http://dx.doi.org/10.18778/1427-9657.08.05

C O P E
Member since 2019
JM14481

EASTERN REVIEW 2019, T. 8

Pavlo Katerynchuk
https://orcid.org/0000-0003-0579-3321
Yuriy Fedkovych Chernivtsi National University
Chernivtsi, Ukraine
Department of International Information
e-mail: pavlo.katerynchuk@gmail.com

Challenges for Ukraine's cyber security: National dimensions

Abstract. The usage of information as a weapon in the foreign and domestic policies of Russia is not a new phenomenon. Still, the sophistication and intensity of it grow with each passing year. Recently the EU and USA have realized the powerful latent influence of Russian media and propaganda, including on electoral processes and the activities of State administration. They have realized that Russian disinformation poses a serious threat to the United States and its European allies, first and foremost with regard to Poland, the Baltic States and Ukraine. Moreover, unlike Soviet propaganda, the modern methods of the Russian information war do not rudely promote the agenda of the Kremlin. Instead, they aim to confuse, daze and divert citizens from supporting the EU and Ukraine. Russia seeks to undermine the support for European values; producing disarray among European allies in order to increase its influence. Ethnic, linguistic, regional, social and historical contradictions and stereotypes are used for this purpose. As current experience shows, Russian advocacy efforts in Europe make up an important part of their hybrid approach to the projection of force. Despite the fact that the crisis in Ukraine for the first time drew the attention of the West to the importance and real meaning of the information campaign in Russia, the Kremlin's use of disinformation was launched long before the crisis. Russia carefully and purposefully prepared an information war against Ukraine.

Keywords: cyberspace, cyber security, hacker attacks, information security.

© by the author, licensee Łódź University – Łódź University Press, Łódź, Poland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license CC-BY-NC-ND 4.0

Introduction

The hybrid war in the East of Ukraine and the information confrontation with the Russian State, a state that systematically uses the media space and the Internet to achieve its political goals, necessitates the study of the issue of protecting the cyberspace of Ukraine as an integral part of the state's information security.

The necessity of building an effective cyber security system as one of the main components of national information security in Ukraine became ever apparent after the annexation of Crimea by Russia and the invasion of Russian troops in the territory of the Ukrainian Donbas.

The problem of cyberspace research and the analysis of cyber security is characterized by a number of uncertainties both in the terminology itself and in the regulatory sphere. For further reference, research into the interconnection of information security and cyber security needs clear form in order to understand the essence of the concepts of "cyber security" and "information space". This, in turn, can only be done when the essence of the concept of cyberspace is clearly stated.

The term "cyberspace" was first coined by Canadian science-fiction writer William Gibson in 1982 in the Burning Chrome novel. In 1984, this concept was further elaborated on in the work *Neuromancer*. According to Gibson, cyberspace is a well-balanced hallucination that is experienced daily by billions of conventional operators around the world.

There are many interpretations of the concept in the scientific literature of Cyberspace. In this case, a myriad understanding of this concept is inherent in the regulatory and legal sphere: practically every country in its legislation gives its own definition. For example, 1) in accordance with an international standard (ISO/IEC 27032, 2012), cyberspace is the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form; 2) in accordance with US regulatory framework (National Military Strategy, 2004), cyberspace is a field characterized by the ability to use electronic and electromagnetic means to memorize, modify and exchange data through network systems and related physical infrastructure; 3) in accordance with official documents of the European Union (European Commission, Glossary and Acronyms), cyberspace is the virtual space in which the electronic data of the world's personal computers (PCs) circulate; 4) According to UK Cyber Security Strategy (2009) documents, cyberspace is all forms of networks and digital activity, including content and activities, implemented through digital networks; 5) according to German Cyber Security Strategy (2011) cyberspace is all the information infrastructure available through the internet outside any territorial boundaries.

