Rivalry between the United States of America and Russia in cyberspace

Dejan V. VULETIĆ[1], Branislav D. ĐORĐEVIĆ[2]

Abstract: Authors analyze cyberspace, a product of the rapid development of information and communication technologies, and its role and importance for leading world powers. Nevertheless, to the undoubted advantages for modern society, cyberspace has certain negative aspects regarding the state functioning. The authors emphasize that there are certain threats in cyberspace and that they are becoming more numerous and sophisticated. In strategic and doctrinal documents of many countries they are among the greatest security challenges in the 21st century. The authors explainthat cyberspace is characterized by increasing militarization and the undoubted military presence of leading world powers such as the United States (U.S.) and Russia. Further, authors develop the argument that the growing dependence and use of information and communication technologies has caused, among other things, a change in the physiognomy of modern armed conflicts. The next part of the paper is dedicated to the conflict of states in cyberspace. In the final part of the article, authors give examples of incidents between the U.S. and Russia and analyze their capability for cyber warfare. The authors conclude that both considered world powers have respectable offensive and defensive capacities for cyber warfare.

Key words: information, information-communication technology, contemporary conflict.

[1] Research Fellow, The Strategic Research Institute, University of Defence, Belgrade.
E-mail: dejan.vuletic@mod.gov.rs

[2] Full Professor, Institute of International Politics and Economics, Belgrade.
E-mail: bdjordjevic@diplomacy.bg.ac.rs

Introduction

The information society is characterized by a high level and speed of transmission, reception and exchange of digital data and information. The information transmitted by information and communication technology serves as a basis for making optimal decisions at all levels of society and contributes to the efficient use of resources needed to make decisions. It provides access to huge amounts and sources of information, possibility of making contacts on a global level and cost reduction. The information society is exposed to various abuses in the information environment. Cyberspace, by its characteristics, provides favorable conditions for criminal behavior of individuals or groups, often sponsored by certain states.

Human civilization is characterized by numerous conflicts, armed and unarmed, which were conducted in accordance with technological and other achievements in those periods. Throughout the course of history, military leaders have considered information superiority a key factor in victory. The struggle to achieve "information superiority" is increasingly emphasized in information society.

The interconnectedness, interdependence and availability of information and communication technologies, such as computer networks, are constantly redefining and changing the characteristics of modern conflicts. Cyber space as unlimited and interactive environment represents a link between different networked entities (individuals, organizations, etc.). The world's leading powers view cyberspace as a new, fifth, area of warfare (along with land, sea and ocean, air and space) (Vuletić 2021, 2).

Cyberspace, with all its advantages and disadvantages, has conditioned an increasing military presence in that domain. Cyberspace is a globally integrated information and communication infrastructures organizations but also vital state structures (banking sector, health care, transport, water, energy, etc.). Although it is predominantly a virtual domain, cyberspace has a significant physical dimension - computers that process and store data, systems and infrastructure that enable the communication and exchange of data and information. This physical dimension indicates that cyberspace is not completely without national sovereignty (Willett 2019, 1; Stojanović 2021, 440-441).

Cyberspace is a global domain within the information environment that consists of an interdependent network of information and communication technologies and appropriate information content (data and information). Cyberspace is a complex, changeable, difficult to predict, insecure and unstable environment that has its own physical dimension (eg computer servers). Although cyberspace provides communication opportunities, it also creates critical vulnerabilities that

an adversary can exploit. Complexity, low cost of access, widely available resources, minimal required technological investments and anonymity in cyberspace allow opponents to inflict serious damage (JDMCO 2019; DoD Strategy for Operations in the IE 2019).

Superiority in cyberspace provides a decisive advantage to commanders at all levels of command (strategic, operational and tactical) in modern conflict. Superiority in cyberspace is the degree of dominance of one force in cyberspace that enables safe, reliable conduct of operations of that force and related ground, air and other forces. Superiority in cyberspace enables, supports, provides and facilitates the realization of the goals of the operation. The ability to act in cyberspace has emerged as a vital requirement of national security. The growing influence of information and communication technologies on military operations further increases the importance of cyberspace for national security (JP 3-12 2018; FM 3-12 2017.

Physiognomy of modern armed conflicts

Changes in the global order of international distribution of power by moving from bipolar, through unipolar, to multipolar structure of international relations (Stojanović i Đorđević 2017, 466-470; Radaković 2012, 120-121; Kostić 2018, 407-409; Kostić 2019, 522). The strategies of the great powers are based on military power, but also on economic means, which is especially characteristic of China (Stanojević 2021, 30). Multiplication of global factors and the intricate network of interactions between the elements of the system causes constant tensions in today's world (Prošić 2015, 13). Transformative effects of globalization and technical-technological development have conditioned the classic use of military power stopped being dominant factor in contemporary conflicts. From the earliest history of human civilization and the formation of the first states until today, military power has determined the fate of civilizations, peoples and states and significantly influenced the harmonization of defense policy and systems, and thus created international relations.

The current moment in the international community is characterized by the growing role of non-state actors (NGOs, religious movements, multinational corporations, etc.) and the frequent disruption of relations between different states, which has numerous negative implications. States use various instruments to conduct foreign policy, such as bilateral and multilateral negotiations, international law, the formation of military, economic or political alliances, acting

through international organizations, starting wars and relying on military force (Proroković 2017, 402-403).

Historically, the rules of international peace and security have been always depended on the system and relations of the international structure among the great powers. The decline of the American the power and rise of other great powers, especially China and Russia, once raises again the question of the direction in which international peace is heading and security order go on (Trapara 2010, 93).

The globalization of political, cultural, information-communication and, especially, economic ties of the subjects of international relations, have resulted in the growing importance of the role of other, non-military forms of power. Globalized international relations continue to be shaped by realpolitik practice. In such conditions of social reality, military power has lost its significance, but it still occupies an important role in world politics.

