A. Rogozińska, *The security of Ukraine in the context of information warfare in cyberspace carried out by the Russian Federation*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 20(2022), z. 2, s. 107-122, DOI: https://doi.org/10.36874/RIESW.2022.2.6.

Agnieszka Rogozińska*

The security of Ukraine in the context of information warfare in cyberspace carried out by the Russian Federation

Bezpieczeństwo Ukrainy w kontekście wojny informacyjnej w cyberprzestrzeni kreowanej przez Federację Rosyjską

Summary: In the public discourse on issues of international security in the context of threats created by the Russian Federation, such threats are determined primarily by actions below the threshold of "war" (of a hybrid nature) and are made using non-military means, e.g. in relation to cyberspace. Actions of this nature are carried out by the aggressor's special services or groups of hackers and activists associated with them whose aim is to paralyse the functioning of the attacked state (its administration, critical infrastructure). Such activities are multilateral; activity is undertaken in many fields (social media, provocative events, establishing pro-Russian organizations, creating information portals) and is still escalating.

The purpose of the research, the results of which are presented in this article, is to identify the activities and assess the impact of Russian information warfare conducted by the Russian Federation in cyberspace in 2014 and 2022 on the security of Ukraine. The research used general-methodological research methods – primarily, analysis and critique of literature. The case study method was used to identify specific examples of information warfare used by the Russian Federation against selected countries in Central and Eastern Europe.

Keywords: security, information warfare, cyberspace, Ukraine, Russian Federation

Streszczenie: W dyskursie publicznym zagadnienia bezpieczeństwa międzynarodowego w kontekście zagrożeń kreowanych przez Federację Rosyjską determinowane są przede wszystkim przez akcje z użyciem działań poniżej progu wojny (o charakterze hybrydowym) za pomocą środków niemilitarnych, m.in. w odniesieniu do cyberprzestrzeni.

Działania o takim charakterze prowadzone są przez służby specjalne agresora lub powiązane z nimi grupy hakerów oraz aktywistów, których celem jest paraliżowanie funkcjonowania państwa atakowanego (jego administracji, infrastruktury krytycznej).

* Agnieszka Rogozińska – PhD, Jan Kochanowski University in Kielce, Poland, ORCID: https://orcid.org/0000-0002-3462-7851, e-mail: arogozinska@ujk.edu.pl.

Działania takie mają charakter wielostronny, aktywność podejmowana jest na wielu polach (social media, prowokowanie wydarzeń, zakładanie prorosyjskich organizacji, tworzenie portali informacyjnych) i wciąż eskaluje.
Celem badań, których wyniki przedstawiono w niniejszym artykule, jest identyfikacja działań i ocena wpływu rosyjskiej wojny informacyjnej prowadzonej przez Federację Rosyjską w cyberprzestrzeni w latach 2014 i 2022 na bezpieczeństwo Ukrainy. W przeprowadzonych badaniach wykorzystano ogólnometodologiczne metody badawcze, przede wszystkim analizę i krytykę literatury. Metoda studium przypadku została wykorzystana do zidentyfikowania konkretnych przykładów wojny informacyjnej stosowanej przez Federację Rosyjską przeciwko wybranym krajom Europy Środkowo-Wschodniej.
Słowa kluczowe: bezpieczeństwo, wojna informacyjna, cyberprzestrzeń, Ukraina, Federacja Rosyjska

Introduction

Hybrid actions in cyberspace are planned and coordinated operations that combine various means of pressure and are conducted with the use of one's own forces and resources or with the use of external actors, i.e. hacktivists acting from political motives (cyber warriors), the use of national, ethnic and religious minorities. Hybrid cyber activism involves simultaneous disinformation campaigns and out-of-the-box attacks in cyberspace. Moreover, these activities may go beyond standard website defacement. Typically, cyber army activity manifests itself during armed conflicts and international crises.

A classic cyberattack may involve unauthorised interference with software or hardware. The authors of the document "Cybersecurity Strategy of the Republic of Poland" define a cyberattack as an intentional disruption of the proper functioning of cyberspace[1]. Contemporary information warfare is the exercise of influence on mass consciousness in networks and communication spaces using methods of information resource control. The state needs access to information to ensure it can make quick and reliable decisions on the battlefield.This requires unlimited access to information and maintaining advantage over the opponent by making it difficult or impossible to obtain reliable data. The complexity of such actions with clearly defined political goals creates a uniform form of information warfare by causing public dissatisfaction, dividing political elites, lowering the reputation of

1 *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej,* Ministerstwo Administracji i Cyfryzacji, Warszawa 2013.

the state in the international arena, which in turn leads to the political isolation of the enemy.