© by the author, licensee Łódź University – Łódź University Press, Łódź, Poland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license CC-BY-NC-ND 4.0

In general, most definitions boil down to understanding cyber security as a state of cyberspace security of the state as a whole, or of some of its infrastructure against external influences and risks, which ensures their sustainable development, as well as the timely detection, prevention and neutralization of real and potential challenges, cyber interventions and threats to personal, corporate and /or national interests.

Russia’s hybrid aggression against Ukraine developed into an active phase in early 2014, but long before the direct military intervention it was accompanied by tactical information support, which contained a wide range of information and psychological influences on the population of Ukraine and Russia, more or less since Ukraine’s Declaration of Independence in 1991.

Estimates from Ukrainian experts also indicate that Russia has always worked to weaken Ukraine, and this activity has been particularly intensified with the coming to power of Putin.

The main focus of the war on the hybrid nature of the Russian Federation against Ukraine is the information sphere, however, Russian influence is also exercised on the cultural, humanitarian, military, financial, energy and diplomatic and economic spheres, as well as cyberspace. This proves that Russia’s hybrid war against Ukraine is aimed at non-military spheres, and its primary focus is outreach, where cyber aggression is a key component.

Analysis of recent research and publications

The study of the security of cyberspace as a component of information security has become the subject of scientific research by many foreign scientists: J. Nye, S. Morgan, M. Schmidt, A. Klimburg, M. Gedeker, M. Libitsky, I. Zubarev, M. Bezkorovayny. It should be also noted that since the beginning of the Russian armed aggression Ukrainian scientists have also become interested in this issue, in particular, M. Ozhevan, V. Buryachok, V. Furashev, V. Butuzov, V. Tolubko, O. Dovgan, V. Khoroshko, S. Tolyupa, M. Pogoretsky, K. Titunin and other scientists.

I would like to mention separately the works of researchers of the National Institute for Strategic Studies under the President of Ukraine, especially B. Parahons’kij and G. Javors’ka *Ontology of War and Peace: Security, Strategy, Meaning* (Maksym Rozumnyĭ…, 2018; Parahons’kij, Javors’ka, 2019: 560); *Putin’s regime: reboot-2018* / M. Razumny (ed.) (Parahons’kij, Javors’ka, 2019: 480), and D. Dubov *Cyberspace as a new dimension of geopolitical rivalry* (Dubov, 2014).

That said, despite a fairly large number of studies and publications on the topic of information and cyber security, analysis shows that researchers have considered the general issues of developing a national system of cybernetic

© by the author, licensee Łódź University – Łódź University Press, Łódź, Poland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license CC-BY-NC-ND 4.0

security as an integral element of the information security system. Therefore, the purpose of this article is to study the national dimensions of cyberspace as a component of Ukraine's information security.

Presentation of the main research material

For the first time, Russian cyber threats and possible cyber attacks began to peak during the 2016 US election campaign, when, according to many researchers, the intervention of Russian hackers and the hacking of the electronic mailbox of the Democratic Party and Hillary Clinton, influenced the electoral campaign and electoral sympathies of Americans. However, these were only echoes of a long and purposeful campaign of Russian intelligence services, which increasingly involve cyberspace and electronic media of mass communication for espionage and undermining the interests of the Kremlin. At the same time, hacker attacks on government structures and industrial facilities occurred earlier, and not only within the same continent.

The United States reacted to Russia's hacking attacks by introducing new sanctions against companies and individuals thus prohibiting any operations within the US financial system. Among the examples of "malicious and destabilizing activity", the US Department of the Treasury calls the NotPetya virus an attack on power distribution networks. In February 2018, the White House said that the damage caused by the NotPetya virus in Europe, Asia, and America was calculated to be billions of dollars. The NotPetya attack in the White House was named a part of the Kremlin's efforts to destabilize the situation in Ukraine, which is increasingly demonstrating Russia's participation in the ongoing conflict (CShA takozh zvinuvatili…, 2018).

