Bógdał-Brzezińska, A., 2023. *Effectiveness of Russia's cyberaggression against Ukraine in 2022/2023,* Przegląd Geopolityczny, 44, s. 25-40.

Agnieszka BÓGDAŁ-BRZEZIŃSKA
University of Warsaw
ORCID: 0000-0003-0247-1941

EFFECTIVENESS OF RUSSIA'S CYBERAGGRESSION AGAINST UKRAINE IN 2022/2023[1]

SKUTECZNOŚĆ CYBERNETYCZNEJ AGRESJI ROSJI PRZECIWKO UKRAINIE W LATACH 2022/2023

Abstract:
The purpose of this article is to examine the determinants and evaluate the effectiveness of the impact of cyber measures used during the Russian-Ukrainian war. The analysis is primarily concerned with the subject dimension, in order to show that the cyber dimension of this war involves not only the parties to the kinetic conflict, i.e. Russia and Ukraine. Therefore, both non-state actors and international institutions, as well as state actors supporting Ukraine, will be assessed. The conclusions indicate that as a conflict in cyberspace, this war is not a bilateral conflict, but a multilateral one with changing dynamics, in which the number and type of combatants also change.

Keywords: cybersecurity, cyber warfare, Russia, Ukraine.

Russian concepts of the cyberspace sovereignty

Years of Cold War political rivalry between the USSR and the USA also resulted in a technological arms race. The system of central economic planning and a single-party political system with an extensive control apparatus made the USSR the best candidate to create a state, hierarchically structured computer network (Goodman, 1987). In the Soviet Union, the prototyping of digital machines was already developing in the late 1940s (Peters, 2012), and successes in the conquest of space in the 1950s accelerated and intensified the work of cybernetic thought centers in three Soviet republics: Russian (Moscow and centers in the

[1] The content of the article was presented and discussed during the Polish-Ukrainian Scientific Seminar entitled: *Ukraine in the face of Russian aggression. Problems of security of the state, society and the region.* The seminar, under the patronage of the Consul of Ukraine, was held on January 19 this year at the Jagiellonian University on the initiative of the Polish Geopolitical Society. In its organization also participated University of Gdansk and Warsaw University.

Urals), Belarusian (Minsk) and Ukrainian (Kassel, 1971). A great research and development center in computer science was the Institute of Cybernetics of the Ukrainian Academy of Sciences in Kiev and the Institute of Control Machines in Severodonetsk. The Kiev center was referred to as the forge of Soviet cadres for the concept of digital circulation of documents, and the 1961 report entitled "*Cybernetics in the service of communism*" was indicated as the first attempt to construct a computerized economic management system (Napolitano, 2021). The aforementioned triad of republics was joined in the 1980s by Estonia, where the development of cybernetics will result in the state administration and the economy being the most prepared in the region to jump into the digital era after regaining independence. Suffice it to say that at the time when Poland was computerizing public administration from 1994, Belarus and Estonia stood out from other Eastern European countries in terms of digital services or high-level Internet access.

Although at the beginning of the 21st century it seemed that the general pace of digitization of the former Soviet republics had slowed down (Bógdał-Brzezińska 2004), references to the key role of digital technologies in strengthening the defense sector appeared in political and military doctrines. This was most clearly seen in Russian strategic documents, in particular the Information Security Doctrine of the Russian Federation of 2000. It emphasized the multiple usefulness of digital technologies for the country's information policy, the link between information policy and national security policy, and finally - it referred to the foundations of digital sovereignty by postulating the creation of Cyrillic software that would guarantee Russia's autonomy from Western technology concerns (Bógdał-Brzezińska, Wendt 2020). It was also then that representatives of the power ministries announced their readiness to take kinetic retaliation in response to a cyber attack against the Russian critical infrastructure. This is important because it makes us aware of the continuity of thinking of the Russian political and military elites about cyberspace as a strategic domain, which precedes similar decisions and declarations of Western countries by several to several years (cf. NATO - 2008, USA - 2010).

The Russian perception of the political and defense role of digital technologies, in addition to the experience of Soviet cybernetics, is conditioned by the experience of Soviet propaganda and information policy (Radu 2022). This is the source of the difference in the treatment by the Russian Federation and Western countries of the conceptual designation of security problems implied by the development of digital

technologies. The Russians are interested in protecting and managing the content of digital technological instruments (information), the West is interested in protecting the tools themselves (software and devices), regardless of their content. Hence, different terms are born: information security (Russia) and cybersecurity (West) (Limonier, Gerard 2017) and different: holistic (Russia) or specialized (West) approach to the use of ICT in the defense sphere.

