Petar Djukic, MSc in Security Studies

PhD Candidate at the Faculty of Security Studies, University of Belgrade
Senior Assistant at the University of Modern Sciences, Mostar
E-mail: petar.djukic96@yahoo.com

DOI: 10.37458/ssj.3.2.7
Research Paper
Received: November 16, 2022
Accepted: December 17, 2022

(RE)CONCEPTUALIZATION OF THE TERM *CYBERSECURITY* IN THE EUROPEAN UNION'S SECURITY POLICY

Abstract: *The term Cybersecurity has been in use for a while now. Yet, the current level of technological development of society intensifies its usage. The largest number of requests to change the traditional security agenda goes in the direction of expanding the research of security science in the sector of cybersecurity. A precondition for something like that is the removal of existing unclarities about the theoretical designation and practical value of the concept. That certainly asks for detailed scientific research. In the last decade, a tendency of emphasizing the concept of cybersecurity in the security policy of the European Union has been noted. It mostly follows its implementation in various strategic documents, but also its operationalization and institutionalization within the EU and its activities. Therefore, the topic of this essay is the (re)conceptualization of the term Cybersecurity in the security policy of the EU. The aim is to determine the term and clarify and demystify the concept of cybersecurity as much as possible. Another aim is to look into how the EU, as a specific supranational organization, approaches this concept through its general and special strategic documents, i.e., its entire security agenda. The methodology of this essay is the overview of the existing scientific and expert literature, an analysis of the EU's strategic and normative framework, as well as documents and reports of the EU institutions. The conclusion should be that the EU recognizes the potential and importance of the concept of cybersecurity within its security policy. However, it is necessary to keep the continuity in work on the definition and operationalization of the concept of cybersecurity, so it would not encompass too extensive range.*

Keywords: *Cybersecurity, European Union, strategy, security policy, concept*

INTRODUCTION

It is difficult to find a word used more often in the vocabulary of modern politics and geopolitics than it is the case with the word *security*. Security represents one of the basic human needs and it is equally necessary to all human beings, of any gender, race, nationality, religion, social status, etc. However, the very term security has had different interpretations throughout history. It would be defined and redefined numerous times. On the other side, the development of security science went parallelly with the development of human society. Nowadays, the number of supporters of the initiative to widen-deepen classic security paradigms is growing and they argue that the world has changed so much that the classic paradigm is getting too narrow and not inclusive for numerous security issues (Kucekovic, 2014, p. 76). In that sense, we can argue that the technology is definitely one of the numerous driving forces influencing the development of this scientific discipline in the sense of changing the nature of dangers and possible vulnerability of reference objects. Perhaps the most characteristic example is cyber security, where the fast development in the field of ICT has provided a variety of new functions and services, both for private and business use, creating in the same time a number of vulnerabilities and security issues. Today, cyber security is a separate topic in most of analysis and discussions. Impressive technological advances will only increase the significance of this category for the overall security framework in the future (Dragas, 2020; Todorovic & Trifunovic, 2020). The dynamics of security that used to fill out the real space have swamped the so-called **cyberspace** long ago.

Modern informational technology transforms the industrial into an informatic society irreversibly and changes lifestyles and habits drastically. The majority of mundane interactions as well as state functions have been moved to cyberspace: from e-banking and e-trade, homeschooling and work from home, e-government to the digitalization of national defense and security systems or international links between states and nations. The idea of space and time has seen a radical transformation with relevant consequences for related concepts such as distance, territory, limits, separations, or borders (Mijalkovic et al., 2010; Putnik, 2012). In simple terms, the internet made the world seem smaller. It also however leaves huge possibilities for IT-educated individuals with dishonorable intentions to jeopardize people's safety in many ways and make "old crimes in a new way". Besides, cyberspace is a field of competition between great powers and other

participants in political, ideological, economic, military, and other areas. Countries have recognized cyberspace as a fifth battlefield, after land, water, air, and cosmos. The new cyberspace offered great possibilities for conducting special propaganda activities and also carrying out attacks on rival IT systems. That is **cyber warfare** (Miljkovic, Putnik 2016, p. 16, Ifrah 2008; Seemma et al., 2018). Also, permanent conflicts in cyberspace have already taken the form of political struggle, since this virtual sphere also affects the outcomes of elections in the most developed world democracies (Dragas, 2020).

The aforementioned argument that technology is the driving force of the development of security science brings us to the following: the development of ITC technology changed the nature of dangers and vulnerability of reference objects, thus expanding the security agenda. So security threats now include cyber threats and vulnerabilities (whether it being of individual, collectivity, state, or international systems) are expanded to so-called "cyber-goods" (Mijalkovic et al., 2010). However, this technology did not only indicate new threats; it also made the identification of a potentially dangerous individual or group much harder. There can be various threat actors – malicious individuals, organized crime groups, terrorist organizations, and economic subjects, but also states and their institutions (army, security service) with different motives: economy, politics, ideology, religion, or military (Miljkovic, Putnik, 2016, p. 164). Joseph Nye (2012) identifies four main categories of cyber threats that may differ amongst themselves based on their actual connection with the state or non-state actors. So cyber war and espionage are encouraged and started by states, while cyber terrorism and crime are by non-state affiliated elements, such as terrorists or criminals.

There is something that will represent a higher challenge for security in the future and that is the possibility to manipulate distant objects, i.e. satellites. Huge flaws are discovered in satellite systems and they are caused by the "mentality of unclear security" by the producers of these products. Security analysis of satellite user terminals unveiled that many producers use hardcode credentials, Insafe protocols, and weak mechanisms of authentication. This mentality is not favorable for the systems that use cyber technology, especially if they are to support critical infrastructure that attracts the interest of the hacker community (Manulis et al., 2020).

There is no doubt that the widening-deepening security agenda left its mark on the security policies of nation-states, and regional and international organizations, including the European

Union. This essay aims to analyze the concept of *cybersecurity* through the basic strategic documents that make the frame of the security agenda of the EU, i.e. the way the EU adjusted its security policy to new challenges of cybersecurity such as cyber threats and cyberattacks.

THEORETICAL DETERMINATION OF THE TERM *CYBERSECURITY*

Cybersecurity as a term can be often found in the academic literature where it is defined and used by different authors in various ways. The oldest term known that is alike to cybersecurity is the term *information security* (also: computer security, IT security). The idea of this concept emerged in the late 1980s in the USA and it integrated previously separated areas of staff security, computer security, communication security, and operation security (Mijalkovic et al., 2010, p. 8). Cybersecurity as a modern term has a much wider meaning and it is multidisciplinary. The popularity of this term is also related to the USA and its former president Barack Obama who called for the people of the USA to recognize the importance of cybersecurity in 2009 (Schatz et al., 2017).