Russia, however, denies involvement in the attack and indicates that Russian companies have also suffered from it. However, British ministers also said that Russian cyber attacks are NotPetya (Uryad Brytaniyi zvynuvatyv…, 2018). On the first day of the spread of the virus, June 27, it struck 2,000 organizations; 75% of the victims fell to Ukraine. Ukrainian ministries, police, banks, Boryspil airport, Kyiv metro, media, mobile operators, medical companies suffered. The virus blocked computers and demanded money in exchange for restoring access to locked programs. British prime minister Theresa May blamed President Putin in November last year for trying to "sow discord" in the west: through interference in elections, dissemination of disinformation and cyberwar.

Theresa May has accused Russia of meddling in elections and planting fake stories in the media in an extraordinary attack on its attempts to "weaponise information" in order to sow discord in the west. Listing Russia's attempts to undermine western institutions in recent years, she said: "I have a very simple

© by the author, licensee Łódź University – Łódź University Press, Łódź, Poland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license CC-BY-NC-ND 4.0

message for Russia. We know what you are doing. And you will not succeed" (Mason, 2017).

American and British officials said that the attacks affected a wide range of organizations including internet service providers, private businesses and critical infrastructure providers. They did not identify victims or provide details on the impact of the attacks. "When we see malicious cyber activity, whether it be from the Kremlin or other malicious nation-state actors, we are going to push back", said Rob Joyce, the White House cyber security coordinator (Finkle, Chiacu, 2018).

Earlier, in February 2018, German officials also accused Russia of hacking attacks on government sites. In particular, according to media reports, hackers from the grouping of APT28, also known as Fancy Bears, successfully attacked the German Foreign and Defence Ministries at the end of February. They entered the so-called Berlin-Bonn Information Network (IVBB), which is used by the Federal Chancellery of Germany, the federal ministries and services security, as well as the Bundestag and the Bundesrat (Nimechchyna zvynuvatyla Rosiyu…, 2018).

Along with the statements of the official agencies of the United States, Great Britain and Germany, NATO has adopted a consolidated decision on Russia's destabilizing role in the modern world, which is expressed by

> a long illegal and illegitimate annexation of the Crimea, violations of sovereign borders with the use of force; the intentional destabilization of the situation in eastern Ukraine; the sudden launch of large-scale military exercises contrary to the spirit of the Vienna Document and provocative military action at NATO's borders, including in the regions of the Baltic and Black Seas and the Eastern Mediterranean; irresponsible and aggressive nuclear rhetoric, as well as repeated violations NATO Allied airspace *(Warsaw Summit Communiqué*, 2016).

In the communiqué after the Warsaw summit, NATO noted that cyber attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack.

> We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate and recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. It will support NATO's broader deterrence and defence: cyber defence will continue to be integrated into operational planning and Alliance operations and missions, and we will work together to contribute to their success. Furthermore, it will ensure the more effective organization of NATO's cyber defence and better management of resources, skills, and capabilities»" (*Warsaw Summit Communiqué…*, 2016).

However, these examples of violations of the national cyberspace of Western powers are just the tip of the iceberg, which hides years of agency activity and Russian attempts to control the media.

© by the author, licensee Łódź University – Łódź University Press, Łódź, Poland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license CC-BY-NC-ND 4.0

Undoubtedly, Ukraine is the main target for cyber crime and cyber attacks by Russia. This is the meaning of the hybrid nature of the war, which, besides the military component itself, also includes powerful information campaigns, disinformation, fake news and hacking activities.

Purposeful cyber attacks against Ukraine began simultaneously with the events of March 2014, when Russia virtually annexed the Crimea by bringing its troops into the peninsula . At the same time as the annexation of the Crimea there began in Ukraine massive DDoS attacks carried out by the so-called CyberBerkut. CyberBerkut is a modern organized group of pro-Russian hacktivists. The group became locally known for a series of publicity stunts and distributed denial-of--service (DDoS) attacks on the Ukrainian government, and western or Ukrainian corporate websites (Soshnikov, 2017).

