Dejan Z. Milenkovic
Ministry of the Interior of the Republic of Serbia
E-mail: dejanmilenkovic1979@yahoo.com

DOI:
Review Paper
Received: January 19, 2023
Accepted: March 1, 2023

CYBER SECURITY AND DATA COLLECTION

Abstract: *Every country that seeks to protect its national interests and security in the information age faces the problem of adequately protecting the national information sphere. As a confirmation of this thesis, modern security studies talk about cybersecurity and its importance for national security. Therefore, we can say that cybersecurity protects the vital interests of individuals, society and the state in the information sphere from external and internal dangers*[1] *and risks. The main threat in the sphere of international cybersecurity is the use of information and communication technology as an information weapon for the achievement of political and military goals that conflict with international law, for violating public order, inciting inter-ethnic, inter-religious and inter-denominational hatred, as well as for carrying out criminal and intelligence - subversive activities. The paper's subject is a comprehensive overview of cyber security and its impact on national security.*

Keywords: *intelligence service, cyber security, cyber warfare, subversive activities.*

1. INTRODUCTION

The beginning of the 21st century in international relations and world politics was marked by new violent conflicts and the destruction of critical infrastructure using cyberspace. Cyber weapons have a direct effect on information and information systems and an indirect effect on dependent systems, processes, services and people. Cyberspace extends worldwide and includes physical infrastructure in the state and private ownership. In parts, it is subject to the jurisdiction of state sovereignty, but it also grows in common world areas, inside and outside state borders

[1] Internal cyber security threats are threats posed by individuals that originate within an organisation itself. They can be current employees, former employees, external contractors or vendors. Anyone who has access to company devices or data. This form of data breach involves an internal attacker accessing sensitive company information with malicious intent. Attackers can include both current and former employees.

(Mladenovic, Drakulic, Jovanović, 2011). During a cyber-attack, data does not physically cross state borders in cyberspace, because they do not exist, but move from, to and through physical connections and devices that extend across physical boundaries, over land, sea, space or air. It has not yet been established whether this violates the sovereignty and neutral status of the transit states. In this regard, there has been a kind of escalation of non-state asymmetric violent conflicts in recent years. New tendencies were manifested in a series of local wars at the end of the 20th century and the beginning of the 21st century. Some authors classify them in a particular category, the so-called third type of conflict, because they are neither classic civil wars nor interstate wars, and are closely related to the fragmentation of the state. Accordingly, cyberspace is a training ground where great powers and other numerous actors compete in political, ideological, economic, military and many other spheres. From a military perspective, cyberspace acquired the fifth combat space at the end of the last century, along with land, sea, air and space. Virtual space, a new domain[2] of conducting combat operations, is characterized by using electronic and electromagnetic spectrum tools for storing, modifying and exchanging data via networked systems connected to physical infrastructure. In this sense, given that cyberspace represents a colossal database of information, especially secret information, it is no surprise that it is the focus of interest of all intelligence services today. According to known sources, espionage has been used to gather information since ancient China. Since the release of the Internet into commercial use, developed countries began to take advantage of computers and the Internet in intelligence activities. There is no professional intelligence service in the world that is not interested in this method of intelligence research, not least because of the effectiveness of this activity compared to other ways of collecting confidential data (Miljković, Putnik 2016). The development of modern information technologies, as a significant factor in the system organization of the state, contributes to the creation of favorable circumstances for a wide range of challenges, risks and threats to defense. Cyber-attacks on critical infrastructure objects, high-tech crime, endangering information and communication systems, and the spread of fake news and disinformation within the concept of hybrid and information warfare can negatively impact the functioning of elements of the defense system. That is why it is necessary to continuously develop the technological and informational protection of elements of the defense system at all