In order to fully grasp the concept of cybersecurity and determine it adequately, we need to start with its etymology. There is no need to elaborate on the meaning of security, but we will briefly explain the "cyber" part of this term. Prefix "cyber" is tied to the term "cybernetics" (from Greek *κῠβερνάω* (kubernáō) - to steer), it marks cyberspace and refers to electronic communication networks and virtual reality. Cybernetics is a scientific discipline that studies living and non-living systems, their structure, communication possibilities, principles of actions, and especially mechanisms of control, regulation, and autoregulation of the balance through feedback. The first modern meaning of the word "cyber" was given by Canadian author William Gibson in his novel "Neuromancer" (1984), where the term "cyber" has represented something virtual, invisible, unlimited, and based on technology (Vuletic, 2017). Gibson is the first to coin the term cyberspace which will become very important for the concept of cybersecurity. Gibson's cyberspace is a digital universe of billions of legitimate operators, a graphical representation of constellations of data abstracted from the banks of every computer in the human system (Putnik, 2012). According to *Webopedia*, cyberspace is a metaphor for describing the non-physical terrain created by computer systems within which people can communicate with one another. The most

precise definition of cyberspace is given by the U.S. Department of Defense; they define cyberspace as a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. That is an "imagined surrounding where digital data is transmitted via computer networks" (Vuletic, 2017, p. 174).

Cyberspace is far from static; it is a dynamic, multi-layered ecosystem of physical infrastructure, software, regulations, ideas, innovation, and interactions that constantly evolve. By its nature it is expansive and limitless, growing without consideration for any physical or political border (Craigen et al., 2014; Goutam, 2015). The term *cyber* is much wider than the term *Internet* and that can be seen from the aforementioned definition. Most national strategies for cybersecurity adopt a holistic approach to cyberspace. German strategy, however, specifies only IT communications on Internet as cyberspace. Australia, Canada, Spain, and New Zealand have a similar approach. The strategy of the Netherlands, for example, expands the term to chip cards, vehicle systems, or informative media. Czech Republic, Estonia, France, and South Africa have similar approaches (Luiijf et al., 2013).

Before we move to the attempt of defining or theoretically determining the concept of cybersecurity, it is necessary to make a distinction between cybersecurity and information security. Although they might overlap, these two concepts are not completely equal. Cybersecurity overcomes the limits of traditional information security and involves not only the protection of information but also the protection of people and assets. Information security focuses on the role of the human factor in the security process. On the other side, cybersecurity has another dimension to it – people as potential targets of cyberattacks or even being unaware to participate in a cyberattack. This extra dimension separates cybersecurity from the traditional concept of information security and it has ethical implications for the entire society. The protection of certain vulnerable groups, i.e., children, can be seen as a social responsibility (Von Solms & Van Niekerk, 2013).

Cybersecurity is defined from different standpoints of various scientific disciplines: IT, engineering, political science, psychology, sociology, criminal science, etc. Cybersecurity has been defined by various authors, states, and organizations. According to Lewis (2006),

cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and malicious damage or disruption. Radomir Milasinovic et al. (2012, p. 32) see cybersecurity as the safety of the Internet and modern information society, technology, and its users. An interesting definition of cybersecurity is given by Canongia and Mandarino (2014) who interpret it as "the art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets, and critical infrastructure". According to Oxford's Dictionary (2014), cybersecurity represents the state of being protected against the criminal or unauthorized use of electronic data, including the measures to achieve that state. For example, the National strategy of cybersecurity of France gives the following definition: "Cybersecurity is an information system allowing to resist likely events resulting from cyberspace which may compromise the availability, the integrity or confidentiality of data stored, processed or transmitted and of the related services that information and communication (ICT) systems offer" (Luiijf et al., 2013). In the end, it is interesting to mention research titled "Towards a More Representative Definition of Cybersecurity" by Schatz et al (2017). In this work, they study the existing literature to identify the main definitions provided for the term *cybersecurity* by authoritative sources. Then they conduct various lexical and semantic analysis techniques in an attempt to better understand the scope and context of these definitions, along with their relevance. Finally, based on the analysis conducted, they propose a new improved definition that we then demonstrate to be a more representative definition using the same lexical and semantic analysis technique. This concept includes guidelines, policies, and collections of protection mechanisms, technologies, tools, and training to provide the best protection for cyberspace and its users.

In the attempt to build a conceptual analysis of the term cybersecurity, we will use the conceptual frame set by Lipovac (2014), based on the following questions:

1. What is the reference object?
2. What are the values to be protected?
3. What are the security threats?
4. Who provides security?
5. By which means security is accomplished?

Reference objects of cybersecurity are individual, state, a complex of states, and the international system as a whole. Values that are supposed to be protected are so-called “cyber-goods” of reference objects. There is a wide range of cybersecurity threats and it goes from criminal activities against individuals to cyber operations that jeopardize the security of entire states or international organizations, so we can talk about cybercriminal, cyberterrorism, and cyberwarfare (Nedeljkovic & Forca, 2015; Milosevic & Putnik, 2017, p. 178). Besides conventional security providers, cybersecurity is provided by individuals and organizations with specific knowledge of IT technology. There is an open question if police officers, soldiers, or security service officers should be trained in IT technology or turn IT experts into policemen, informants, or military officers. Also, conventional security instruments and methods are useless on the fifth battlefield.

In the end, it is important to look back at the relation between the term “cybersecurity” and the terminology developed in the context of the new practices of waging warfare – cyberwarfare, IT warfare, hybrid warfare, etc. These terms are closely tied and are often used as synonyms. Yet, all of them are basically lower parts of cybersecurity and do not include a variety of challenges, risks and cyber threats. In her article “Information Warfare: What and How?” (1999), Megan Burns defines information warfare as a class of techniques, including collection, transport, protection, denial, disturbance, and degradation of information, by which one maintains an advantage over one's adversaries. The term of cyberwarfare is narrower and can be defined as an information warfare that is being waged via computer network (Putnik, 2012). Also, today we are witnesses of a very intensified use of the term “hybrid warfare”. This should not refer to any classical war with the usage of conventional weaponry. On the contrary, hybrid warfare should be waged with unconventional means such as information technologies in a cyberspace. Hybrid warfare is a part of a special warfare, yet this term refers to a specific action supported by a foreign security service or services by using modern means such as: internet, social networks, web portals and websites designed specially for the needs of cybersphere (Trifunovic and Obradovic, 2020). According to the US Department of Defense (2019), hybrid warfare can include “information operations, troop movements, disinformation campaigns, cyberattacks or a combination of all these things. It is an amorphous definition for an amorphous strategy”. Therefore, we can conclude that hybrid warfare is one of the leading challenges for cybersecurity of states and international organizations.