During the period of 2014–2017, about 6,000 hacker attacks were committed against Ukraine (Prezident, 2016). Undoubtedly, the most powerful of the famous cyber attacks took place on June 27, 2017 (Borys, 2017). A series of powerful cyber attacks using the Petya malware began on 27 June 2017 that swamped websites of Ukrainian organizations, including banks, ministries, newspapers and electricity firms. Similar infections were reported in France, Germany, Italy, Poland, Russia, the United Kingdom, the United States and Australia. ESET estimated on 28 June 2017 that 80% of all infections were in Ukraine, with Germany being the second hardest hit with about 9% (Cyber-attack…, 2017). On 28 June 2017, the Ukrainian government stated that the attack was halted. On 30 June 2017, the Associated Press reported that experts agreed that Petya was masquerading as ransomware, while it was actually designed to cause maximum damage, with Ukraine being the main target (Bajak, Satter, 2017).

The cyber attack was based on a modified version of the Petya ransomware. As with the WannaCry ransomware attack in May 2017, Petya uses the EternalBlue exploit previously discovered in older versions of the Microsoft Windows operating system. When Petya is executed, it encrypts the Master File Table of the hard drive and forces the computer to restart. It then displays a message to the user, telling them their files are now encrypted and to send US$300 in bitcoin to one of three wallets to receive instructions to decrypt their computer. At the same time, the software exploits the Server Message Block protocol in Windows to infect local computers on the same network, and any remote computers it can find.

Security experts found that the version of Petya used in the Ukraine cyber attacks had been modified, and subsequently has been named NotPetya or Nyetna to distinguish it from the original malware. NotPetya encrypted all of the files on the infected computers, not just the Master File Table, and in some cases the computer's files were completely wiped or rewritten in a manner that could not be undone through decryption. Some security experts saw that the software could intercept passwords and perform administrator-level actions that could further ruin computer files. They also noted that the software could identify specific

© by the author, licensee Łódź University – Łódź University Press, Łódź, Poland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license CC-BY-NC-ND 4.0

computer systems and bypass infection of those systems, suggesting the attack was more surgical in its goal. There also has yet to be discovered a "kill switch" as there was with the WannaCry software, which would immediately stop its spread. According to Nicholas Weaver of the University of California, the hackers had previously compromised MeDoc, that is made it into a remote-control Trojan, and then they were willing to burn this asset to launch this attack (Borys, 2017).

During the attack, the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant went offline. Several Ukrainian ministries, banks, metro systems and state-owned enterprises (Boryspil International Airport, Ukrtelecom, Ukrposhta, State Savings Bank of Ukraine, Ukrainian Railways) were affected. In the infected computers, important computer files were overwritten and thus permanently damaged, despite the malware's displayed message to the user indicating that all files could be recovered "safely and easily" by meeting the attackers' demands and making the requested payment in Bitcoin currency.

The attack came on the eve of the Ukrainian public holiday, Constitution Day (celebrating the anniversary of the approval by the Verkhovna Rada (Ukraine's parliament) of the Constitution of Ukraine on 28 June 1996). Most government offices were to be empty, allowing the cyber attack to spread without interference. In addition, some security experts saw the ransomware engage in wiping the affected hard drives rather than encrypting them, which would be a further disaster for companies affected by this. A short time before the cyber attack began, it was reported that an intelligence officer and head of a special forces unit, Maksym Shapoval, was killed in Kiev by a car bomb. A former government adviser in Georgia and Moldova, Molly K. McKew, believed this assassination was related to the cyber attack (McKew, 2017).

On 30 June, the Security Service of Ukraine (SBU) reported it had seized the equipment that had been used to launch the cyber attack, claiming it to have belonged to Russian agents responsible for launching the attack. On 1 July 2017, the SBU claimed that available data showed that the same perpetrators who in Ukraine in December 2016 attacked the financial system, transport and energy facilities of Ukraine (using TeleBots and BlackEnergy) were the same hacking groups who attacked Ukraine on 27 June 2017. This testifies to the involvement of the special services of the Russian Federation in this attack it concluded (Ukraine Security Service Blames Russia For Recent Cyberattack, 2017). Ukraine claims that hacking Ukrainian state institutions is part of what they describe as a "hybrid war" by Russia on Ukraine (Polityuk, 2017).

