CYBERNETIC WARFARE – AN ELEMENT OF MODERN MILITARY OPERATIONS

Rafał Kochańczyk*, Tomasz Pączkowski
Jan Długosz University in Częstochowa, WSB University in Dąbrowa Górnicza
Correspondence: rafal.kochanczyk@interia.pl

Abstract

Russia's aggression against Ukraine also meant the outbreak of a cyber war, which is being waged via the Internet practically all over the world. It covered many aspects of modern life - from trolling to the use of cybernetic technology directly on the battlefield. Without the use of advanced digital technology modern conventional weapons become quite useless, deprived of information about the battlefield, and also massively inaccurate. This may be clearly seen in the example of Russian aggression.

The basic conclusion from the issues presented indicates that there is now no longer a division between front and rear in cyber warfare. Any information read on the web can, on the one hand, be a hacker's tool, and on the other hand, it provides specific data about us, even if we are not aware of that ourselves. So it can be said that cyber warfare has reached homes, offices and telephones. This is a completely new quality of threats.

Both the range and the variety of topics covered mean that it is impossible to fully master all aspects of the subject. This is due to the high dynamics of operations, both in the classical war and in the information war.

Keywords: Internet, security, cyber warfare, threats, cyberbullying, cybercrime, smart weapons and ammunition

1. Development of threats in cyberspace

In recent decades, a gradual transfer has taken place of an increasing range of social activities to the Internet. This phenomenon began with the exchange of information, through industry and banking, and eventually took over a large part of modern life. Of course, war, similarly as any other human activity, has not been free from the influence of the Internet. Initially, it took place mainly in the sphere of logistics, then it turned out that the network could be used to disrupt the enemy's

DOI: 10.5604/01.3001.0053.7150
Received: 02.01.2023 Revised: 03.04.2023 Accepted: 05.04.2023

communication, influence propaganda addressed at the society (especially the so-called black propaganda), both its own and that of the enemy, and even inflict physical damage using cyberspace.

An example of such a physical impact can be the use of the Stuxnet virus. According to Yahoo! News, the virus released in 2007 ushered in the "era of digital warfare". Specially designed to sabotage Iran's nuclear program, the virus struck just after Iran began installing the first batch of centrifuges at a uranium enrichment facility near the village of Natanz (CyberDefence24). Uranium enrichment centrifuges began to fail on a massive scale for no apparent reason. In such a way, digital sabotage was able to bring tangible results. Another example could be a potential attack on air or rail traffic management systems. The disruption of these systems can lead to disorganization using aviation and rail accidents with numerous fatalities.

The years 2020–2021 were a specific period, because with the onset of the coronavirus epidemic, the process of transferring professional activities and social contacts to the Internet in Poland has drastically accelerated. In addition to the advantages of such a solution, there was a threat that by staying at home and transferring their life needs online, people become more vulnerable to all types of cyber threats.

Meanwhile, over-usage of new technologies carries with it many risks. The most popular channels of cyberattacks, i.e. offensive activities on the Internet, which may target IT systems, computer networks or personal devices, included:

- Email and instant messaging,
- Loopholes in the system,
- USB (e.g. flash drive),
- Social networks.

Every day we hear about massive blockades of government websites, large enterprises, or even streaming services that cease to function under the pressure of DDoS attacks. Today's cyberattacks tend to exploit increasingly the unawareness of Internet users. Social engineering is most often practiced by people who steal confidential data causing certain consequences for the user. The threat is difficult to recognize, and the attack can be carried out over a prolonged time. The victim is often manipulated and the attacker may pose as someone else or use a stolen identity. In the course of attacks, hackers use so-called Eksploit to install viruses and other harmful tools on computers. They take advantage of security vulnerabilities in browsers such as Internet Explorer or applications such as Adobe PDF Reader to inject a virus or a Trojan horse into someone's system.

According to the Spokesman of the Minister, the Special Services Coordinator Team CSiRT GOV[1], the ABW is recording an increased number of computer

[1] CSIRT NASK is a Computer Security Incident Response Team, operating at the national level, run by the Scientific and Academic Computer Network – National Research Institute based in Warsaw.

incident reports. The most frequently reported incidents include phishing campaigns, spoofing, malware, scanning and DDoS attacks. The listed types of cyberattacks are currently the most serious threats to ICT networks and systems (gov.pl, 2022).