FOUNDATION OF THE CONCEPT OF CYBERSECURITY IN THE STRATEGIC DOCUMENTS OF THE EUROPEAN UNION

The first significant document about the important area of threats to the cybersecurity of individuals and states – high-tech crime, is the Council of Europe **Convention on Cybercrime** formed on November 23rd, 2001 in Budapest, Hungary. The treaty had three prime objectives, including the improvement in investigative techniques, increase in cooperation among nations, and lastly, harmonizing national laws. Yet, there was no mention of the term "cybersecurity". The next important document was the **European Security Strategy** adopted on December 12th, 2003, under the title "A Secure Europe in a Better World". One of the three strategic aims defined in this document refers to fighting cyber threats and in Javier Solana's report to the Council of Europe in 2008, it is emphasized that more work is required in this area, as identified threats are more complex. Since attacks against private or government IT systems have not stopped but given this a new dimension as cybercrime (Ivetic & Pavlovic, 2012). However, not even this document defined cybersecurity nor even mentioned this term in detail.

The first time cybersecurity is mentioned as a term in public documentation is in the Council of Europe study from 2009, which is a report on the implementation of the European Security Strategy from 2003. It is where it is said that "it is no exaggeration to say that the 21st-century economy, and much of society itself, is dependent upon a broadband-enabled, cyber-knowledge complex". The EU Strategy for a Secure Information Society, adopted in 2006 addresses internet-based crime. However, attacks against private or government IT systems in EU Member States have given this a new dimension, as a potential new economic, political and military weapon. It is emphasized that more work is required in this area, to explore a comprehensive EU approach, raise awareness and enhance international cooperation (European Security Strategy - A Secure Europe in a Better World, 2009). Based on that and as a response to more complexities in new challenges and threats to security, **the Stockholm Programme** has been adopted in 2009. Following that, in 2010 the EU adopted its **Internal Security Strategy (ISS)**. Among five

strategic EU-level priorities one that stands out is raising "levels of security for citizens and businesses in cyberspace" (Carrera & Guild, 2011; Ivetic and Pavlovic, 2012:56). Until 2013, EU strategic acts were rather abstract when cybersecurity is concerned. The first precise strategic document on cybersecurity is **The EU Cyber Security Strategy (EUCSS)** adopted in 2013 under the motto "an Open, Safe and Secure Cyberspace". Ever since there have been multiple general and specific strategic documents on the security agenda of the European Union and a few of them are the subjects of interpretation in this essay. Those are:

1. The EU Cyber Security Strategy – EUCSS (2013)
2. Security Agenda of European Union (2015-2020)
3. A Global Strategy for the European Union's Foreign and Security Policy (2016)
4. Joint communication to the European Parliament and the Council - Resilience, Deterrence and Defense: Building strong cybersecurity for the EU (2017)
5. The EU Security Union Strategy (2020)
6. The EU's Cybersecurity Strategy for the Digital Decade (2020)
7. The Cyber Resilience Act (2022).

The EU Cyber Security Strategy – EUCSS (2013)

This is the first actual strategic document on cybersecurity. For cyberspace to remain open and free, the same norms, principles, and values that the EU upholds offline should also apply online. Fundamental rights, democracy, and the rule of law need to be protected in cyberspace. But freedom online requires safety and security too. The safety and security of cyberspace depend on both governments and the private sector. Threats can have different origins — including criminal, politically motivated, terrorist, or state-sponsored attacks as well as natural disasters and unintentional mistakes. All of these notes can be found in the introduction part of this strategy, but the definitions of cybersecurity and cybercrime are found in the footnotes.

"Cybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber
domain, both in the civilian and military fields, from those threats that are associated with or that, may harm its interdependent networks and information infrastructure. Cyber-security strives

to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein" (European Commission, 2013, p. 3).

"Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offenses (e.g. fraud, forgery, and identity theft), content-related offenses (e.g. online distribution of child pornography or incitement to racial hatred), and offenses unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)" (European Commission, 2013, p. 3).

EUCSS gives us the principles for cybersecurity:

- The EU's core values apply as much in the digital as in the physical world
- Protecting fundamental rights, freedom of expression, personal data, and privacy
- Access for all
- Democratic and efficient multi-stakeholder governance
- A shared responsibility to ensure security

The EU vision presented in this strategy is articulated in five strategic priorities (European Commission, 2013).

The first strategic priority is to promote cyber resilience in the EU through a policy on Network and Information Security (NIS) owned by the European Network and Information Security Agency (ENISA). Member States are obliged to: designate national competent authorities for NIS; set up a well-functioning Computer Emergency Response Team - CERT; and adopt a national NIS strategy and a national NIS cooperation plan. National NIS competent authorities should collaborate and exchange information with other regulatory bodies, and in particular personal data protection authorities. The emphasis is also on developing informal and voluntary cooperation, including between public and private sectors through the European Public-Private Partnership for Resilience.

The second strategic priority is drastically reducing cybercrime with the help of strong and effective legislation, enhancing operational capability to combat cybercrime, and improving coordination at the EU level.

The third strategic priority is developing a cyber-defense policy and capabilities related to the framework of the Common Security and Defense Policy. Cyber-defense capability development should concentrate on detection, response, and recovery from sophisticated cyber threats. These efforts should be supported by both civilian and military approaches. Closer cooperation with NATO and other international organizations has been advised.

The fourth strategic priority is the development of industrial and technological resources for cybersecurity. It should be done by promoting a single market for cybersecurity products and fostering R&D (research and development) investments and innovation.

Finally, the fifth strategic priority is to establish a coherent international cyberspace policy for the European Union and promote EU core values. Preserving open, free, and secure cyberspace is a global challenge, which the EU should address together with the relevant international partners and organizations, the private sector, and civil society. Therefore, the key should be mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy. EU supports the development of norms of behavior and confidence-building measures in cybersecurity. Also, the fifth strategic priority asks for the utilization of different EU aid instruments for cybersecurity capacity building, as well as supporting the creation of relevant national policies, strategies, and institutions in third countries.

Security Agenda of European Union (2015-2020)

The European Agenda on Security has been adopted in 2015 by the European Commission. This document fortifies the joint approach of all EU member states on security. According to the Agenda, all actors involved have to work together in the area of security, and that cooperation is based on five key principles: full compliance with fundamental rights; providing more transparency, accountability, and democratic control, to give citizens confidence; ensuring better application and implementation of existing EU legal instruments; encouraging joined-up inter-agency and a cross-sectorial approach and bringing together all internal and external dimensions of security (European Commission, 2015).