Beginning in the second half of the twentieth century, modern society is characterized by certain controversies which indicated the so-called "dark side of progress." Numerous technological achievements have led to the numerous threats to both individuals and countries (Aleksić 1995, 16-20).

Technological progress and the development of the information society have conditioned the change and physiognomy of modern armed conflicts. The progress of development in all segments of society has imposed the need for a different strategic thinking on how and by what means to achieve and protect vital national values and interests. The presence of non-state actors, the absence of rules and organized units in the struggle are a feature of the conflict at the beginning of the 21st century, fundamentally different from the previous ones guided by the principles formulated by Karl von Clausewitz (Kaldor 2012, 1-14). John Mueller (1996, 221), pointed to a a change in the nature of contemporary conflict. He further indicates that the conflict of power in the so-called Great War became almost inconceivable. According to him, there is little chance that armed conflict will be used as a method of politics to achieve certain goals, such as conquering territory, moving borders or establishing supremacy in international relations, has been overcome. The author sees the main reason for these claims in the changed psychology of statesmen and peoples, as well as in general absence of aggression in developed countries to start a war.

The processes of globalization and technical-technological development have resulted in the reduction of the role of military power in modern international relations, which affects the physiognomy of modern armed conflicts, more precisely its character. The transformation of armed conflicts into postmodern ones conducted at the highest level, through a different, less important role of the

military instrument of power, in relation to other non-military instruments of power (economic, informational, political), in achieving ultimate strategic goals. Numerous and diverse social relationships create an environment where asymmetric challenges, risks and threats are becoming the dominant forms of security threats.

The military power of states, expressed by engagement of armed force, is increasingly proving ineffective in pursuing foreign policy interests. The current conflict in Ukraine may refute such claims. The trend of decreasing its efficiency can be explained by the impact of the process of globalization and the information revolution on social flows. Globalization has led to the growing role of non-state actors in international politics, thus transforming international relations into global ones. In addition, the information revolution has led to the development of new areas in which unarmed international conflicts take place (Vuletić i Vračar 2018, 137).

The institutionalization of diplomacy in the new conditions and the construction of a modern security system influenced the limitation of the engagement of the military resources in the realization of the set goals by states as subjects of international relations. A new way of resolving disputes has also caused the development of new means, and with them new ways of warfare (information, hybrid, etc.). Thanks to the efficiency of implementation, these new ways of warfare are a characteristic of modern conflicts and ways of resolving disputes in the international community.

Today's multipolar world sees the changing role of international organizations, the changing role of states, the delegation of competencies to the institutions of the union (for example, member states of the European Union), different interests which consequently lead to various conflicts adapted to the achieved level of technological and social development (Mikić 2002, 113).

Modern conflicts differ in nature and in their impact on other social phenomena. The essence of each individual conflict expresses the characteristics that represent a series of events and activities related to technological progress, military capabilities, economic development, and so on, of conflicting states. Due to the continuous development of human society, science, weapons and military equipment, there is a constant development and diversity of conflict characteristics. Thus, the above mentioned conflict characteristics cannot be viewed as a universal category, but as a variable category that depends on a different factor.

Contemporary conflicts are multidimensional (economic, diplomatic, informational …), complex and continuous. The focus, in the contemporary conflict, is shifting from armed to unarmed content, which leads to changes in the order of phenomena and processes that take place in it. Armed violence, as the dominant content, is pushed to the end (it becomes the ultimate method of the conflict

itself). Time is of the essence in an armed conflict. The conflicting parties are trying to achieve their goals as soon as possible, and modern weapons and combat equipment significantly contribute to that.

Conflicts often lead the world's most powerful states far from their home territories, thus protecting their vital (mostly economic) interests. A typical example of this kind is the Gulf War, led by several major world powers against oil-rich Iraq. Contemporary conflicts differ in certain elements such as: the space in which they are conducted, the intensity and duration of actions, and so on. In the modern conflict, the importance of electronic and anti-electronic actions has increased. Domination in the information environment is very important as well as domination, i.e. control of the situation in space, airspace and on land. (Stišović i Sivaček 1998, 12).

Various modern weapons are widely used in modern conflicts and there is a growing asymmetry between the conflicting parties. Each side in the conflict strives to preserve and spend as little of its resources as possible, above all, people, are the least exploited. Saving one resource category in conflict leads to increased consumption by others. What is accepted as the norm of shaping the modern conflict is the maximum engagement of people, rational spending of war equipment and energy, all at the expense of using an extremely large amount of information. In all conflicts there is a great need for information and the amount of relevant information available is of great importance for final outcome of the conflict.

Modern armed conflict is inconceivable without a large amount of information about the enemy, one's own forces, the environment in which it is conducted. Information provides numerous advantages to the information superior side in the conflict. At the same time, information has also become an important target for opponents. Information is becoming increasingly important for national security in general and in armed conflict in particular. Accordingly, contemporary conflicts are strongly characterized as a battle in the sphere of information. Information management has become an important weapon in changing the attitudes of opponents and imposing one's own will.

State conflict in cyberspace

Necessary condition for a certain state to have the status of a superpower in the twenty-first century, it must have respectable capabilities for cyber warfare. Besides to using cyberspace to seize various types of classified information, like

traditional espionage, states use cyberspace to initiate their own economic development: disruption of financial institutions, interference in electoral processes, obstruction and diminishing the capacity of another state to develop nuclear weapons, etc. (Willett 2019, 1).

State-sponsored cyber operations are happening more often, and the consequences for the target can be more serious. Some cyber operations have been revealed in the media, while most remain in the domain of the most closely guarded secrets. Cyber operations can cause the death and destruction of people and property, intentionally or accidentally. In certain cases, the uncontrolled action of a computer virus can occur, as has happened with e.g. the British national health system which was probably the unintentional victim of a North Korean cyber attack targeting the UK banking system (Willett 2019, 1).