As a response to these threats the Charlie alarm level in Poland has been introduced. The Charlie-CRP alert level active throughout Poland is the third of four levels. As the Government Centre for Security explains: "This level is introduced in case of an event confirming a probable target of a terrorist attack in cyberspace or obtaining credible information about a planned event" (Siewko, 2022).

Safety during the application of alert levels depends not only on the services, but also on citizens who should be especially vigilant during the introduction of individual levels and inform the services of noticing any unusual situations, including, for example, about unusual behaviour of people, parcels or luggage left unattended in public places.

It should be pointed out that the introduction of the anti-terrorist law and the placement it had a positive impact on raising the level of anti-terrorist security in Poland (Staszczak, 2022).

Modern armed forces are not only armies and conventional means of warfare used on a large scale. An important component – if not in terms of the number of people and equipment, but to a much larger extent in terms of the seriousness of the tasks performed as well as the efficiency of operation – are special forces. This stems from efforts to ensure the ability of the state's armed forces to quickly adapt to these new challenges and threats. In the age of conflicts; in which an actor deprived of legal and international subjectivity may become a party without a permanent territory or even a clearly defined base of operation, the armed forces must assume a form that allows a flexible response, with high precision, to suddenly emerging threats from small, determined groups (de Wijk, 2005).

It is reasonable to say that we currently live in a world in which there are few fields that have not been computerized and not connected to the global Internet network. In addition, the COVID-19 pandemic has accelerated the technological progress, especially as regards the use of communication and educational platforms, enabling so-called distance working and learning. On the one hand, the Internet is a place of work for people forced to stay at home by the virus, a source of information and a possibility of contact with relatives, and on the other hand, it generates new cyber threats and intensifies the occurrence of "old" ones (Kochańczyk, Pączkowski, 2021).

2. Elements affecting security in cyberspace

Problems related to cybercrime are not yet widespread in our country. Currently, there is no specific and unique definition of cybercrime in space. On a daily basis, one can come across various terms that are used interchangeably, e.g. computer

crime, computer-related crime, high-tech crime, digital technology crime (SEC, 2007), crimes related to information processing technology, Internet crimes (for more, see e.g. Adamski, 2000).

So far, three generations of cybercrimes could be distinguished, and namely:

– the first generation of cybercrime involved targeted attacks on computers, computer networks and data,
– the second generation was associated with the development of ICT networks and attacks on their integrity and availability through so-called hackers,
– the third one - taking place at present – is related to the noticeable process of automation of cybercrime, which is, among others, the result of the use of special software (Siwicki, 2013).

According to M. Siwicki, some studies also distinguish the fourth generation of cybercrime, characterized by the increasingly common use of hacking tools by the perpetrator and the further development of the computer underground. This results in the expansion of the milieu of people for whom cybercrime no longer requires special abilities and skills, but merely access to criminal cyber tools.

The classification of modern cyber threats includes:

- Cybercrime.
- Cyberterrorism.
- Addiction risks.
- Health risks.
- Threats related to cyber warfare.

The attack of the Russians on Ukraine has highlighted the emergence of the last-mentioned generation of cyber threats – related to cyber warfare.

As regards the normative acts (laws, regulations), programmes, etc., in force in Poland relating to cyberspace and ensuring security in it, the Act on Martial Law and on the competences of the Commander-in-Chief of the Armed Forces and the principles of his/her subordination to the constitutional bodies of the Republic of Poland should be mentioned first and foremost. By "cyberspace" the Act understands the space for processing and exchanging information created by ICT systems together with relationships with users related to them. "Cyberspace" is defined in the same way in the government document called the National Cybersecurity Framework of the Republic of Poland for 2017–2024 (Terlikowski, 2019).