In addition to the practice of combining the technical dimension of cyberspace with the information dimension, the specifics of the Russian approach to digital sovereignty were also influenced by the WikiLeaks and Snowden scandals. It is pointed out that the turning point for the Russian government's abandonment of free-market ICT development was Snowden's testimony about the NSA's direct access to the data from Apple, Facebook, Google, Microsoft, Skype, AOL, YouTube and PalTalk via the PRISM spying program (Bertran 2020). Data deposited by entities from various countries in top-trust technology corporations has become a subject of geostrategic importance. The Snowden affair made it easier for the security services of the Russian Federation to control the digital assets of Russian companies and citizens. The latter returned to an attitude of peculiar passive helplessness in the face of surveillance practices, considering them a continuation of Soviet-era anti-citizen actions (Ermoshina & Musiani, 2017). According to Bertran, the authorities treated foreign digital software as tools to facilitate access to digital resources within the Federation by states hostile to Moscow, both in terms of cyberattacks and digital espionage. Since Medvedev's presidency, protectionism for the country's IT industry and digital services has deepened, and the propaganda term 'indigenous technologies' (native/domestic) has begun to appear in political discourse. Government campaigns have also been developed, with stakeholders ranging from the general public to the IT sector, including private companies.

The need for technological emancipation of the Russians from the influence of American companies (especially Microsoft) was publicized, and the benefits of the development of Cyrillic "open sources" for the competitiveness of the Russian economy were promoted, especially in the Russian-speaking space of the former Soviet republics.

Most attention, however, was paid to the relationship between "indigenous technologies" and state information security. This was another step toward the implementation of the Russian Federation's

digital sovereignty program, set in the context of the revision of the political balance of power in the world.

State cyberaggression as an emanation of digital sovereignty

If we take as a starting point that Russia's broad perception of information security is integrally linked to its vision of a global order in which the Russian Federation is rebuilding its position as a de facto world power, it will be easier to understand the reasons why cyberspace has been talked about and thought about in Russia since the early 2000s. It is also worth remembering that the 1990s, a period of political instability in the Russian Federation, fostered cyberterrorist practices by actors supporting the Federation's centrifugal tendencies. The experience of the Second Chechen War brought the first material and image losses to the Russian financial sector, revealing the effectiveness of cyber-terrorist operations claimed by hacktivists associated with kavkaz.org (Bógdał-Brzezińska, Gawrycki 2003).

In this context, the cyberattacks on critical infrastructure in Estonia and Georgia (2007/2008) attributed to the Russian side are the first manifestations of the implementation of the announcement of treating cyberspace as a domain of struggle (Gardocki, Worona 2020). It seems important that in the case of Georgia a pattern of action emerges that constitutes a matrix of preparations for the invasion of Ukraine both in 2014 and in 2022. At the conceptual and operational level, cyber attacks have been sought to be fully integrated into both strategic information campaigns and the full spectrum of military operations (McDermott 2022). Such cyber operations are therefore as much an arm of the Russian propaganda machine and a means of creating and delivering disinformation as a tool to disrupt critical infrastructure or military capabilities of the adversary in terms of communication and connectivity between operational units.

In 2013, the chief of the Russian General Staff, Valery Gerasimov, presented an interpretation of the so-called wars of a new type, emphasizing the blurring of boundaries between war and peace (cf. Schroedinger's cat metaphor: Bógdał-Brzezińska, 2017). Military specialists treat the so-called Gerasimov's doctrine as an announcement of Russia's attack on Ukraine in 2014 and fighting in cyberspace after the end of operations in the land domain (White, 2018; Zalewski, Dzierżyński 2019.) Bearing in mind that a new type of war occurs in the literature in connection with the concept of hybrid war, let us note its attribution by formulating: actions below the threshold of war or overt