[2] The cyber domain includes all energy that flows through the electromagnetic spectrum (radio-waves, microwaves, x-waves, gamma rays and "directed energy")

levels of the organization. The expansion of cyber-attacks, an element of modern hybrid warfare, began in the last decade of the 20th century with the development of modern information and communication technologies or, more precisely, with the release of the Internet into commercial use[3]. Cyberspace can be affected by any group that owns computers that can be connected to existing computer networks. Cyber-attacks on some social groups can be aimed at intentionally inserting misinformation on certain websites[4]and forums[5]. It is very diverse and specific - it involves the application of various IT instruments, programs and techniques. The essential specificity of cyber warfare is that the battlefield, encyclopedias and blogs can be strictly directed toward network sabotage. Impeding the normal functioning of information systems in a modern society that has become dependent on them can seriously affect all spheres of social life. The consequences can be even fatal if critical information infrastructures[6] such as, for example, land and air traffic control systems, hydro-dams, nuclear power plants, security and health services, or electricity and oil distribution systems are compromised. The arsenal of cyber war (the weapon used to cause dysfunction of the information infrastructure[7]) is not physical but cyberspace[8] (Putnik, 2012).

2. CYBER SECURITY, CYBER WAR, CYBER TERRORISM AND CYBERCRIME

Cybersecurity is one of the newest areas of state security policies that is becoming increasingly important in the security sectors of states in Europe. Given the rate of innovation, policymakers and others are continuously seeking to understand the range of modern

[3] A decisive move in this sense was the definition of a new - World Wide Web (WWW) - architecture by CERN (European Council for Nuclear Research) in 1991. The new architecture has greatly simplified navigation on the Internet. In 1993, the first graphical instrument for searching the Internet was created - the Mosaic program. Since 1994, the World Wide Web has turned the Internet into an instrument of mass communication.

[4] A web site is a set of web pages, that is, documents that can be accessed via the World Wide Web on the Internet. To access the website, it is necessary to use special software applications called web browsers

[5] An Internet forum (message board) is an application that allows registered users of a website to have an online discussion through messages published on the website. Certain members of the forum can be moderators of the site, with the right to delete messages or stop writing on topics that do not comply with the rules of the site.

[6] Critical information infrastructures are information infrastructures that guarantee the operability and accuracy of IT structures. The destruction of the foundations of these structures and their accompanying equipment, that is, the disruption of their operability over a long period of time, can significantly threaten the safety of the population.

[7] Information infrastructures – electronic devices that can be programmed, as well as connective and communication network structures, together with the data contained in them.

[8] Cyberspace refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication.

technologies, techniques and their application. This situation requires rapid and comprehensive development of new legal and political frameworks.

In addition to ensuring national security, safe and secure networks are essential in boosting the economy in the country and modernizing public sector management in Southeast European countries (consider, for example, how crucial the role of secure networks is for the excellent functioning of e-government services). Cyberspace cannot be completely secure because every device connected to the Internet is vulnerable and it is also necessary to guarantee the ability of citizens to enjoy their rights, such as access to information and freedom of expression. Therefore, it is essential to have a thorough awareness of the opportunities, risks and threats that cyberspace carries. In foreign and domestic literature, there are different definitions of the term cyber security, and in this regard, there are other differences in the world in terms of technological capacities and legal frameworks between different countries. Cyber security can be defined as the application of technology, processes and controls to defend computers, servers, mobile devices, electronic systems, networks and data from cyber-attacks[9]. Cyber security aims to reduce the risk of cyber-attacks and protect against the unauthorized use of systems, networks and technology. While many countries, such as the USA and Great Britain, are spending millions on cyber security and rapidly developing legislation in that area, others do not even have a basic IT infrastructure, let alone a strategy to deal with cyber threats that affect and originate from their territories. Sometimes basic IT infrastructure protects devices from cyberattacks much more than the developed one, for example, Ukrainian power plants were able to start their work manually after the blackouts caused by cyberattacks. Hence the need to pass laws on cyber security and cybercrime (which would include adequate democratic control). Where both relevant capacity and legislation are lacking, investigating and prosecuting cyber incidents becomes difficult, if not impossible. At the same time, the absence of appropriate oversight bodies makes violations of the rights to freedom of expression, privacy and association far more confident.

In the theory of security sciences, there are numerous definitions of terms in the field of cyber security, from the definition of cyber war, cybercrime and cyber-terrorism.

[9] "What is Cyber Security?". www.kaspersky.com

Cyberwarfare[10] is used in a broad context to denote the interstate use of technological force within computer networks in which information is stored, shared or communicated online.