3. New threats from cybernetic means in conventional warfare

The beginnings of wars and conflicts between states have assumed the form of a clash of military forces, in which the tools were the size of the armed forces, the tactical and strategic preparation of commanders and the terrain conditions of the clash. Of course, these factors are still important, but nowadays cyber conflicts appear as clashes that do not take place in physical space, but rather in the virtual one. This causes specific problems – how to use conventional weapons online?

How to find and identify the attacker? Naturally, the answer to these questions is to prepare one's own "internet units" that would be able to suppress the enemy's impact and, at the same time, conduct offensive actions against them. These can often comprise anonymous or false flag activities.

Trolls at war

With the start of the war in Ukraine, the fight for information in the web has reached a hitherto unprecedented scale. There are thousands of comments supporting the actions of Vladimir Putin's regime or denigrating Ukraine as a state, but this is not all. In addition to great politics, there is no shortage of social engineering plays aimed at the society, intended to create antagonistic moods in Poland, which has so far been helpful and friendly towards our eastern neighbour (Urbaniak, 2022).

According to experts from Sentione, a company professionally involved in monitoring Internet content, various methods are used in Kremlin disinformation. What is worse – not only from the Kremlin, but also from other sources – for example unreliable media. Particular caution needs to be maintained in particular with respect to the following:

- clickbait[2] title – some portals want to earn money from the war and increase traffic on their website, so they will attract attention with catchy titles bordering on lies;
- information that arouses extreme emotions – shock, fear, anger, but also laughter and joy, has a high viral potential[3]. For this reason information about blocking access to Pornhub in Russia, which eventually turned out to be false, spread so quickly. And in the case of war, crafting shocking and scary content is not a problem;
- videos, reels and social media stories also have a lot of viral potential, not least because the algorithms of these platforms are geared towards promoting video content. Also, we as humans perceive video content much more intensively than text as such;
- photos from other places or times – it is easy to manipulate with the help of archival materials, e.g. photos from the war in Yemen presented as photos from Kiev. Social media allow quick provision of information, but unfortunately there is often no time to verify data;
- deepfake[4] i.e. fabricated video material – it is now very easy to prepare or edit a film so that it shows all kinds of content or people in false situations (Kralka, 2022).

[2] The clickbait title of the text in the form of a link in electronic media is one that is both intriguing and unclear, and therefore prompts one to click.

[3] Virals are content in the form of video, graphics or text, the mission of which is simple: to spread very quickly and reach as many recipients as possible.

[4] Deepfake is a sound and image manipulation that aims to create fake images and sounds using artificial intelligence techniques.

When using social media, including Twitter, the basic rule is to check the profile of the user/interlocutor whose post has raised our concern: recently Russian trolls quite frequently set up set up new accounts in recent days, and those that have denied the pandemic in the last two years remain active and the vaccination campaign - now their message is aimed, for example, at refugees. The number of followers of a given profile should arouse vigilance - troll accounts are often followed by a few users (or none) or other fake profiles associated with it (Bochyńska, 2022).

Internet communication specialists warn against the activities of pro-Russian trolls who publish and disseminate false information on a massive scale about Ukrainian refugees in Poland on all sorts of social networking sites.

The most popular topic at the moment is emphasis on evoking negative emotions and reactions towards Ukrainians, e.g. regarding the increase in fuel prices or food products in stores. Added to this is the fuelling of hatred against the backdrop of history of the genocide in Volhynia and the popularity of Bandera (https://geekweek.interia.pl/internet/news-uwazajcie-na-prorosyjskie-trolle-probuja-nas-sklocic-z-ukrai,nId,5907897).

Information war

In 2021, the GOV CSIRT Team (Computer Security Incident Response Team) registered a total of 762,175 notifications of potential ICT incidents, of which 26,899 were considered real incidents. In 2021, more than three times more notifications were registered as compared to the previous year, where a total of 246,107 notifications were recorded. The increase in registered notifications is primarily due to the number of alerts generated by the ARAKIS GOV system (an early warning system for Internet threats). The ARAKIS GOV system enables the identification of threats, among others, on the basis of dedicated security signatures.

