sciendo

Social Communication
Volume 1 (2021), pp. 124-142
DOI: 10.2478/sc-2021-0012

AWARENESS AND FOLLOWING OF INFORMATION SECURITY POLICIES AS THE MAIN RULE TO PROTECT AGAINST THREATS IN DIGITAL COMMUNICATION PROCESSES. CYBERSECURITY AS THE ARENA OF MODERN WARFARE

Piotr Łuczuk PhD[1]

Abstract

Nowadays, due to the benefits of technological development and the spread of the Internet, various threats have started to be recognized. Still, the awareness of society, especially politicians and state administration in this area is insufficient. This is also evidenced by the fact that initially this topic was not discussed at all in the scientific and even popular literature. The author of the article poses a question: is there, then, an effective method of defense against cyber threats, since their effects can be so disturbing? According to the author, the key to cyber security is the awareness of users of the digital communication process, both at the administrative and social levels.

Key words: cyberspace, cyber security, cyber defense, hacking, trolling, fake news, disinformation, propaganda, ransomware, phishing

Introduction

Not so long ago (January 2019) sensational news spread around the world about one of the largest hacker attacks in the history of the Federal Republic of Germany. As a result of the cyber-attack, data (even documents and records of conversations from the messengers and social media) of almost a thousand German politicians, journalists and celebrities were sent to the network. In such moments, cyber security is number one topic in media all over the world. The more, that it was made by a 20-year-old. Since he

1 Media expert, publicist, cybersecurity expert. Assistant professor at the Department of Social Communication, Public Relations and New Media at the Institute of Media Education and Journalism at UKSW. Staszic Institute expert. Editor-in-chief of FilaryBiznesu.pl. The book debut „Cyberwar. War without ammunition?" (Cyberwojna. Wojna bez amunicji?) appeared in the publishing house Biały Kruk in 2016, https://orcid.org/0000-0002-6275-1550,

easily managed to wreak considerable havoc in the ranks of the German Ministry of Interior and cause panic throughout Germany, it is dreading to think what a group of such hackers could do.

Threats related to cyberspace and digital communications do not apply only to strategic IT systems of a given country. In order to obtain information and classified data, hackers, cybercriminals and secret services are able to use the computers of bystanders and use them to blur traces, confuse clues, and most importantly gain unnoticed access to desired information. The attackers have many options to choose from, including thousands of viruses, bots, worms and the Distributed Denial of Service (DDoS) mechanism used in the 2007 attack on Estonia.

The potential of cyberspace was recognized relatively quickly - during the Cold War. In fact, the entire 1980s were a kind of testing ground. Developers and hackers have worked on behalf of governments to effectively infiltrate the IT networks of antagonized countries. In 1982, the so-called "Logical bomb" (CIA sabotage in Siberia). In 1987, a group of hackers from Germany repeatedly broke into US NASA servers and the Rammstein base.

In the 90s, with the use of the series of cyber-attacks, the opponent's IT systems were already effectively jammed or completely blocked.

Without going into technical and technological details, the most serious cyber threats include: activism (the Internet is used to support the campaign), hactivism (a combination of activism and criminal activities to destroy the enemy's resources) cyberterrorism (politically motivated attack or threat of attack to destroy) infrastructure and intimidation or extortion of actions). An extremely serious type of cyber threat is also the use of the Internet for propaganda and disinformation purposes (fake news, trolling).

Therefore, it is difficult to disagree with the thesis that the arms race known from the Cold War has moved to cyberspace, and subsequent reports of new types of cyberthreats confirm that issues related to this phenomenon from scientific literature and virtual reality have moved to the real world.

During an in-depth analysis in my book *Cyberwojna. War without ammunition?*[2] of the general state of consciousness of individual countries about cybersecurity, I pointed out that there is still a lot to do in the matter of protection against cyberwar. Despite the desire to develop effective cyber defense methods at the national level, a lot of new threats emerged at the turn of the 20th and 21st centuries. Although the first cyberwar in Estonia (2007) was a turning point in this case, it took a long time before effective methods of protection against cyberwar and cyberterrorism began to be implemented. It was not until 2011 at NATO level that the new security strategy in cyberspace was adopted. More precisely, for years the topic of cybersecurity was treated by many military men in science fiction categories, still in military and governmental circles not only in Poland but also in the world, there is an approach that assumes that we are just entering a "new stage of warfare". The head of the British Ministry of Defense said that even a year ago arguing that "we have entered the age of a new type of warfare". Wait a minute! Nowadays it's obvious that we entered this era long ago... We have known these "new warfare" at least since the 1990s.

Although it would seem that nowadays no one should be surprised that along with the benefits of technological development and the spread of the Internet, various types of threats have started to be noticed, all the time the awareness of society, especially politicians and state administration in this regard is small. This is also clearly demonstrated by the fact that initially this topic was not dealt with at all by scientific literature, or even by popular science. Much greater importance to the scale of the problem began to be attached only at the time of a significant increase in individual threats related to cy-

2 Łuczuk P. (2016), Cyberwojna. Wojna bez amunicji?, Kraków 2016.

berspace and the computer environment. Interestingly, until the 1990s, threats in cyberspace did not foretell even the first symptoms of cyberwar and hybrid war, which remain the most serious challenges for domestic and international cybersecurity.

The first cyberwar (Estonia 2007) proved how easy it was to paralyze key state institutions and cause panic among citizens. In turn, the second cyberwar (Georgia 2008) proved, that at that time, war doctrine was being practiced, which after the attack on Ukraine began to be called the "hybrid war". In addition to the conventional strike of troops, hackers found themselves on the battlefield. As a consequence, Georgia was cut off from communication. It is significant that immediately after taking over government websites a massive propaganda campaign began at once.

We met the full strength and effectiveness of hybrid impact in 2014. The combined hit of special forces, information and propaganda campaigns, and cyber-attacks has given alarming results. The armed forces were used to increase military advantage and to seize enemy territory as quickly as possible, with a massive cyber-attack that paralyzed the enemy's defenses.

Is there an effective method of defense against cyber threats, since their effects can be so alarming? Yes of course. The problem, however, is that the key to cyber security is awareness at both administrative and social levels. If we are not aware of the reality of threats in cyberspace, then even the best cyber army will not be able to defend us. It is high time to understand that we are all on the front lines. We are also cyber soldiers.

That is why public debate on cybersecurity and drawing public attention to the seriousness of the situation is so important.

Talking about the importance of the above-mentioned circumstances, in this article the author will analyse selected aspects of cybersecurity, primarily in the aspect of using information as a strategic weapon in hidden and covert international conflicts. The main purpose of this analysis is to answer the question to what extent the average Internet user may be a participant or a victim of the aforementioned activities of disinformation, manipulative nature or threatening information security. The analysis is qualitative; the author will use the case study method, discussing the following examples:

1. The Phenomenon of Wikileaks,
2. The case of Edward Snowden and the disclosure of PRISM and XKeyscore surveillance,
3. The case of large-scale disinformation and fake news operation against Poland,
4. The case of the intensification of cyber threats during the coronavirus pandemic,
5. The case of "Computational Propaganda Research Project".

As the article is exploratory in nature, the author does not make any hypotheses.

The Phenomenon of Wikileaks – link between exposing secrets and cyber defence

Despite the huge publicity, WikiLekas remains one of the most mysterious organizations in the world. For many years, in public awareness, WikiLeaks existed as an almost mythical organization fighting for the disclosure of confidential and secret documents that would help in discovering the manipulation of governments and politicians and of course exposing scandals. How have the creators of WikiLeaks managed to maintain that image over the years?