The Agenda prioritizes terrorism, organized crime, and cybercrime as interlinked areas with a strong cross-border dimension, where EU action can make a real difference. Cybercrime is an ever-growing threat to citizens' fundamental rights and the economy, as well, as to the

development of a successful Digital Single Market. As commerce and banking shift online, cybercrime can represent a huge potential gain to criminals and a huge potential loss to citizens. Cybercriminals can act from outside the Union to harm critical infrastructures and simultaneously target a large number of victims across the Member States, with minimum effort and risk. Similarly, threats such as those posed by cyber-terrorism and hybrid threats could increase in the years to come. Criminals abuse anonymization techniques and anonymous payment mechanisms for illicit online trade in drugs or weapons, criminal transactions, and money laundering. Cybercrime is also closely linked to child sexual exploitation, with a growing and alarming trend of child abuse through live streaming (European Commission, 2015).

We see that there was a lot about cyber criminals as a form of endangering cybersecurity, its causes, modalities, and consequences. An entire section of the Agenda (3.3) has been dedicated to battling cybercriminals. Cybersecurity is the first line of defense against cybercrime. The 2013 EU Cybersecurity Strategy focuses on identifying high-risk areas, working with the private sector to close loopholes, and providing specialized training. An important element in implementing the Strategy will be the swift adoption of the proposal for a Directive on network and information security. The implementation of this Directive would not only promote better cooperation between law enforcement and cybersecurity authorities but also provide for cyber-security capacity building of competent Member States' authorities and cross-border incident notification. The EU Agency for Network and Information Security also contributes to the EU's response to cybersecurity issues by working towards a high level of network and information security. Ensuring full implementation of existing EU legislation is the first step in confronting cybercrime. The 2013 Directive on attacks against information systems criminalizes the use of tools such as malicious software and strengthens the framework for information exchange on attacks. Cybercrime is by its nature borderless, flexible, and innovative. In prevention, detection, and prosecution, law enforcement has to be able to match and anticipate the ingenuity of the criminals. Cyber criminality requires competent judicial authorities to rethink the way they cooperate within their jurisdiction and applicable law to ensure swifter cross-border access to evidence and information, taking into account current and future technological developments such as cloud computing and the Internet of Things. Gathering electronic evidence in real-time from other jurisdictions and ensuring its admissibility in court are key issues. It also requires

highly-skilled law enforcement staff able to keep pace with the considerable increase in the scope, sophistication and types of cybercrime.

Clear rules are needed to ensure that data protection principles are respected in full, while law enforcement gains access to the data it needs to protect the privacy of citizens against cybercrime and identity theft. Cooperation with the private sector is also of critical importance, with public-private partnerships to structure a common effort to fight online crime. The response to cybercrime (e.g. phishing) must involve the entire chain: from Europol's European Cybercrime Centre, Computer Emergency Response Teams in the Member States concerned by the attack, to internet service providers that can warn end-users and provide technical protection. In short, cybercrime demands a new approach to law enforcement in the digital age (European Commission, 2015).

From the all above we can see that the European Agenda on Security (2015) identifies the term cybersecurity with cybercrime or high-tech crime as an elementary threat to cybersecurity. The conclusion is that the successful implementation of the Agenda depends on the political commitment of all actors concerned to do more and to work better together. This includes EU institutions, Member States, and EU agencies. The EU must be able to react to unexpected events, seize new opportunities and anticipate and adapt to future trends and security risks, including, of course, the challenges of cybersecurity.

A Global Strategy for the European Union's Foreign and Security Policy (2016)

A Global Strategy for the European Union's Foreign and Security Policy is formed as a document giving basic directions for EU Foreign Affairs Policy in an ever-changing world of globalization and dynamics. This strategy promotes efforts on defense, cybersecurity, counterterrorism, energy, and strategic communications. The EU will step up its contribution to Europe's collective security, working closely with its partners, beginning with NATO, and countries such as USA and Canada (European Commission, 2016).

EU should be able to assist in protecting its Members upon their request. This means living up to our commitments to mutual assistance and solidarity and includes addressing challenges with both an internal and external dimension, such as terrorism, hybrid threats, cyber and energy security, organized crime, and external border management. Alongside, the EU will support the

swift recovery of Members States in the event of attacks through enhanced efforts on the security of supply, the protection of critical infrastructure, and strengthening the voluntary framework for cyber crisis management. So, in the introductory parts of the Global Strategy, cybersecurity has been already mentioned twice.

Then there is an entire section titled *Cyber Security*. The EU will increase its focus on cyber security, equipping the EU and assisting Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace. This entails strengthening. the technological capabilities aimed at mitigating threats and the resilience of critical infrastructure, networks, and services, and reducing cybercrime. It means fostering innovative information and communication technology (ICT) systems that guarantee the availability and integrity of data while ensuring security within the European digital space through appropriate policies on the location of data storage and the certification of digital products and services. It requires weaving cyber issues across all policy areas, reinforcing the cyber elements in CSDP missions and operations, and further developing platforms for cooperation. The EU will support political, operational and technical cyber cooperation between Member States, notably on analysis and consequence management, and foster shared assessments between EU structures and the relevant institutions in the Member States. It will enhance its cyber security cooperation with core partners such as the US and NATO. The EU's response will also be embedded in strong public-private partnerships. Cooperation and information-sharing between Member States, institutions, the private sector and civil society can foster a common cyber security culture, and raise preparedness for possible cyber disruptions and attacks (European Commission, 2016).

The Global Strategy points out that the EU will be a forward-looking cyber player, protecting our critical assets and values in the digital world, notably by promoting a free and secure global Internet. The EU will engage in cyber diplomacy and capacity building with its partners, and seek agreements on responsible state behavior in cyberspace based on existing international law. Also, the Union will support multilateral digital governance and a global cooperation framework on cybersecurity, respecting the free flow of information (European Commission, 2016).

In conclusion, cybersecurity has had a significant place in A Global Strategy for the European Union's Foreign and Security Policy since 2016. Yet this document does not give an explicit definition of the term. It explains the term implicitly by enumerating threats to cybersecurity,

strategies, and actors. It is important to emphasize that the Strategy is using terms*: cyberspace, cyber diplomacy, cyber crisis, cyber player, cyber disruption, cyber-attack* and *cybercrime.*

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defense: Building strong cybersecurity for the EU (2017)

This document follows up on A Global Strategy for the European Union's Foreign and Security Policy. In the introductory part, it is emphasized that cybersecurity is critical to both our prosperity and our security. Malicious cyber activities not only threaten our economies and the drive to the Digital Single Market, but also the very functioning of our democracies, our freedoms and our values. The risks are increasing exponentially. Cyber threats come from both non-state and state actors: they are often criminal and motivated by profit, but they can also be political and strategic. The next topic is the security of the "Internet of Things" devices. A failure to protect the devices which will control our power grids, cars and transport networks, factories, finances, hospitals and homes could have devastating consequences and cause huge damage to consumer trust in emerging technologies. The risk of politically-motivated attacks on civilian targets, and shortcomings in military cyber defense, deepen the risk still further (European Commission, 2017).