Threats in cyberspace are real, fast-growing and changeable. The most significant threats in cyberspace come from national actors. Nation-states are not the only threat actors. Numerous growing threats in cyberspace include cybercriminals, individuals or groups that may be politically motivated, mercenaries capable of using existing or acquiring new tools for malicious activities, i.e. for the realization of desired goals. Cyber attacks will be part of any future conflict, including attacks on a particular state, before or during an armed conflict. With that in mind, the critical information infrastructure of a particular country is at risk of cyber threats and must be protected (Porche III 2020, 4-20;Vuletić 2019, 55-60).

States are engaged in increasing competition in cyberspace "at a level below the armed conflict". Cyber espionage has become a common occurrence in cyberspace, and increasingly cyber sabotage, making threats in cyberspace destabilizing and potentially escalating (Inkster 2019, 1).

The consequences of cyber attacks are growing. The malicious program NotPetya exploit from 2017, initially directed against Ukraine, paralyzed the activities of the world's major corporations and ports, disrupted significant parts of global supply chains for several weeks (Inkster 2019, 1). The material damage caused by the cyber attack is estimated at billions of US dollars. Major problems in the Internet functioning are caused by attacks on the most important elements of the Internet infrastructure, such as Domain Name System[3]. The problem in the future will be bigger due to the increasing use and dependence on the "Internet

---

[3] It is a system that converts hostnames into IP addresses, making it easier to use the Internet, because Internet communication is based on numerical IP addresses that are difficult for people to remember.

of Things"[4], which includes millions of vulnerable and potentially insecure devices that connect via the Internet, which significantly increases the number of possible targets that may be endangered (Inkster 2019, 1).

Russia has often been brought into a negative context, trying to influence the outcome of the US presidential election held a few years ago. The media reported that Moscow carried out an orchestrated disinformation campaign to influence public opinion and their voting (Bina and Dragomir, 2020, 125).

There is a growing concern that the Internet, on which almost every function of human society depends, will be threatened by an increase in harmful activities and in itself become a catalyst for growing global instability. "Global Commission for the Stability of Cyberspace" was created to solve problems and create a safer virtual environment. The Commission held numerous meetings in several different countries during which cyber threats were analyzed and measures to mitigate them were considered (Inkster 2019, 1). Commission was dissolved in 2019.

Considering its origins, modern Internet management is dominated by a different approach of several stakeholders. Trust, openness and consensus are emphasized, with cyberspace considered incompatible with traditional models of control of the Internet and other computer networks. Different interests and approaches to a number of issues related to cyberspace, create favorable conditions for individuals, organizations and certain countries to go unpunished for certain malicious activities that they commit in the mentioned domain. (Willett 2019, 1).

The doctrine of information security of the Russian Federation specifies what information security is, with an emphasis on the protection of the individual and the state in the information environment. This segment of national security has been identified as one of the priorities. The Doctrine lists the negative factors that affect information security with special emphasis on foreign interference and influence. Additionally, the lack of generally accepted regulations and procedures also poses a problem. (Doctrine of Information Security RF 2016).

Russia is committed to defining generally accepted principles for regulating rules of conduct, legal norms and other important elements related to the information security. Russia has prepared and presented two resolutions at the United Nations General Assembly in September 2018. The resolution recommends

---

[4] These are a number of networked devices, sensors, home appliances, vehicles, facilities, machines and the like that can exchange data with the operator and other connected devices. They are applied in various areas of life and work. It is estimated that the current number of such devices is tens of billions and with a tendency of constant growth.

re-establishing the United Nations (UN) Group of Governmental Experts on Cyber Security and the adoption of regulations and legal norms that would apply to cyberspace. However, due to different points of view and different interests, these resolutions were not accepted by the United States and certain countries. (IISS 2018a, 1).

At the scientific conference dedicated to cyber security held on July 6, 2018 in Moscow, Russian President Vladimir Putin invited the participants to international cooperation in order to solve problems in cyberspace. He pointed out that threats in cyberspace have reached a high level, that they can only be countered by the joint efforts of a large number of countries, and that cyber security requires multilateral communication and coordination (IISS 2018b, 1).

The international conference "Cyberstability: Approaches, Perspectives, Challenges" was held in the Russian Federation in 2018. The conference was organized by the Journal of International Affairs. Besides promoting views on Russia's information security policy, the conference played an important role in continuing the discussion on military cyber stability between China, Russia and the U.S. The meeting, held in Paris in November 2018, included representatives of the leading European countries and was an upgrade of the meetings realized in previous years in China, Germany and the USA. The participants were suggested to go beyond theoretical exchange and work on it by organizing joint exercises that reflect realistic scenarios of conflict in cyberspace. The conference contributed to a better understanding of mutual differences and the prevention of possible conflicts in cyberspace (IISS 2018c, 1).

Russia is trying to establish a greater degree of control over the flow of information on its territory. It advocates a multilateral regulatory procedure aimed at using information and communication technologies for military, terrorist and criminal purposes. The U.S., a country with probably the greatest cyber capabilities, focuses discussions on state actions, and less on internal security and information threats. The U.S. continues to strongly oppose state regulation in the area of information flows proposed by Russia.

This strategic emphasis, in turn, influenced the way Russia organized its cyber forces (Connell and Vogler 2017, 5-6). In 2013, Russia revealed that it plans to form a unit for action in cyberspace that would have offensive and defensive capacities, research and development potentials in order to improve the level of security in cyberspace and information security in general. It is assumed that Russia, as well as other countries, has a problem with recruiting that profile of experts (Connell and Vogler 2017, 8).

