines plans to make international cyberspace 'open, free and secure', according to the council. Cybersecurity as an economic means enables the creation of a single digital market if cybersecurity risks are minimized. The paper discusses the EU cyber security strategy and policy, as well as the challenges it faces. The role of new

[1] Alika Guchua, PhD, Associate Professor at Caucasus International University, Head of the Strategic Studies Institute for Research CBRN Threats and Risks, Email: alika_guchua@ciu.edu.ge
[2] Thornike Zedelashvili, PhD, Caucasus International University, Founder of the Internet Publication “Leader”, Email: thomaszedelashvili@gmail.com

technologies in EU development and security. Significant attention is focused on economic issues and how they affect the cyber security strategies of EU member states.

Keywords:
Cyber Security, EU, Russia, China, G5, NATO, Economic Security.

Introduction

The Internet and technological advances have transcended physical boundaries and changed the world. Global giant networks, known as cyberspace, are extremely complex systems. It is available to everyone and it is often difficult to determine where a cyber-attack will take place, when it will take place, or what the capacity will be. There are a lot of uncontrolled spaces on the Internet and we have a high resource of opportunities in social, economic, political or other areas. Improvements in technology have also become a major cause of lawlessness, conflict and geopolitical controversy. Before we move on to the main issue, directly to the EU positions, to the economic situation, we must first clarify the small considerations related to cyber, which should not be confused with each other. The word 'cyber' is used today in a combination of many directions, for example, cyber security, cyber defence, cyber-attack, cyber deterrence, etc. Even the words associated with cyber have many definitions and interpretations. Although cyber security and cyber defence are often used in the same context, these are two different issues. Cyber security includes information and communication security (IT platforms required for operational technologies and digital assets). Cyber defence is a broader concept and includes cyber security as one of the sub-items; it includes threat analysis and defence strategies. For example, threats against citizens, institutions and governments. As for cyber-attacks, these are targeted activities aimed at disrupting or destroying computer systems and networks. We also have the term 'cyber deterrence', which means to take measures: to avoid a potential attack with strong technological defence systems, sanctions mechanisms and cyber diplomacy.

General aspects of cybersecurity in modern international politics

The EU, together with NATO, has recognized that cyber security is critical to prosperity as cyberspace becomes a growing, sought after, geopolitically necessary subject. In economic activity, as in all other areas, cyberspace is an important resource, especially in the face of a global pandemic. Here we must take into account the important event that has been going on around the world for

almost two years – a biological virus that has taken the cyber world to a much higher level and led to the transition of various institutions to a fully virtual world**.** Hybrid jobs have also emerged here and people have been given more opportunities to work from one end of the earth to the other. This has happened in diplomatic relations as well as in various international or local conferences. Online meetings are held between the main figures of the country and many important issues are resolved remotely – economic, political or conflict.

The coronavirus pandemic has impacted cybersecurity in several ways. The challenges range from the infrastructure of the internet itself to the spread of disinformation online. The challenges are abundant and are related to: (a) infrastructural limits, (b) the increase in cybercriminal activity (d) the growth of surveillance and espionage, and (d) the spread of disinformation online. Therefore, despite the marginal attention paid to it during the first stages of the outbreak, cybersecurity is emerging as an essential tool to cope with society's new demands[3].

The coronavirus pandemic has created new challenges for states, international organizations and businesses as they adapt to an operating model in which working from home has become the 'new normal'. Companies are accelerating their digital transformation, and cybersecurity is now a major concern[4].

Public attitudes towards the Internet have been growing over the years, as well as the number of cyber threats and the sophistication of cyber-attacks. Experts estimate that 125 billion devices will be connected to the Internet by 2030, of which 90% will be people over the age of six[5].

The current situation in cyberspace is becoming increasingly worrying, because according to research conducted by security analysts: large countries are building their programs on cyber-warfare capabilities. There are already serious speculations that cyber-war and related activities will sooner or later become more active and states will have to deal with it seriously. Accordingly, states, regional and international organizations are adopting and implementing new cyber security strategies, taking into account from what threats and challenges they will have to protect their cyberspace.