direct violence. In the light of Gerasimov's conception, the war is permanent, and the choice of tools to fight the enemy is only a matter of circumstances. So-called non-military measures are to contribute to the disintegration of enemy state institutions through political, economic, information and humanitarian activities, which are carried out together with the use of the "protest potential" among the societies of the countries that are the target of aggression (Wojnowski 2015, p. 15; Mickiewicz 2023). If we were to assess the phase nature of the actions, we should distinguish the stage of non-military preparations within the area of psychological impacts, including disinformation, in order to manage social moods; in the second phase, the aim is to attack critical infrastructure (especially energy, financial and communication), with elements of indirect actions. In this approach, traditionally understood kinetic actions constitute the final phase of the fight, supplemented at the same time with means from the first and second phases. "Gerasimov also believes that the differences between the strategic, operational and tactical levels of operation, as well as between offensive and defensive operations are now blurring" (Skoneczny 2015, p. 44). From the perspective of a new type of war, cyberspace actions preceding and parallel to conventional actions become elements of "cognitive" warfare, where the elements of controlling the perception of public opinion and the introduction of information chaos deepen social anxiety and weaken trust in state institutions.

Analysts point out that during Putin's presidency, political and military actions, in line with the idea of a new type of war, have been combined with an increase in revisionist tendencies toward the West and a deepening of rhetoric that questions the indisputability of the borders of the former Soviet republics (Kaczmarski 2009), and the stability of their state systems. With this motivation, cyber-attacks became tools used to destabilize state institutions hostile to the Russian authorities in the republics of Estonia (2007) and Georgia (2008). They were a kind of experiment: they diagnosed the West's response to non-conventional attacks and tested the cyber defense capabilities of Russia's "near abroad" states. In the first case, they replaced military operations, in the second they complemented them. In both cases, these activities fulfilled Russia's concept of information security as embodied in strategic documents of a doctrinaire nature. One of the important contexts in shaping the content of both the first (2000) and second (2016) information security doctrines of the Russian Federation is the belief in the threat of Western political indoctrination with elements of

democracy promotion and liberalism as a negation of Russian state and political tradition. They convey the message of a growing threat to Russia's national identity and perception of its political history, and Western democracies themselves are portrayed as interested in a destructive influence on the Russian mentality. However, it should be remembered that cyberattacks are now considered to imply the right to self-defense in the spirit of Article 51 of the UN Charter if they result in the destruction of the attacked state's critical infrastructure as in the case of an attack using traditional means of warfare (Kulesza, Kulesza 2011). Thus, Russian information security doctrines fall within the spectrum of legal interpretations of defensive actions.

Democratic states and Western ICT companies as parties supporting Ukraine in cyber defense activities

Due to the treatment of cyberspace by both Russia and democratic states as a domain of struggle and taking into account the risk of kinetic confrontation resulting from the extension of Art. 51 of the KNZ, since 2014 the West has only used support for Ukrainian cyber defense, which is accompanied by great caution in terms of tools for offensive activities. Ukraine's cyber security has been strengthened by the Anglo-Saxon powers since the annexation of Crimea. The U.S. Department of Energy conducted advisory activities to prevent further Russian attacks on Ukrainian energy infrastructure, and the Treasury Department undertook similar activities to secure the Ukrainian financial system (Willett, 2022). Ukraine was a beneficiary of the NATO Cyber Defense Trust Fund as well as the Science for Peace and Security (SPS) Cooperative Program (Spînu, 2020). These funds were used to train national institutions in responding to cyberattacks against critical infrastructure, inspiring Kyiv's initiatives within regional international institutions, e.g. a working group for cybersecurity was established within the GUAM structures.

We can talk about an ad hoc cyber coalition of Ukraine with Western countries, and the support provided by international institutions: the EU and NATO was an extension of similar cyber-resistance activities from previous years and prepared Ukraine for another invasion. The UK was, next to the US, the most involved in financing Ukrainian cyber defence, and in November 2022 it was revealed that the amount of this aid oscillated around £6 million. At the end of 2021, the US Cyber Command delegated technical experts to Ukraine to strengthen and modernize the defense tools and practices of

the local cyber defense units. Training was also conducted by the US Cybersecurity and Infrastructure Security Agency, and Ukraine's admission to the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) in March, a month after the beginning of the Russian aggression, was considered a special gesture of support. According to experts, technical, training and political support were crucial to limiting, slowing down and changing the techniques of Russian cyberattacks in the first phase of the war (Beecroft, 2022).