Russia has been brought into context, by certain countries, for demonstrating cyber capabilities, among other things, by attacking the Ukrainian power grid. Estonia, Georgia and Ukraine have served as a testing ground for Russian cyber capabilities, providing them with opportunities to hone their techniques and procedures in cyber warfare and techniques to deter potential adversaries. The simple DDoS attacks[5] and DNS hijackings[6], sophisticated malwares such as BlackEnergy[7] and Ouroboros[8]. In addition to the security services (Russia's military intelligence service – GRU, and the Federal Security Service – FSB), the offensive cyber activities of the Russian Federation involve individuals, various criminal organizations and associations. However, some experts believe that the techniques and tools they use are no longer as effective as they were five or ten years ago (Connell and Vogler 2017, 27-28).

It is estimated that preparations for cyber (information) attacks took a long time to prepare, which resulted in unauthorized intrusion into many critical information infrastructures in Ukraine at the beginning of the conflict. These activities indicate the prior planning and selection of the goal, compliance with the broader plan of the information operation, which is the difference from e.g. unauthorized access by a hacker group (Connell and Vogler 2017, 27-28).

Besides the adoption of normative and doctrinal documents and the formation of a special unit for cyber warfare, a special center (Cyber Defense Center) for managing cyber activities has been established, which has improved the level of security in cyberspace in Russia (Connell and Vogler 2017, 27-28).

It is very likely that Russia will use cyber operations in the pre-conflict scenario or even in peacetime when there is an opportunity that in this way they can influence the strategic outcome. The advanced level of cyber capabilities has, above all, a deterrent role, but it is to be expected that in the future it will have an increasingly offensive role to achieve strategic goals. (Connell and Vogler 2017, 27-28).

As already mentioned, responsibilities for cyber activities of the Russian Federation are primarily within the competence of the intelligence and security

---

[5] These are attacks from thousands of computers aimed at overloading a web server, network or other part of the infrastructure and thus denying access to their users.

[6] DNS Hijacking is a form of intrusion that directs web traffic to unauthorized domain systems. That way, users' requests are intercepted and redirected to the attacker's compromised DNS server.

[7] BlackEnergy is a Trojan malware designed to launch distributed denial-of-service (DDoS) attacks, download custom spam, and banking information-stealer plugins.

[8] Ouroboros ransomware is a malicious cryptovirus.

structures (civil and military) of the Russian Federation. The FSB (Federal Security Service) is probably the main organization in the Russian Federation in charge of information security (Heickero 2010, 4).

Cybe weapons are unnecessary if physical control of information infrastructures is provided, as shown in the case of the occupation of Crimea. Occupying an Internet access point (Simferopol Internet Exchange Point) and disconnecting cable connections to the mainland, have contributed to the overall information dominance in Crimea, greatly facilitating the operation (Giles 2016, 49).

An extremely important aspect of Russian information activities are the activities of trolls, personnel managed by individuals and bots managed by automated processes. Paid trolls are joined by "seduced" individuals in target countries that support certain activities for a large number of different, often personal reasons, discussion group members, or Twitter users. (Giles 2016, 54-56).

Russian concepts of operations are constantly evolving, and future campaigns will not resemble those seen so far. Engagement and replacing numerous staff and their operational deployment on the Ukrainian border and in Syria reflects, among other things, the intensive conduct of various forms of information warfare. The American assessment is that eastern Ukraine represents "a newly created laboratory for the future warfare." Russia and the citizens of Ukraine who support them have taken advantage of access to highly sophisticated electronic attack technologies, including GPS[9] spoofing, which has compromised positioning and guidance systems. Numerous operations from the recent past show that modern conflict is a mix of different diplomatic, informational and other non-military means, carried out with the support of military force" (Giles 2016, 64).

Individuals or organizations have compromised or hijack users accounts on social networks in the interest of Russia. Another campaign that Russia seems to have developed, is the capacity of mass targeting individuals on a personalized basis. Cyber attacks on Ukrainian energy networks in December 2015, were followed by an action of mass prevention of energy consumers from contacting service providers. The incident was likely denial of service (DoS) attack on the target server (Giles 2016, 72).

---

[9] A satellite system for accurately determining the geographical position anywhere on Earth, with an error radius of several meters. There are more than 30 satellites in the system for positioning, and in order to determine the precise connection of a device or object, it is necessary to establish a stable connection with a minimum of 4 satellites.

Military operations against Ukraine in 2014 and 2015 were accompanied by various information operations, which affected the morale, mobilization and response of Ukrainian forces. (Molder and Sazonov 2018, 327).

Computer viruses and other malicious software are important for compromising enemy computer systems, stealing information and intelligence, and developing and testing one's own cyber warfare weapons. Attacks range from high-level approaches, including targeting information and communication infrastructure at the strategic level, to much more focused targeting of individuals on a personal basis. Russia has also used the available resources to take over existing accounts on social networks in order to spread misinformation. Targeted SMS messages, emails or posts on social networks had a great effect on people who participated in the protest against Russia (Giles 2015, 5-14).

Russia's consideration of various forms of information warfare includes the perception of cyberspace as an important domain. Information is the most important element of the operation. The desired goal is complete domination in the information spectrum. In short, in Russia's comprehensive approach to information, cyber is not an independent discipline. According to Major General Stephen Fogarty, Commander of the US Cyber Command, Russian activities in Ukraine represent an effective integration of various forms of information warfare (electronic, cyber, psychological ...) in order to achieve the desired goal (Giles 2015, 13).

In the American understanding of cyberspace operations, they are based on the goal of achieving goals in or through cyberspace. (DOD Dictionary of Military and Associated Terms, 2018). The doctrine of the Ministry of Defense of the United Kingdom defines operations in cyberspace as "Planning and synchronization of activities in and through cyberspace in order to enable freedom of maneuver and achieve military goals" (Porche III 2020, 18).

The concept of strategic deterrence by the USA in cyberspace has not proven to be effective enough in practice. The American attitude towards cyberspace was more defensive in nature and aimed primarily at deterring potential attackers. The United States calculated that the perception of his offensive abilities could deter opponents from attacking (SGI 2019, 1).