Table 1. Number of registered notifications and incidents in particular years

Itemization	**2018**	**2019**	**2020**	**2021**
Sum of reported incidents	31 865	226 914	246 107	762 175
Sum of registered incidents	6 235	12 405	23 309	26 899

Source: Report on the state of cyberspace security in Poland in 2021. CSIRT GOV team (Computer Security Incident Response Team)

In turn, the RAND Corporation (Research ANd Development) – an American think tank and non-profit research organization, originally formed for the needs of the United States Armed Forces, presented the results of a report on an analysis of the impact of manipulation activities and their effectiveness in shaping election results in various parts of the globe. The first conclusion of the report is that regardless of the effectiveness of this influence, the fact is that the Kremlin has

developed a very strong package of tools that have the potential to influence and have the ability to decide on the election results.

Researchers have also found that autocratic countries such as Russia and China began to use information channels to gain advantage, and they believed that they were involved in an information war with the West, which, in their opinion, was unleashed by the United States and its allies (https://cyberdefence24.pl/polityka-i-prawo/czy-rosyjska-dezinformacji-nalezy-sie-obwiac-okiem-amerykanskich-naukowcow-nie).

The situation in which communication systems are interconnected worldwide causes additional problems. Interconnected networks can be attacked and disrupted not only by states, but also by non-state actors, including dispersed groups and even individuals. Potential opponents can also have a wide range of possibilities. In this way, the threat to US interests can be greatly multiplied and will change as the systems develop and become progressively more complex and the required expertise becomes increasingly disseminated.

Traditional boundaries of influence become blurred

Given the wide range of possible adversaries, weapons and strategies, it is increasingly difficult to distinguish between foreign and domestic sources of CW threats and activities. It is impossible to know who is being attacked by whom or who is behind them. This greatly complicates the traditional distinction of roles between national law enforcement authorities on the one hand and national security and intelligence authorities on the other. Another consequence of this blurring is the disappearance of clear distinctions between different levels of anti-state activity, ranging from crime to warfare.

Expanded role of perception management

The ability of CW agents to manipulate information that is crucial to public perception may become intensified. In addition, there is also the possibility that the "facts" of the event themselves may be manipulated through multimedia techniques and widely disseminated. Conversely, there may be a diminished ability to build and maintain national support for a controversial political action. One consequence is that future US administrations may include a robust online component as part of any public information campaign.

No strategic intelligence

For various reasons, traditional methods of intelligence gathering and analysis may be of limited use in meeting the challenge of strategic intelligence (Internet War). Collection purposes are difficult to identify; the allocation of intelligence

resources is difficult due to the rapidly evolving nature of the threat, and moreover vulnerabilities and target assemblies are not yet well understood. In conclusion, the US may have difficulty identifying potential adversaries, their intentions or capabilities. One implication is that new organizational relationships are needed within the intelligence community and between that community and other actors. Restructuring of roles and missions may also be required.

Difficulty of tactical threat and attack assessment

This feature of warfare creates entirely new problems in the cyberspace environment. The fundamental problem is distinguishing between "attacks" and other events such as accidents, system crashes, or hacking by "thrill-seekers". The main implication of this feature is that the US may not know when an attack is underway, who is attacking, or how the attack is carried out.

Consequently, the RAND Corporation has compiled and presented the fundamental problems arising from information warfare.

Difficulty of building and maintaining coalitions

Many US allies and coalition partners are vulnerable to IW attacks on their basic information infrastructure. For example, dependence on mobile phones in developing countries can make telephone communication in these countries very vulnerable to disruption. Other sectors in the early stages of exploiting the information revolution (e.g. energy and finance) may also present certain vulnerabilities that an adversary may attack to undermine coalition participation. Such attacks can also serve to break the "weak links" in the implementation of coalition plans. On the other hand, uncertain coalition partners who are in dire need of military assistance may want reassurance that the US deployment plan in their region is not vulnerable to IW disruption.

Vulnerability of the US terrain to attacks

Information warfare has no front lines. Potential battlefields are found wherever network systems allow access. Current trends suggest that the US economy will increasingly rely on complex, interconnected network control systems such as oil and gas pipelines, electrical grids, etc. The vulnerability of these systems is currently poorly understood. Moreover, deterrence and retaliation measures are uncertain and may rely on traditional military instruments in addition to CI threats (adapted from: Molander, Riddile, Wilson).