The issue of information warfare in the context of the actions carried out by the Russian Federation has been a particular focus of public attention since December 2013, i.e. since the events that took place in Kyiv's Maidan. The widespread adoption of such an approach has meant that the general public has often overlooked the fact that elements of this kind of action had been taken by Russia before, for example in Georgia in 2008, and were also present in Transnistria and the Baltic States. Nevertheless, it was the actions undertaken by the Russian Federation in Ukraine in 2014 and 2022 that will go down in history as conflicts that not only changed the security architecture of the modern world but were the first wars role. Further attacks undertaken both by Russian services and by intermediaries acting under orders from Moscow (proxies) are anticipated, the likelihood of their uncontrolled proliferation from Ukraine to other regions is growing, and in the short term they may contribute to increased destabilisation of the international situation.

This problematic situation has led to the formulation of the main research problem of the article, which is as follows: During the Russian information war conducted in cyberspace in 2014 and 2022 against Ukraine, how were the cyber warfare activities implemented? The main problem can be broken down into the following questions: 1) What is the essence of Russian information warfare conducted in cyberspace? 2) What actions attributed to information warfare were undertaken by the Russian Federation during the annexation of Crimea and operations in eastern Ukraine in 2014? 3) How was Russian activity in cyberspace expressed during hostilities in Ukraine in 2022?

The purpose of the research, the results of which are presented in this article, is to identify activities and assess the impact of Russian information warfare conducted in cyber space on the security of Ukraine in 2014 and 2022. The research used general-methodological research methods – primarily, analysis and critique of the literature. The case study method was used to identify specific examples of information warfare used by the Russian Federation against selected countries of Central and Eastern Europe.

1. The essence of information warfare in cyberspace

A precise definition of the term "information war" is difficult[2] to determine conclusively. The definitions available in the literature indicate that "it is an action taken to achieve information advantage... while protecting one's own information, processes based on information processing, information systems, and computer networks"[3]. Other definitions define information warfare as any attack against an information system, regardless of the methods and means used. The main feature of such a definition of information warfare is its multidimensionality. An analysis of the literature allows us to formulate a thesis according to which the main goal of attacking the enemy's information or information systems is to weaken its will to resist. Modern information warfare is *an attack on mass consciousness* "in the network and communication space using the methods of information resources control"[4].

Psychological warfare occupies a special place in the concept of rebel wars discussed by Yevgeny Messner. According to the author, new technologies make it possible to gather and process information quicker, which makes it possible to anticipate the actions of the enemy. The leading form of realisation of political goals becomes information warfare, understood as a massive impact on the sphere of consciousness of entire societies and aimed at changing their views in a particular area of life. The main factor affecting the course of such conflicts involves psychological and informational activities aimed at unifying their own people around a particular idea and winning over for it part of the nation of the enemy state, the "psychological processing" of all social strata, causing in the hostile society feelings of fear, up to the level of panic, undermining trust and respect for state authority and confidence in the strength of the country and the nation, including in its

2 According to the statement of M. Libicki: "Every form of competition for control or domination in the sphere of information is, in principle, considered to be one of its kind, and information warfare techniques are perceived as aspects of the same discipline. Those who master the techniques of information warfare will find themselves in a position of advantage over those who have not. [...] Information warfare will dominate the more traditional, conventional forms of war". See: M. Libicki, *What is Information Warfare?*, Washington D.C. 1995, p. 9.

3 K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warsaw 2008, pp. 15-16.

4 B.C. Lewis, *Information Warfare, Federation of American Scientists*, http://fas.org/irp/eprint/snyder/infowarfare.htm [22.02.2022].