The first part of this document focuses on strengthening the resilience of the EU to cyber-attacks. Resilience may be achieved by the following:

- Strengthening the European Union Agency for Network and Information Security - ENISA
- Formation of a Single Cybersecurity Market as an EU cybersecurity certification framework covering products, services and/or systems
- Implementing the Directive on the Security of Network and Information Systems in full
- Resilience through rapid emergency response
- A cybersecurity competence network with a European Cybersecurity Research and Competence Centre

- Building a strong EU cyber skills base starting from regular training of a cyber workforce, additional cybersecurity training for all ICT specialists, and new specific cybersecurity curricula

- Promoting cyber hygiene and awareness through e-government and awareness campaigns.

The next part of the document is characterized as “creating effective EU cyber deterrence”. Effective deterrence means putting in place a framework of measures that are both credible and dissuasive for would-be cyber criminals and attackers. This framework consists of the following:

- Identifying malicious actors
- Stepping up the law enforcement response by Effective investigation and prosecution of cyber-enabled crime
- Public-private cooperation against cybercrime
- Stepping up the political response - joint EU diplomatic response to malicious cyber activities
- Building cybersecurity deterrence through the Member States' defense capability

The third part is about strengthening international cooperation on cybersecurity. Guided by the EU's core values and fundamental rights such as freedom of expression and the right to privacy and protection of personal data, and the promotion of open, free and secure cyberspace, the EU's international cybersecurity policy is designed to address the continuously evolving challenge of promoting global cyber stability, as well as contributing to Europe’s strategic autonomy in cyberspace. It is based on the following:

- Cybersecurity in external relations - the position that international law, and in particular the UN Charter, applies in cyberspace
- Cybersecurity capacity building
- EU-NATO cooperation

In conclusion, EU cyber preparedness is central to both the Digital Single Market and its Security and Defense Union. Enhancing European cybersecurity and addressing threats to both civilian and military targets is a must (European Commission, 2017).

The EU Security Union Strategy (2020)

European Commission presented a new strategic document for the Security Union in order to offer a security dividend to protect everyone in the EU and the "European way of life". This Strategy covers the period 2020-2025 and focuses on building capabilities and capacities to secure a future-proof security environment. Among other things, this document recognizes the importance of cybersecurity in the introductory part that cyber-attacks and cybercrime continue to rise.

The ever-increasing ways in which digital technologies benefit our lives have also made the cybersecurity of technologies is an issue of strategic importance. Homes, banks, financial services and enterprises are heavily affected by cyber-attacks. The potential damage is multiplied still further by the interdependence of physical and digital systems. The rise of the Internet of things and the increased use of artificial intelligence will bring new benefits as well as a new set of risks. Online dependency has opened the door to a wave of cybercrime, especially cyber theft and different types of cyber-attacks. Economic operators must take greater responsibility for the cybersecurity of products and services they place on the market; while individuals need to have at least a basic understanding of cybersecurity to be able to protect themselves (European Commission, 2020a).

The Strategy as well as other documents, contains a section only about cybersecurity. It is said that the number of cyber-attacks continues to rise. These attacks are more sophisticated than ever, come from a wide range of sources inside and outside the EU and target areas of maximum vulnerability. State or state-backed actors are frequently involved, targeting key digital infrastructures like major Cloud providers. Cyber risks have emerged as a significant threat to the financial system as well. The EU now needs to make sure that its cybersecurity capabilities keep pace with reality, to deliver both resilience and response. One of the most important long-term needs is to develop a culture of cybersecurity by design, with security built into products and services from the start. The aim should be to create mandatory and high common standards for the secure exchange of information and the security of digital infrastructures and systems across all EU institutions, bodies and agencies. Given its global nature, building and maintaining robust international partnerships is fundamental to further prevent, deter and respond to cyber-attacks (European Commission, 2020a).

A section on tackling evolving threats has the topic of Cybercrime in first place and the resilient environment created by strong cybersecurity is seen as the first defense. According to this document, nearly half of EU citizens worry about data misuse and identity theft is a major concern. The fraudulent use of identity for financial gain is one aspect, but there can also be a major personal and psychological impact, with illegal postings made by the identity thief able to stay online for years.

The EU's Cybersecurity Strategy for the Digital Decade (2020)

In March 2021, the Council of Europe adopted a document titled "The EU's Cybersecurity Strategy for the Digital Decade", presented by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. This strategic document is the EU's response to rapid digitization and increased reliance on new technologies, where working patterns have been accelerated by the COVID-19 pandemic (Novicic, 2021).

The introductory part of the Cybersecurity Strategy is mostly descriptive. In this section, cybersecurity is recognized as an integral part of European security. Cybersecurity is therefore seen as essential for building a "resilient, green and digital Europe". Transport, energy and health, telecommunications, finance, security, democratic processes, space and defense are heavily reliant on network and information systems that are increasingly interconnected. Hybrid threats, that combine disinformation campaigns with cyberattacks on infrastructure, economic processes and democratic institutions, are seen as activities that undermine international security and stability. The investigation of nearly all types of crime has a digital component. Digital services and the finance sector are among the most frequent targets of cyberattacks, along with the public sector and manufacturing, yet cyber readiness and awareness among businesses and individuals remain low, and there is a major shortage of cybersecurity skills in the workforce. Improving cybersecurity is therefore essential for people to trust, use, and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information (European Commission, 2020b).

Following the progress achieved under the previous strategies, it contains concrete proposals for deploying three principal instruments –regulatory, investment and policy instruments – to

address
three areas of EU action – (1) resilience, technological sovereignty and leadership, (2) building operational capacity to prevent, deter and respond, and (3) advancing global and open cyberspace. In the following paragraphs, we will show you some aspects of cybersecurity from the Cybersecurity Strategy (European Commission, 2020b).

First of all, the Commission proposes to reform these rules under a revised NIS Directive to increase the level of cyber resilience of all relevant sectors, public and private, that perform an important function for the economy and society. The review is necessary to reduce inconsistencies across the internal market by aligning the scope, security and incident reporting requirements, national supervision and enforcement and the capabilities of competent authorities (Novicic, 2021). Strengthening the cyber resilience of democratic processes and institutions is a core component of the European Democracy Action Plan for safeguarding and promoting free elections, and democratic discourse, and media plurality.

Secondly, the Cybersecurity Strategy proposes building a so-called **European Cyber Shield**. That is a network of Security Operations Centers across the EU. This network should be able to detect potential threats and provide timely warnings on cybersecurity incidents to authorities and all interested stakeholders. It will serve as a real cybersecurity shield for the EU by exchanging important information and preventing cyber-attacks to improve European cybersecurity.