Cyber touches any part of society (everything), and from that 'everything' she identifies and recommends focusing on five areas in which cyber warfare impacts society:

- Elections;

---

[3] B. Toso de Alcântara, *The coronavirus pandemic and its impact on cybersecurity*, <https://www.hiig.de/en/the-coronavirus-pandemic-and-its-impact-on-cybersecurity/> (30.06.2021).

[4] C. Nabe, *Impact of COVID-19 on Cybersecurity*, <https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html> (22.06.2021)

[5] IHS Markit, *The Internet of Things: a movement, not a market*, 2017, pp. 2-8, <https://cdn.ihs.com/www/pdf/IoT_ebook.pdf> (30.06.2021).

- Military secrets;
- Damage to infrastructure;
- Political and corporate espionage;
- Polluting information spaces.

Cyberattacks by state and non-state 'foreign actors' including state-sponsored actors, against democratic institutions, critical infrastructure and other governmental, military, economic, academic, social and corporate systems of both EU and the NATO Member States have noticeably multiplied in the past few years, and have become more sophisticated, more destructive, more expensive and often indiscriminate[6].

Also worth noting are the timely and correct policies of different countries in matters of cyber security, of which Estonia and Finland are good examples with other EU member states. The usage of cyber-attacks in an armed conflict originates from the 2008 Russia-Georgia war. A mass cyber-attack undertaken parallel to ongoing military operations is the first precedent of the usage of cyberspace in armed conflicts. The 2007-2008 DDos attacks undertaken against Estonia and Lithuania were punitive operations and represented a sort of a political message, the aim of which was to incite civil unrest and mass panic, yet were not attempts of implementing any kind of military tasks or providing informational support to military actions[7].

Estonia attaches great importance to the protection of its cyberspace and focuses on the security of information systems. The recommendation measures are civil and are based on legal regulations, training and cooperation. And, the cyber security strategy was adopted by Finland in 2008 and it is based on the understanding of cyber security as an economic problem that is closely linked to the development of the country's information systems and society.

The 2008 Russia-Georgia war showed the whole world how necessary and important it is to protect cyberspace and develop national cyber security strategies. During the war, the Russian Federation carried out targeted and massive cyber-attacks against Georgia, in parallel with the ground, air and naval attacks. These cyber-attacks have shown that protecting cyberspace is as important to national security as protecting land, air and sea spaces.

Unlike conventional combat, which uses physical force and combat equipment, cyber-warfare is a more sophisticated tool in which a task performed at a strategic level can cause large losses and inflict colossal damage on an opponent. Much of modern networking is based on the Internet and its computer systems, which involve the banking, healthcare, energy and other vital sectors,

---

[6] P. Poptchev, *NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages*, "Information & Security: An International Journal", Volume 45, (2020), p. 38.

[7] A. Gotsiridze, *The Cyber Dimension of the 2008 Russia-Georgia War*, <https://www.gfsis.org/blog/view/970> (4.04.2021).

and with this in mind, a targeted attack on critical infrastructure facilities could be catastrophic. The most unprotected and vulnerable sectors today are:

- Banking sector and other financial institutions;
- Stock exchanges;
- Nuclear power plants;
- Water supply and treatment systems[8].

Risk management is more difficult as a result. Interdependencies in critical infrastructure have multiplied to the extent that it is difficult, if not impossible, to define defensive perimeters. Such a concept has little meaning when connectivity is valued above security. Broad sectors such as food, water and transport are labelled 'critical', leaving ambiguity as to what needs to be prioritized within these sectors. Risk assessments are often conducted with only vague metrics for threats, vulnerabilities or potential impacts. This requires scrutiny for countries that are dependent on complex, interdependent global networks – in short, for nearly every country around the world[9].

There are some differences in modern cybersecurity: both in cyber-attacks between states and in cyber-attacks by private hackers. One clear example is the cyber-attack on pipelines in the U.S. The Colonial Pipeline Company reported on May 7, 2021, that it was the victim of a 'cybersecurity attack' that 'involves ransomware', forcing the company to take some systems offline and disabling the pipeline. The Georgia-based company operates the largest petroleum pipeline in the United States, carrying 2.5 million barrels a day of gasoline, diesel, heating oil, and jet fuel on its 5,500-mile route from Texas to New Jersey[10]. This fact shows that we can easily see how significant the threat of cyber-attacks is. And also, how many threats emanate from cyberspace.