WikiLeaks project assumes that the information placed on the Internet should be available to everyone, but the web page on which it is placed, must be out of reach for attacks. To enhance the safety and anonymity of broadcasters all the data is distributed

across servers throughout the world and there is no way that all of it could be deleted.[3]

Such scale diffusion of information and global reach ensures that the complete removal of Wikileaks from the Internet and blocking the activities of the organization is simply impossible.

Despite the activities of a large-scale environment Wikileaks is still a riddle. It is hardly surprising, therefore, that while the activities of the organization are held confidential, scandals caused by Julian Assange, Bradley Manning and Edward Snowden quickly hit the headlines.

WikiLeaks came into existence almost in front of our eyes. Therefore, it is up to us to seek answers to two fundamental questions:

1. What exactly is the phenomenon of WikiLeaks?
2. What is the impact on the democratic freedom of speech of scandals and secret information disclosed by WikiLeaks with the general dislike of governments?

Here are the answers...

It is no secret that for many people and institutions (mainly in the area of economy and government administration) the disclosure of classified or confidential information brings disastrous results. From the weakening of the market position through the loss of credibility in the eyes of potential partners and customers, to complete elimination by the competition. Still, however, not everyone is aware of the fact that the effects of a similar power of impact can also be caused by data that we, ourselves, make available on the network. The digital footprint we leave behind on the internet can have far-reaching consequences. Where did the idea to create a website that exposes scandals with global reach and causes an earthquake in the institutions and governments of many countries and permanently modifies the concept of classification come from? If we really care for hiding our own secrets, so do why we want to know others' secrets? The demand for this type of information has been used for years by tabloids and newspapers. Thus, if the rumours about celebrities' life have gained so much popularity, the founder of WikiLeaks decided to go a step further and gave us access to the secrets of which we have not even dreamed of. Focusing on the phenomenon of WikiLeaks, in the first place, we must think about who is behind it all.

The solution to this puzzle, which, for many years, could not be found by the best special forces in the world, suggests Daniel Domscheit-Berg, a person, which along with Julian Assange, was one of the "faces" of the organization. In his book, "WikiLeaks from the inside" he decided to break the silence and told the surprising story of WikiLeaks, which nobody had ever heard. Over the years, the organization has been shrouded in legend. The only thing that was known was that its members were fighting for the disclosure of sensitive and confidential documents and were committed to exposing the manipulation of large corporations, governments and politicians. After some time, it became clear that the method of operation and structure of the organization resembles the techniques used by special forces around the world, with the exception that the full WikiLeaks game operating takes place on virtual reality and uses all the benefits of the Internet.

The universal access to information is among the main objectives of its functioning. Data published on the webpage should be accessible to everyone, and the website must ensure safety and to be out of reach for the attacks. One of the slogans is "time to open the archives", but the organization did not find allies around the world immediately. Initially, even hackers treated WikiLeaks suspiciously. It has even been suggested that the mysterious Julian Assange and his work is a hoax and a trap set by special forces

3 Sontheimer M, We Are Drowning in Material. SPIEGEL Interview with Julian Assange, [online: October 12, 2019] http://www.spiegel.de/international/world/spiegel-interview-with-wikileaks-head-julian-assange-a-1044399.html

and intelligence services, which will help locate and arrest all those trying to lead to the disclosure of highly classified government secrets.[4]

Over time, the project began to gain favour with hackers' environment and the public. Daring actions against scientology cult and the U.S. government as well as the disclosures of diplomatic cables and secret documents from the wars in Iraq and Afghanistan have brought WikiLeaks a significant publicity around the world immediately. There is no doubt that the conduct of operations on this scale requires the preparation of complex structures which are able to quickly evolve and adapt to changing rules set by the system of information flow. One of the biggest phenomenon of WikiLeaks is that the structure details of the world's largest website that exposes scandals with global reach are held in the strictest confidence. To date, little is known apart from the fact that the website provides secret documents from anonymous sources.

To increase the security and anonymity of broadcasters all the data has been distributed to servers located in different parts of the world. This protects the content from being so easily erased and the WikiLeaks informants being disclosed. The existence of hundreds or maybe even thousands of data security copies guarantees WikiLeaks immunity despite its clear dislike for the world powers.

The organization has got many enemies. They will use every opportunity to attack. As it has been determined, to increase the data safety, some of them are stored in Belgium in an old anti-nuclear bunker of the Cold War. Other data are scattered all over the servers in Iceland and other countries where press freedom is protected by the relevant provisions of national law. Only this type of security can guarantee that computers containing secret data will not be seized by anyone, and their content will not be searched.

The name of the organization, which directly relates to the "Wiki" (association of Wikipedia here is not accidental),is also significant. It is software that allows creating and editing web pages directly in a browser window. The use of this fine mechanism that makes changes to the content can indeed be used by all users on the network, but any modification causes an automatic data backup. Understanding the mechanism of Wiki allows us to understand the main idea behind the WikiLeaks. Access to disclosed data has to be unlimited for all who want to read the content. As far as the content is concerned, it is worth paying attention to the second part of the name of the organization. "Leaks" is a jargon term of "leak" the disclosure of secret information, which has so far been revealed to most of the public and access to it, had only a trusted person. WikiLeaks wants to prevent it and does not accept the use of functioning of the so called "controlled leak" in the world of media and politics. As intended by the WikiLeaks project founders, "controlled leaks" used in politics and media are a type of manipulation and are often used for social engineering purposes. Meanwhile, the overriding goal of WikiLeaks is to raise the awareness of the society and provoke citizens to check the source of information on their own. The Assange organization, however, only appeals to this idea when it suits it. It should be noted; however that during its activity WikiLeaks often uses the methods of manipulation. To change its image in the public eye Julian Assange less frequently refers to the idea of hacking and more often refers to the role of investigative and exposing journalism.[5]

Many users can think that WikiLeaks is very similar to Wikipedia. Everyone can draw a text and anyone can change it (...) the leaks authors may submit documents anonymously, and their location can't be determined (...) Members can discuss documents and analyse their credibility. Political weight and credibility of the documents is checked by thousands of people"- as proclaimed in a manifesto published on the first version of the WikiLeaks website.

4 Domscheit-Berg D., WikiLeaks od środka, Warszawa 2012.
5 Görig C., Nord K., Julian Assange – Człowiek, który rozpętał WikiLeaks, Warszawa 2012.

It quickly became clear, however, that the creators of the lofty plans were reviewed. Invented by Assange, the idea of entrusting to hundreds of thousands of volunteers the task to identify and verify the authenticity of the documents turned out to be totally unrealistic and completely failed in practice. The structure of WikiLeaks needed a breakthrough. The system, opened so far, became much more air-tight and the organization took over the complete control of publications.

WikiLeaks was an organization which operated without a face - its actions were shrouded in an aura of mystery for a long time. More and more legends about its founders appeared on the web. After a while, it became clear that this was a deliberate action of WikiLeaks creators who, initially, depended mainly on the fact that the most important were the documents, not the people, involved in its disclosure. There was concern that if someone suddenly found himself in the foreground, he/she would turn attention away from the merits of the case, which was publishing messages of great importance and focused entire splendour itself. Then it was decided that the aura of mystery will be the main feature of the organization.[6]

Over time, however, it turned out that the media is so much interested in the intriguing story of Wikileaks and all kinds of myths about the organization that it could no longer function as usual. The public was curious why an organization that wants to reveal secret documents and calls for unrestricted access to all the information is surrounded by a wall of secrets. Then Julian Assange quickly won the hearts of the audience, winning over many fans around the world immediately. He became a celebrity and told stories about the success of his organization and the importance of disclosure of secret documents by WikiLeaks.