ability to defend itself, and inspiring and financing the development of radical and extremist groups (including political and religious) in the country and the nation. Such activities include inspiring and financing the development of radical and extremist groups (e.g. political or religious) in hostile countries and developing them on the basis of a strategy of unguided resistance. Decisive here are long-term psychological and informational actions[5]. General Makhmut Gareev is the author of a thesis according to which a change in the nature of modern war will be a consequence of technological development[6]. According to Vladimir Slipchenko, information warfare, global networking and the use of the internet will play an important role in future conflicts[7]. Issues on the topic of information warfare were described by Valeriy Gerasimov[8]. According to the so-called Gerasimov doctrine, the key to the new generation of wars will be the use of information warfare measures. They will be based on non-contact disinformation, propaganda and cyber warfare, which will bring adequate results with the minimum use of military means. The concept of a new generation of war was presented by Sergei G. Chekinov and Sergei Bogdanov. The model proposed by them consists of eight consecutive phases. The first is asymmetric actions through psychological, diplomatic and informational means leading to the weakening of the opponent. The second phase consists of disorientation of the command and political leaders of the state by means of covert actions, media, non-governmental agencies, circulation of false information and provocation. The third phase involves all activities associated with intimidating, deceiving, and corrupting opposition figures from the state that is to be weakened. Such actions severely disintegrate the entire administration and gov-

5 Messner E.Ye., *Khochesh' mira, Pobedi bunt!* [Е.Э. Месснер, *Хочешь Мира, Победи Мятежевойну!*], Moscow 2005, p. 110, http://militera.lib.ru/science/0/pdf/messner_ea01.pdf [22.02.2022].

6 M. Gareev, *If War Comes Tomorrow? The Contours of Future Armed Conflict*, Abingdon 1998, p. 54.

7 P.A. Mattsson, N. Eklund, *Russian Operational Art. In The Fifth Period: Nordic And Arctic Applications,* vol. 1, 2013, no. 1, p. 37, https://www.stratcomcoe.org/peter-mattsson-niklas-eklund-russian-operational-art-fifth-period-nordic-and-arctic-applications [22.02.2022].

8 V. Gerasimov, *Tsennost' nauki v predvidenii* [В. Герасимов, *Ценность науки в предвидении*], "Военно-промышленный курьер" 2013, no. 8, pp. 2-3. Despite the fact that the term Gerasimov Doctrine is widely used, it seems reasonable to suppose that its author should be considered the previous Chief of Staff, Nikolai Makarov. See: M. Banasik, *Bezpieczeństwo w aspekcie zagrożeń hybrydowych*, "Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej" 2016, no. 3(19), p. 9.

ernment structures, often resulting in erroneous decisions by the political and military leadership. The next stage is aimed at the widespread use of propaganda measures, which increases uncertainty in society. The next two phases are to establish a blockade of communication routes, a no-fly zone, and to launch reconnaissance and intelligence operations in the controlled area. Within the framework of the theory of new-generation war, Russian experts and analysts have defined the term information-strike operation, the basic premise of which is to bring about the destruction of the enemy's information resources.

The authors of the concepts in question attached particular importance to the use of the "protest potential" in the enemy's country. Therefore it should come as no surprise that the use of local political parties and organizations inspired, financed and developed by the Kremlin was one of the basic elements of the Crimean operation. The main weapons used by the Russian side during the operation were actions bearing the hallmarks of ideological diversion and of so-called reflexive management[9] measures.

The typology of information warfare includes the following divisions: personal, corporate, global, civil and military. In the context of the topic under discussion, the last two dimensions are interesting. The military plane of information warfare involves carrying out attacks on the resources and infrastructure of the opponent, both in cyberspace and in terms of psychological impact. The civilian dimension concerns the social context and materialises in the sphere of business, finance, technology and science, among others[10].

9 The term "reflective management" should be understood as the entirety of manipulation and social control techniques consisting of energy methods (force, coercion, pressure, fear) and information and psychological methods (propaganda, disinformation), the preparation of which is based on the creation of a special model of an opponent imitating his behaviour. See: M. Wojnowski, *Zarządzanie refleksyjne jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, "Przegląd Bezpieczeństwa Wewnętrznego" 2015, no. 7, pp. 11-36.

10 Characteristically, Russian strategic documents use the term "information space" as a synonym for cultural heritage and its elements (language, culture, tradition, history). In a document published by the Ministry of Defence of the Russian Federation, the concept of the activities of the armed forces of the Russian Federation in the information space was defined as "the sphere of activities related to shaping, creating, transforming, transmitting, using and storing information, influencing individual and social awareness, and also information infrastructure and strictly – information". See: *Kontseptual'nyye vzglyady na deyatel'nost' Vooruzhennykh Sil Rossiyskoy Federatsii v informatsionnom prostranstve* [*Концептуальные взгляды на деятельность*