A special group of non-state actors providing assistance to the Ukrainian side are Western companies from the ICT sector with the status of transnational corporations, referred to by the acronym GAFAM. It consists of digital giants monopolizing the social media sector (Facebook), e-commerce (Amazon), the most common digital communication products - hardware and software (Microsoft and Apple) and data selection and sequencing (Google). Although in recent years there have been signs of competition between GAFAM and the governments of European countries and pressure exerted on the American government, which represents the country of headquarters of these companies in matters of tax or user data management, the Russian-Ukrainian war made them allies of the political West, especially since Microsoft and In recent years, Apple and Google have had political disputes with Russia over the enforcement of Russia's digital sovereignty.

Western technology companies provided technical and informational assistance to the Ukrainian side, including ad hoc analysis of Russian cyber attacks and forecasting their further directions. Against this backdrop, it is worth mentioning the role of Microsoft, which reported in late 2021 on the growing number of cyberattacks identified as of Russian origin on Ukraine's government domains and strategic infrastructure. In an April 2022 report, Microsoft experts indicated that the regrouping of Russian troops in the spring of 2021 was accompanied by cyberattacks on Ukrainian targets (*Microsoft's Digital Security Unit*, 2022). The actions of Microsoft, Google and Cisco were also expressed in technical and informational assistance, providing current data on detected Russian cyber attacks and providing similar data to NATO. Spectacular were Elon Musk's decisions to provide the Ukrainian side with Starlink mobile terminals to connect to the Internet via satellite. Coordinating drone attacks, helping besieged Ukrainian troops in Mariupol maintain contact with their commanders, and facilitating

communication between the Ukrainian president and Western leaders are cited as the main areas of successful use of Starlink.

Lessons learned from the range of assistance provided by states and non-state actors affiliated with various cyber security initiatives indicate that the expectations of Ukraine's political and military leadership have been met with a lack of Western willingness to expand defense measures to include cyber tools. A February 2023 Aspen Institute report shows that Western private companies affiliated with the Cyber Defense Assistance Collaborative (CDAC) continue to refuse to provide cyber instruments to the Ukrainian side (Rattray, Brown, Moore, 2023). It should be assumed that the private cyber security sector views the state's offensive actions in cyberspace as synonymous with hacking and cybercriminal practices. This also means that the sector has no formal support for the activities of activists from the IT Army of Ukraine.

Risk of uncontrolled spread of cyber warfare due to participation of non-state actors

Non-state actors have been portrayed as participants in international relations as independent as states since the 1970s, when attempts to include them first appeared (Potulski, Bógdał-Brzezińska, Wendt 2022). Since the early 1990s, we have seen an increase in their activity in cyberspace, revealing the enormous opportunities it generates for these entities. This is due to their characteristics such as their cross-border nature, varying levels of institutionalization and formalization, and distance from activities defined in terms of interests or strategic goals. Non-state actors in cyberspace cannot be treated as a homogeneous group, and in order to distinguish them more clearly from states it seems more appropriate to use the term "cyber-active participant", which includes, in addition to those who carry out deliberate and long-term activities in cyberspace (cf.: GAFAM), also those whose activity is ad hoc, temporary or incidental (Bógdał-Brzezinska 2022). Universal tools for measuring the power of influence in cyberspace have not yet been developed, and the reason for this is largely attributed to the diversity of "cyber participants," especially among non-state actors. Hence, the alternate terms "digital power" and "cyberpower" remain labels for the effects of cyber behavior, rather than categories related to military or economic power. In order to assess their impact on the course of Russian cyber-aggression against Ukraine in 2022/2023, it is worth looking at the participation of non-state actors in

initiating and controlling the components of information warfare: i.e., netwar and cyberwar.

Cyber-terrorist mercenaries from Russian hacking groups: "Turla" operating against the Armenian government, or "Shaltai Boltai" involved in factional fights in the Kremlin and attacks on US administration servers have been written about for a long time. However, it was only the Russian-Ukrainian war that revealed the scale and scope of the capabilities of non-state cyber actors. Damjan Štrucl (Štrucl, 2022) diagnoses that the Russian Federation's past successes in hybrid warfare were undermined in the first months of the 2022 war, due to the fact that various hacking and hacktivist groups joined the fight as parties to the conflict. In the case of Ukraine, we can speak of an implicit agreement by state institutions to selectively perform cyber defense functions by non-state cyber actors. In February 2022, Ukrainian Deputy Prime Minister M. Fedotov called for the creation of the Information Technology Army of Ukraine. Anti-Russian and anti-Belarusian activities have involved hacktivist groups such as Network Battalion 65, Elves, Cyber Guerrillas, Cloud Atlas, and the most media-savvy cyber participant in the conflict has become the group Anonymous (Svyrydenko, Możgin 2022).