Recently, when CIA Director Bill Burns appeared before the Senate Intelligence Committee to speak about the situation in Ukraine, he was asked about Russia's use of disinformation and self-presentation as a means of legitimizing the invasion.

"This is one information war that I believe Putin is losing" – Burns replied (Demus, Paul, 2022).

Information blockade – what is it?

The armed aggression against Ukraine did not cause significant protests in Russia. Since February 24, 2022, there have been few anti-war demonstrations, largely spontaneous ones, including one-man pickets. In every case they are broken up by the security services. On 24 February, the number of participants reached a maximum of several thousand in Moscow and St. Petersburg. In the following days, according to available information, they gather, on average, from a few dozen to several hundred people.

Participants in demonstrations are detained en masse. The independent media project OVD-Info, which monitors cases of human rights violations, reports that a total of almost 7,000 people were detained on February 24–28 (mostly due to participation in actions on February 24 – almost 1,980 people in 67 cities). On February 28, according to preliminary data, 492 people were detained in 14 cities. There are reports of overcrowded detention centres in Moscow, hundreds of administrative cases have already been filed (demonstrators face arrest and fines) and the first criminal cases (Domańska, 2022).

Since March 1, 2023, many Russian organizations and state entities have been banned from using foreign instant messengers. A new law has been adopted in the Russian Federation that prohibits many Russian organizations from using foreign messengers. The list of banned messengers is established by Roskomnadzor (Russian Federal Service for Supervision of Communications, Information Technology and Media). The tentative list includes such applications and messengers, as: Discord, Microsoft Teams, Skype for Business, Snapchat, Telegram, Threema, Viber, WhatsApp, WeChat (Kruczek, 2023).

Smart Weapon

The Russian aggression against Ukraine and the actions of Ukrainian troops trying to repel the invasion of Vladimir Putin show how dangerous combat drones have become in recent years. After all, the Ukrainian army uses them extremely effectively and has already received further equipment of this type. More specifically, these are Switchblade drones, which can be best described as "smart" bombs which are capable of staying in the air for a certain amount of time before striking a target (Mileszko, 2022).

Deliveries of intelligent anti-tank (anti-tank guided missiles) and anti-aircraft sets (MANPAD) are crucial. This weapon is light and easy to transport, and at the same time instantly increases the defensive capabilities of infantry. These are

tools sufficient to fight the most powerful tanks and the most modern aircraft and helicopters in favourable conditions.

Most valuable to the Ukrainians are third-generation PPK anti-tank Guided Missiles which operate on a 'shoot and forget' system - and they are the most important part of the supply of anti-tank weapons. Ukraine receives mainly FGM-148 Javelin and NLAW missiles. MANPADs (from Man-portable air-defence system) are anti-aircraft guided missiles that can be carried and launched by one man – almost all modern missiles of this kind can be fired from the arm. Today, the most valuable are those that, similarly to anti-tank weapons, do not require long-term specialist training.

Already in the first week of the war, Turkey delivered the first of several dozen Bayraktar TB-2 drones ordered by Ukraine at an express pace. These strictly combat machines are large and capable of carrying a total of four guided bombs.

The United States has provided Ukraine with 100 Switchblade drones. These are lightweight "kamikaze" drones fired from a tube similar as an ATGM missile and capable of flying for 30 minutes.

During the war in Ukraine MANPAD systems were also used for anti-missile defence for the first time on a large scale. They are capable of shooting down, above all, Kalibr cruise missiles owing to similar flight characteristics as in the case of some aircraft. The Ukrainians boasted of shooting down at least several dozen Kalibrs in this way (Głowacki, 2022).

The Pentagon says the Russians have run out of good, smart ammunition. Now they are forced to use so-called "dumb bombs", i.e. missiles that cannot be controlled in any way. After they are dropped from the plane or launched, it is no longer possible to control the flight. This means that the weapon is less effective, causes more accidental damage, and its accuracy is even affected by weather conditions (Waszczuk, 2022).