2. The annexation of Crimea and the war in eastern Ukraine 2014

The events unfolding in Kyiv from October 2013 to February 2014 were portrayed in the Russian media as an unlawful rebellion against legitimate authority, initiated by a "third force" from outside. From February to March 2014, a similar campaign aimed to portray the alleged demoralisation of the civilian and military authorities in Crimea and to convince world public opinion of the Russian narrative that it was both historically and legally justified to annex Crimea to Russia[11]. Disinformation was the primary tool of these actions, the participation of Russian soldiers in military operations in Ukraine was carried out under the guise of creating volunteer separatist forces, and the concentration of Russian troops transferred to Ukraine was called exercises in the super-regional regions. This tool can be counted among the permanent set of Russian measures, having been used successfully in the war with Georgia, but the cyber activity was a novelty in the actions in Ukraine[12]. Hundreds of websites and social networks, seemingly independent, objective and informative in nature, but in fact linked to each other and effectively carrying out disinformation activities, were published on the internet in connection with the launch of military operations[13].

Вооруженных Сил Российской Федерации в информационном пространстве], https://function.mil.ru/news_page/country/more.htm?id =10845074@cmsArticle [22.02.2022]

11 Soviet Union, Nikita Khrushchev, although this event was also attempted by Soviet propaganda to discredit: "The Russian authorities are fighting for 'historical justice' and, after taking over Crimea, they are preparing a bill on illegal handover of the half-island to Ukraine in 1954 by the then secretary of the Central Committee of the Communist Party of the Soviet Union, Nikita Khrushchev. The bill was discussed by Valentina Matvyenko, chairwoman of the Federation Council, the upper house of the Russian parliament. She expressed the hope that the rules would be adopted during the spring session of the parliament. She admitted that the act would have no legal consequences. – It will be a historical document for future generations, stating that the decision on the Crimea in 1954 was unfair – emphasized Matvyenko. – At that time, no one asked whether the inhabitants of Crimea and Sevastopol agreed with the decision, no one asked the regional authorities on this matter – added one of Vladimir Putin's closest collaborators". See: *W Moskwie szykują ustawę, która "naprawi błąd" Chruszczowa*, TVN24, http://www.tvn24.pl/wiadomosci-ze-swiata,2/nikita-chruszczow-przekazal-krym-ukrainie-nielegalnie,512415.html [22.02.2022].

12 J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, Warsaw 2014, p. 2; A.I. Kuk, *Kanwa wywiadu agenturalnego*, Warsaw 1994, p. 2; *Raport OSW. Zmiany w potencjale militarnym Federacji Rosyjskiej (po rosyjskiej operacji wojskowej w Gruzji)*, Warsaw 2009, p. 4.

13 J. Darczewska, op. cit., p. 28; R. Cheda, *Rosyjska wojna informacyjna – lekcja z Ukrainy*, Wiadomości WP, http://wiadomosci.wp.pl/kat,1356,title,Rosyjska-wojna-informacyjna-lekcja-

The information war against Ukraine is in fact not limited to the territories of the interested countries; the Russian Federation has also conducted an intensified information campaign aimed at highlighting the divisions within the European Union and NATO regarding the legitimacy of aid to Kyiv and the sanctions imposed on Moscow[14]. It used personal contacts with Western politicians, economic incentives and media influence to do so. The Russian narrative was presented in the information space, with the main goal being to divide public opinion. The basic assumption of such activity was to shape the image of Russia as a victim of the cynical game played by the Western establishment, which was accused of creating a false image of the Russian president and the causes and course of the Ukrainian conflict.

Despite the fact that the accumulated military potential guaranteed complete operational freedom, the Russian side used a whole set of camouflaged actions, such as the use of humanitarian convoys as one of the elements of rearming the separatist forces, which was confirmed by observing the coincidence of the presence of Russian humanitarian convoys and the intensity of military operations conducted by separatist units[15].

In particular, the way in which the Russians annexed the Crimean peninsula confirmed the powerful potential of the use of information. Operations to capture Crimea began on the night of 27-28 February 2014. A group of armed men invaded the facilities housing the local parliament and the government of the Autonomic Republic of Crimea in Simferopol and displayed Russian state flags. The incident took Ukrainian forces completely by surprise, and they failed to take any countermeasures. It cannot be ruled out that this first strike group claiming to be the Crimean Self-Defence Force was made up of sol-

z-Ukrainy,wid,17301467,wiadomosc.html?ticaid=118406 [22.02.2022]; *Sankcje i Rosja*, J. Ćwiek-Karpowicz, S. Secrieu (eds.), Warsaw 2015, p. 99.