The American approach to cyberspace has evolved in line with technological change. The establishing of the U.S. Cyber Command (USCYBERCOM) in 2009 and the achievement of the status of an independent operational command in May 2018 (until then it was part of the Strategic Command), shows the importance of cyberspace for the Pentagon (SGI 2019, 1).

In many ways, the separation of the American cyber command from the Strategic Command, which oversees strategic deterrence, is a symbol of the change in American attitude in cyberspace from defense to what has been described as "persistent engagement." In its vision for 2018, the Cyber Command states its goal that the U.S. must defend itself in advance, and as close as possible to the source of hostile activities and actors before they can achieve tactical, operational and strategic advantages. This belief is reinforced in the National Cyberspace Strategy published in September 2018 (SGI 2018, 1). The operationalization of the mentioned strategy through doctrinal and other documents would create conditions for effective action against certain entities, marked as hostile (for example Iran, due to the downing of the American drone) in cyberspace. The cyber attack on Iran has been publicly acknowledged by certain United States officials (SGI 2019, 2-5).

Cyber deterrence has not been successful in practice. That's why the interference and harassment, as opposed to deterrence, has been shown to be a more efficient and optimal model of action in cyberspace. American opponents know that in the event of a cyber attack on U.S., this would lead to a fierce response and serious consequences for the attackers. Therefore, they engage various groups, organizations or movements in order to realize their goals against the U.S. and its allies (SGI 2019, 3).

The U.S. emphasized the right to take action and to self-defense in the event of a cyber attack (Office of the Coordinator for Cyber Issues 2018, 1-3). In May 2019, the former President of the U.S., Donald Trump, declared the state of emergency in cyberspace at the national level, citing threats to the country's critical infrastructure. It was the third such declaration by the American president in four years (IISS 2020a, 1).

The U.S. carry out cyber operations at the strategic, operational and tactical levels. For almost three decades, they have been developing strategies and plans for cyberspace. The U.S Cyber Command has thousands of members who can be engaged in various types of cyber attacks both nationally and globally. The United States' advantage over other world and regional powers in terms of cyber capabilities has diminished in recent years (IISS 2020b, 1).

Protection of national interests, achieving domination and superiority in cyberspace are the main goals stated in the U.S. National Strategy for Cyberspace (National Cyber Strategy of the USA 2018).

US infrastructure is the most common target of numerous attackers, often sponsored by certain states. Their findings reportedly include data on the involvement of about 20 countries, most of which participated in the United

Nations Group of Governmental Experts (GGE) discussions (Tikk 2019, 479). The complicated procedure of initiating cyber attacks and the problem of inter-ministerial coordination was solved by passing the PPD-20 order in August 2018. (SGI 2019, 5).

Despite differing views, both Russia and the U.S. were pleased with the outcome of the 2014-2015 UN Group of Governmental Experts meeting, especially by the recommendation of 11 norms of responsible behavior of states (UNGA Rep. A / 70/174). At the meeting of the working group of government experts, it was said that such norms, rules and principles are voluntary, not binding. The report can also be interpreted as saying that Russia and certain countries are right when they try to overcome ambiguities and controversial elements in international law regarding cyberspace.

The U.S. has also developed offensive capabilities in cyberspace in the past, but this development has been far more intense in the last ten- fifteen years. According to some sources (NCERT 2012, 6) the U.S. is linked to involvement in the 2010 malicious program Stuxnet, which degraded Iran's nuclear weapons development program. Ways of using cyber weapons to sabotage North Korea's ballistic missile program were also investigated. Confidential information like this is difficult to verify, and there are often strategic reasons why it is not disclosed (SGI 2019, 1).

In January 2019, France announced the strategy which, instead of "active defense", emphasizes offensive cyber operations. It was also declared that the budget will be increased and that the forces for cyber warfare will be expanded. In 2013, the United Kingdom became the first Western country to announce the development of offensive cyber weapons, and in 2018, it planned to form new cyber forces, numbering about 2,000 staff, which could face a threat from Russia. NATO has announced that it will not independently conduct offensive cyber operations. Instead, it will integrate them and coordinate activities with member states. (SGI 2019, 5).

Examples of incidents between the U.S. and Russia in cyberspace

According to reports from certain cyber security companies, between the two rounds of presidential elections in France, Russian hackers allegedly interfered in Emanuel Macron's election campaign. Macron, one of two candidates voted in the second round of the presidential election, accused Russia of discrediting his

campaign, and his staff complained about constant, sophisticated cyber-attack attempts (SGI 2017, 1).

Russia is suspected by some countries of the international community of carrying out a series of attacks testing the defense of critical infrastructure of the U.S. (SGI 2019, 1). Certain TV stations, such as NBC, reported that the former U.S. president, Donald Trump, personally approved the cyber attack of the US military on the Russian "Internet Research Agency" during the parliamentary elections in Russia, in 2018.

In mid-April 2017, a letter from IT expert Ruslan Stoyanov was published in certain Russian media. Stojanov claimed that Russia was recruiting hackers for numerous cyber campaigns, offering them immunity from criminal prosecution for crimes committed abroad. Earlier, an indictment was filed against four people who are allegedly agents of the Russian Federal Security Service (SGI 2017, 1).

Regardless of the risks and possible consequences, individuals and organizations motivated by different things, engage to achieve someone's goals. States strive to gain supremacy in cyberspace and to recruit the best, highest paid, experts. Peter Levashov, a Russian citizen, arrested on the orders of the U.S. in Spain in 2017, allegedly paid dearly for his services. He was allegedly not paid a large amount of money, but other people, such as Levashov, are being offered other rewards. Most countries with advanced intelligence capabilities hire operatives under unofficial cover. This way of engaging is realized in order to protect one's own image. Russia is not alone in recruiting its citizens, who live abroad, to perform certain tasks for their needs (SGI 2017, 1).