According to reports cited in January 2018, the United States Central Intelligence Agency claimed Russia was behind the cyber attack, with Russia's Main Intelligence Directorate (GRU) having designed NotPetya (Nakashima, 2018). Similarly, the United Kingdom Ministry of Defence accused Russia in February 2018 of launching the cyber attack, and that by attacking systems in Ukraine, the cyber attack spread and affected major systems in the United Kingdom and

© by the author, licensee Łódź University – Łódź University Press, Łódź, Poland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license CC-BY-NC-ND 4.0

elsewhere. Russia denied its involvement, pointing out that Russian systems were also impacted by the attack (Marsh, 2018).

The reaction of the Ukrainian state to such actions by its northern neighbour was predictable. First of all, the role of the Department of Cyber Police of the National Police of Ukraine was strengthened – the inter-regional territorial body of the National Police of Ukraine, which is part of the structure of the criminal police of the National Police and in accordance with the legislation of Ukraine, ensures the implementation of state policy in the field of combating cybercrime. This division specializes in the prevention, detection, termination and disclosure of criminal offences where the mechanisms of preparation, execution or concealment of which, involves the use of electronic computers (computers), telecommunication and computer Internet networks and systems (Pro utvorennya terytorial'noho orhanu…, 2015). On July 19, 2017, within the framework of the project "Capacity building for cyber police", representatives of the OSCE Project Coordination in Ukraine transferred 194 units of specialized equipment to the units of the cyber police of the National Police of Ukraine (*Kiberpoliciya*…, 2017).

In addition, repeated cyber attacks have prompted the accelerated adoption of a law in Ukraine on the protection of cyberspace, which was adopted on October 5, 2017, but came into force only on May 9, 2018 (Pro osnovni zasady…, 2017).

This Law defines the legal and organizational foundations for ensuring the protection of the vital interests of: a person and a citizen; society and the state, as well as the national interests of Ukraine in cyberspace. To that end, the main goals, directions and principles of state policy in the field of cyber security; the powers of state bodies, enterprises, institutions, organizations, persons and citizens in this area; as well as the main principles of coordination of their work on the provision of cyber security have been laid out in this legislation.

The law explicitly interprets the meaning of the notion of cyberspace – the environment (virtual space), which provides opportunities for communication and/or implementation of social relations, formed as a result of the operation of compatible (connected) communication systems and the provision of electronic communications using the Internet and/or other networks' global data networks (Pro osnovni zasady…, 2017); and cyber defence – a set of organizational, legal, engineering and technical measures, as well as measures of cryptographic and technical protection of information aimed at preventing cyber incidents, detecting and protecting against cyber attacks, eliminating their consequences, restoring the sustainability and reliability of the functioning of communication and technological systems.

The law also stipulates that the main subjects of the national system of cyber security are the State Service for Special Communications and Information Protection of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence agencies, and the National Bank of Ukraine (Pro osnovni zasady…, 2017).

© by the author, licensee Łódź University – Łódź University Press, Łódź, Poland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license CC-BY-NC-ND 4.0

The objects of critical infrastructure are enterprises and organizations that provide services in the economic sphere, in the energy and chemical industry, transport and information and communication industries, utility companies, healthcare, or objects of potentially dangerous technologies and industries. The coordination of activities is carried out by the President of Ukraine with the help of the National Security and Defence Council of Ukraine, which he heads. The Cabinet of Ministers of Ukraine ensures the formation and implementation of state policy in the field of cyber security (Pro osnovni zasady…, 2017).

Thus, the Ukrainian authorities have taken a number of steps to protect the national cyberspace, both normative and practical. However, this does not reduce the level of threats that cyber attacks pose. After all, despite the adoption and enactment of the law on the protection of domestic cyberspace and the creation of the Department of Cyber police and a number of other actions by Ukraine, attempts at cyber attacks on our country have not been stopped.