14 Rada Europejska, Rada Unii Europejskiej, *Kalendarium – sankcje UE wobec Rosji w sprawie Ukrainy*, http://www.consilium.europa.eu/pl/policies/sanctions/ukraine-crisis/history-ukraine-crisis/; *Nowe sankcje USA wobec Rosji. Uderzają w największe przedsiębiorstwa*, Onet Wiadomości, http://wiadomosci.onet.pl/swiat/nowe-sankcje-usa-wobec-rosji-uderzaja-w-najwiek-sze-przedsiebiorstwa/w9lkp [22.02.2022].

15 H. Coynash, *Russia brings 'humanitarian' convoys to Ukraine by day, military trucks carrying death by night*, Kharkiv Human Rights Protection Group, http://khpg.org/en/1564595792 [22.02.2022].

diers and officers of the Russian special forces[16]. The consistent observance of radio silence made it impossible to locate the command centres and information nodes of the Russians. Number plates were removed from rebel vehicles moving around the peninsula, and all signs of national and organizational affiliation were removed from the uniforms of regular Russian troops. In addition, fighters deployed in irregular formations had different weapons and uniforms, which made it impossible to identify them. Preparation and disinformation security proved essential not only in the case of the Crimean operation, but also at further stages of Russian aggression on Ukrainian territory.

3. The War in Ukraine 2022

The ongoing Russian-Ukrainian war will go down in history as a conflict that changed the security architecture of the modern world. It will also be the first war with such a crucial digital dimension. The expansion of the theatre of war into the domain of cyberspace, the geopolitical significance of the digital technologies used in it, and the growing importance of technology companies are discernible in many of its aspects. The Russian military action, which began on 24 February, was preceded by limited-range cyberattacks against Ukraine, primarily targeting public administration websites (so-called distributed denial of service – DDoS – attacks) and the deployment of data-destroying malware (wiper)[17]. The first attack, which took place on 14 January, targeted the official services of the public administration, the portal of the Ministry of Education, the Ministry of Foreign Affairs, the Ministry of Energy, government websites, including

16 When the operation in Crimea began, the Ukrainian and Russian forces were more or less aligned (over 14,500 Ukrainian soldiers and sailors were pitted against 15,000 Russian soldiers). In the last days of February, the advantage of the Russian side began to increase rapidly. This was due to the creation of new branches of the so-called Self-defence of Crimea and the transfer of Russian military units from the territory of the Russian Federation, in which the Black Sea Fleet played a decisive role. In public statements, Vladimir Putin denied the participation of Russian soldiers in Ukrainian separatist units: "Look at the post-Soviet republics. You can go into any store and buy such uniforms. Were they Russian soldiers? No. These are well-trained self-defence units". See: M. Olchawa, *Misja Ukraina*, Warsaw 2016, pp. 173-174.

17 *Russia unleashed data-wiper malware on Ukraine, say cyber experts*, The Guardian, https://www.theguardian.com/world/2022/feb/24/russia-unleashed-data-wiper-virus-on-ukraine-say-cyber-experts [22.02.2022].

the application "Dija" and the State Emergency Service[18]. As a result of the attack, the value of the websites was not changed, no personal data was revealed, and the attack was based on provocative messages displayed on the main pages of the attacked sites.

In mid-February, there was another Russian attack on Ukrainian entities operating in key sectors, including energy, telecommunications and transport. The DDoS attacks were directed against the Ukrainian Ministry of Defence and state-owned banks; as a result, the websites of the Ministry of Defence and the Ukrainian Armed Forces were disrupted, and the mobile services of state-owned banks, PrivatBank, Oshchadbank and Sberbank, were blocked. Cash withdrawals from ATMs were also suspended[19].

The attack conducted on 15 February was described by the services of Ukraine as the largest in the history of the country[20]. Ukraine has identified the Russian Federation as the originators of both cyberattacks. These assumptions confirmed the findings of U.S. analysts who said that the main purpose of the cyberattacks was to destabilise Ukrainian society. At a White House press conference on 18 February, President Joe Biden's cyber-security adviser Anne Neuberger reported credible evidence that the Kremlin was responsible for the attacks targeting Ukraine's Ministry of Defence and state-owned banks[21]. On the basis of observations of the infrastructure of the Main Intelligence Directorate (GRU), which transmits considerable amounts of data to IP addresses located in Ukraine, this organization was identified as the author of both attacks. Neuberger assessed that the DDoS attack aimed at overloading and blocking online services of Ukrainian institutions did not cause the intended extensive damage, which

18 *Ukraine hit by 'massive' cyber-attack on government websites*, The Guardian, https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers [10.05.2022].