The next topic is the so-called **Internet of Secure Things** – devices connected online in a way they can exchange data without human agency. The number of such devices is already higher than the number of people on Earth (Novicic, 2021). Every connected thing contains vulnerabilities that can be exploited with potentially widespread ramifications. The Commission is already working to ensure transparent security solutions and certification under the Cybersecurity Act and to incentivize safe products and services without compromising on performance. It includes care for connected device manufacturers to address software vulnerabilities including the continuation of software and security updates as well as ensuring, at the end of life, the deletion of personal and other sensitive data.

One of the aims of the Cybersecurity Strategy is the increased presence of European companies in the supply chain of technology (Novicic, 2021). It can unlock private investments through

public-private partnerships and support for small and medium businesses. The objective is to trigger a similar number of investments by the Member States, in the proposed Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centers (CCCN). The Commission intends to support, potentially with the CCCN, the development of a dedicated cybersecurity Masters's program, and contribute to individual Internet innovators developing privacy-enhancing and secure communication technologies based on open-source software and hardware.

The Cybersecurity Strategy also refers to the workforce with cybersecurity-related skills. It is estimated that there are 291.000 open work positions in Europe for cybersecurity experts. The EU's efforts to upskill the workforce, develop, attract and retain the best cybersecurity talent and invest in world-class research and innovation, form an important component of protecting against cyber threats generally. This field offers great potential. Hence specific attention must be paid to developing, attracting and retaining more diverse talent in order to raise cybersecurity awareness among individuals, especially children and young people, and organizations. It is also necessary to encourage women's participation in science, technology, engineering, and mathematics education and ICT jobs upskilling and reskilling in digital skills.

Sixthly, a smaller chapter in the Cybersecurity Strategy is about protection from high-tech crime. As mentioned above, the investigation of nearly all types of crime has a digital component. Tackling cybercrime effectively is a key factor in ensuring cybersecurity: deterrence cannot be achieved through resilience alone but also requires the identification and prosecution of offenders (Novicic, 2021). As one important element of that response, EU and national authorities need to expand and improve the capacity of law enforcement to investigate cybercrime, fully respecting fundamental rights and pursuing the required balance between various rights and interests.

Finally, the Cybersecurity Strategy promotes the so-called **cyber diplomacy toolbox** used by the EU to prevent, discourage, deter and respond to malicious cyber activities. The High Representative of the Union for Foreign Affairs and Security Policy will encourage and facilitate the establishment of a Member States' EU cyber intelligence working group residing to advance strategic intelligence cooperation on cyber threats and activities. In addition, the EU should further integrate the cyber diplomacy toolbox in EU crisis mechanisms, and seek synergies with

efforts to counter hybrid threats, disinformation and foreign interference. Building on the work under the cyber diplomacy toolbox to date, the **cyber deterrence posture** should contribute to responsible state behavior and cooperation in cyberspace, and should give particular direction on countering those cyber-attacks that have the most significant effect, notably those affecting our critical infrastructure, democratic institutions and processes, as well as supply chain-attacks and cyber-enabled theft of intellectual property (Novicic, 2021).

The Cyber Resilience Act (2022)

In September 2022, members of EU Parliament proposed the Cyber Resilience Act. This document contains rules and standards of cybersecurity for products with digital elements (computers, phones, home devices, vehicles, toys). Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of EUR 5.5 trillion by 2021. It is acknowledged that most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity. In particular, the current EU legal framework does not address the cybersecurity of non-embedded software, even if cybersecurity attacks increasingly target vulnerabilities in these products, causing significant societal and economic costs (Cyber Risk GmBH, 2022a). The adoption of this act shows the shift in speed of changes in the cybersphere and such changes require adequate and timely response. Following that, EU recognized the importance of the security of products in a connected environment. It is hugely significant to bring order in the market of those products so both producers and customers know their obligations.

The proposed Cyber Resilience Act brings a couple of key measures, including basic security demands for products as well as the obligations for their product owners regarding dealing with vulnerabilities once they are discovered. According to that, this Regulation lays down:

- rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products;
- essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;

- essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;
- rules on market surveillance and enforcement of the above-mentioned rules and requirements (Cyber Risk GmBH, 2022a).

The EU Cyber Resilience Act, among other things, demands from companies the following: from the placing on the market and for the expected product lifetime or for a period of five years after the placing on the market of a product with digital elements, whichever is shorter, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate. This Regulation lays down essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA any actively exploited vulnerability contained in the product with digital elements and, where applicable, any corrective or mitigating measures taken (Cyber Risk GmBH, 2022a). Considering this Act is still in the phase of proposition, we are yet to see the manners and effects of its implementation.

The Cybersecurity of European Union – Challenges, risks, threats

The challenges, risks and threats to cybersecurity of European Union we can divide into two groups: a) those coming from the "independent hackers" with elements of cybercrime in their actions and b) those coming as threats from other countries. The aims of cyber criminals may be (and in most cases are) of lucrative nature – obtaining illegal property benefits – or terrorism – causing fear or disturbance for greater number of people. Unlike them, state activities in the cyberspace are more sophisticated and organized by intelligence services. Their aims may vary – destabilization of order in another country, causing riots, generating fake news, social engineering, obtaining secret data etc. in simple terms, we talk about waging a hybrid cyber warfare or cyber espionage.

Both types of cyber challenges, risks or threats jeopardizes EU cybersecurity. It is important to emphasize that each new strategic act of European Union related to cybersecurity represents an expression of need to coordinate cybersecurity policies with the latest trends in this area. Yet the speed of adopting new relevant documents cannot keep up with the dynamics of technological development which is the primary generator of the need to expand this concept, i.e. to reconceptualize cybersecurity. This is, in part, the reason why the full implementation of all strategic instructions by the relevant documents is missing. Basically, EU and its members, as the ones addressed by those instructions, simply cannot act in time as new changes in technological sphere happen very fast. That also answers why these strategies are being adopted so often. Also, new strategies and directives are adopted regularly because risks for cybersecurity may change and expand, including cyber incidents. For example, The EU's Cybersecurity Strategy for the Digital Decade (2020) represents an answer to rapid digitalization and increased relying on new information technologies and trends caused by the crisis that followed the Covid-19 pandemic. The pandemic-influenced crisis demanded changes in the EU security policy, especially in the cyberspace. New strategic documents are also the fruit of EU's persistence in confronting the cyberthreats coming from Russia, which grew especially in the context of recent Russian military aggression on Ukraine.