Due to the alleged connection of Kaspersky with the Russian government, the U.S. Department of Homeland Security has demanded that federal agencies remove all Kaspersky products from their computer systems. They justified their demands by arguing that Kaspersky's products, like those of several other companies, were designed to provide complete recording and supervision of all traffic on computer networks (IISS 2017, 1).

Microsoft has released information about a new cyber offensive, which they said was carried out by Russian government hackers. Russia's APT28 group, considered part of Russia's military intelligence service (GRU), has created fake websites to attract visitors and ask them to leave personal information. Microsoft points out that the perpetrators' intention is to collect certain information from clients (IISS 2018d, 1).

There are reasonable suspicions that individuals, organizations and movements, sponsored by Russia, are invading American critical infrastructures.

Probable goal of the attacker was to create remote access capabilities and disruption of the conflict management system (Connell and Vogler 2017, 27-28).

After the United Kingdom, the Netherlands and the U.S. published news about malicious Russian cyber operations. Certain Latvian officials said that Russia's military intelligence service, the GRU, had been attacking their central intelligence agency for years (IISS 2018e, 1). Certain allegations have been made against the Russian state over the alleged attack on the Organization for the Prohibition of Chemical Weapons. The incident allegedly happened in April 2018, after which four Russian intelligence officers were expelled. The Dutch government also stated that Russian hackers tried to infiltrate and obstruct the investigation into the crash of the Malaysia Airlines MH17 plane (IISS 2018f, 1).

The US Department of Justice has filed an indictment against seven Russian military intelligence officers on charges of unauthorized access to computer systems, fraud, identity theft and money laundering. The indictment alleges that certain individuals intended to compromise international anti-doping efforts in revenge for publishing a state-funded Russian doping program (IISS 2018f, 1).

Cyber warfare capabilities of the U.S. and Russia

The importance of cyberspace and the use of information resources are critical to the outcome of modern armed conflict. Dominance in cyberspace and protection of own resources is the goal of both countries, which can be seen in the analysis of their strategic and doctrinal documents. In the U.S. strategic documents, cyber operations are viewed as separate operations, while the Russian side views them as a component of a broader, information war. Both countries have formed units, respectable capacities and capabilities for cyber warfare. Significant attention is paid to the protection of information resources in both countries. The analysis of the documents shows the emphasis on the greater threat to the United States from Russia (and China) than vice versa. The degree of dependence on information and communication technologies is higher in the U.S. than in Russia, which represents a higher risk and possible consequences in case of compromising these systems. Russia is increasingly relying on the development of its own industry and sophisticated tools. As in China, the perceived abuse of social media in Russia is considered a significant issue of national security. Both countries are aware of the numerous threats to their information and communication infrastructure (IISS 2021, 15-28, 103-114).

A possible cyber war is currently a disadvantage for the U.S., according to cyber security experts. Measuring capabilities, in addition to the offensive aspect, includes defense (a measure of national capacity to block or mitigate the consequences of an attack) and dependence (reliance on computer networks and systems that may be vulnerable to cyber attacks). The measurement of cyber warfare capabilities, according to Richard Clarke and Robert Knake, is based on the assessment of offensive power, defense capabilities and dependence on a computer system. Addiction refers to critical information systems that do not have an adequate replacement in cyberspace. A lower degree of dependence means a higher number when ranking (Clarke and Knake 2010, 99-101).

The relationship of the considered countries from the aspect of cyber capabilities is as follows:

- United States – total 11 (cyber attack: 8; cyber addiction: 2 and cyber defense: 1)
- Russia – total 16 (cyber attack: 7; cyber addiction: 5 and cyber defense: 4)

Both countries are among the world's leading powers when it comes to cyber capabilities. The U.S. probably has more modern offensive capabilities for cyber warfare, but there are certain weaknesses when it comes to defense. Russia has paid much more attention to the defense of national computer networks. Control of critical information infrastructures and the possibility of disconnection from the rest of cyberspace is far greater in Russia than in the U. S. (Clarke and Knake 2010, 99-101).

Disagreement over regulations between the United States and Russia (as well as China) remains high. None of the considered countries is ready for certain restrictions on the freedom of action in cyberspace, which would be regulated by generally accepted norms of behavior and action.

The great world powers compete with each other in several domains to secure their interests and promote their security. In recent years, perhaps the most dramatic area of growing competition has been in cyberspace, where these countries have pursued very different competition strategies, including some that appear to be very risky or destabilizing for international security. The scope and variety of different tools and mechanisms of action in cyberspace is expanding to include such activities as interference in democratic processes and theft of industrial secrets on an increasing scale and level of sophistication. The great powers are also looking for ways to wage large, destructive forms of conflict by virtual means (Mazarr et al. 2022, 1).

Conclusion

Cyberspace is a global information and communication infrastructure, created as a result of social needs and technological innovations. Economic prosperity, national security and geostrategic influence of states depend on their capabilities in cyberspace.

The constant technological progress with the complexity of the nature of threats imposes the need for constant risk management. From the aspect of security in the domain of information, the negative aspect is that the government is not able or does not have mechanisms to control all computer networks in its territory, among other things due to the ownership issue. Discovering the origins and understanding the seriousness of the threat is very difficult, given the complexity of cyberspace and the very nature of the threat (Vuletić i Đorđević 2021, 251-253).

The society in which we live is characterized by global connectivity, increasing use of personal computers, ease of Internet access. Companies are involved, in all segments, in the race for information as a key resource. Global, interconnected computer networks require global connectivity in solving cyber security problems. Based on all the above, it can be concluded that cyberspace is an unsafe environment and that numerous incidents between the world's leading powers pose a growing social danger due to constant improvement of techniques, relatively simple execution of certain acts and an increasing number of possible perpetrators, from individuals to states. The various non-traditional forms of endangering the information infrastructure of the society can certainly include threats that come from cyberspace.