Hacker groups also cooperate with the Russian authorities. In the realities of the decision-making mechanisms of a democratic state, one could talk about a private-public partnership, but in the case of autocracy, it is worth recalling the historical concept of condottiere services. While we think of the Wagner group in terms of traditionally understood military mercenaries, we will not find studies that focus on cyberactivists and hackers, treating them in this context. Meanwhile, in the analyzes of cybercondominium practices carried out on behalf of the Russian authorities, a list of groups as long as pro-Ukrainian ones is mentioned, including: ARMAGEDDON/GAMAREDON/PRIMITIVE BEAR (associated with the FSB), SANDWORM (associated with the GRU), APT28/FANCY BEAR (associated with GRU), APT 29/COZY BEAR (associated with SVR), UNC1151/GHOSTWRITER (associated with Belarusian and Russian secret services), also: XAKNET, KILLNET, Z-TEAM, CYBERARMYOFRUSSIA_REBORN (pro-Russian groups - called "cyberterrorists" by SSSCIP ") (Štrucl, 2022).

The change in the attitude of the Russian authorities to domestic cybercrime after February 2022 is interesting. An example is the activity of the Russian Conti group, which (similarly to cybercrime groups associated with the North Korean government) has been focusing on

ransomware attacks against several hundred companies from different regions of the world since at least 2017 (*Check Point Research*, 2022). At the beginning of the war, the group announced its support for the authorities by launching attacks against Ukrainian institutions using the aforementioned method of blocking data and digital infrastructure.

After several initial weeks of massive actions by cyberactivists supporting the warring parties, these spectacular actions began to wane. The participation of non-state actors in interstate wars proved episodic, and more importantly, non-state cyberactivists are largely uninterested in pursuing strategic goals in the sense inherent in state strategies (Bógdał-Brzezinska 2022).As entities providing condottiere services, they must demonstrate at least a basic level of institutionalization (cf. Conti Group), and in the absence of a formal organizational structure, the willingness to act long-term to support the state in the cyberspace fight weakens. This is due to the relatively short period of interest in the development potential of IT skills of individuals acting cyberactively, correlated with the low level of influence of ethics (conviction about the justice of war) or ideology (support for liberalism or democratization) on the behavior of cyberactivists.

Reasons for the ineffectiveness of Russian cyberspace operations

Forecasts on the use of fighting tools in cyberspace by the Russian Federation during the war with Ukraine turned out to be wrong (Nehrey, Kostenko, Kravchenko 2023). They were expected to be long-term, highly effective and closely synchronized with kinetic actions (Alperovitch, 2022). According to representatives of the State Service for Special Communications and Information Protection of Ukraine (SSSCIP), over 1,500 cyberattacks on Ukraine were carried out by the end of summer 2022 (Beecroft, 2022). Analyzes of cyberspace operations accompanying the military activities of both sides after the Russian aggression against Ukraine in February 2022 focus on the lack of clear successes of the Russian side. There are different diagnoses. Already in March 2022, the "Washington Post" presented 11 justifications that appear in the debate on the lack of success of the Russian cyberwar. Among them, the key was the belief that the Russian side had not prepared synchronous kinetic actions and cyberattacks as an important tool of combat, that there were serious fears of the Kremlin about the escalation of the conflict with the West, and that from the perspective of Russian interests it was important to maintain Ukraine's critical infrastructure for a time after victory. These arguments were developed