EU and NATO Cyber Security Environment and Existing Challenges and Economic Factors

Countries in the world are actively developing in terms of cyber capabilities, in the 21st Century cyberweapons have become a determinant of geopolitical prosperity and status. Today, the global value of cybercrime is 530 billion euros[11]. Daily attacks are on the rise, causing huge financial losses. Protecting oneself from large-scale attacks goes beyond the defence

[8] V. Svanadze, A. Gotsiridze, *Cyber Defence. The main players in cyberspace. Cyber Security Policy, Strategy and Challenges*, Tbilisi 2015, pp. 13-14.

[9] D. Clemente, *Cyber Security and Global Interdependence: What Is Critical?*, Chatham House, February 2013, p. 1.

[10] S. Morrison, *How a major oil pipeline got held for ransom*, <https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices> (20.06.2021).

[11] European Parliament, *Cyber: How big is the threat?*, p. 1, <https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf> (8.04.2021).

mechanisms of governments. In 2017, EU President Jean-Claude Juncker said that cyber-attacks pose a greater threat to democracies and the economy than weapons and tanks[12].

There is no agreement on the definition of cyber security at the international level. Definitions of cyber security, cyberspace, cybercrime, and related key terms may differ significantly from country to country. Each country's approach to developing a cyber-security strategy also differs. Although the importance of international cooperation is recognized by all countries, the lack of common key terms and a common so-called 'language' makes cooperation at the international level very difficult.

Cyber risks and threats in the modern world pose a serious threat to the EU and NATO. This is why both organizations attach great importance to cybersecurity and are developing different protection mechanisms. The Communication on the Critical Infrastructure Protection, adopted by the European Commission on October 20, 2004, sets out the definition of critical infrastructure and its facilities, as well as the criteria for facilities that may arise in the future. In November 2005, the European Commission adopted the European Green Paper on Critical Infrastructure Protection, which sets out EU action in this area. In 2008, the European Commission launched a project to develop a common strategy for the protection of critical information infrastructure.

Cyber-attacks can damage not only the EU economy but also its democratic foundations, as cyberspace can be used in many ways, including disinformation, economic pressure and so on. Even in the case of a conventional military attack, cyber can be part of a hybrid operation, risks from the digital realm can pose a threat to governments and political systems, try to divide society and provoke conflict outside or inside the country, and we have many similar examples around the world.

The cyber-attack can be found in the World Economic Forum's 2019 Global Risk Document, which outlines cyber threats in five key economic risks. One of the most famous examples was the WannaCry cyber-attack, which spread to 300,000 computers in 150 countries. The Petya and NotPetya cyber-attacks took place, which also resulted in financial losses of hundreds of millions. These attacks and heavy losses have led to the disruption of strategic sectors and critical infrastructure, as well as interstate tensions[13].

Russia's malicious activities against the EU The extensive scope of Russia's cyber operations is generally recognised by EU policymakers. The

[12] European Commission, *State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks*, <https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193> (12.04.2021).

[13] *Wild Wide Web – Consequences of Digital Fragmentation*, <https://reports.weforum.org/global-risks-report-2020/wild-wide-web/> (14.04.2021).

European Parliament in November 2016 adopted a resolution stating that Russia's goal is to distort truths, provoke doubt, divide member states, engineer a strategic split between the European Union and its North American partners, discredit the EU institutions and transatlantic partnerships as well as to undermine and erode (the European narrative based on democratic values, human rights and the rule of law). A report presented by the Estonian Foreign Intelligence Service in 2018 also asserted that the past few years have shown that the cyber threat against the West is growing and that most of the malicious cyber activity originates in Russia's An analysis by the Alliance for Securing Democracy found, for instance, that the Russian government has "used cyberattacks, disinformation, and financial influence campaigns to meddle in the internal affairs of at least 27 European and North American countries since 2004".[14]