Given the complexity and possible consequences of cyber abuse, the adoption of internationally accepted regulations is necessary but insufficient in counteracting this phenomenon. Proactive action deters, disables or prevents potential perpetrators, while reactive action eliminates the consequences of compromising the security of computer systems.

Cyberspace is an area that many countries are dealing with more and more, they have their own forces and resources. In addition to being a new area of warfare, cyberspace also represents a domain in peacetime in which there are certain disagreements between great powers, such as the U.S. and Russia. Mentioned examples prove it.

The mentioned domain is not completely regulated by generally accepted agreements and arrangements, which makes it suitable for abuse, which can result

in certain incidents between the United States and Russia causing serious disruption of relations and potentially leading to armed conflict.

References

Aleksić, Živojin i Milovanović, Zoran. 1995. *Leksikon kriminalistike*, Beograd: Glosarijum.

Bînă, Marian Valentin and Dragomir Cristian. 2020. ''Informative combat of the Russian hybrid war''. *Journal of Defense Resources Management* 11 (1): 124-132.

Clarke, Richard and Knake, Robert. 2010. *Cyber War – The next threat to National Security and What to do about it,* Pymble: HarperCollins Publishers.

Connell, Michael and Vogler, Sarah. 2017. *Russia's Approach to Cyber Warfare*, Washington: Center for Naval Analyses.

[Doctrine of Information Security RF 2016] Doctrine of Information Security of the Russian Federation. 2016. Decree of the President of the Russian Federation No. 646 (5 December). https://www.mid.ru/en/foreign_policy/official_ documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

DOD Dictionary of Military and Associated Terms. 2018. Washington: U.S. Department of Defense.

[DoD Strategy for Operations in the IE 2019] Department of Defense Strategy for Operations in the Information Environment. 2016. https://dod.defense.gov/ Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf

[FM 3-12 2021] Field Manual 3-12, Cyberspace and Electronic Warfare Operations, 2021. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN33127-FM_3-12-000-WEB-1.pdf

Giles, Keir. 2015. *The Next Phase of Russian Information Warfare*, Riga: NATO Strategic Communications Centre of Excellence.

Giles, Keir. 2016. Handbook of Russian Information Warfare. Rome: NATO Defense College.

Heickero, Roland. 2010. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*. Stockholm: Swedish Defence Research Agecy (FOI).

Inkster, Nigel. 2019. *It's time to stabilise cyberspace – our well-being depends on it*, Washington: International Institute for Strategic Studies.

[IISS 2017] International Institute for Strategic Studies. 2017. *Cyber attacks: fight the disease, not the symptom*. https://www.iiss.org/blogs/analysis/2017/11/cyber-attacks

[IISS 2018a] International Institute for Strategic Studies. 2018. *Cyber report: 29 June to 5 July*. https://www.iiss.org/blogs/cyber-report/2018/07/cyber-report-29-june-to-5-july

[IISS 2018b] International Institute for Strategic Studies. 2018. *Cyber report: 6 to 12 July*. https://www.iiss.org/blogs/cyber-report/2018/07/cyber-report-6-to-12-july

[IISS 2018c International Institute for Strategic Studies. 2018. *Cyber report: 7 to 13 December*. https://www.iiss.org/blogs/cyber-report/2018/12/cyber-report-7-to-13-december

[IISS 2018d] International Institute for Strategic Studies. 2018. *Cyber report: 17 to 23 August*. https://www.iiss.org/blogs/cyber-report/2018/08/cyber-report-17-to-23-august

[IISS 2018e] International Institute for Strategic Studies. 2018. *Cyber report: 5 to 11 October*. https://www.iiss.org/blogs/cyber-report/2018/10/cyber-report-5-to-11-october

[IISS 2018f] International Institute for Strategic Studies. 2018. *Cyber report: 28 September to 4 October.* https://www.iiss.org/blogs/cyber-report/2018/10/cyber-report-28-september-to-4-october

[IISS 2020a] International Institute for Strategic Studies. 2020. *Cancelled – Cyber emergencies and national defence: lessons from the US.* https://www.iiss.org/events/2020/03/cyber-emergencies-and-national-defence

[IISS 2020b] International Institute for Strategic Studies. 2020. *Cyber war fighting: matching US capabilities to ambitions in offence and defence.* https://www.iiss.org/events/2020/01/cyber-war-fighting-us-capabilities-and-ambitions

[IISS 2021] International Institute for Strategic Studies. 2021. *Cyber Capabilities And National Power: A Net Assessment*, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

[JDMCO 2019] Joint Doctrine for Military Cyberspace Operations (Denmark), 2019. https://www.fak.dk/globalassets/fak/dokumenter/publikationer/-fakpub-150-1-eng-.pdf

[JP 3-12 2018] Joint Publication 3-12, Cyberspace operations, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Kaldor, Mary. 2012. *New and Old Wars: Organized Violence in a Globalized Era*. Cambridge: Polity Press.

Kostić, Marina. 2018. ''Čija hegemonija? – Svet u uslovima takmičenja za novu globalnu vladavinu'', *Međunarodni problemi,* 4: 391-411.

Kostić, Marina. 2019. ''Isključiva priroda evropskih, evroatlantskih i evroazijskih integracija i previranja na evropskom postsovjetskom prostoru'', *Međunarodni problemi,* 4: 498-526.

Mazarr, Michael, Frederick, Bryan, Ellinger, Emily and Boudreaux, Benjamin. 2022. Competition and Restraint in Cyberspace (RAND – Research Report), https://www.rand.org/pubs/research_reports/RRA1180-1.html

Mikić, Slobodan. 2002. ''Karakteristike savremenih ratova'', *Vojno delo* 4–5: 113-138.

Molder, Holger and Sazonov Vladimir. 2018. ''Information Warfare as the Hobbesian Concept of Modern Times - The Principles, Techniques, and Tools of Russian Information Operations in the Donbass''. *The Journal of Slavic Military Studies* 31 (3): 308-328.