Cyberwarfare uses digital attacks to attack nations by inflicting damage comparable to actual fighting or disrupting vital computer systems. However, there is considerable debate among experts regarding the definition of cyber warfare, even if such a thing exists. One view is that "cyber warfare"[11] is a misnomer, as no offensive cyber action to date could be described as "war". The alternative idea is that "cyberwarfare" is a convenient label for cyberattacks that cause physical harm to people and objects in the real world (Singer, 2014).

Cyberterrorism represents attacks and threats directed against computers, computer networks and IT equipment for data storage to intimidate and influence governing structures and the public in political and social life. These attacks are mainly aimed at personal computers and are carried out using viruses. "Cyber terrorism is premeditated politically motivated attacks by national groups or secret agents or individuals against information and computer systems, computer programs and data that lead to violence against civilian targets[12]." The official definition of cyber terrorism given by experts from the Center for the Protection of National Infrastructure of the United States of America defines cyber terrorism as "a criminal act committed through computers resulting in violence, death and destruction, creating terror to persuade the government to change its policy". Mark Pollitt states that cyberterrorism is a premeditated, politically motivated attack against information, computer systems, programs and data that cause violence and fear in civilian targets.

Cybercrime is a form of criminal behavior in which computer technology and information systems are manifested as a way of committing a crime, where a computer or computer network is used as a means or goal of execution. Computers and computer technology can be misused in various ways, and the crime committed using computers can take the form of any of the traditional types of crime, such as theft, evasion, or embezzlement. In contrast, data obtained without authorization through misuse of information systems can be used to acquire illegal benefits. In this regard, relevant international instruments include Resolutions 55-63 of the General Assembly of the United Nations of December 4, 2000, and 56/121 of December 19,

[10] *Cyber warfare : a multidisciplinary analysis*. Green, James A., 1981-. London. 7 November 2016. ISBN 9780415787079. OCLC 980939904

[11] "Cyber war - does it exist?". NATO. June 13, 2019.

[12] Center for Strategic and International Studies 1998.

2001, on "Combating the Criminal Abuse of Information Technologies"; "Guidelines for cooperation between the police and Internet service providers in combating cybercrime", adopted at the world conference "Cooperation against cybercrime" held in Strasbourg on April 1 and 2, 2008, and at the regional level Council of Europe Recommendation No. R (89) 9 on computer crime and the European Convention on Cybercrime requires many countries to adopt legal measures to establish powers and procedures for criminal investigations related to criminal offenses committed using computer systems and electronic data collection. International and regional instruments for the protection of human rights are also necessary, including the International Convention on Civil and Political Rights (especially Article 17 on the right to privacy, Article 19 on freedom of expression and Article 22 on freedom of association), the European Convention on Human Rights, the African Charter on Human and Peoples' Rights and the American Convention on Human Rights. International and regional organizations have also particularly tried to pay attention to the protection of electronic data through measures and instruments, such as the Guidelines of the General Assembly of the United Nations for the regulation of computer files with personal data and the Convention of the Council of Europe on the protection of individuals during the automatic processing of personal data which, in particular, reemphasizes protections relating to privacy and freedom of expression concerning electronic data and correspondence. The fight against cybercrime at the state level also requires the cooperation of all parties involved. The private sector is the most common target of cybercriminals, and its experiences and interests should be considered when planning cybercrime strategies. Cybercrime experts from the private sector, academia and civil society can contribute to policy planning to combat cybercrime with technical capacity and knowledge. Therefore, to effectively combat cybercrime, governments must foster public-private cooperation and support establishing a trusted network. Cybercrime prevention and support for individual users are equally important. Through general awareness raising and capacity building, users should learn how to recognize e-mail messages with potential scams, malicious content and potentially fraudulent contacts. Even relatively small efforts, such as training users to maintain basic cyber hygiene and use strong passwords or up-to-date licensed software and encryption, can significantly prevent cybercrime. At the international level, progress was achieved by adopting the Council of Europe Convention on High-tech Crime, also called the Budapest Convention. The Budapest Convention is the only binding international instrument on cybercrime to date and

prescribes guidelines for states to develop comprehensive national legal frameworks to combat cybercrime and establish a framework for international cooperation between signatory states. However, with sixty-one signatories and ten more expected to join, the Budapest Convention is still not a universal global document. Nevertheless, cases of international cooperation can be seen in recent years. For example, organizations for international police cooperation, especially Europol and Interpol, have become involved in frameworks for strengthening global capacities and facilitating cross-border cooperation between police services. Moreover, due to the previously mentioned requirement of maintaining national cybercrime units, such frameworks can compensate for limited national capacities, including developing public-private partnerships and networks of trust between experts from different parts of society.