in various order of importance in later studies and analyses. As a frequently repeated and important determinant, the approach to cyberspace and digital resources, which is different from the Western one, was indicated, which has already been presented above in this article. The tradition of the Russian security services has influenced the tendency to strengthen the propaganda and disinformation dimension of the fight against the enemy and to formulate content that affects the enemy's society. However, the financing and modernization of structures, tools and personnel responsible for the technical and IT dimension of combat in cyberspace have been neglected. As mentioned above, some of the activities in this area were carried out with the participation of non-state actors, cybercriminal groups or hacker groups with a nationalist ideological profile. "Russian cyber doctrine emphasized intelligence, subversion and psychological warfare rather than combat integration" (Wilde 2022). It was also emphasized that the Russians did not use the early phase of the war for effective information warfare, which the command theorists regarded as crucial. It is equally about the accurate identification of targets, as well as a reliable assessment of the enemy's preparation. Another reason for the lack of success of the Russian side was the long-term rivalry between the various types of special services: FSB, GRU, SVR, which prevented the effective implementation of the intended information operations and cyberattacks in the initial phase of the war. Experts also emphasize that the cyber units of the Russian Federation are too few to significantly contribute to a full-scale war, and they turned out to be too weakly connected with kinetic operations, especially in the later months of the war. There are also opinions that the Russian army is too slow to regenerate cybernetic capabilities once used. In the second half of the year, the same variants of cyberattack tools were used as before, combined with a decrease in the number of subsequent operations (Bateman 2022). It is also indicated that only a part of Russia's potential in the field of cyber operations has been directed to Ukraine, as Moscow is seriously considering the possibility of cyber counterattacks from the West, especially when Ukraine has become a participant in NATO's cyber defense system. The lack of success of Russian cyber operations was also influenced by the fact that the Ukrainian side learned how to use cyber technology to defend against an attack and use foreign assistance, both state and commercial entities. The Ukrainian National Cybersecurity Coordination Center, established in 2016, was responsible for coordinating foreign cooperation in the field of cyber resilience.

Can we talk about the first global war in cyberspace?

In the face of the Russian-Ukrainian war, it is worth addressing the question that has been resonating since the beginning of 2022: are we dealing with the first world digital war? And in the context of the assumptions of the theory of hegemonic wars - does it meet the conditions for another conflict of this kind? Theories of hegemonic wars are based on the assumption of cyclical rivalry between world powers with the highest potential, culminating in a global armed conflict. It occurs approximately every hundred years (usually in the second decade of the new century), and its total character is expressed by the involvement in the conflict of all areas of state activity (in addition to the military, also the economy, technology, the rules of society). Hegemonic conflicts promote the formation of coalitions around the current leading power and around its rival. Each alliance group consists of states defining their strategic interests in maintaining the existing global status quo or in challenging it.

In the course of the initial phase of the Ukrainian-Russian war, mechanisms were created to construct a coalition of states supporting Ukraine in cyberspace activities, concentrated in international institutions in the form of the European Union and NATO. These institutions have cyber defense instruments and mechanisms that have been developed for over a decade. In 2008, the NATO Cyber Defense Policy was adopted in Bucharest and the NATO Cooperative Cyber Defense Center of Excellence – NATO CCD COE was established. Since 2016, the North Atlantic Treaty Organization as a whole and its key members have treated cyberspace as the domain of military operations. This means that the Russian cyberattacks are treated as a prerequisite for the possible activation of the provisions of Art. 51 of the Collective Defense Pact, the only question that remains open is whether the retaliatory operation should be and will be limited to cyberspace. In this matter, cybersecurity practitioners and researchers take divergent positions. Against the backdrop of this debate, it is worth mentioning the postulations of renowned cyber security expert Marcin Libicki (2014). He spoke of a kinetic attack in response to a cyberattack as the greatest threat to peace, pointing to the extraordinary potential ease of exploiting the unclear attribution of cyber perpetrators and gaps in international law in identifying them. The exposure of civilian victims to the effects of cyber attacks should also be considered. In this context, R. Neilsen's (2023) concept of "cyber-humanitarian intervention" deserves attention,

arguing the need to link the problem of cyber warfare to the protection of civilians affected not only by the loss of data (including virtual financial resources), but also by attacks on critical infrastructure.

An oft-cited aspect of the Russian-Ukrainian war in cyberspace is the fundamental change it could cause in the global international order. This change is expected to result from the multi-level nature of the theaters of warfare, accompanied by the formation of coalitions of states with non-state actors. The latter participate in cyberdefensive (technology corporations, NGOs) or offensive (formalized cyber groups, spontaneously activated collectives of hackers and hacktivists). The fact that such configurations are created by sovereign and non-sovereign actors, differing in goals and time of existence, can increase the unpredictability and chaotic nature of the international order. The new international order may therefore be destructive and herald the short-lived and relative nature of such phenomena as power, subjectivity and legitimacy.