Mueller, John. 1996. *Retreat from Doomsday: Obsolescence of Major War*, New York: Basic Books.

[National Cyber Strategy of the USA 2018] National Cyber Strategy of the USA. 2018. United States of America, President Donald J. Trump, The White House (September). https://digital.library.unt.edu/ark:/67531/metadc1259394/m2/1/high_res_d/National-Cyber-Strategy.pdf

[NCERT] Nacionalni CERT-PUBDOC-2012-10-338. 2012. *Zlonamjerni programi u službi država.* https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2012-10-338.pdf

Porche III, Isaac R. 2020. *Cyberwarfare An Introduction to Information-Age Conflict*, Boston and London: Artech House.

Proroković, Dušan. 2017. ''Geopolitičke determinante spoljnopolitičkog pozicioniranja Srbije na početku 21. veka'', *Međunarodni problemi,* 4: 401-422.

Prošić, Slobodan. 2015. ''From Power Balance to Conflicting Intensities''. *The Review of International Affairs*, LXVI (1158-1159): 5-17.

Radaković, Milovan. 2012. ''Russian Foreign Policy and Serbia''. *The Review of International Affairs*, LXIII (1146): 119-127.

Stanojević, Nataša. 2021. ''Geoeconomic concept and practice: Classification of contemporary geoeconomic means''. *The Review of International Affairs*, LXXI (1183), 29-46.

Stojanović, Stanislav i Đorđević, Branislav. 2017. ''Svetsko društvo rizika i zaštita nacionalnih interesa Republike Srbije'', *Međunarodni problemi,* 4: 465-482.

Stišović, Milinko i Sivaček, Jože. 1998. ''Vojni činilac bezbednosti SRJ na početku 21. veka'', *Vojno delo* 3: 9-27.

[SGI 2019] Stratfor Global Intelligence. 2019. *The U.S. Unleashes Its Cyberweapons*. https://worldview.stratfor.com/article/us-unleashes-its-cyberweapons-iran-russia-china-cyberwar

[SGI 2018] Stratfor Global Intelligence. 2018. *A New, More Aggressive U.S. Cybersecurity Policy Complements Traditional Methods*. https://worldview.stratfor.com/article/new-more-aggressive-us-cybersecurity-policy-comple-ments-traditional-methods

[SGI 2017] Stratfor Global Intelligence. 2017. *Untangling the Web of Russia's Cyber Operations.* https://worldview.stratfor.com/article/untangling-web-russias-cyber-operations

Stojanović, Bogdan. 2021. ''Transformation of outer space into a warfighting domain in 21st century'', *Međunarodni problemi,* 3: 433-454.

Tikk, Eneken. 2019. *Armaments, Disarmament and International Security - SIPRI Yearbook online*, Oxford: Oxford University Press.

Trapara, Vladimir. 2010. ''Pravila o međunarodnom miru i bezbednosti u svetlu odnosa između svetskih sila'', *Međunarodna politika,* 1140 (4): 80-93.

[UNGA] UN General Assembly. Report A/70/174, Developments in the field of information and telecommunications in the context of international security. July 22, Office for Disarmament Affairs, New York. https://undocs.org/A/70/174

Vuletić, Dejan i Vračar, Milinko. 2018. ''Promena fizionomije savremenih sukoba''. U: *Upotreba sile u međunarodnim odnosima*, urednik Žaklina Novičić, 137-15. Beograd: Institut za međunarodnu politiku i privredu.

Vuletić, Dejan i Đorđević, Branislav. 2021. ''Problemi i izazovi upravljanja internetom na međunarodnom nivou'', *Međunarodni problemi,* 2: 235-258.

Vuletić, Dejan. 2019. ''Sprečavanje incidenata između NATO i Rusije i mere za izgradnju poverenja'', *Vojno delo* 4: 1-14.

Vuletić, Dejan, Milenković, Miloš i Đukić, Anđelija. 2021. ''Sajber prostor kao područje sukobljavanja: Slučaj SAD – Iran i Severna Koreja'', *Vojno delo* 1: 1-14.

Willett, Marcus. 2019. *Cyber instruments and international security*, Washington: International Institute for Strategic Studies.

Dejan V. VULETIĆ, Branislav D. ĐORĐEVIĆ

RIVALSTVO SJEDINJENIH AMERIČKIH DRŽAVA I RUSIJE U SAJBER PROSTORU

Apstrakt: U radu autori analiziraju sajber prostor, koji predstavlja proizvod brzog razvoja informaciono-komunikacionih tehnologija, njegovu ulogu i značaj koji ima za vodeće svetske sile. Ipak, uz nesumnjive prednosti za savremeno društvo, sajber prostor ima i određene negativne aspekte u pogledu funkcionisanja države. Autori ističu da u sajber prostoru postoje određene pretnje i da su one sve brojnije i sofisticiranije. U strateškim i doktrinarnim dokumentima mnogih zemalja one su nalaze među najvećim bezbednosnim izazovima u 21. veku. Autori objašnjavaju da sajber prostor karakteriše sve veća militarizacija i nesumnjivo vojno prisustvo vodećih svetskih sila poput SAD (SAD) i Rusije. Dalje, autori razvijaju argument da je sve veća zavisnost i upotreba informaciono-komunikacionih tehnologija izazvala, između ostalog, i promenu fizionomije savremenih oružanih sukoba. Sledeći deo rada posvećen je sukobu država u sajber prostoru. U završnom delu članka autori daju primere incidenata između SAD i Rusije i analizira njihovu sposobnost za sajber ratovanje. Autori zaključuju da obe svetske sile imaju respektabilne ofanzivne i odbrambene kapacitete za sajber ratovanje.

Ključne reči: informacija, informaciono-komunikaciona tehnologija, savremeni konflikt.