According to Jarno Limnell: "Elections lie at the heart of the democratic political process. They are seen as nothing less than democracy in practice. The risk of cyber-enabled meddling in European elections is real, and, when assessing the hybrid threat, elections have emerged as key targets. The Italian general election in 2018, the French presidential election in 2017, the Brexit referendums and U.S. General Election in 2016, to name but a few, have all been subject to influence by malign external agents. It is hard to evaluate precisely how strong or far-reaching an impact these cyber-psychological operations have had, but interfering in European elections is something that should not be tolerated under any circumstances"[15]. And, subsequently: "The interference in the election campaign in France is a good example of how cyber operations include not just hacking and leaks, but the use of fake news and other forms of manipulation. According to several research findings and reports, the interference originated from Russia. Russia not only denies responsibility for these activities but claims that European countries were meddling in its presidential election. But Western countries are becoming more vocal in their accusations against Moscow as Russia's cyber interference in European elections shows no signs of abating. Clearly a set of measures to defend digital democracies against disinformation campaigns, hackers and cyberattacks is urgently required"[16].

You will often hear that dealing with cyber threats requires a collective and large-scale approach. That's *not news* that NATO and the EU are actively cooperating in the direction of both information warfare and cyber warfare. NATO has identified cyber warfare as one of the major challenges, and more

[14] J. Limnell, *Russian cyber activities in the UE*, [in:] *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, eds. N. Popescu, S. Secrieru, European Union Institute for Security Studies (EUISS), 2018, p. 68.
[15] *Ibidem*.
[16] *Ibidem*.

and more money is being spent each year on technological advances and protection against cyber-attacks. But noteworthy is a new initiative launched by French President Emmanuel Macron in 2018 – "The Paris Call for Trust and Security in Cyberspace"[17]. To tell the truth, this initiative is without a legal basis, but the call for cooperation in cyberspace is a high-level declaration, which was supported by 64 countries, including various international NGOs, universities and hundreds of private companies. There is also a Tallinn Guide to Defense Norms, developed by Estonia in cooperation with NATO. It is also known that this guideline is being refined and the European Union is actively involved in this issue. The EU strategy emphasizes that cyber-attacks pose a major threat to EU member and non-EU countries and that it should become a key 'future cyber player' in global politics, which will be fully involved in cyber diplomacy and will seek to deepen the partnership in the field of cyber security.

For the EU, cyber security is an attempt to create a stable digital Europe. In 2020, the EU and its High Representative for Foreign Affairs and Security Policy introduced a new cyber security strategy – the "EU Cybersecurity Strategy'' (EUCSS)[18]. This document is very ambitious in its content; it aims to provide secure and reliable digital tools and connectivity across Europe, which means Europe to become a global leader in the digital economy. Vital sectors such as electricity, transport, healthcare, finance, telecommunications, security, defence, democratic processes and so on are becoming interdependent daily through information systems. For these interdependent devices, the EU has started to create a scheme and invest. For example, on issues such as artificial intelligence, encryption, and quantum computing. The digital transformation of society, intensified by the COVID-19 crisis, has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses. The number of cyber-attacks continues to rise, with increasingly sophisticated attacks coming from a wide range of sources both inside and outside the EU[19].

The EU should therefore be leading the efforts for secure digitalisation. It should be driving norms for world-class solutions and standards of cybersecurity for essential services and critical infrastructures, as well as

[17] *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*, <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in> (15.04.2021).

[18] *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*, <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391> (17.04.2021).

[19] *The Cybersecurity Strategy*, <https://digitalstrategy.ec.europa.eu/en/policies/cybersecurity-strategy> (16.04.2021).

driving the development and application of new technologies. Governments, businesses and citizens will all share a responsibility in ensuring a cyber-secure digital transformation[20].

And yet, what constitutes the structure of the EU Cybersecurity Strategy, which is directly linked to economic well-being? The new EU Cybersecurity Strategy is divided into three parts:

1) Sustainability, technological sovereignty and leadership;
2) Capacity building, prevention, containment and response;
3) Advancing global and open cyberspace[21].

According to the EU, both the private and public sectors should be able to choose between the most secure infrastructure and services.