19 *Ukrainian Defense Ministry's Website Among Several Hit By Cyberattack*, https://www.rferl.org/a/ukraine-defense-ministry-cyberattack/31705206.html [22.02.2022].

20 V. Hopkins, *A hack of the Defence Ministry, army and state banks was the largest of its kind in Ukraine's history*, The New York Times, https://www.nytimes.com/2022/02/15/world/europe/ukraine-cyber-attack.html [22.02.2022].

21 *Press Briefing by Press Secretary Jen Psaki and Deputy NSA for Cyber and Emerging Technologies Anne Neuberger*, 21 March 2022, https://www.whitehouse.gov/briefing-room/press-briefings/2022/03/21/press-briefing-by-press-secretary-jen-psaki-and-deputy-nsa-for-cyber-and-emerging-technologies-anne-neuberger-march-21-2022/ [22.02.2022].

was a result of Ukraine's quick response and the support provided by the United States[22].

Since the beginning of hostilities in Ukraine, cyberspace has become an important domain of hostilities. According to information provided by the Israeli company Check Point, the number of cyberattacks targeting Ukrainian political and military institutions increased by 196 percent between 24-27 February 2022[23].

The areas most vulnerable to hacking attacks are the public sector, financial sector and critical infrastructure. The key objective of Russian offensive actions carried out in cyberspace is to paralyse the functioning of the attacked ICT infrastructure.

According to official data, Ukraine has been the target of around 2.8 thousand cyberattacks since 15 February. The Russians are using a wide range of methods to paralyse the functioning of key institutions for the functioning of the Ukrainian state, especially in the area of defence operations conducted by Ukraine. As an example, Russian services have attempted to compromise the applications used to control the Ukrainian artillery. Such an operation could also be used to obtain the geographical coordinates and locations of specific targets in order to bomb them.

The effects of the economic sanctions imposed on the Russian Federation may be relevant to the escalation of cyber operations. Hackers, especially those specialising in ransomware attacks, such as the Russian group #Conti, may seek financial retaliation against overseas entities. APT (Advanced Persistent Threats) attacks targeting critical infrastructure and industrial automation systems would be particularly worrying in this perspective[24]. The capabilities for advanced application attacks are certainly possessed by Russia and China, but also by Ukraine's allies, including especially the U.S., which was the first to use an advanced cyberweapon called Stuxnet against

22 *Attack on Ukrainian Government Websites Linked to GRU Hackers*, Bellingcat Investigation Team, https://www.bellingcat.com/news/2022/02/23/attack-on-ukrainian-government-websites-linked-to-russian-gru-hackers/ [22.02.2022].

23 *Fake News of Cyber Attacks Fast-Spreads, as Conflict between Russia and Ukraine Escalates*, https://blog.checkpoint.com/2022/03/03/hacktivism-in-the-russia-ukraine-war-questionable-claims-and-credits-war/ [22.02.2022].

24 D. Patterson, *The ransomware wars: Here's how much cash the top gangs reel in*, CBS News, https://www.cbsnews.com/news/ransomware-war-conti-revil-hellokitty/ [22.02.2022].

Iran in 2010, and later also the Russian disinformation agency Internet Research Agency[25].

The above indications suggest that cyberattacks used in the Russian-Ukrainian war may reach an unprecedented scale in history, supporting Russian military actions. Consequently, cyber warfare may contribute to tilting the balance of victory to one side of the conflict as digital attacks can have a very tangible impact on the course of a conflict.

Conclusions

Russian military theorists define information warfare as the advantage of having access to information that makes it possible for quick and reliable decisions to be made on the battlefield. It requires unlimited access to information and maintaining an advantage over the opponent by making it difficult or impossible for him to acquire information. Having an advantage in information warfare stimulates the development of modern technologies, command systems, intelligence and communications. Information warfare will be fought in the future on an increasingly larger, unprecedented scale. An assessment of the theory of information warfare allows us to conclude that information warfare involves multi-level efforts aimed at destabilising the functions of states and changing their internal order. The centre of interest of its activities is society.