For example, the proposed Cyber Resilience Act from September 2022, is the fruit of challenges brought by the global nature of markets for products with digital elements, as Member States face the same risks for the same product with digital elements on their territory. Joint action at EU level is thus necessary to increase the level of trust among users and the attractiveness of EU products with digital elements. Practices of production and design of these devices give space for extra risks for home and business networks. In a commonly cited case, hackers allegedly could steal data from a well-protected computer network of a casino after they broke into the network via temperature sensors connected to internet. That sensor was placed in an aquarium. "Computers, phones, household appliances, virtual assistance devices, cars, toys… each and every one of these hundreds of million connected products is a potential entry point for a cyberattack," said Thierry Breton, commissioner for the internal market (Informacija, 2017). Therefore, the very proposal of a document such as the Cyber Resilience Act, demonstrates the significance that internet safety has within the concept of EU cybersecurity. Products that are

connected either directly or indirectly to another device or network are often an easy target for cyber criminals of different profiles.

Another great threat to EU cybersecurity comes from hybrid activities of other states, especially Russia. According to the annual report of The European Union Agency for Cybersecurity (ENISA, 2022), conflict between Russia-Ukraine reshaped the threat landscape during the reporting period. States and other cyber operations will very likely adapt to this new state of affairs and take advantage of the novelties and challenges brought about by this war. However, this new paradigm brought by the war has implications for international norms in cyberspace and, more specifically, for state sponsorship of cyberattacks. Due to the volatile international situation, we expect to observe more cyber operations being driven by geopolitics in the near to mid-term future. The war between Russia and Ukraine has shown new ways to use misinformation campaigns, targeting people's perception of the status of the war and the responsibilities of the parties involved.

All the above (including many challenges, risks and threats to cybersecurity that remained unmentioned here) point out the need of continuous reconceptualization of the term cybersecurity in the EU security policy. Two things encourage this reconceptualization: technological development and progress and, on the other side, current events (Covid-19 pandemic or Russian aggression on Ukraine). Precisely such things generate new challenges, risks and threats to cybersecurity and the need to propose and adopt new acts and create new policies.

CONCLUSION

The concept of cybersecurity is no longer a new thing. Yet the use and significance of this term within the security agenda of the modern age have grown. The usage of the term cybersecurity in international and national strategic documents is much higher than it used to be. Its constant usage in political, security and military discourse is causing numerous confusions regarding its theoretical determination and the conceptualization of cybersecurity.

In that context, European Union has directed its security policy towards cybersecurity and the questions and challenges of cyber risks and threats. We have seen the number of times the term cybersecurity has been mentioned and widely interpreted in numerous policies, strategies,

agendas, initiatives, directives and other EU documents. There used to be attempted conceptualization of the term in certain general EU policies. However, since 2013, a tendency of adopting specific strategic documents regarding cybersecurity is noted. It is important to add that these tendencies have been followed with the building of new and strengthening of existing EU institutional capacities for cybersecurity. The rapid development of the technological revolution should bring an increase in social changes and the intensity of these processes.

After analyzing the EU's security policy regarding cybersecurity, we can determine that this concept is very widely defined, as are the terms related, such as cyber defense, cyberspace, cyber threat, cyber challenge, cyber risk, etc. Especially important was to see how the EU perceives cyber threats. We have seen that cybercrime is perceived as one of the greatest threats to the cybersecurity of individuals, Member States and the EU in its entirety. International conflicts and incidents in cyberspace are distinguished, especially hybrid threats. Since it is still a field not researched enough, there is space left for securing multiple phenomena. The EU policies will need to be focused on identifying key cyber threats that jeopardize its security and of its Member States. Also, it is crucial to properly define the term cybersecurity.

To conclude, the EU has recognized the potential and significance of cybersecurity in the framework of its general security agenda. However, in order to keep the concept adjuvant, it is necessary to continue working on its definition and operationalization. In that way, the EU would avoid large spending due to a lack of focus on cyber phenomena. That would also create better foundations for action, i.e. better prevention of cyber threats and cyber-attacks; better risk management in cybersecurity, and better handling of consequences of cyber-attacks and similar incidents.

REFERENCES

Canongia, C., & Mandarino, R. (2014). *Cybersecurity: The New Challenge of the Information Society*. In Crisis Management: Concepts, Methodologies, Tools and Applications. Hershey, PA: IGI Global. p. 60-80.

Carrera, S. and Guild, E. (2011) *Towards an Internal (In) Security Strategy for the EU?* Brussels: CEPS Liberty andSecurity in Europe Paper.

Council of the European Union, General Secretariat of the Council. (2010). *Internal security strategy for the European Union: towards a European security model, Publications Office.* https://data.europa.eu/doi/10.2860/87810

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4(10): 13-21. http://doi.org/10.22215/timreview/835

Cyber Risk GmBH (2022a). *The European Cyber Resilience Act.* Availible 7. 12. 2022. at: https://www.european-cyber-resilience-act.com/

Cyber Risk GmBH (2022б). *The Articles of the Cyber Resilience Act.* Availible 7. 12. 2022. at: https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Articles_(Proposal_15.9.2022).html

Dragaš, O. (2020). Security as an Independent Scientific Discipline - A Contribution to a Comprehensive Security Study to Meet the Requirements of the Contemporary Globalized World. *Security Science Journal*, Vol. 1 No. 1., p. 85-100.

Enisa Threat Landscape 2022. (2022). ENISA. Availible 12. 7. 2022. at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

European Security Strategy - A secure Europe in a better world. (2009). Council of the European Union. Availible 24. 8. 2022. at: https://www.consilium.europa.eu/en/documents-publications/publications/european-security-strategy-secure-europe-better-world/

European Comission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Brussels, 7.2.2013; JOIN(2013) 1 final.

European Comission. (2015). *The European Agenda on Security.* Strasbourg, 28.4.2015 COM(2015) 185 final.

European Commision. (2016). *A Global Strategy for the European Union's Foreign and Security Policy - Shared Vision, Common Action: A Stronger Europe.* Availible 1. 9. 2022. at: https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf

European Comission (2017*). Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.* Brussels, 13.9.2017 JOIN(2017) 450 final.

European Commision. (2020a). *Communication from the Commission to the European Parliament, The European Council, The Council, The European Economic and Social Committee and The Committee of the Regions on the EU Security Union Strategy.* Brussels, 24.7.2020 COM(2020) 605 final.

European Commision (2020b). *The EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 16.12.2020 JOIN(2020) 18 final.

Goutam, K. R. (2015). Importance of Cyber Security. *International Journal of Computer Applications* (0975 – 8887), Volume 111 – No 7, February 2015.

Informacija (2017). *EU donosi novi zakon o sajber bezbednosti,* Vesti, 16.09.2022, 08:30 AM. Availible 12. 7. 2022. at: https://www.informacija.rs/Vesti/EU-donosi-novi-zakon-o-sajber-bezbednosti.html

Ivetić, S., Pavlović, G. (2012). *Borba protiv sajber kriminala u Evropskoj uniji sa osvrtom na Republiku Srpsku.* U: Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal. (53-64). Laktaši: Visoka škola unutrašnjih poslova.