The EU has the Network and Information Security Directive, (NIS, or NIS Directive), which is a unified internet cyber-security database. According to the directive, it is necessary to upgrade the cyber technologies of all relevant sectors, for example, energy, transport, health, the financial sector. Reform of the NIS Directive has begun and it will help reduce internal market inconsistencies and set specific rules for strategically important sectors. It is known that Information Sharing and Analysis Center (ISAC) – Computer Security Case Response Group (CSCRG), Computer Security Incident Response Team (CSIRT) and SOC Security Operations Centers[22] – will play an important role in a cyber technology competition. The establishment of these centres is based on overcoming cyber security threats by the public and private sectors, which means disseminating relevant information, identifying anomalies in real-time, or detecting hacker, viral attacks. The EU is ready to spend € 300 million to set up and operate such centres, which will create collective knowledge and best practices in the fight against cyber threats. The Commission plans to work with the EU Member States to establish a secure quantum communications infrastructure (QCI) for Europe that ensures the security of state government communications. The QCI will be equipped with fibre-optic communication networks as well as connected satellites, covering areas *inside and outside the European Union*.

In the context of the modern threats facing the EU and NATO, it is important to focus on G5 technology. The security risks inherent in Chinese-made 5G networking equipment are easy to understand. Because the companies that make the equipment are subservient to the Chinese government, they could

[20] *Ibidem*.

[21] *Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade*, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018> (17.04.2021).

[22] *EU coordinated risk assessment of the cybersecurity of 5G networks*, 2019, pp. 4-12, <https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security> (18.04.2021).

be forced to include backdoors in the hardware or software to give Beijing remote access. Eavesdropping is also a risk, although efforts to listen in would almost certainly be detectable. More insidious is the possibility that Beijing could use its access to degrade or disrupt communications services in the event of a larger geopolitical conflict. Since the internet, especially the 'internet of things', is expected to rely heavily on 5G infrastructure, potential Chinese infiltration is a serious national security threat[23].

In March 2019, the EU Commission started working on 5G technology and the security of the next generation of mobile networks, the EU issued a recommendation on cyber security of 5G networks. The recommendation was followed in October 2019 by the EU 5G network cybersecurity risk assessment and in January 2020 by the 5G (EU 5G Toolbox) the adoption and mitigation of cybersecurity risk mitigation measures. In October 2020, the Council of Europe called on EU member states to make full use of 5G cyber security tools, as well as to apply appropriate restrictions on high-risk providers. It should be noted that in December 2020, the EU published a report on the impact of EU recommendations, which shows the important process that EU member states have undergone in the installation and implementation of EU 5G. However with some changes and in some cases remaining shortcomings. The EU called on member states to continue to implement the 5G key recommendations and improve them in the second quarter of 2021[24].

EUCSS stresses the vitality of EU-NATO cooperation and proposes to further advance inter-institutional cooperation, most notably in connection with cyber defence interoperability. The EUCSS is an ambitious strategy that tries to prepare the Union for the major cyber threats of the 21st Century. While the strategy itself is considered 'soft law' and is not legally binding, it introduces several initiatives that could be a real game-changer in cybersecurity[25].

Thus, it is clear that the EU is fighting on several fronts in the field of cyber security and cyber technology; it seeks to increase cyber resilience, fight cybercrime, enhance cyber diplomacy, strengthen cyber defence skills, enhance research, implement innovative technologies and protect critical infrastructure.

Internet disinformation has far-reaching consequences. It threatens the democratic debate and endangers the health, safety and environment of the population. The EU is therefore taking clear, multifaceted and comprehensive measures to prevent the spread of disinformation through the Internet in

[23] B. Schneier, *China Isn't the Only Problem With 5G*, <https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/> (20.04.2021).
[24] *EU coordinated risk assessment…*
[25] O. Noyan, *The New EU Cyber Security Strategy – Exploring Ways to Shape Europe's Digital Future*, <https://finabel.org/the-new-eu-cyber-security-strategy-exploring-ways-to-shape-europes-digital-future/> (18.04.2021).

Europe. NATO is also involved in combating the spread of Internet disinformation.