The basic method used by Assange was manipulating and influencing consumers. As soon as the conversation turned to another track and questions were asked about the structure of the organization Assange became much less talkative. To date, WikiLeaks is surrounded by an aura of mystery. Contrary to the idea behind the organization, the basic assumptions regarding the transparency information on the WikiLeaks co-workers and how to finance it are held in the strictest confidence. In the eyes of the public, in the context of WikiLeaks, an image of organization created on the model of a secret brotherhood which is reserved exclusively for selected group of people still works. Although, most of the time, the only contact with the outside world in WikiLeaks was Julian Assange. Later, Daniel Domscheit-Berg appeared on the scene, and he, after leaving the WikiLeaks, decided to reveal many secrets that had been hidden by Assange.

In order to justify their actions related to exposing scandals and disclosure of classified information, Wikileaks began to increasingly use the keyword “freedom of speech”. This technique is still being used these days and it takes all arguments of Assange’s organization opponents. In so doing, “freedom of speech” as their propaganda slogan WikiLeaks executives repeatedly assured that the disclosure of classified information is to be dictated by the desire for transparency and is based on the democratic principle of unrestricted access to information.[7]

In fact, it turned out that the verification of the documents disclosed by WikiLeaks is only a myth. The network hit a lot of “fakes” and for some time the organization seems to be guided by the principle of “publish everything, as long as it was interesting.” When the authenticity of the documents was questioned, people began to wonder whether, in the context of affairs disclosed by WikiLeaks they can actually talk about freedom of speech. Julian Assange’s organization began to fall into trouble and disclosure of confidential information of doubtful authenticity which caused quite a stir in the public

6 Domscheit-Berg D., WikiLeaks od środka, Warszawa 2012.

7 Sontheimer M, We Are Drowning in Material. SPIEGEL Interview with Julian Assange, [online: October 12, 2019] http://www.spiegel.de/international/world/spiegel-interview-with-wikileaks-head-julian-assange-a-1044399.html

space, it was considered more critically by the public. Therefore, the authenticity of the documents recedes into the background, even members of the media began to wonder is it possible that the scandals caused by the WikiLeaks publications were fiction.

And then there was a breakthrough. The whole world heard the information that Bradley Manning gave WikiLeaks hundreds of thousands of secret U.S. documents which he had had access to. When the materials were made available to the media by WikiLeaks, they caused a sensation in 2011. It was found out that among nearly half a million documents there were even the classified war reports from Iraq and Afghanistan. Hundreds of thousands of diplomatic cables and information about prisoners allegedly detained without a trial in Guantanamo Bay prison. Without a doubt, the greatest sensation was induced by a Video showing a helicopter attack in Iraq in 2007 which WikiLeaks entitled "Collateral Murder". During the attack, civilians were killed, including the employees of the Reuters news agency.[8]

25-year-old Bradley Manning, who passed all the documents to WikiLeaks has been found guilty of spying, theft and computer fraud. During the process which has remained at the centre of media interest around the world, Manning's defense argued that their client, by revealing secret information, was guided by honour and he wanted to cause social debate on the activities of the U.S. government to have done everything that "people know the truth." Then the defense also returned to the slogan "freedom of speech".

When the Manning's case was still controversial, a new hero of WikiLeaks appeared – a computer scientist Edward Snowden. It all started with the disclosure of information about the program PRISM. According to information provided to the media by Snowden, the special services have collect data from Google, Facebook, Yahoo, Paltalk, AOL, Skype, YouTube and Apple servers since 2007. I do not need to convince anyone that access to that kind of data means that the special services, that Internet users use, provide information about everything from music, culinary taste, sexual pleasure, to the interests and hobbies, especially for those that may pose a threat to national security.

Snowden quickly became a public enemy, but in the face of support from WikiLeaks further details of the surveillance on the Internet were revealed. Revealing the National Security Agency documents for which, until recently he had worked, Snowden revealed the existence of a system XKeyscore and caused its reach and capabilities outshine even the wake of controversy PRISM. XKeyscore provides access to almost everything that a typical user is doing on the internet and can penetrate the database where information is gathered about what is happening on the network globally. As a result, we can easily find e-mail addresses files downloaded from the internet and even phone numbers and the discussions of the online chat rooms.

Edward Snowden fled the U.S. and is hiding in Russia, where he applied for asylum. Although Snowden virtually disappeared the problem remained.

Hacking, trolling and all the rest

Cyberspace and technological innovations usage for propaganda purposes is not a secret anymore. In addition to direct cyber-attacks on IT structures, servers and even information services, propaganda on the Internet is the main pillar of the new war doctrine - the doctrine of hybrid war. Although there has been talk of online trolls and propaganda for a long time, the real breakthrough in this case took place only a few years ago. In 2015, the media received sensational news. The operation of the "troll factory" in St. Petersburg was disclosed. The Internet Research Agency was officially active there, headed by an oligarch Yevgeny Prigozhin - privately a close friend of Vladimir Putin. In fact, the agency employed over 300 "bloggers" who were tasked with publishing up to

8 Domscheit-Berg D., WikiLeaks od środka, Warszawa 2012.

30,000 during the "business day" praising Russia and Putin himself posts on Facebook, Twitter, as well as on news portals both in Russia and abroad. Since then, no one has any illusions that there are many more such places in Russia alone.

Analysing a large-scale operation against Poland gives us a lot to think about. First of all, an army of online trolls was thrown into the fight. According to the report of the Governmental Computer Incident Response Team CERT.GOV.PL, 2014 was the hardest year to date, if we consider the number of cyber-attacks on government institutions. In addition to extremely dangerous attacks on the servers of the National Electoral Office, the structures of the Stock Exchange and government services, there was a rapid increase in the activity of the so-called Internet trolls acting on behalf of Russia, and often simply paid by special services to carry out propaganda actions that look like a grassroots initiative. Therefore, there were justified fears that elements of the hybrid war began to be used against Poland.[9]

The content of the report shows that out of 12017 registered notifications, as many as 7498 were considered as incidents. Comparison of this data with previous years points to a significant increase in infected devices that were part of the botnet network controlled by hackers. The highest increase in alerts regarding cyber-attacks was found in cases classified as high and medium priority. This data already shows the scale of the threat, but if we add to this information about a significant increase in long-term, massive attacks, carried out using technologically advanced equipment and complex methods, fears will be justified that cyber-attacks themselves may be a prelude to something much more dangerous. However, the biggest concern after reading the report is the fact that the CERT.GOV.PL team has already found the first symptoms of a hybrid war against Poland. It was about a sudden increase in social media, discussion forums and news sites of all kinds of propaganda activities and large-scale disinformation. To a large extent, such cases concerned the conflict in Ukraine and focused mainly on information related to participation in the fighting of Russian troops.[10]

A significant intensification of threats from cyberspace was also noted in the following years. Referring to the latest Cisco Umbrella data (a security service delivered in the cloud), which I managed to find during the research, it is difficult to ignore the information that only in the context of the threat of phishing (extortion or theft of confidential data) 86 percent of organizations are at risk. Of course, depending on the industry and the structure of the company, individual types of threats and the forms of cyber-attacks themselves will differ from each other. It is no secret that the financial sector is most at risk from all kinds of identity and confidential data theft (phishing, identity theft, spoofing online banking sites and hacking bank accounts), while the entire manufacturing sector grapples blackmail in the form of ransomware attacks (blocking access to a computer or data with a ransom demand). Taking into account the coronavirus pandemic, a significant intensification of this type of activity can be seen.