Threats that have been primarily targeting nation-states and their associated entities have expanded the target zone to include the private and corporate sectors. This class of threats, well known as **Advanced Persistent Threats** (APT)[13], are those that every nation and well-established organization fears and wants to protect itself against. While nation-sponsored APT attacks will always be marked by their sophistication, APT attacks that have become prominent in corporate sectors do not make it any less challenging for organizations.

According to the National Institute of Standards and Technology (NIST)[14], an APT attacker: (a) pursues its objectives repeatedly over an extended period of time; (b) adapts to defenders' efforts to resist it; and (c) is determined to maintain the level of interaction needed to execute its objectives. These objectives are the exfiltration of information or undermining or impeding critical aspects of a mission or program through multiple attack vectors.

3. INTELLIGENCE SERVICES AND CYBER SECURITY

The modern concept of national security (the security of the so-called post-Westphalian state) is a state of runaway realization, development, enjoyment and optimal protection of national and state values and interests, which is achieved, maintained and improved by the function of citizen security, the national security system and supranational security mechanisms, as well as the absence (individual, group and collective) fear of endangering them, and a collective sense of

[13] Advanced Persistent Threat, as the name itself implies, is not like a regular attack or attack done by a regular hacker. APTs are achieved often by a group of advanced attackers that are well-funded by an organization or government to gain crucial information about their target organization or government.

[14] Kissel, R: (2011) Glossary of key information security terms. Diane Publishing.

tranquillity, certainty and control over the development of future phenomena and events of importance for the life of society and the state[15]. On the threshold of the 21st century, it is clear that the competence of intelligence and security services is expanding (e.g., suppression of organized, financial, high-tech, energy and cyber security). However, they still do not respond to all threats to society and the state. As a rule, their attention is generally directed towards the prevention and suppression of organized and conspiratorial activities, many of which are secret or clandestine (that is, politically motivated incidents of endangerment carried out by individuals, groups, organizations and institutions that directly organize or carry out intelligence or subversive activities in the country or abroad). In current conditions, the intelligence-security activity represents the scope of competence, rights and duties of intelligence services and other institutions within the security-intelligence system of the state, which systematically collect, process and present intelligence and carry out other activities as requested by legal regulations and political decisions. As holders of the function of national security, intelligence and security services are integral subjects of the security-intelligence system, which is one of the subsystems of the national security system[16]. The phenomenon of spying through cyberspace is discussed both in populist and contemporary professional and scientific literature. The governments of many leading countries, including the US, China and the Russian Federation, complain about the problem of cyber espionage. That the security of computer networks is no longer just a technical problem but also an important strategic issue is confirmed by the invitation sent in 2011 by the veteran American diplomat Henry Kissinger to the representatives of the USA and China to start a "cyber détente"[17]. Kissinger advocated for some agreement between the two countries, which would declare certain areas of cyberspace off-limits to computer spies, burglars and hackers. Theoretically, the possibility of collecting intelligence data exists, even when such intelligence operations are directed toward essential and sensitive political and military communications from a great distance and any part of the world. The aspiration of all secret services is the so-called

[15] Mijalković, S.: (2011) Intelligence and security services and national security, Bezbednost 1, Criminal and Police Academy, Belgrade, pp.84

[16] Ibid

[17] "It's time for cyber detente", Politika, World section, 15/06/2011. The Bloomberg agency quotes what the outgoing Chief of the Joint Chiefs of Staff of the US Armed Forces, Mike Mullen, said in a conversation with its editorial board, for whom cyber security is "one of the two existential threats facing the US, the second is nuclear weapons", which is why it should be "in all our war thinking".