Unfortunately, as part of cooperation between the regimes, Iran has provided Russia with a large amount of the so-called kamikaze drones. They are relatively easy to build, but unfortunately, when sent in large numbers, they cause considerable losses, especially for Ukraine's energy infrastructure.

Recently, there have been more and more press reports about the use of electronic weapons to interrupt the control of drones or even intercept enemy drones.

4. Internet and helping war victims

Free Internet from UPC (Polish internet distributor) was introduced in connection with the war in Ukraine. This is to be another aid step addressed at Ukrainians who are staying in Poland. Interestingly, help is provided not only to people from Ukraine, but also to some Poles. UPC will provide free access to fibre-optic Internet and television for a period of six months. The services can be used by Ukrainian

citizens who came to Poland after February 24, as well as Poles who are the owners of premises used as accommodation for those fleeing the war. What is important, according to information from UPC, this applies to those who make their flat or house fully available (Mering, 2022).

Victims of the war in Ukraine can seek free legal assistance at the telephone number +48 800 088 544. The Bar Association and other legal professions have launched a free hotline in several languages, e.g. Polish, Ukrainian and English (Mikowski, 2022).

Since the outbreak of the war, many websites have appeared on the Internet that compile information about people who can provide shelter to refugees and ask for their details and telephone number. More groups on Facebook eagerly provide links to Google sheets, which collect information about housing opportunities, addresses and phone numbers - the same ones used to verify a bank account. Consequently, an accurate database of people bringing help and refugees is created, available to literally everyone. Perhaps this information will be used to organize help for Ukrainian families, but it can also be sold or used in other ways (Kralka, 2022).

Of course, online collections of cash and in-kind funds for refugees are still underway, and as a curiosity, it is worth quoting online collections for the purchase of Turkish drones for the Ukrainian army.

5. New threats for computers and mobile devices – conclusions and recommendations

The key element in managing security in cyberspace remains the human being. On the one hand, it is usually the thoughtless and unwise behaviour that brings threats to the computer network at work or at home. On the other hand, it is criminal tendencies, undoubtedly combined with the outstanding skills of hackers, that cause a constant arms race in the network. It is worth noting the analogy with the development of conventional weapons - always a new weapon motivated the construction of the next new, more powerful generation. So we cannot expect this race to ever be sufficiently successful, we just have to constantly keep up with new technology.

Nowadays, it is no longer bored and experimenting hackers who commit digital crimes because they consider the Internet to be an anonymous space and a legal gray area. They still exist, of course, but today it is the professional, global organizations that do the most damage.

Until a few years ago, cybercriminals could clearly distinguish themselves from each other based on their modus operandi. Today, these boundaries are becoming increasingly blurred, attribution of responsibility is proving extremely unreliable, and false flag attacks are becoming more common and much easier. At the same time, the degree of specialization of the digital forces of nation states, hacktivists

and cybercriminals is constantly increasing. States should definitely take steps to reverse the asymmetry in cyber conflicts.

In the US, the White House has banned the use of the Chinese company's Tiktok social media app on government smartphones. Similar prohibitions apply to members of the House of Representatives and employees. Several states and the U.S. military have issued similar regulations in the past. This naturally was connected with potentially sensitive information collected by the application.

In 2021, the Nation States, Cyber conflict and the Web of Profit study commissioned by HP (Hewlett-Packard) and conducted by the Department of Criminology at the University of Surrey found that ca. 35 percent of nation state cyberattacks target businesses. Between 2017 and 2020, there was a 100% increase in "significant incidents by nation state". The study analyzed over 200 known cybersecurity incidents, as well as testimonies exposing the activities of the Dark Net and interviews with cybersecurity experts, government, intelligence, academia, and national and international law enforcement agencies. While ca. 35 percent of the nation-state hacker attacks investigated were against businesses, about 25 percent were for cyber defence, and further 14 percent were attacks against media and news sites. Attacks against other government agencies and critical infrastructure accounted for 12 and 10 percent, respectively. The primary target of the attacks investigated in the HP study can clearly be attributed to the international cybercrime economy. According to the study, cybercriminals generate at least $1.5 trillion (Laufenburg, 2022).