When it comes to security, deciding about the allocation of resources is crucial. In order to do this optimally, companies need to know which threats in this field are most likely to appear in their organizations in the near future and what impact they may have on them. The challenge is that the peloton of the most active dangers changes very dynamically, and the frequency of individual attacks varies greatly. That is why it is so helpful to know about the key trends in the threat landscape. It can provide ammunition for effective defense and information on where to best allocate resources.

Cisco experts, when analysing traffic from the Umbrella platform, look at the activities that occur in the threat environment, thus, analysing traffic on infected sites and

---

9 CERT.GOV.PL, Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku, [online: October 12, 2019] http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html.

10 Dmochowski A., Cyberwojna Putina, w: Gazeta Polska nr 15(1131) z 15 kwietnia 2015 roku.

DNS protocols. They do this by looking at the organization as a whole, and only in the next step do they analyse the number of endpoints that can potentially connect to malicious sites and the number of queries that these sites receive. These actions give you an insight into how many users click infected links in your email, how active RAT (remote access Trojan) viruses are, or whether crypto mining continues to grow. The collected data can be a source of knowledge on where to invest more resources, e.g. for security training or areas where guides on how to hunt cyber threats should be built.

By analysing DNS queries sent to suspicious domains and those infected with specific viruses in the period from January to December 2020, Cisco experts reviewed a number of trends related to cyber threats. On this basis, they distinguished those which organizations may encounter most often.

According to Cisco Umbrella data, in 86 percent of organizations, at least one user tried to connect to a phishing site, possibly by clicking a link in the message.

Interestingly, similar scenarios appear in other categories:

- In 70 percent of organizations, there were users who were presented with malicious ads in their browser.
- 51 percent of companies experienced ransomware-related activity.
- 48 percent of organizations have detected information-stealing malware.

The troll factory - it's not a fairy tale

Considering the analysis of propaganda activities carried out via the Internet, two basic groups should be distinguished: online trolls. The first of them are the Internet users performing their tasks on behalf of their work and they are paid for it. Their duties include placing entries and comments intended to show the "principal" in a positive light, based mainly on facts - only which properly selected and manipulated. The second group is made up of internet users called the so-called "Useful idiots". Their duties include setting up profiles in social media and blogging, where they should display properly prepared and crafted information. This group also includes all those who, unaware of the entire operating game, disseminate read information further, believing in its authenticity and thus contributing to its credibility in the eyes of the public.

The CERT.GOV.PL team warned that both social media and the entire internet are eagerly used to support conventional military, intelligence and propaganda activities. Analysing these types of cases, administrators of social networking sites and the largest news sites in the country noticed that in many cases entries appearing on the internet was almost the carbon of those appearing in other websites. All of them were published almost simultaneously. Initially, they were characterized by poor Polish language, ridiculed by other Internet users, but over time their quality in terms of language improved significantly. The CERT.GOV.PL team warned that the increase in this type of behaviour has long exceeded a level close to natural and constitutes an increasingly serious threat in the information war.[11]

However, the real sensation was revealed by the disclosure of the functioning of the "troll factory" in St. Petersburg. The exact mechanism of operation of the Kremlin-paid Internet trolls was quite simple: The officially employed people as bloggers were supposed to set up fictitious accounts on social networks. Then they started their activities on the Internet using many fictitious identities. In this way, they generated and published hundreds of entries and comments, intensifying the information noise around the selected topic. What is extremely important, trolls usually connecting to the Internet through a

11 CERT.GOV.PL, Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku, [online: October 12, 2019] http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html.

network of proxy servers. This is to be the guarantor of anonymity, and in the worst case, effective blurring of traces and misleading the lead in reaching the source of information. The use of a proxy is to create the impression that entries are published by persons who have no connection with Russia and are not on the territory of that country. From the point of view of an ordinary user, unaware of the entire propaganda machine, everything looked as if Internet users were actually in a country where propaganda was being undertaken. The "troll factories" thriving like thriving marketing companies were basically able to flood the internet around the clock with comments of more or less pro-Russian meaning. Often, to authenticate the whole action, individual trolls even entered into a polemic with each other. A typical action was also a group reporting to social network administrators of alleged abuses and a request to block or remove entries deviating from the propaganda line.

Unfortunately, the recognition of entries written by commissioned Internet trolls from those distributed only by naive Internet users has proved increasingly difficult over time. Therefore, it was difficult to find incontrovertible evidence of using elements of information warfare and manipulation on the Polish Internet. A reliable assessment of this phenomenon was undertaken by Andrzej Gołoś, a sociologist from the ARC Rynek i Opinia marketing agency, who decided to treat the entire problem from the scientific point of view.

Gołoś began his research by trying to measure the real presence of Russian influence on the Polish Internet. He also analysed a number of discussions taking place there and traced the content of hundreds of comments. Some regularities were found in this way. It turned out that pro-Russian entries accounted for 39 percent, and in only 10 of the most popular articles on Ukrainian-Russian subjects as many as 70 percent. Of all the analysed entries, pro-Ukrainian ones constituted 32 percent, and in the 10 most popular articles alone there were only 17 percent. The same pattern could be seen in discussions on social media. As soon as any pro-Ukrainian entries appeared, there was an avalanche of pro-Russian voices. After a few hours, the attack ended and the situation returned to normal.

Similar observations were also made after analysing the entries appearing under texts about Russia on the CNN and BBC websites. This mechanism of action means that numerous forces were thrown into the cyberspace war to prepare the ground for any subsequent phases of the hybrid war. It would be naïve to say that such coordinated actions are only a coincidence.

In addition to the "propaganda soldiers" themselves, the weapons they use in cyberspace are extremely important. Most often it is generating information noise in the form of spreading a large amount of false information, like fake news. There are several reasons for the huge firepower of fake news. First of all, the mere "bombing" of the internet (mainly social media) with false information about a subject of high public interest makes it much more difficult to find facts and reach the source of news in the flow of information. Secondly, there will always be some percentage of Internet users who will uncritically believe in Internet propaganda, and sometimes even will provide this type of information further, only increasing their reach. Thirdly, publishing fake news at the right time can help divert public attention from other topics.

Russia is well aware of the potential of digital propaganda. On May 9, 2017, Vladimir Putin signed a decree "On the strategy for the development of the information society in the Russian Federation for 2017-2030." The main goal of the document is the need to "create conditions for shaping the knowledge society in the Russian Federation." Experts from the Center for Propaganda and Disinformation Analysis operating in Poland have no doubt, however, that Russia is in fact "preparing for a total information war with the world," which is planned as a protracted conflict. The Russian strategy focuses on two main threads: the first is to extend the authorities 'control over the internet within the territory of the Russian Federation, while the second is to plan to displace foreign infor-

mation and communication technologies and replace them with Russian counterparts. There is one more intriguing thread in the content of the document. It concerns the development of a mechanism to regulate the functioning of the media and the principles and methods of accessing information. Interestingly, from the document we learn that, in line with the intention of the creators of the strategy, in the category of media cannot be considered Internet TV, social networks, websites and instant messengers. This legal approach gives the Kremlin the possibility of easily limiting access to information transmitted via digital media, or limiting access to the Internet in general, and creating something like an "information bubble" in which Russian society will exist.