References

Alperowicz, D., 2022. *How Russia Has turned Ukraine Into a Cyber - Battlefield. The Kremlin's Hackers Are Already Targeting Kyiv*. Foreign Affairs, 28.01.2022.

Bateman, J., 2022. *Russian Cyber Operations During the War in Ukraine: Military Effects, Influences, and Implications*, Carnegie Endowment for International Peace, Washington.

Beecroft, N., 2022. *Evaluating the International Support to Ukrainian Cyber Defense*, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (dostęp: 31.01.2023)

Bertran, M.-G., 2020. *La place des logiciels libres et open source dans les nouvelles politiques du numérique en Russie*, Hérodote, 2-3 (177-178), s. 235-252.

Bógdał-Brzezińska, A., 2004. *Rosja, Ukraina i Białoruś: koncepcje społeczeństwa informacyjnego i gospodarki opartej na wiedzy*, Stosunki Międzynarodowe, 30, s. 169-189.

Bógdał-Brzezińska, A., 2017. *Państwo a wojna. Rozważania z pogranicza teorii i historii stosunków międzynarodowych*, Stosunki Międzynarodowe - International Relations, 53, s. 191-204.

Bógdał-Brzezińska, A., 2022. *Aktorzy niepaństwowi w cyberprzestrzeni i przestrzeni kosmicznej* in: R. Bania, Z. Bednarek (eds.), Aktorzy niepaństwowi: między stabilizacją a destabilizacją relacji międzynarodowych, s.11-32.

Bógdał-Brzezińska, A., Gawrycki, M.F., 2003. *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, ASPRA-JR, Warszawa.

Bógdał-Brzezińska, A., Wendt, J., 2020. *Geopolityczny kontekst suwerenności informacyjnej Rosji w cyberprzestrzeni i jej wpływ na bezpieczeństwo międzynarodowe,* De Securitate et Defensione, 2, s. 97-113.

Check Point Research, 2022. *Leaks of Conti Ransomware Group*, https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/, (dostęp: 31.01.2023)

Cybulski, M.A., Maciorowska, M., 2021. *Wykorzystanie cybertechnologii w walce informacyjnej przez Rosję*, Przegląd Geopolityczny, 38, s. 116-131.

Ermoshina, K., Musiani, F., 2017. *Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era*, Media and Communication, 5(1), s. 42–53.

Gardocki, S., Worona, J., 2020. *Wykorzystanie przez Rosję cyberprzestrzeni w konfliktach hybrydowych a rosyjska polityka cyberbezpieczeństwa*, Colloquium, 2(38), s.33-46.

Goodman, S.E., 1987. *The Information Technologies and Soviet Society: Problems and Prospects*, Idee Transactions on Systems, Man, and Cybernetics, 17 (4).

Kaczmarski, M., 2009. *Rosyjski rewizjonizm wobec Zachodu.* Prace Ośrodka Studiów Wschodnich, 33.

Kassel, S., 1971. *Soviet Cybernetics Research: A Preliminary Study of Organizations and Personalities*, RAND Co, Santa Monica.

Kulesza, J., Kulesza, J., 2011. *Odpowiedzialność państw za podejmowane w cyberprzestrzeni działania zagrażające międzynarodowemu pokojowi i bezpieczeństwu*, Studia Prawno-Ekonomiczne, LXXXIII, s. 149–167.

Libicki, M., 2014. *De Tallinn à Las Vegas. Une cyberattaque d'importance justifiet-elle une réponse cinétique ?,* Hérodote, 1-2 (n° 152-153), s. 221-239.

Limonier, K., Gerard, C., 2017. *Guerre hybride russe dans le cyberespace*, Hérodote, 3-4 (166-167), s. 145 -163.

McDermott, R., 2021. *Electronic Warfare in Contemporary Russian Military Thought*, https://jamestown.org/program/electronic-warfare-in-contemporary-russian-military-thought/ (dostęp:02.02.2023).

Mickiewicz, P., 2023. *Russian special operations and the so-called Gerasimov doctrine*, Przegląd Geopolityczny, 43, s, 12-28.