In 2021, the EU adopted a new cyber security strategy. It must be said that overall it is a pretty good document and takes into account many important aspects and factors in the cyber security dimension. But, problems remain in terms of the effectiveness of the cyber security strategy. The reason for this is that this field is quite complex and multidimensional. Threats come from private companies, states, hackers, cyberterrorists, non-state aggressive groups, etc. This all complicates the effectiveness of cyber strategies. It must be said that these subjects create new threats and challenges. Therefore, these strategies need to be periodically updated and countermeasures developed. All of this will focus on the effective management of threats, risks and challenges.

The EU and NATO must take into account the significant threats and risks posed by cyberspace to implement their cyber strategy. Therefore, the following issues should be addressed: resilience, operational capacity to prevent, deter and respond; technological sovereignty, cooperation to advance global and open cyberspace. For all this, it is necessary to develop a strong cyber strategy. This is associated with significant financial costs.

Conclusion

The EU Cyber Security Strategy responds today to the challenges and threats posed by cyberspace, although some issues need to be improved and require active efforts by member states. The economic sector is actively tied to cyberspace and for its effective operation, it is necessary to protect cyber security. International cooperation is one of the key conditions and prerequisites for the development of the cyber security sector. It is, therefore, necessary to have partnerships with organizations operating within the EU, a joint NATO-EU cyber security effort, as well as active involvement in various projects that will increase cyber security and exchange information between partner countries.

The modern world that is developing and advancing daily is experiencing and evolving cyber threats. EU member states, which are constantly facing new challenges and global threats in cyberspace, benefit greatly from having a flexible and operational cyber security strategy. The transboundary nature of cybercrime forces member states to work closely with each other and at the international level in general. Such cooperation is essential not only for effective preparation for cyber-attacks but also for timely response to them. Therefore, the approach of the state strategy towards cyber security should be comprehensive. While cyber terrorism is becoming quite dangerous and hacking cyber-attacks on government infrastructure, strategic facilities,

economic sector, citizens, various regional or international organizations and so on, are becoming more and more active.

Bibliography:

1. Clemente D., *Cyber Security and Global Interdependence: What Is Critical?*, Chatham House, February 2013
2. *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*, <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity - paris-call-of-12-november-2018-for-trust-and-security-in>
3. *EU coordinated risk assessment of the cybersecurity of 5G networks*, 2019, pp. 4-12, <https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>
4. European Commission, *State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks*, <https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193>
5. European Parliament, *Cyber: How big is the threat?*, <https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf>
6. Gotsiridze A., *The Cyber Dimension of the 2008 Russia-Georgia War*, <https://www.gfsis.org/blog/view/970>
7. IHS Markit, *The Internet of Things: a movement, not a market*, 2017, <https://cdn.ihs.com/www/pdf/IoT_ebook.pdf>
8. Limnell J., *Russian cyber activities in the UE*, [in:] *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, eds. N. Popescu, S. Secrieru, European Union Institute for Security Studies (EUISS), 2018
9. Morrison S., *How a major oil pipeline got held for ransom*, <https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices>
10. Nabe C., *Impact of COVID-19 on Cybersecurity*, <https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html>
11. Noyan O., *The New EU Cyber Security Strategy – Exploring Ways to Shape Europe's Digital Future*, <https://finabel.org/the-new-eu-cyber-security-strategy-exploring-ways-to-shape-europes-digital-future/>
12. *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*, <https://ec.europa.eu/commission /presscorner/detail/en/ip_20_2391>

13. Poptchev P., *NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages*, "Information & Security: An International Journal", Volume 45, (2020)
14. Schneier B., *China Isn't the Only Problem With 5G*, <https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/>
15. Svanadze V., Gotsiridze A., *Cyber Defence. The main players in cyberspace. Cyber Security Policy, Strategy and Challenges*, Tbilisi 2015
16. *The Cybersecurity Strategy*, <https://digitalstrategy.ec.europa.eu/en/policies/cybersecurity-strategy>
17. Toso de Alcântara B., *The coronavirus pandemic and its impact on cybersecurity*, <https://www.hiig.de/en/the-coronavirus-pandemic-and-its-impact-on-cybersecurity/>
18. *Wild Wide Web – Consequences of Digital Fragmentation*, <https://reports.weforum.org/global-risks-report-2020/wild-wide-web/>