Researchers have also been interested in the subject of propaganda and disinformation in the media and on the Internet for some time. Extremely relevant analyses have been carried out at Oxford University. The "Computational Propaganda Research Project" carried out by the Oxford Internet Institute showed how dangerous it can be to ignore the risks associated with online troll activities, spread fake news, and the information and propaganda war, which is already a permanent feature of the hybrid war. A team of twelve researchers in nine countries analysed the use of social media to manipulate public opinion. Based on millions of entries from top social networks collected in 2015-2017, a really alarming picture emerges. Scientists analysed entries published during major social tensions, presidential and local elections, political crises and incidents in the field of national security in Brazil, Canada, China, Germany, Poland, Taiwan, Russia, Ukraine and the USA.

It turns out that, in addition to using the "human factor" for propaganda purposes, some automation of war and disinformation in cyberspace can be seen more and more often. The place of Internet trolls is slowly taken by specially developed programs - bots, which are algorithms that allow you to significantly improve the mechanism of disinformation and the deliberate dissemination of false information through social media. The use of bots allows you to significantly reduce the cost of propaganda, while expanding the power of fake news. Today, there is no doubt that social media have become key platforms for social engagement and at the same time act as key news channels. In addition, social media are currently the basic type of media that shape the political awareness and identity of many young people around the world. In many countries, websites such as Facebook and Twitter have monopolized the entire segment of public life. A study at the University of Oxford showed that in most countries, during elections, social media are the main channel for exchanging information on political views. In addition, social media has been shown to be widely used as a tool for manipulating public opinion, although this happens in different ways. For example, in countries under authoritarian rule, social media is an essential means of social control. In democracies, on the other hand, social media are most often used to spread information, including propaganda and impact on specific segments of society.

The most shocking data relate to propaganda actions directed against Ukraine and Poland. It turns out that the analysis of social media in Ukraine confirms the conduct of one of the most advanced propaganda operations around the world. Over the years 2015-2017, numerous disinformation and propaganda campaigns were conducted against Ukrainian citizens via social networking sites VKontkte, Facebook and Twitter. Interestingly, the first cases of disinformation campaigns were found in this country in the early 2000s.

Oxford researchers have also shown that authoritarian governments direct propaganda and disinformation campaigns on the internet that are not only directed at their own people, but also at citizens of other countries. For example, Chinese campaigns were largely directed at political actors in Taiwan, and Russia's campaigns targeted political actors in Poland and Ukraine.

As can be seen, the unleashing of an information war on a large scale by using cyberspace to spread propaganda and even causing panic among the local population

can have far-reaching consequences. It is therefore crucial to develop appropriate mechanisms for responding to this type of action.

In order to fully understand the scale of the threat, it is worth looking at the latest research on Internet access in Poland. In the August issue of the PC World magazine, Ludwik Krakowiak cites Eurobarometer statistics, which show that in 2011 only 59% of households in the country had Internet access, and only 5.5 million could have a Facebook account Poles. Amazingly intriguing, these data have changed dramatically for six years. It turns out that even 80% of households across the country have access to the Internet. It is estimated that the number of Internet users in Poland already exceeds 30 million people. However, according to data compiled by Gemius / PBI, 22.6 million Poles already have their Facebook account. Almost universal access to the Internet in the country, apart from many undeniable benefits, is also associated with a considerable threat. The data presented above leave no doubt that over 30 million Polish Internet users are a fairly easy target for propaganda specialists. Starting from advertising and marketing, through media misinformation, to the world of great politics, Internet users are exposed to various forms of manipulation on a daily basis.

Extremely important analyses were carried out at the University of Oxford. Oxford Internet Institute project the "Computational Propaganda Research Project" has shown how dangerous it can be to ignore the risks associated with online troll activities, spreading fake news, and the information and propaganda war, which is already a permanent feature of the hybrid war. A team of twelve researchers in nine countries analysed the use of social media to manipulate public opinion. One of the researchers - Robert Gorwa - as part of his part of the project, in the study "Computional Propaganda in Poland: Falsce Amlifiers and the Digital Public Sphere" looked at the mechanisms of internet propaganda. He pays special attention to three types of information warfare: bots, trolling and fake news. The term "bots" should be understood as computer algorithms, machines whose main task is to improve the mechanism of account management in social media. Interestingly, the bots can be programmed in such a way as to resemble other Internet users. It is increasingly difficult to distinguish between content distributed by bots and content created by network users. Obviously, the computer program is not able to cope with all tasks, which is why Internet trolls' services enjoy unflagging interest from propaganda specialists. Considering the analysis of propaganda activities carried out via the Internet, two basic groups should be distinguished: online trolls. The first of them are Internet users performing their tasks on behalf of their paid work. Their duties include placing entries and comments intended to show the "principal" in a positive light, based mainly on facts - only which properly selected and manipulated. The second group is made up of internet users called the so-called "Useful idiots". Moreover, in addition to the mechanism of functioning of this type of Internet users described last month, it is worth adding the intriguing findings from Robert Gorwa's report. The Oxford researcher in his study describes the mechanism of creating artificial identities on the Internet in order to spread large-scale propaganda activities. Gorwa refers to information obtained from a Polish communications and marketing specialist who, for obvious reasons, reserves anonymity. As an employee of a company dealing with creating false accounts and entire identities on the Internet for years, he has extremely valuable knowledge in the use of this type of mechanism in various branches of marketing - from trade to political marketing. It turns out that only this one company was able to create almost 40 thousand artificial identities in just 10 years. It is worth mentioning here that each such fake internet user had unique attributes assigned to him, a relevant history and a group of accounts in social media. Fake users have also been given unique IP addresses so that their online activities do not arouse anyone's suspicions and are reminiscent of standard

Internet activity.[12]

The process of creating a fake user resembles the espionage activities of special services, especially the process of functioning of the so-called illegal or sleepyheads (spies who, after recruiting and developing the right legend, sometimes wait several to a dozen or so years "in dormancy" for orders to start operations). In the case of the Internet, creating a false identity is much simpler and much less risky. Such an artificial creation is primarily to act as a warmonger, who at the right moment will direct the discussion on Internet forums and popular services to specific tracks. Everything starts, however, with the acceptance of a specific order. Often, it is the company or political formation that accurately defines the "psychological profile" and main goals. Then a team of specialists comes into action, which creates the right number of artificial Internet users. Personal data is invented, stories and biographies are developed, and unique email addresses and social media profiles are created for everyone. In order to authenticate a given "person", even properly crafted photos are published and entries are regularly added on various topics that are in the sphere of interest of the subject and in close relation with the given version of the legend. After building a history of activity on a given account, the artificial surfer is fully ready for action. As it turns out in companies dealing with this type of activity, each employee is able to control / monitor in parallel up to fifteen of these types of artificial accounts. These types of activities significantly impede the user's identification as an artificial creation, and the use of this mechanism for propaganda and disinformation purposes is much more effective in the long run than using bots. Compared to the use of bots, the creation of artificial accounts controlled by man gives almost unlimited possibilities, and above all allows for reliable interaction with other Internet users. In this model of information warfare, bots are mainly used to conduct agitation, spread fake news on a large scale or send spam, as well as to discredit any opponents.