Microsoft's Digital Security Unit, 2022. *An overview of Russia's cyberattackactivity in Ukraine*, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Napolitano, M., 2021. *Ukraine: home of cybernetics made in the USSR*, https://www.balcanicaucaso.org/eng/Areas/Ukraine/Ukraine-home-of-cybernetics-made-in-the-USSR-208234

Nehrey, M., Kostenko, I., Kravchenko, Y., 2023. *Digital Transformation in Ukraine During Wartime: Challenges and Prospects*. In: Z. Hu, Y. Wang, M. He (eds.) *Advances in Intelligent Systems, Computer Science and Digital Economics IV*. CSDEIS 2022. Lecture Notes on Data Engineering and Communications Technologies, vol. 158. Springer, Cham.

Neilsen, R., 2023. *Coding protection: 'cyber humanitarian interventions' for preventing mass atrocities*. International Affairs, 99 (1), s. 299–319.

Peters, B., 2012. *Normalizing Soviet Cybernetics*. Information & Culture, 47 (2), s. 145–175.

Potulski, J., Bógdał-Brzezińska, A., Wendt, J., 2022. *Aktorzy–Relacje–Przestrzenie. Wyzwania dla geografii politycznej, stosunków międzynarodowych i geopolityki*, Wydawnictwo PTG. Kraków.

Protasowicki, I., 2018. *Rola szkodliwego oprogramowania w geopolityce*, Przegląd Geopolityczny, 26, s. 85-94.

Radu, C.-C., 2022. *Russia's Approach to Cyberspace*, International Scientific Conference "Strategies", 18 (1), s. 533-544.

Rattray, G., Brown, G., Moore, R.T., 2023. *The Cyber Defense Assistance Imperative Lessons from Ukraine*, Aspen Institute.

Skoneczny, Ł., 2015. *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, Przegląd Bezpieczeństwa Wewnętrznego, 4.

Spînu, N., 2020. *Ukraine Cybersecurity Governance Assessment*. Geneva Centre for Security Sector Governance/nov. 2020.

Štrucl, D., 2022. *Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare*, Contemporary Military Challenges, 24(2), s.103-123.

Svyrydenko, D., Możgin, W., 2022. *Hacktivism of the Anonymous Group as a Fighting Tool in the Context of Russia's War against Ukraine*, Future Human Image, 17, s. 39-46.

White, W.P., 2018. *The Cyber Crucible: Eastern Europe, Russia, and the Development of Modern Warfare*, ch. 9, s. 151-162, in: Historical Case Studies of Information Operations in Large-Scale Combat Operations, eds. Mark D. Vertuli & Bradley S. Loudon, Army University Press Fort Leavenworth, Kansas.

Wilczyński, P. L., 2017. *Problematyka bezpieczeństwa we współczesnym dyskursie eksperckim w Polsce*, Przegląd Geopolityczny, 21, s. 48-66.

Wilde, G., 2022. *Cyber Operations in Ukraine: Russia's Unmet Expectations*, https://carnegieendowment.org/files/202212-Wilde_RussiaHypotheses-v2.pdf (dostęp: 3.03.2023).

Willett, M., 2022. *The Cyber Dimension of the Russia–Ukraine War*, Survival, 64(5), s. 7-26.

Wojnowski, M., 2015. *Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, Przegląd Bezpieczeństwa Wewnętrznego, 7 (13), s. 13-39.

Zalewski, J., Dzierżyński, D.G., 2019. *Wojna informacyjna w odbudowie rosyjskiej mocarstwowości*, Wojskowa Akademia Techniczna, Warszawa.

Streszczenie:

Celem niniejszego artykułu jest zbadanie uwarunkowań i ocena skuteczności oddziaływania środków cybernetycznych zastosowanych podczas wojny rosyjsko-ukraińskiej. Analiza dotyczy przede wszystkim wymiaru podmiotowego, aby pokazać, że w cyberprzestrzennym wymiarze tej wojny uczestniczą nie tylko strony konfliktu kinetycznego, tj. Rosja i Ukraina. Dlatego też ocenie poddane zostaną zarówno podmioty niepaństwowe i instytucje międzynarodowe, jak i podmioty państwowe wspierające Ukrainę. Wnioski wskazują, że jako konflikt w cyberprzestrzeni wojna ta nie jest konfliktem dwustronnym, lecz wielostronnym o zmiennej dynamice, w którym zmienia się także liczba i rodzaj walczących.

Słowa kluczowe: bezpieczeństwo cybernetyczne, Rosja, Ukraina, wojna cybernetyczna.