Authorities in the United States said they broke up a potential digital attack called VPN Filter that affected half a million internet routers and could have caused widespread havoc in Ukraine. The US Justice Department said this was the most recent attack programmed by the Sofacy Group; the Russian hackers – also known as Fancy Bear – are suspected of being behind cyber attacks on several governments, international agencies and infrastructure providers. The largest number of infections was in Ukraine but affected routers in 54 countries, according to the technology company Cisco Systems and antivirus company Symantec, which cooperated with the FBI during the operation (FBI thwarts potential cyberattack…, 2018).

Conclusion

The study of cyberspace as a component of Ukraine's information security gives a number of important conclusions. For a long time, Cyber security and the cyber space of Ukraine was if little interest to domestic researchers and, therefore, civil servants. For more than 20 years, the young Ukrainian state did not waste its efforts on the formation of not only effective and reliable troops, but also information security. The government did not endeavour to strengthen the country's defence, and this probably only compounded its lack of progress in fighting corruption and the dominance of Russian media and intelligence. As a result, in the spring of 2014, after a long confrontation between the regime of Viktor Yanukovych and the citizens of Ukraine, Russia conducted special operations with the aim of annexing the Crimea and facilitating the war in Donbas. An important part of this campaign were raids for information and offensive actions carried out by cyber

© by the author, licensee Łódź University – Łódź University Press, Łódź, Poland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license CC-BY-NC-ND 4.0

Russian hackers. The purpose of which was to paralyse government agencies and influence public opinion in Ukraine through Russian-controlled media.

As a result of prolonged and massive cyber attacks, Ukrainian state structures, banking system, industrial facilities and private business suffered significant material and reputational losses. As a result, Ukraine began to realize the seriousness of cyber security as a component of national security. This contributed to the creation of a cyber police department, national cyber security strategy, the acceptance of a number of regulations on cyber security, and the overall strengthening of public defence for the protection of domestic cyberspace. At the moment, Ukraine is on the way to rethinking the role of cyber security and the formation of a national system for protecting against cyber threats.

References

Bajak, F., Satter, R. 2017. Companies still hobbled from fearsome cyberattack. *USNews*. 30.06.2017, https://www.usnews.com/news/business/articles/2017–06–30/companies-still-hobbled-from-fearsome-cyberattack (accessed 11.11.2019).

Borys, C. 2017. Ukraine braces for further cyber-attacks. *BBC News*. 26.07.2017, https://www.bbc.com/news/technology-40706093 (accessed 11.11.2019).

CShA takozh zvynuvatyly u virusi NotPetya Rosiyu. 2018. *BBC*. 16.02.2018, https://www.bbc.com/ukrainian/news-43082212 (accessed 11.11.2019).

Cyber-attack was about data and not money, say experts. 2017. *BBC News*. 29.06.2017, https://www.bbc.com/news/technology-40442578 (accessed 11.11.2020).

Dubov, D. 2014. *Nat͡sional’nyĭ Instytut Stratehichnykh Doslidz͡hen’*, https://niss.gov.ua/sites/default/files/2015–02/Dubov_mon-89e8e.pdf (accessed 18.01.2020).

FBI thwarts potential cyberattack on Ukraine. 2018. *Deutsche Welle*. 24.05.2018, http://www.dw.com/en/fbi-thwarts-potential-cyberattack-on-ukraine/a-43905916 (accessed 11.11.2020).

Finkle, J., Chiacu, D. 2018. U.S., Britain blame Russia for global cyber attack. *REUTERS*. 16.04.2018, https://www.reuters.com/article/us-usa-britain-cyber/u-s-britain-blame-russia-for-global-cyber-attack-idUSKBN1HN2CK (accessed 11.11.2019).

Kiberpoliciya otrymala 194 odynyci special’noho obladnannya dlya protydiyi kiberzahrozam. 2017. Ministerstvo vnutrishnix sprav Ukrayiny. 19.07.2017, http://mvs.gov.ua/ua/news/9208_Kiberpoliciya_otrimala_194_odinic_specialnogo_obladnannya_dlya_protidii_kiberzagrozam_FOTO_VIDEO.htm (accessed 11.11.2019).