The basic conclusion drawn from the presented issues indicates that currently there is no longer a division into the front and the back in cyber warfare. Any information we can read on the web can, on the one hand, be a hacker's tool, and on the other hand, it provides specific data about us, even if we are not aware of it ourselves. Consequently we can conclude that cyber warfare has reached our homes, offices and even telephones. This is a completely new quality of threats.

Both the range and the variety of topics covered indicate that it is impossible to fully master all aspects of the subject. This is due to the high dynamics of operations, both in the classic war and in the information war. Therefore, in the near future, I would like to present the individual elements of the issue in more detail in subsequent publications.

References

1. Adamski, A., (2020). *Computer criminal law*, Warsaw: C.H. Beck.
2. Bochyńska, N., (2022). *War, trolls and fake news. So what to pay attention to on social media*. https://publicystyka.ngo.pl/zanim-podamy-dalej-post [10.05.2022].
3. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards an overall strategy to fight cybercrime, {SEC(2007) 641}{SEC(2007) 642}, http://eur-lex.europa.eu [30.05.2017]

4. CyberDefence24.The secret of the attack on Iran's nuclear program has been revealed. Who helped introduce the virus into the system? https://cyberdefence24.pl/polityka-i-prawo/zdraznie-tajemnice-attack-on-iranski-nuklearny-program-who-helped-wlead-virus-into-the-system.
5. CyberDefence 24 (2022). *Hostile Social Manipulation Present Realities and Emerging Trends report for: Is Russian disinformation to be feared?* https://cyberdefence24.pl/polityka-i-prawo/czy-rosyjska-dezinformacji-nalezy-sie-obawiac-okiem-amerykanskich-naukowcow-nie [17.05.2022]
6. Demus, A., Paul, Ch., (2022). *Don't Sleep on Russian Information-War Capabilities*. https://www.defenseone.com/ideas/2022/04/dont-sleep-russian-information-war-capabilities/364050/ [05.04.2022].
7. Domańska, M., (2022). *Social reactions in Russia to the invasion of Ukraine. Center for Eastern Studies*. https://www.osw.waw.pl/pl/publikacje/analyses/2022-03-02/reakcje-spoleczne-w-rosji-na-invasion- na-ukraine ANALYZES [13.05.2022]
8. de Wijk R., The Limits of Military Power In: Howard R.D, Sawyer R.L. (ed.), (2005). *Terrorism and Counterterrorism. Understanding the New Security Embrace*, Guford: McGraw Hill Higher Education, p. 452.
9. Głowacki, W., (2022). *What weapons exactly does Ukraine receive from the West and what other weapons could it get?* https://oko.press/jaka-bron-dokladnie-obtains-ukraine-from-the-west-and-jaka-jeszcze-moglaby-dostac/ [04.05.2022]
10. Kochańczyk, R., Pączkowski, T., (2021). Threats in cyberspace as a challenge for security culture. In: *Rationalization of the management of uniformed formations responsible for internal security*, Wiśniewski, B., Gikiewicz, M., Kochańczyk, R. (eds.). Warsaw: SGSP.
11. Kralka, J., (2022). How to recognize a Kremlin troll on the Polish Internet? https://bezprawnik.pl/jak-rozpoznac-kremlowskiego-trolla-w-polskim-internecie/ [10.07.2022]
12. Kruczek, J., (2023). *Applications and messengers a threat to national security?* https://satkurier.pl/news/226423/aplikacje-i-komunikatory-zagrorzenie-bezpieczenstwa-narodowego.html [03.03.2023]
13. Laufenburg R., (2021). *Cyberkriminelle: Wie sehen sie aus?* https://www.pcspezialist.de/blog/2021/05/26/cyberkriminelle/ [20.08.2022].
14. Mering P., (2022). *UPC, in connection with the war in Ukraine, gives away free fiber optic Internet and television for six months*. https://bezprawnik.pl/darmowy-internet-od-upc-w-zwiazku-z-wojna-w-ukrainie/ [19.06.2022]
15. Mikowski, M., (2022). *Ruszyła bezpłatna infolinia z pomocą prawną dla ofiar wojny na Ukrainie*. https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8391991,uchodzcy-z-ukrainy-bezplatna-infolinia-z-pomoca-prawna.html [03.06.2022]
16. Molander, R.C., Riddile, A., Wilson P.A., (1996). *Strategic Information Warfare A New Face of War*. https://www.rand.org/pubs/monograph_reports/MR661.html.
17. Mileszko, T., (2022). *The US sends modern kamikaze drones to Ukraine*. https://www.komputerswiat.pl/aktualnosci/militaria/usa-wysylaja-na-ukraine-nowoczesna-drony-kamikaze-wyjasniamy-co-potrafia-switchblade/kdmc448. [19.05.2022]
18. Siewko, T., (2022). CHARLIE-CRP alert level extended again across Poland TVN24 [04.06.2022]