The research conducted shows that information warfare is an important tool used by the Russian Federation. To achieve its strategic goals, the Russian Federation uses a combination of many instruments of influence, including disinformation, manipulation and propaganda. Their implementation reduces the opponent's will to fight and introduces chaos and the disintegration of its forces and means. Some of the main strategic goals that the Russian Federation sets for itself through the implementation of actions in information warfare are as follows: strengthening the international position of the Russian Federation, expanding its sphere of influence at the expense of the West,

25 W.J. Broad, J. Markoff, D.E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Dela*, Strategy International, https://strategyinternational.org/experts/mark-voyger/ [22.02.2022].

especially in relation to the area of post-Soviet states, protecting Russian economic interests, and discrediting the structures of democracy.

As far as information operations in cyberspace are concerned, the Russian Federation has an advantage over Ukraine. This advantage stems, for example, from the Kremlin's experience in operations in this area, and it also has the necessary infrastructure at its disposal. Moscow also has one of the most advanced cyber offensive capabilities in the world. The Russian Federation has already carried out actions of this type in the past, for example against Estonia in 2007, against Georgia in 2008, and against Ukraine in 2014.

Of particular importance here is the experience gained in the battles carried out over Crimea and Donbas. The Russian Federation conducted a kind of testing ground in Ukraine, where it tested the use of attacks on critical infrastructure objects. As a result, Ukraine experienced, among other things, an electricity blackout lasting several hours, and in 2017 it was the first victim of the NotPetya malware, by far the most destructive, widespread, and costly cyberattack in world history, affecting thousands of companies and institutions[26]. Ukraine is not defenceless. It has learned lessons from both the 2014 and subsequent 2015 and 2016 attacks on its energy infrastructure, but especially from the aforementioned 2017 NotPetya. Moreover, it is not alone in its actions. Hacktivists Anonymous as well as hacker groups GNG (Georgian Hackers Society) and NB65 (Network Battalion 65) have taken Ukraine's side in the conflict[27]. Hackers from the Anonymous group have attacked a number of Russian websites, including governmental websites, the Russia Today television channel and Gazprom. In addition, they obtained confidential data from the Ministry of Defence of the Russian Federation and the Belarusian company Tetraedr, an arms manufacturer supporting the Russian Federation.

26 *'NotPetya' malware attacks could warrant retaliation, says Nato affiliated-researcher*, The Guardian, https://www.theguardian.com/technology/2017/jul/03/notpetya-malware-attacks-ukraine-warrant-retaliation-nato-researcher-tomas-minarik [1.05.2022].

27 D. Todd, *NB65 Hackers Attacking Russian Orgs in Ukraine Retaliation*, SecureWorld.io, https://www.secureworld.io/industry-news/nb65-hackers-russia-ukraine [1.05.2022].

References

Attack on Ukrainian Government Websites Linked to GRU Hackers, Bellingcat Investigation Team, https://www.bellingcat.com/news/2022/02/23/attack-on-ukrainian-government-websites-linked-to-russian-gru-hackers/.

Banasik M., *Bezpieczeństwo w aspekcie zagrożeń hybrydowych*, "Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej" 2016, no. 3(19).

Broad W.J., Markoff J., Sanger D.E., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, Strategy International, https://strategyinternational.org/experts/mark-voyger/.

Cheda R., *Rosyjska wojna informacyjna – lekcja z Ukrainy*, Wiadomości WP, http://wiadomosci.wp.pl/kat,1356,title,Rosyjska-wojna-informacyjna-lekcja-z-Ukrainy,wid,17301467,wiadomosc.html?ticaid=118406.

Coynash H., *Russia brings 'humanitarian' convoys to Ukraine by day, military trucks carrying death by night*, Kharkiv Human Rights Protection Group, http://khpg.org/en/1564595792.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, Ośrodek Studiów Wschodnich, Warszawa 2014.

Fake News of Cyber Attacks Fast-Spreads, as Conflict between Russia and Ukraine Escalates, https://blog.checkpoint.com/2022/03/03/hacktivism-in-the-russia-ukraine-war-questionable-claims-and-credits-war/.

Fryc M., *Polska strategia obronności wobec zagrożenia militarnego z elementami „wojny hybrydowej"*, "Bezpieczeństwo Narodowe" 2015, no. 33.

Gareev M., *If War Comes Tomorrow? The Contours of Future Armed Conflict*, Routledge–Abingdon 1998.

Hopkins V., *A hack of the Defense Ministry, army and state banks was the largest of its kind in Ukraine's history*, The New York Times, https://www.nytimes.com/2022/02/15/world/europe/ukraine-cyberattack.html.