Maksym Rozumnyĭ and Nat͡sional’nyĭ Instytut Stratehichnykh Doslidz͡hen’. 2018. *Rez͡hym Putina : perezavantaz͡hennia – 2018*, Kyyiv: Nat͡sional′nyĭsInstytut Stratehichnykh Doslidz͡hen’.

Marsh, S. 2018. US joins UK in blaming Russia for NotPetya cyber-attack. *The Guardian*. 15.02.2018, https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine (accessed 11.11.2019).

© by the author, licensee Łódź University – Łódź University Press, Łódź, Poland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license CC-BY-NC-ND 4.0

Mason, R. 2017. Theresa May accuses Russia of interfering in elections and fake news. *The Guardian*. 14.11.2017, https://www.theguardian.com/politics/2017/nov/13/theresa-may-accuses-russia-of-interfering-inelections- (accessed 11.11.2019).

McKew, M. 2017. A killing in Kiev shows how the West continues to fail Ukraine. *The Washington Post*. 27.06.2017, https://www.washingtonpost.com/news/democracy-post/wp/2017/06/27/a-killing-in-kiev-shows-how-the-west-continues-to-fail-ukraine/ (accessed 18.01.2020).

Nakashima, E. 2018. Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. *The Washington Post*. 12.01.2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html (accessed 11.11.2019).

The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow 2004, http://www.defenselink.mil/news/Mar2005/d20050318nms.pdf (accessed 18.03.2020).

Nimechchyna zvynuvatyla Rosiyu v kiberataci na uryadovi merezhi. 2018. TCH. 11.04.2018, https://tsn.ua/svit/nimechchina-zvinuvatila-rosiyu-v-kiberataci-na-uryadovi-merezhi-1138362.html (accessed 11.11.2019).

Parahons'kij, B.O., Javors'ka, G.M. 2019. *Ontolohiya vijny i myru: bezpeka, stratehiya, smysl: monohrafiya.* Kyyiv: NISD, https://niss.gov.ua/sites/default/files/2019–07/Monografiya_Ontologiya_print.pdf (accessed 11.11.2020).

Polityuk, P. 2017. Ukraine points finger at Russian security services in recent cyber attack. *Reuters*. 1.07.2017, https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine--points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P (accessed 11.11.2019).

Prezydent zatverdyv Stratehiyu kiberbezpeky Ukrayiny. 16 bereznya 2016. 2016. Prezydent Ukrayiny: oficijne internet-predstavnyctvo, http://www.mil.gov.ua/news/2016/03/16/prezident-zatverdiv-strategiyu-kiberbezpeki-ukraini--/ (accessed 11.11.2020).

Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny. Zakon Ukrayiny № 2163-VIII vid 5.10.2017. 2017. *Vidomosti Verxovnoyi Rady*, https://zakon.rada.gov.ua/laws/show/2163–19 (accessed 11.11.2020).

Pro utvorennya terytorial'noho orhanu Nacional'noyi policiyi: Postanova Kabinetu Ministriv Ukrayiny 2015. *Uryadovyj kur'yer* 831, p. 195.

Soshnikov, A. 2017. Inside a pro-Russia propaganda machine in Ukraine. *BBC Russian*. 13.11.2017, https://www.bbc.com/news/blogs-trending-41915295 (accessed 18.01.2020).

Ukraine Security Service Blames Russia For Recent Cyberattack. 2017. Radio Free Europe. 1.07.2017, https://www.rferl.org/a/cyberattack-ukraine-blames-russia/28589606.html (accessed 11.11.2019).

Uryad Brytaniyi zvynuvatyv Rosiyu u kiberataci na Ukrayinu. 2018. *BBC*. 15.02.2018, https://www.bbc.com/ukrainian/news-43069110 (accessed 11.11.2019).

Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016. 2016. NATO. 6.07.2016,: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en (accessed 11.11.2019).

© by the author, licensee Łódź University – Łódź University Press, Łódź, Poland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license CC-BY-NC-ND 4.0