"zero-day"[18], that is, the ability to secretly infiltrate other people's systems (without causing any damage) so that the owner of the system does not know that it is the object of "silent" surveillance (Putnik 2009). Zero-day is a security flaw in software, hardware, or firmware that is unknown to the party or parties responsible for patching or otherwise fixing the flaw. The term *zero-day vulnerability* refers to the flaw itself, while *zero-day attack* refers to an attack that has zero days between the time the vulnerability is discovered and the first attack. *Zero-day exploit* refers to the method or technique hackers use to take advantage of a vulnerability - often via malware - and execute the attack. Computer-network exploitation includes intelligence gathering and other operations that enable access to an adversary's data through its information system. Computer-network exploitation is a deliberate and thought-out act of infiltrating the adversary's information system, intending to influence the adversary's decision-making process, and enhancing allied forces' intelligence. These operations achieve the extraction of information from the opponent's networks (passive form), as well as the insertion of data and information into the opponent's networks, which degrades the opponent's ability to correctly assess the combat space (active form, i.e. the so-called covert operation of influence). Data extraction and insertion operations are defined as follows[19]:

- data extraction is a passive technique that involves capturing data traveling through the opponent's network or extracting information from the opponent's database. Access to malicious links and nodes is, therefore, necessary to obtain information. The intelligence obtained by the extraction technique can later be used, modified and fed back into the adversary's network. It is necessary to mention that the data can be copied, so their extraction can remain undetected;

- the insertion is an active technique that involves inserting data into the opponent's database, which enables the manipulation of the opponent's information. With this technique, it is achieved that the opposing side acquires a wrong intelligence picture, which gives an advantage to the other side.

Unlike computer and network exploitation, cyber espionage is a relatively new intelligence gathering based on different strategies, tactics and tools. Cyber espionage is using computers or digital communications on an international level to gain access to sensitive information about an

[18] ttps://www.csoonline.com/article/3284084/zero-days-explained-how-unknown-vulnerabilities-become-gateways-for-attackers.html, Accessed on November 19, 2021.

[19] Cooperative Cyber Defence Centre of Excellence, International Cyber incidents: Legal considerations, Abbrevations and glossary, Eneken Tikk, Kadri Kaska, Liis Vihul (Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010) http://www.ccdcoe.or (preuzeto 30.07.2021).

adversary to achieve political, military, economic and other advantages, use data for their purposes or to sell the obtained information for financial gain (Deibert, Rohozinski 2009). In the era of the expansion of information and communication technologies, security risks and threats to the national security of states are increasing significantly, and in this connection, the roles of intelligence services in cyberspace are gaining significant importance. Namely, intelligence services have been intensively working on cyberspace intelligence research in the context of gathering and protecting intelligence information, attacking and defending critical infrastructure, recruiting cyberwarriors and identifying them in the enemy's ranks.

4. Cyber security and subversive activities

In modern military doctrines, virtual, non-Euclidean space - cyberspace - has acquired the status of the fifth combat space along with land, water, air and space. More and more authors believe that "virtual space" is the place where primary battles could be fought in the future and some countries are heavily preparing for such a concept of waging wars.[20] Cyberspace is not only a suitable environment for carrying out propaganda activities, but substantial physical damage can also be caused through it - by attacking the information infrastructure of a specific state - which can result in human and material victims, as well as in the violation of the sovereignty of the attacked state. Because of this, cyberspace today has become the target of attacks and a powerful tool (weapon of attack) in the arsenal of technologically advanced armies and their specialized "computer warriors" (Miljkovic 2016). The media and information technology revolution is fundamentally changing how society interacts and how states (and paramilitary, anti-state formations) wage wars. In military-technological terminology, it is clear that the continuous fusion of revolutionary achievements in the field of computers, satellite communications and media radically "improved" the possibilities of warfare, even if the information and communication revolution did not fundamentally change the geostrategic and political-economic goals of the war itself (Gardner, 2016). Cyber warfare uses various techniques and instruments to attack adversary information and communication (IC) systems and manipulate data for offensive and defensive purposes. In the information age, the importance of information and all activities related to the dissemination and production of

[20] *L' Armement*, No. 60, XII., Paris, 1997 - I. 1998.; *From cybercrime to cyberwarfare*, "Défense nationale et sécurité collective", No 6, The Committee for National Defence Studies, Paris, 2008.