The manipulation scenario

In this context, the public manipulation model developed by Trend Micro - an international company specializing in security of the IT sector - is extremely interesting. It consists of eight basic stages:

Stage 1 - reconnaissance

It assumes collecting information about the planned action and analysing the target recipients. As part of these activities, information is gathered about people potentially interested in the topic of the activities, their loyalty, as well as knowledge in a given area.

Stage 2 - reinforcements

It assumes the preparation and preparation of a key history and own version of the facts, which are then to be forwarded to the target recipients. This stage also involves the preparation of additional fake news supporting the key story and the development of various "alternative versions" of the event. This leads to the creation of information noise around a given topic and the literal flooding of the internet with a manipulated message.

Stage 3 - delivery

It assumes the distribution of previously prepared, crafted materials and fake news through specific communication channels, e.g. social media or traditional media. In addition, activities at this level also provide for the possibility of using all possible channels

12 Gorwa, R.: Computational Propaganda in Poland: False Amplifiers and the Digital Public Sphere, [online: October 12, 2019] http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Poland.pdf.

for distributing fake news, including primarily manipulation and disinformation using bot networks and troll internet farms.

Stage 4 - operation

It assumes constant heating of the topic in social media and strengthening the credibility of fake news by fuelling the moods of specific social groups and supporters, as well as activists who identify with the promoted idea.

Stage 5 - fixing

One of the key steps to increase the credibility of the entire propaganda campaign. It assumes reaching the largest possible target group, including critically oriented people. The main goal at this stage is to force users to interact and the so-called viral effect. The more people write / talk about a topic, the more people read and hear about it and in this way the number of potential supporters of the promoted idea or the group of people who simply believe in the fake news propagated in this way will increase. The impression of a quarrel on a given topic is often used here, and entries with positive and negative overtones are prepared in order to raise the rank of fake news and draw the attention of initially critical persons.

Stage 6 - maintaining commitment

It assumes the introduction to the game of "supporting stories" prepared at earlier stages and fuelling activities at the highest possible level.

Stage 7 - moving from words to deeds

It assumes the implementation of the actions announced at the beginning of the action. It may result in additional motivation of the target recipient and lead, for example, to the implementation of actions assumed by the initiators of the campaign, e.g. organization of a rally, manifestation, appeal, open letter.

Stage 8 - blurring the tracks

It assumes the fastest possible distraction of public opinion from a given problem and its transfer, appropriate canalization on a completely different topic. In extreme cases, this stage is even associated with complete negation and obliteration of the memory of all previous activities in order to calm social moods. Such action ensures full control over the situation and gives the opportunity to efficiently "switch" public attention to other tracks, subject to the possibility of reactivation of the target group if the need arises in the future.

Summary

As mentioned in the introduction, the main purpose of this analysis is to answer the question to what extent the average Internet user may be a participant or a victim of the activities of disinformation, manipulative nature or threatening information security. The case study method was applied in order to help to find an answer to this question. The author discussed the following examples:

1. In case of the Phenomenon of Wikileaks, it turned out that the verification of the documents disclosed by this organization was only a myth. The network hit a lot of "fakes" and for some time the organization seemed to be guided by the principle of "publish everything, as long as it was interesting." It turned out that the disclosure of confidential information of doubtful authenticity caused quite a stir in the public space, and was received more critically by the public.

2. In the case of Edward Snowden and the disclosure of PRISM and XKeyscore surveillance, the most astonishing fact is that given the importance of the information disclosed and the potential dangers of large-scale surveillance and restriction of the right to privacy, the subject quickly disappeared from public debate. Snowden revealed the existence of a system XKeyscore and caused that its reach and capabilities outshine even the wake of controversy PRISM. XKeyscore provides access to almost everything that a typical user is doing on the internet and can penetrate the database where information is gathered about what is happening on the network globally. Edward Snowden fled the U.S. and is hiding in Russia, where he applied for asylum. Although Snowden virtually disappeared, the problem of global surveillance remained.

3. The case of large-scale disinformation and fake news operation against Poland, leads us to the conclusion that we can already find the first symptoms of a hybrid war against Poland. It was about a sudden increase in social media, discussion forums and news sites of all kinds of propaganda activities and large-scale disinformation.

4. The case of the intensification of cyber threats during the coronavirus pandemic, leads us to the conclusion that according to Cisco Umbrella data, in 86 percent of organizations, at least one user tried to connect to a phishing site, possibly by clicking a link in the message. Interestingly, similar scenarios appear in other categories such as ransomware-related activity and information-stealing malware.

5. The case of "Computational Propaganda Research Project" proves that the process of creating a fake user resembles the espionage activities of special services, especially the process of functioning of the so-called illegal or sleepyheads (spies who, after recruiting and developing the right legend, sometimes wait several to a dozen or so years "in dormancy" for orders to start operations). In the case of the Internet, creating a false identity is much simpler and much less risky.

It turns out that, in addition to using the "human factor" for propaganda purposes, some automation of war and disinformation in cyberspace can be seen more and more often. The place of Internet trolls is slowly taken by specially developed programs - bots, which are algorithms that allow you to significantly improve the mechanism of disinformation and the deliberate dissemination of false information through social media. The use of bots allows you to significantly reduce the cost of propaganda, while expanding the power of fake news. Today, there is no doubt that social media have become key platforms for social engagement and at the same time act as key news channels. In addition, social media are currently the basic type of media that shape the political awareness and identity of many young people around the world. In many countries, websites such as Facebook and Twitter have monopolized the entire segment of public life.

At this point, the question probably arises: "Can we defend ourselves against this?" The only sensible solution seems to be the widespread use of the principle of limited trust. In the Internet age, checking facts and sources of information takes just a few moments. Such a high susceptibility to fake news means, therefore, that often we are just... too lazy.

References:

ADAMSKI A. (2012), Mass media vs. public and national safety, w: Ad Alta Journal of Interdisciplinary Research volume 2, issue 2, s. 7-10.;

ADAMSKI A. (2012), The Mass Media and National and Public Safety in the Context of Terrorism, w: Akimjak A. (red), Disputationes Scientificae, Ružomberok 2012, s. 154-163;

ARQUILLA J., RONFELDT D. (1993), Cyberwar is coming!, International Policy Department, RAND Corporation;

BALL J., BECKETT CH. (2012), WikiLeaks, New York City;

BARBER B. R. (2007), Dżihad kontra McŚwiat, Warszawa;

BARBER. B. R. (2005), Imperium strachu. Wojna, terroryzm i demokracja, Warszawa;

BARBER B. R. (2009), Skonsumowani, Warszawa;

BENDYK E. (2012), Bunt sieci, Warszawa;

BRENNER J. (2011), America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare, London;

BURDEA G., COIFFET P. (2003), Virtual Reality Technology, New Jersey;

CAMPEN A., DEARTH D. (1996), Cyberwar: Security, Strategy, and Conflict in the Information Age, Virginia;

CAMPEN A., DEARTH D. (1998), Cyberwar 2.0: Myths, Mysteries & Reality, Virginia;

CAMPEN A., DEARTH D. (2000), Cyberwar 3.0: Human Factors in Information Operations and Future Conflict, Virginia;

CARR J. (2011), Inside Cyber Warfare: Mapping the Cyber Underworld, Sebastopol;