Ifrah, L. (2008). States face new challenges from cyberwarfare and cybercrime. *Revue Défense Nationale,* Vol. 714 (2008): pp. 154-170.

Kučeković, Z. (2014). *Uloga teorije u istraživanju bezbednosti i pojam teorijske paradigme.* U: M. Lipovac, D. Živojinović (ur.), Međunarodna bezbednost: Teorijski pristupi (str. 73-85). Beograd: Inovacioni centar Fakulteta bezbednosti.

Lewis, J. A. (2006). *Cybersecurity and Critical Infrastructure Protection.* Washington, DC: Center for Strategic and International Studies.

Lipovac, M. (2014). *Konceptualna analiza bezbednosti.* U: M. Lipovac, D. Živojinović (ur.), Međunarodna bezbednost: Teorijski pristupi (str. 49-71). Beograd: Inovacioni centar Fakulteta bezbednosti.

Luiijf, E., de Graaf, P., Besseling, K. (2013). Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructure Protection,* 9(1-2), 3–31. DOI: https://doi.org/10.1504/IJCIS.2013.051608

Manulis, M., Bridges, C.P., Harrison, R. et al. (2021). Cyber security in New Space. *Int. J. Inf. Secur.* 20, 287–311 (2021). https://doi.org/10.1007/s10207-020-00503-w

Mijalković, S., Arežina-Đerić, V., Bošković, G. (2010) *Korelacija informacione i nacionalne bezbednosti.* U: Savetovanje o zloupotrebi IT - ZITEH, Beograd.

Milašinović, R., Mijalković, S., Amidžić, G. (2012). *Bezbednost i internet.* U: Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal. (31-42). Laktaši: Visoka škola unutrašnjih poslova.

Milošević, M., Putnik, N. (2017). Sajber bezbednost i zaštita od visokotehnološkog kriminala u Republici Srbiji – strateški ipravni okvir. *Kultura polisa*, god. XIV (2017), br. 33, str. 177-191.

Miljković, M., Putnik, N. (2016). Aktivnosti savremenih obaveštajnih službi u kiber prostoru. *Vojno delo*, 2016, vol. 68, br. 7, str. 164-180.

Nedeljković, S, Forca, B. (2015). Evropska strategija bezbednosti i sajber pretnje – značaj za Srbiju. *Vojno delo*, 3/2015, str. 135-154.

Novičić, Ž. (2021). *Nova strategija sajber bezbednosti EU za digitalnu deceniju — analiza.* Razvojni pravci Evropske unije nakon pandemije KOVID 19 / [ed. Nevena Stanković, Dragana Dabić, Goran Bandov]. - ISBN 978-86-7067-289-5. - (2021), str. 123–145.

Nye, J. (2012). "*Cyber War and Peace*." Availible 15. 8. 2022. at: http://www.project-syndicate.org/commentary/cyber-war-and-peace

Oxford University Press. (2014). Oxford Online Dictionary. Oxford: Oxford University Press. Availible 18. 8. 2022. at: http://www.oxforddictionaries.com/definition/english/Cybersecurity

Putnik, N. (2012). *Kiber ratovanje – novi oblik savremenih društvenih konflikata*. Doktorska disertacija. Beograd: Fakultet bezbednosti.

Seemma, S. P., Nandhini, S., Sowmiya, M. (2018). Overview of Cyber Security. IJARCCE - *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 7, Issue 11, November 2018.

Schatz, D., Bashroush, R., Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*: Vol. 12: No. 2, Article 8.

Todorović, B., Trifunović, D. (2020). Security Science as a Scientific Discipline - Technological Aspects. *Security Science Journal*, Vol. 1 No. 1., p. 9-20.

Trifunović, D., Obradović, D. (2020). Hybrid and Cyber Warfare – International Problems and Joint Solutions. *National Security and the Future*, 1-2 (21) 2020, p. 23-48.

U.S. Department of Defence. (2019). *Military Must Be Ready to Confront Hybrid Threats, Intel Official Says.* Availible 7. 12. 2022. at: https://www.defense.gov/Explore/Features/story/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intelligence-official-says/source/GovDelivery/

Von Solms, R., Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, Volume 38, October 2013, Pages 97-102.

Vuletić, D. (2017). *Sajber bezbednost. Integralna bezbednost Republike Srbije*, 2017, str. 169-184.

****

Petar Đukić, master menadžer bezbednosti

Doktorand na Fakultetu bezbednosti Univerziteta u Beogradu
Viši asistent na Univerzitetu modernih znanosti, Mostar

Apstrakt: Termin „sajber bezbednost“ odavno je u upotrebi. Ipak, na aktuelnom nivou tehničko-tehnološkog razvoja društva, njegova upotreba je intenzivirana. Najveći broj zahteva za izmenu tradicionalne bezbednosne paradigme upravo ide u pravcu proširivanja istraživačkog polja nauke bezbednosti na sektor sajber bezbednosti. Preduslov za tako nešto jeste otklanjanje postojećih nejasnoća oko teorijskog određenja i praktične vrednosti samog koncepta, a što definitivno iziskuje sveobuhvatno naučno istraživanje. U poslednjoj decenici primetna je tendencija

apostrofiranja koncepta sajber bezbednosti u bezbednosnoj politici Evropske unije, pre svega kroz njegovu implementaciju u brojnim strateškim dokumentima, ali i operacionalizaciju i institucionalizaciju kroz institucije EU i njihovu delatnost. U vezi s tim, tema ovog rada jeste (re)konceptualizacija pojma sajber bezbednosti u bezbednosj politici Evropske unije. Cilj rada je da pokušamo pojmovno odrediti, razjasniti i „demistifikovati" koncept sajber bezbednosti, u meri u kojoj je to moguće. Cilj je i da se sagleda način na koji Evropska unija, kao specifična nadnacionalna organizacija, teorijski pristupa ovom konceptu kroz svoje opšte i posebne strateške i druge dokumente, tj. kroz svoju sveukupnu bezbednosnu agendu. Metodološki okvir rada sastoji se od pregleda postojeće naučne i stručne literature, analize strateškog i normativnog okvira Evropske unije, kao i dokumenata i izveštaja institucija EU. Zaključak je da je Unija definitivno prepoznala potencijal i značaj koncepta sajber bezbednosti unutar svoje bezbednosne politike. Međutim, da koncept sajber bezbednosti ne bi ostao preširok, a samim tim i neupotrebljiv, potrebno je, i dalje, kontinuirano raditi na njegovom definisanju i operacionalizaciji.

Ključne riječi: sajber bezbednost, Evropska unija, strategija, bezbednosna politika, koncept