information has grown significantly. But, like physical space, cyberspace often belongs to whoever gets it first. Therefore, any strategy for establishing control over the Internet, the scene of an information war, would have to adopt the following maxims as an imperative: dominate the channels for the flow of information, broadcast one's views and attitudes as much as possible to impose them as effectively as possible, and constantly improve methods and means. Information age technologies on a global scale increase the role of states, organizations, multinational companies, non-governmental organizations, transnational criminal organizations and even individuals in the international arena (Wiliams, 1997). Subjects of cyber warfare, i.e., actors of computer attacks, can be divided into two categories for analytical purposes. The criterion for division is the presence or absence of intent on the part of the perpetrator of computer intrusion. In this sense, we can distinguish between a premeditated cyber-attack and an attack without premeditation (Alford 2000). A premeditated cyber-attack used in cyber warfare is any attack carried out using cyber means to deliberately affect national security or create conditions for further operations against national security. Premeditated attacks can be equated with warfare - the national policy at the level of war. They include any action against an adversary's computer and information communication systems. Actors carry out reckless cyber-attacks, most often individuals, who unintentionally threaten national security and are generally unaware of the potential consequences of their attacks at the international level. These actors include all those who commit cyber infiltration, bypassing the system's defense mechanisms, and manipulating, using or destroying the system's information, i.e., the system itself. These actors have different motives and intentions but do not intend to harm national security or further operations against national security. These actors are most often referred to under the generic term "hacker", and although they commit cybercrimes, they do not conduct cyber warfare intentionally. However, it is essential to note that there are cases where this category of actors is manipulated by those who carry out attacks with intent, using their knowledge and abilities in cyber operations (Alford, 2000). Applying subversive actions is one of the methods of intelligence services[21] used intensively today. It implies the determination of political creators for foreign policy action based on power (use of force), and not only in the classical, physical form (armed force) but also in the form of various subversive content (secret

[21] Director of National Intelligence Dan Coats warned that there is an "increasing threat of foreign cyberattacks that could destroy critical American infrastructure." He linked the cyber-attacks to "alarming activity" detected by US intelligence agencies before the September 11, 2001, attacks by Al Qaeda.

provocative actions, hybrid actions, cyber-attacks, psychological propaganda activities) that have all the characteristics of the destruction of a specific target. These contents of the work of modern intelligence services are distinguished by the exceptional concealment and sophistication of the applied methods, primarily due to the effort to completely conceal the state's participation and avoid any possibility of their public compromise and condemnation on the international level. Subversive activities essentially represent interference in the internal affairs of other states, a disguised, ultimately severe form of aggression. Subversive content (Mijalkovic, 2018), by the way, represents another type of activity of modern intelligence services (the first is intelligence), primarily on the external international level, within the framework of foreign policy actions of states in international relations, which, as we have emphasized, is characterized by the use of force against other states. They are clear proof that the participation of the intelligence services in the creation and implementation of the chosen directions of foreign policy action is not limited only to the decision-making process, in which they actively participate in the initiative phase (collection, processing, assignment and interpretation of intelligence data), and somewhat less often in the content articulation phase. Therefore, the intelligence services directly participate in achieving foreign policy goals through the planning, organizing and implementing subversive content. The role of intelligence services as specific foreign policy mediators in this plan is a consequence of the great possibilities of modern intelligence and security systems in the world which was crucial and influenced the intelligence services to enrich the repertoire of actions with non-intelligence actions maximally. In this context, in combination with foreign policy means, intelligence services as foreign policy mediators usually also determine the nature of the specific foreign policy procedure.

CONCLUSION

A turning point in military activities and the concept of national, regional and global security was the emergence of cyberspace. The new "space" provided enormous opportunities for implementing special propaganda activities and conducting attacks on the opponent's information systems through computer networks. For this new type of confrontation in virtual space, the term cyberwarfare is used in the English-speaking world. Attacks in virtual space, imperceptible to the eye, can result in human casualties and material destruction in the natural,