CHIRILLO J. (2002), Hack Wars. Tom 1. Na tropie hakerów, Gliwice;

CHIRILLO J. (2002), Hack Wars. Tom 2. Administrator kontratakuje, Gliwice;

CLARKE R., KNAKE R. (2010), Cyber War: The Next Threat to National Security and What to Do About It, New York;

DENNING D. (2002), Wojna informacyjna i bezpieczeństwo informacji, Warszawa;

DOMSCHEIT-BERG D. (2012), WikiLeaks od środka, Warszawa;

DOROZIŃSKI D. (2001), Hakerzy. Technoanarchiści Cyberprzestrzeni, Gliwice;

DRABIK L., KUBIAK-SOKÓŁ A., SOBOL E. (2016) (red), Cyberprzestrzeń w: Słownik Języka Polskiego, Warszawa;

FILIPKOWSKI W., MĄDRZEJOWSKI W. (2011), Biały wywiad. Otwarte źródła informacji - wokół teorii i praktyki, Warszawa;

GREENBERG A. (2012), This Machine Kills Secrets: How Wikileakers, Cypherpunks, and Hacktivists Aim to Free the World's Information, Valley Village;

GIANELLI A., TORNIELLI A. (2006), Papieże a wojna, Kraków;

GIBONEY T.B. (2013), CyberWar Vengeance, Amazon Digital Services;

GÖRIG K., NORD K. (2012), Julian Assange. Człowiek, który rozpętał Wikileaks, Warszawa;

GLENNY M. (2013), Mroczny rynek. Hakerzy i nowa mafia, Warszawa;

GLIWIŃSKI M., DYLEWSKI R. (2011), Raport specjalny szkoły hakerów. Część 1. Ataki na sieci bezprzewodowe, Kwidzyn;

JORDAN T. (2011), Hakerstwo, Warszawa;

JONSCHER CH. (2001), Życie okablowane, Warszawa;

KUBIAK M. (2005), „Edukacja Humanistyczna w wojsku – Nowe wojny epoki globalizacji", Warszawa;

LIBICKI M. (2009), Cyberdeterrence and Cyberwar, Santa Monica;

LIEDEL K. (2010), Zarządzanie informacją w walce z terroryzmem, Warszawa;

LIEDEL K., MOCEK S. (2010), Terroryzm w medialnym obrazie świata, Warszawa;

LIDERMAN K. (2008), Analiza ryzyka i ochrona informacji w systemach komputerowych, Warszawa;

LITTMAN J. (2004), Ścigany. Rozmowy z Kevinem Mitnickiem, Gliwice;

LIDERMAN K. (2012), Bezpieczeństwo informacyjne, Warszawa;

LOWENTHAL M. (2011), Intelligence, Thousand Oaks California;

ŁUCZUK P. (2011), Odwaga bycia katolikiem w społeczeństwie McŚwiata. „Zderzenie wizji" Benjamina Barbera, Samuela Huntingtona i George'a Weigela (mps), Warszawa; (praca do wglądu w Archiwum Prac Dyplomowych UKSW).

ŁUCZUK P (2011), Pracuję nad... Cyberwojną, mps;

ŁUCZUK P (2013), Cyberzagrożenia – czyli co czyha na dzieci w sieci. Kilka słów o kontroli rodzicielskiej, mps;

ŁUCZUK P (2013), WikiLeaks – przeciek kontrolowany czy globalny potop? Manipulacja wizerunkiem największego portalu demaskatorskiego, mps;

ŁUCZUK P (2013), The Phenomenon of Wikileaks - Exposing Scandals and Secret Information, and Democratic Freedom of Speech, mps;

ŁUCZUK P (2012), World War Web – manipulacja wojną o wolność sieci, Opole;

MAJKA J. (1969), Zagadnienie wojny i pokoju w nauce Soboru Watykańskiego II, [w:] B. Bejze, W nurcie zagad-

nień posoborowych, t. 3, Warszawa 1969.

MAZANEC B. M. (2015), The Evolution of Cyber War: International Norms for Emerging-Technology Weapons, Nebraska, s.10-20.

MURRAY L. (2014), Psychologia wojny. Strach i odwaga na polu bitwy, Warszawa;

MITNICK K., SIMON, W. L. (2012), Duch w Sieci, Bielsko-Biała;

MITNICK K., SIMON, W. (2006), Sztuka infiltracji, Warszawa;

MITNICK K., SIMON, W. (2003), Sztuka podstępu, Gliwice;

NICKS D. (2012), Private: Bradley Manning, Wikileaks, and the Biggest Exposure of Official Secrets in American History, Chicago;

Opracowanie zbiorowe, Analiza Informacji. Teoria i praktyka, Warszawa 2012.

Opracowanie zbiorowe, Bezpieczeństwo w XXI wieku. Asymetryczny świat, Warszawa 2011.

Opracowanie zbiorowe, Internet Agresja i Ochrona, Warszawa 2005.

Opracowanie zbiorowe, Szkoła Hakerów, Kwidzyn 2009.

Opracowanie zbiorowe, Hakerzy atakują. Jak podbić kontynent, Gliwice 2004.

Opracowanie zbiorowe, Hakerzy atakują. Jak przejąć kontrolę nad siecią, Gliwice 2004.

POINDEXTER D. (2013), The Chinese Information War: Espionage, Cyberwar, Communications Control and Related Threats to United States Interests, Jefferson;

POULSEN K. (2011), Haker. Prawdziwa historia szefa cybermafii, Kraków;

RATTRAY G. J. (2004), „Wojna strategiczna w cyberprzestrzeni", Warszawa;

RID T. (2013), Cyber War Will Not Take Place, Oxford;

SEIBEL P. (2011), Sztuka kodowania. Sekrety wielkich programistów, Gliwice;

SINGER P.W., FRIEDMAN A. (2014), Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford;

STALLINGS W. (2012), Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, Gliwice;

STALLINGS W. (2011), Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii, Gliwice;

STANKOWSKA I. (2010), Ustawa o Ochronie Informacji Niejawnych. Komentarz, Warszawa;

STIENNON R. (2010), Surviving Cyberwar, Lanham;

STROSS R. (2009), Planeta Google. Cel: Skatalogować wszystkie informacje świata, Warszawa;

TOFFLER A. (2007), Szok przyszłości, Przeźmierowo;

TOFFLER A. (2007), Rewolucyjne bogactwo, Przeźmierowo;

TOFFLER A. (2006), Wojna i antywojna, Poznań;

WALZER M. (2006), Spór o wojnę, Warszawa;

WANG W. (2004), Tajemnice internetu, hackingu i bezpieczeństwa, Gliwice;

WASILEWSKI J. (2013), Zarys definicyjny cyberprzestrzeni, w: Przegląd Bezpieczeństwa Wewnętrznego nr 9 (5), s. 225-234.

WILLIAMS S. (2004), W obronie wolności, Gliwice;

WOŹNIAKOWSKI H. (2001), Cywilizacje i terror, „Znak" nr 558, ss. 4-12.

ZALEWSKI M. (2005), Cisza w sieci, Gliwice;

Additional literature:

BIAŁAS A. (2007), Bezpieczeństwo Informacji i Usług w Nowoczesnej Instytucji i Firmie, Warszawa;

BIAŁEK T. (2005), Terroryzm: manipulacja strachem, Warszawa;

BRODA M. (2008), Konflikty współczesnego świata, Warszawa;

BRYK A., Cywilizacja amerykańska, „Znak" nr 596, ss. 13-17.