Jonsson O., Seely R., *Russian Full-Spectrum Conflict: An Appraisal After Ukraine*, "The Journal of Slavic Military Studies" 2015, no. 28.

Kontseptual'nyye vzglyady na deyatel'nost' Vooruzhennykh Sil Rossiyskoy Federatsii v informatsionnom prostranstve, https://function.mil.ru/news_page/country/ more.htm?id=10845074@cmsArticle].

Kuk A.I., *Kanwa wywiadu agenturalnego*, Warsaw 1994.

Lewis B.C., *Information Warfare*, Federation of American Scientists, http://fas. org/irp/eprint/snyder/infowarfare.htm.

Libicki M., *What is Information Warfare?*, Washington D.C. 1995.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008.

Mattsson P.A., Eklund N., *Russian Operational Art.*, "The Fifth Period: Nordic And Arctic Applications", vol. 1, 2013, no. 1, https://www.stratcomcoe.org/peter-mattsson-niklas-eklund-russian-operational-art-fifth-period-nordic-and-arctic-applications.

Messner E.Ye., *Khochesh' mira, Pobedi bunt!*, Moskva 2005, http://militera.lib.ru/science/0/pdf/messner_ea01.pdf].

'NotPetya' malware attacks could warrant retaliation, says Nato affiliated-researcher, https://www.theguardian.com/technology/2017/jul/03/notpetya-malware-attacks-ukraine-warrant-retaliation-nato-researcher-tomas-minarik.

Nowe sankcje USA wobec Rosji. Uderzają w największe przedsiębiorstwa, Onet Wiadomości, http://wiadomosci.onet.pl/swiat/nowe-sankcje-usa-wobec-rosji-uderzaja-w-najwiek-sze-przedsiebiorstwa/w9lkp.

Olchawa M., *Misja Ukraina*, Warsaw 2016.

Patterson D., *The ransomware wars: Here's how much cash the top gangs reel in*, CNS News, https://www.cbsnews.com/news/ransomware-war-conti-revil-hellokitty/.

Perry B., *NonLinear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations*, "Small Wars Journal" 2015, no. 1, http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-criticalrole-of-information-operations-and-special-operation.

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Warsaw 2013.

Press Briefing by Press Secretary Jen Psaki and Deputy NSA for Cyber and Emerging Technologies Anne Neuberger, 21 March 2022, https://www.whitehouse.gov/briefing-room/press-briefings/2022/03/21/press-briefing-by-press-secretary-jen-psaki-and-deputy-nsa-for-cyber-and-emerging-technologies-anne-neuberger-march-21-2022/.

Rada Europejska, Rada Unii Europejskiej, *Kalendarium – sankcje UE wobec Rosji w sprawie Ukrainy*, http://www.consilium.europa.eu/pl/policies/sanctions/ukraine-crisis/history-ukraine-crisis/.

Raport OSW. Zmiany w potencjale militarnym Federacji Rosyjskiej (po rosyjskiej operacji wojskowej w Gruzji), Warsaw 2009.

Reisinger H., Golz A., *Russia's Hybrid Warfare: Waging War below the Radar of Traditional Collective Defence*, "NATO Research Paper" 2014, no. 105.

Russia unleashed data-wiper malware on Ukraine, say cyber experts, The Guardian, https://www.theguardian.com/world/2022/feb/24/russia-unleashed-data-wiper-virus-on-ukraine-say-cyber-experts.

Sankcje i Rosja, J. Ćwiek-Karpowicz, S. Secrieu (ed.), Warsaw 2015.

Todd D., *NB65 Hackers Attacking Russian Orgs in Ukraine Retaliation*, https://www.secureworld.io/industry-news/nb65-hackers-russia-ukraine.

Ukraine hit by 'massive' cyber-attack on government website, The Guardian, https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers.

Ukrainian Defense Ministry's Website Among Several Hit By Cyberattack, https://www.rferl.org/a/ukraine-defense-ministry-cyberattack/31705206.html.

W Moskwie szykują ustawę, która "naprawi błąd" Chruszczowa, TVN24, http://www.tvn24.pl/wiadomosci-ze-swiata,2/nikita-chruszczow-przekazal-krym-ukrainie-nielegalnie,512415.html.

Wojnowski M., *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, "Przegląd Bezpieczeństwa Wewnętrznego" 2015, no. 7.

Wrzosek M., *Konflikt rosyjsko-ukraiński a zmiany w teorii prowadzenia działań militarnych*, "Kwartalnik Bellona" 2014, no. 4.