physical world. That is why cyber warfare is today a key focus of interest to theoreticians and experts in the military, IT, legal and security sciences. From national, regional, and global security, the thesis that safe cyberspace is considered an imperative of the information age is understandable. It should not be forgotten, however, that given the nature and size of cyberspace, a state of absolute security is currently impossible to achieve. The speed with which threats are increasing requires adopting reliable, fast and adequate security measures that should be discriminatory against the threat creators. The danger of cyber-attacks today has significantly multiplied and increased compared to a decade ago, considering the development of information technologies and the significant increase in cyber warriors[22]. Intelligence services received new responsibilities in the field of "information security", bearing in mind that many activities of data collection, analysis, processing and delivery are carried out in the IT sphere, that is, through modern computer and information and communication technologies. In terms of countering subversive activity, the theory points out that information operations also represent a particular task in the work of intelligence services. On a broader social level, by applying counter-psychological operations, the services protect the national information space from the subversive influence of foreign intelligence services to expose, discredit and undermine the carriers of covert psychological operations and disprove the messages of such operations, but also especially protecting critical infrastructure from cyber-attacks (Miljkovic, 2016). Previous experiences in countering security threats in cyberspace point to the need to create a coherent operational framework that applies preventive and repressive measures to create a safe cyber environment. Preventive activities, in the first place, imply the design of various standards and strategies for the protection of information systems and their implementation, the improvement of legal regulations, both at the national and international level, as well as their harmonization with intelligence activities in an attempt to counter cyber threats. Legal measures cannot provide an effective response to cyber threats alone. A satisfactory level of cyberspace protection cannot be achieved even by adopting and implementing technical measures but, above all, by formulating protection strategies and synergistic implementation of a series of countermeasures by international organizations, state institutions, expert associations and individual users of information systems. Modern information and communication technology has led to changes in all spheres of human activity, including in the work of intelligence services. In contemporary

[22] https://www.bbc.com/serbian/lat/svet-59335402,

analytical work, due to the phenomenon of the abundance of information, one of the critical challenges is the ability of analysts and cyber experts to identify potential threats in cyberspace and to eliminate them. Another related challenge is to recognize disinformation, propaganda and misleading information, which has led to the development of numerous methods and tools. Furthermore, given that political decisions of importance for national security are formulated on the final reports of the intelligence services, the information of the intelligence services must be verified, accurate and free from foreign manipulation and influence, which indicates the importance of knowledge of information operations in operational and analytical work.

References

1. Alford L. D. Jr. (2000) "Cyber Warfare: Protecting Military Systems", The Journal of the Defense Acquisition University Review, Quarterly 7, No. 2., USAF, p. 105.
2. Bernays, L. E.: Manipulating Public Opinion: The Why and The How, *American Journal of Sociology*, Volume 33, Issue 6 (May 1928), 958-971.
3. Brunner, M. and Suter, E. M. (2008): *International CIIP Handbook 2008/2009*, Center for Security Studies, ETH Zurich.
4. Boczek, B. (2005), International Law: A Dictionary, Scarecrow Press, Lanham, Maryland.
5. Barkham, J. (2002) "Information Warfare and International Law on the Use of Force", InternationalLaw and Politics, Issue 34, New York University School of Law, стр. 57–113.
6. Gardner H. (2007), Averting Global War: Regional Challenges, Overextension and Options for American Strategy, Palgrave, New York.
7. Deibert R. and Rohozinski, R,. "Tracking GhostNet: Investigating a Cyber Espionage Network", Information Warfare Monitor, 29.03.2009, The SecDev Group &The Citizen Lab,http:// www.nsi.org/pdf/reports/Cyber%20Espionage%20Network.pdf (preuzeto 30.07.2021).
8. Clarke A, R, Knake,K, R, (2010), *Cyber War. The Next Threat to National Security and What to Do About It* 10 , Harper-Collins e-books; Reprint edition, USA.
9. Kissel, R., (2011): Glossary of key information security terms. Diane Publishing.
10. Konvencija o visokotehnološkom kriminalu. Savet Evrope. Ugovor br. 185.
11. Korns S., Kastenberg, J.: "Georgia's Cyber Left Hook ", Parameters, U. S. Army WarCollege's quarterly publication , Winter 2008–2009, Volume 38, No. 4.
12. Мијалковић, С. (2011), Обавештајно-безбедносне службе и национална безбедност, Безбедност 1, Криминалистичко-полицијска академија, Београд.
13. Мијалковић, С. (2018), Национална безбедност, Криминалистичко-полицијска академија, Београд.
14. Miljković, M., Putnik, N., (2016), Aktivnosti savremenih obavestajnih službi u kiber prostoru, Vojno delo broj 7.
15. Младеновић, Д., Дракулић, М., Јовановић, Д., (2011), Неутралност у сајбер ратовању, Војно дело.
16. Nedeljković, S, Forca, B. (2015), Evropska strategija bezbednosti i sajber pretnje - značaj za Srbiju, Vojno delo broj 3.
17. National Cyber Security Strategy Great Britan 2016-2021
18. Putnik, N. (2009), *Sajber prostor i bezbednosni izazovi* (Beograd: Univerzitet u Beogradu, Fakultet bezbednosti.