19. Siwicki, M., (2013). *Cybercrime*, Warsaw: C.H. Beck.
20. Spokesperson of the Minister Coordinator of Special Services Beware of threats in cyberspace (2022). https://www.gov.pl/web/sluzby-specjalne/uwaga-na-zagrorzenia-w-cyberprzestrzeni [10.08.2022].
21. Staszczak, M., (2022). The functioning of the crisis system on the example of alarm levels *Kwartalnik Policyjny*, No. 2.
22. Terlikowski, T., (2019). Security of cyberspace as a challenge of our time. Cybersecurity system in Poland. *Zeszyty Naukowe SGSP*, No. 71.
23. Urbaniak P., (2022). *Russian trolls attack with a new tactic. Don't be approached*. https://www.telepolis.pl/wiadomosci/wydarzenia/rosyjskie-trolle-polska-dezinformacja-hejt. [25.07.2022]
24. Waszczuk, E. (2022). *Russia has run out of effective weapons! Have they already lost?* https://www.planeta.pl/Wiadomosci/Swiat/RUSJI-SKONCZYLA-SIE-SKUTECZNA-BRON!-Maja-wadwane-pociski-25-03-2022. [15.05.2022]
25. *Watch out for pro-Russian trolls. They are trying to quarrel us with the Ukrainians*. https://geekweek.interia.pl/internet/news-uwazajcie-na-prorosyjskie-trolle-probuja-nas-sklocic-z-ukrai,nId,5907897. [23.06.2022]

WOJNA CYBERNETYCZNA – ELEMENT WSPÓŁCZESNYCH OPERACJI WOJSKOWYCH

Abstrakt

Agresja Rosji przeciw Ukrainie również oznacza wybuch wojny cybernetycznej, która toczy się za pośrednictwem Internetu praktycznie na całym świecie. Objęła ona wiele aspektów współczesnego życia – od trollingu po wykorzystanie technologii cybernetycznej bezpośrednio na polu walki. Współczesna broń konwencjonalna bez wykorzystania zaawansowanej technologii cyfrowej staje się wysoce bezużyteczna, pozbawiona informacji o polu walki jest dramatycznie niedokładna. Jest to szczególnie widocznie na przykładzie rosyjskiej agresji.

Podstawowy wniosek płynący z przedstawionych zagadnień wskazuje, że obecnie w cyberwojnie nie ma już podziału na front i tyły. Każda informacja przeczytana w sieci może być z jednej strony narzędziem hakera, a z drugiej strony dostarcza konkretnych danych o nas, nawet jeśli sami nie jesteśmy tego świadomi. Można więc powiedzieć, że cyberwojna dotarła do domów, biur i telefonów. Jest to zupełnie nowa jakość zagrożeń.

Zarówno zakres, jak i różnorodność poruszanych tematów powodują, że nie jest możliwe pełne opanowanie wszystkich aspektów przedmiotu. Wynika to z dużej dynamiki działań, zarówno w wojnie klasycznej, jak i w wojnie informacyjnej.

Słowa kluczowe: Internet, bezpieczeństwo, cyberwojna, zagrożenia, cyberprzemoc, cyberprzestępczość, inteligentna broń i amunicja