CASTELS M. (2008), Siła tożsamości, Warszawa;

CIALDINI R. (2007), Wywieranie wpływu na ludzi. Teoria i praktyka, Gdańsk 2007.

DMOCHOWSKI A, Cyberwojna Putina, w: Gazeta Polska nr 15(1131) z 15 kwietnia 2015 roku. Erickson Jon.

Hacking (2004), Sztuka penetracji, Gliwice;

EVERARD J. (2000), Virtual States: the Internet and the boundaries of the nation-state, Londyn;

FILIPIAK A., Europa i Ameryka – dwie cywilizacje? „Znak" nr 596, ss. 36-52.

FRIEDMAN G. (2009), Następne 100 lat – Prognoza na XXI wiek, Warszawa;

FUKUYAMA F. (2006), Ameryka na rozdrożu. Demokracja, władza i dziedzictwo neokonserwatyzmu, Poznań;

GIBSON W. (1982), Burning Chrome, w: Omni (7/1982), New York City;

GIBSON W. (2001), Neuromancer, Warszawa;

GOBAN-KLASS T. (2009), Media i terroryści. Czy zastraszą nas na śmierć?, Kraków;

GROSSMAN D. (2010), O zabijaniu Warszawa;

HOWARD M., LE BLANC D. (2006), Viega J., 19 grzechów śmiertelnych, Warszawa;

KISIELEWSKI T. (2004), Imperium Americanum?: międzynarodowe uwarunkowania sprawowania hegemonii, Warszawa;

KISIELEWSKI T. (2008), Wojna Imperium. Większy Bliski Wschód w amerykańskiej wojnie z terroryzmem, Warszawa;

MCCLURE S. (2013), Scambray J., Kurtz G., Vademecum hackingu. Skuteczna obrona sieci przed atakami, Warszawa;

MCCONNEL M., War in the Fifth Domain, „The Economist" z 1 lipca 2010 r.

PAOLUCCI H. (1962) (red), The Political Writings of ST. Augustine, Chicago 1962.

SKALMOWSKI W. (2002), Dobrzy kontra źli, „Znak", nr 560, ss. 96-102.

SUN ZI (2010), Sztuka Wojenna, Kraków.

Online resources:

AHMARI S., The View From NATO's Russian Front, WAll Street Journal, http://www.wsj.com/articles/weekend-interview-gen-frederick-hodges-on-natos-russian-front-1423266333, [online 12.10.2019 r.].

BARTOSZEK B., Cyberwojna – wojna XXI wieku, 12.07.2008, http://www.mojeopinie.pl/cyberwojna_wojna_xxi_wieku,3,1215862210 [online 12.10.2019 r.].

BROAD W. J., MARKOFF J., SANGER D.E., Israeli Test on Worm Called Crucial in Iran Nuclear Delay, w: New York Times, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&hp [online 12.10.2019 r.].

BRONK C.,Blown to Bits: China's War in Cyberspace, August–September 2020, w: U.S. Air Force journal Strategic Studies Quarterly, http://www.au.af.mil/au/ssq/2011/spring/bronk.pdf

CLAY W., Network Centric Operations: Background and Oversight Issues for Congress, http://www.fas.org/sgp/crs/natsec/RL32411.pdf [online 12.10.2019 r.].

DEMCHAK CH., Cybered Conflict vs. Cyberwar, http://www.acus.org/new_atlanticist/cybered- conflict-vs-cyber-war, [online 12.10.2019 r.].

Department of Homeland Security, National Strategy to Secure Cyberspace, https://www.dhs.gov/national-strategy-secure-cyberspace [online 12.10.2019 r.].

KRĘTKOWSKI M., Wirtualna rzeczywistość i jej zastosowania w medycynie, http://aragorn.pb.bialystok.pl/~mkret/Lectures/ib_14.pdf [online 12.10.2019 r.].

LAKOMY M., Cyberwojna jako rzeczywistość XXI wieku, http://www.geopolityka.org/analizy/miron-lakomy-cyberwojna-jako-rzeczywistosc-xxi-wieku [online 12.10.2019 r.].

LEWIS J. A. , Tresholds for Cyberwar, http://csis.org/files/publication/101001_ieee_insert.pdf [online 12.10.2019 r.].

ŁUCZUK P., Tak wygląda WikiLeaks od środka, http://niezalezna.pl/28739-tak-wyglada-wikileaks-od-srodka [online 12.10.2019 r.].

ŁUCZUK P., Poligon geopolityczny: Nadeszła era cyberwojen i cyberterroryzmu, http://wpolityce.pl/artykuly/2454-poligon-geopolityczny-nadeszla-era-cyberwojen-i-cyberterroryzmu, [online 12.10.2019 r.].

MARCINIAK M., Prawdy i mity o chińskich hackerach, w: Computerworld październik 2011, http://www.computerworld.pl/news/376257/Prawdy.i.mity.o.chinskich.hackerach.html [online 12.10.2019 r.].

NORTON-TAYLOR R., Titan Rain - how Chinese hackers targeted Whitehall, https://www.theguardian.com/tech-

nology/2007/sep/04/news.internet [online 12.10.2019 r.].

SCHMIDT M.N. (red), Tallin Manual, https://ccdcoe.org/tallinn-manual.html

SZCZEREK Z., Co się stanie z naszym światem?, http://fakty.interia.pl/news/co-sie-stanie-z-naszym-swiatem,1268240, [online 12.10.2019 r.].

WYSOCKI K., Wojna hybrydowa już trwa. Rosja może odciąć świat od internetu, http://niezalezna.pl/72384-wojna-hybrydowa-juz-trwa-rosja-moze-odciac-swiat-od-internetu, [online 12.10.2019 r.].

http://europe.newsweek.com/were-middle-cyerwar-166196?rm=eu [online 12.10.2019 r.].

http://www.gchq.gov.uk/Challenges/Pages/index.aspx, [online 12.10.2019 r.].

http://niezalezna.pl/22177-zmasowany-atak-hakerow [online 12.10.2019 r.].

http://niezalezna.pl/18487-poczatek-swiatowej-cyberwojny [online 12.10.2019 r.].

http://niezalezna.pl/12322-cyberwojna-chin-i-usa-fikcja [online 12.10.2019 r.].

http://niezalezna.pl/25461-pentagon-przygotowuje-sie-do-cyberwojny [online 12.10.2019 r.].

http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/ [online 12.10.2019 r.].

National Coordinator for Counterterrorism, Jihadis and the internet, 2007, https://fas.org/irp/world/netherlands/jihadis.pdf [online 12.10.2019 r.].

http://www.informationliberation.com/?id=3959 [online 12.10.2019 r.].

https://support.google.com/adsense/bin/answer.py?hl=pl&topic=19363&answer=32759, [online 12.10.2019 r.].

http://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies, [online 12.10.2019 r.].

http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2009:337:SOM:pl:HTML, [online 12.10.2019 r.].

http://www.dziennikustaw.gov.pl/DU/2012/1445, [online 12.10.2019 r.].

Koniec z „drobnym druczkiem" – od dziś obowiązuje nowe Prawo telekomunikacyjne, https://mac.gov.pl/dzialania/koniec-z-drobnym-druczkiem-od-dzis-obowiazuje-nowe-prawo-telekomunikacyjne/, [online 12.10.2019 r.].