19. Путник, Н. (2012), Кибер ратовање, нови облик друштвених конфликата, докторска дисертација,(Београд, Универзитет у Београду, Факултет Безбедности.
20. Симић, Д. (2002) *Наука о безбедности, савремени приступи безбедности,* Службени лист, Београд.
21. Сингер, П. В.. Сајбер сигурност и сајбер рат: оно што сви треба да знају. Фриедман, Аллан. Окфорд., 2014, ИСБН 9780199918096. ОЦЛЦ 802324804.
22. Sinks, M. A. (2001): Cyber Warfare and International Law, unpublished research paper, AirUniversity, Air Command and Staff College, Maxwell AFB, Alabama, 2008.5. Joyner, C., Lotrionte, C.: "Information Warfare as International Coercion: Elements of a Legal Framework ", European Journal of International Law 12, No. 5.
23. Стратегија одбране Републике Србије „Службени гласник РС“, број 94 од 27. децембра 2019.
24. Вулетић,. Д. (2017), "Сајбер безбедност": „Интегрална безбедност Републике Србије., Универзитет "Унион-Никола Тесла", Београд.

Internet sources / Електронски извори:

1. *BBC NEWS*, 2. 5. 2007; *The Economist*, 10. 5. 2007; *Telegraph*, 19. 5.2007.https://www.nytimes.com /2016/02/17/world/middleeast/ us-had- yberattack-planned-if-iran- nuclear- negotiations-failed.html, (31.07.2022).
2. Brussels, COM(2006) 251, http://ec.europa. eu/ information_society /doc /com 2006251. pdf, (15.08.2022).
3. Euronews.rs/evropa/ neistrazena – evropa /39395/ besni- hakerski- rat- ukrajina- formirala - sajber-dobrovoljacku- gardu- anonimusi- protiv- rusije/vest. (08.08.2022).
4. https://charlesdenyer.com/blog/even- bigger-than-stuxnet-nitro-zeus -americas- plan-to-decimate- irans-critical - infrastructure-part-iii/, (17.09.2021).
5. https://www.rtv.rs/sr_lat/ evropa/rusija -na-udaru -milijardi-sajber-napada- vecina-iz-sad_1297588. html. (15.12.2022.)
6. European Commission, Brussels, JOIN(2013),http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.
7. International Strategy for Cyberspace, U.S. White House, Washington, 2011,http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf (15.12.2022).
8. *Cybersecurity for Critical Infrastructure Protection – Technology Assessment*, United States General Accounting Office, GAO-04-321, http://www.gao.gov; *Guideline for Identifying an Information System as a National Security System*, National Institute of Standards and Technologies, http://csrc.nist.gov (22.12.2022).
9. *Cyber warfare* : a multidisciplinary analysis. Green, James A., 1981-. London. 7 November 2016. ISBN 9780415787079. OCLC 980939904. (28.02.2023).

10. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, (11.11.2022).
11. Convention on Cybercrime, Council of Europe, Budapest, 2011, http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc,
12. Cooperative Cyber Defence Centre of Excellence, International Cyber incidents: Legal considerations, Abbrevations and glossary, Eneken Tikk, Kadri Kaska, Liis Vihul (Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010) http://www.ccdcoe.or (30.07.2022).
13. Network and Information Security, 2011, https://www.enisa.europa.eu/ activities/ Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategy-of-czech-republic-2011-2015/at_download/file. (30.07.2022.)
14. What is Cyber Security?". www.kaspersky.com (на језику: енглески). Приступано сајту (29.07.2022).
15. Сајбер рат - да ли постоји?". НАТО. 13. јуна 2019. (28.07. 2021.)
16. https://www. Slobodna evropa.org/a/ sajber- napad- crna-gora /32031931. html. (05.09.2022).