Polish Political Science Yearbook vol. 46 (1) (2017), pp. 30–39
DOI: 10.15804/ppsy2017102 PL ISSN 0208-7375

Joanna Świątkowska
Pedagogical University of Kraków (Poland)

Central and Eastern European Countries under Cyberthreats

Abstract: The paper aims to analyse how information warfare can be conducted in cyberspace and to look at this issue from the perspective of Central and Eastern European Countries. It argues that this form of hostile actions will be increasingly utilized in the region. The main assumption, following Alvin Toffler's theory, is that 'information' – as an increasingly important element of modern societies and as their strategic resource – also serves as a significant tool of modern conflicts. Since information is nowadays strongly related to new technologies, mainly the aspects connected to cybersecurity are analysed. The article looks closer at different aspects of cyberthreats and explains their possible consequences. It may serve as good material for further research and recommendations on countermeasures that may increase security in Europe.

Keywords: *information warfare; cybersecurity; cyberthreats; CEE region; information security; hybrid conflict; security; cyberattacks*

The 2003 Security Strategy of the European Union entitled *A Secure Europe in a Better World* stated that "Europe has never been so prosperous, so secure nor so free. The violence of the first half of the 20th Century has given way to a period of peace and stability unprecedented in European history" (A Secure Europe…, 2003, p. 1). Fourteen years later, not only do we know that this assessment of the security landscape was far too optimistic, but we also observe changes in the nature of threats. The article aims to analyse how information warfare can be conducted in cyberspace and to look at this issue from the perspective of Central and Eastern European Countries. Case study methodology as well as a desk research technique is applied.

The Role of Information in the Modern World

Modern societies and states are built on information (Toffler, 2006; Ciborowski, 1999). Although it is very hard to present one, commonly agreed, definition of information, the one presented by Roman Kwiećka will be applied in this article. "Information is a portion of the energy accumulated in the material projection" (Kwiećka, 2001, p. 90), and therefore it can emerge in context of people and machines. Taking into consideration this definition, it may be said that information has at least two functions: it can be defined as any potentially behavior-altering transmission for individuals and social communities; on another level, information refers to order-giving, steering mechanisms for machines and infrastructures.

The role of information has grown significantly. Not only does information empower all societal processes but it also – thanks to modern technologies, mostly information and communication technologies (ICT) – constitutes a significant element of everyday life (Ciborowski, 1999, pp. 8–9; Singer, 2010, p. 435). New technologies, which function based on information in digital form, create cyberspace. "Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. In effect, cyberspace can be thought of as the interconnection of human beings through computers and telecommunication, without regard to physical geography" (TechTarget, 2008). The emergence of cyberspace was one of the main factors that enabled information to play an even greater role within society[1]. This process can be observed in various spheres. For instance, cyberspace has influenced the way people communicate and gain information. Thanks to the Internet, people can easily interact and exchange ideas in real time (e.g. through social media). Moreover, new technologies, interconnected in cyberspace, have influenced economies as "information communications technology is not only one of the fastest growing industries – directly creating millions of jobs – but it is also an important enabler of innovation and development" (Kvochko, 2013). Currently, most of the critical infrastructure – e.g. energy systems, transportation systems or the health care system – is functioning on the basis of interconnected ICT (Rządowe Centrum Bezpieczeństwa, 2013, p. 29). The new technologies and cyberspace have affected the military sphere, transforming the traditional battlefield into "network centric warfare" (Alberts, Garstka & Stein, 2000). Cyberspace has modified how society functions and has influenced the mechanisms of our political structures: today's world is decentralized and the relations between various actors are no longer built only on a hierarchical structure (Castells, 2008). New shapes

[1] The societal, not only technical function of cyberspace is also seen in the definition.

of interaction or influence are to be taken into account, in a way that concerns both state and non-state actors. The possibilities given by new technologies are crucial in enabling various subjects to play a significant role and to influence the whole system. On top of that, as information modifies power relations, it also influences conflicts[2]' *modus operandi* (Toffler A. & Toffler H. 2006, p. 16). All of these changes have led to the creation of a new type of society – the information society (Goban-Klas & Sienkiewicz, 1999, p. 53).

Information Warfare Conducted in Cyberspace

In the information society, information warfare serves as an ideally suited tool to influence a rival. As mentioned earlier, information steers the functioning of both humans and machines – so by interfering in the information sphere, an aggressor can have impact on both. Moreover, thanks to cyberspace, it can be done in a relatively easy way. It requires mainly a computer, Internet access, skills to operate it and knowledge about a target (Libicki, 2012, p. 14). Moreover, it is now possible to purchase tools required for cyberattacks in the Darknet. What is important, time and distance are not obstacles any more – thanks to cyberspace. The aggressor and the target can reside in different places as well as in different time zones, and they can still interact. The fact that it is possible to impact another entity, and cause real consequences only by using computers, was proven by the cyberattack conducted with use of malware named as Stuxnet. Detected in 2010, it was the first worm known to attack SCADA systems that led to the destruction of systems running centrifuges in Iran's nuclear-enrichment program (Kushner 2013). Cyberspace and new technologies greatly influenced the emergence of new possibilities in the information sphere, bringing information warfare to an entirely new level. In order to understand the implications of these processes, it would be useful to first analyze the nature of information warfare itself.

Information warfare can be defined through its three main functions: gaining, protecting and disturbing information (Ciborowski, 1999, p. 9). By knowing more about our competitor, we can defeat him more easily. By protecting information about ourselves, our entity can be safer. By manipulating information, one can effectively influence a rival and change its behavior. By exercising these three functions, we can have an impact on both humans and machines. Thanks to the connectivity of cyberspace, these processes can be remotely initiated anywhere in the world. Because cyberspace offers new opportunities for information warfare, this phenomenon will be closely analysed.

[2] Not only military conflicts.

To understand and systematize facts related to the information warfare conducted in cyberspace, a typology will be proposed. By looking at the consequences of hostile usage of cyberspace, two general types of phenomena can be distinguished – soft and hard. The presented differentiation is inspired by the theory invented by Professor Joseph Nye, who proposed the conception that countries can influence each other by persuasion or by coercion (Nye, 2004). This concept, in a modified version, can be applied to cyberspace[3].

Soft cyber activities are usually not oriented towards destructive, kinetic consequences. The goal here would be to steal information with a view to gaining information superiority, or to manipulate information in order to steer someone's behaviour. In the case of so-called hard cyberattacks, the main aim is to physically affect a victim and to cause as much harm as possible – financial or material damage or loss of life. To obtain such results, the aggressor must attack the systems that control physical devices, e.g. critical infrastructure. The Stuxnet example illustrated the hard cyberattacks. Due to the increasing presence of the Internet of Things, cloud solutions and other modern technologies, the physical and digital worlds penetrate each other. This is why hard types of cyberattacks are increasingly dangerous and that trend will continue[4].

It should be underlined that even though soft and hard actions can lead to different outcomes, the main aim is always the same: to achieve one's goals by gaining information superiority and weakening the opponent. The tables below exemplify the concept.

Table 1. Examples of different types of cyberspace usage: soft and hard

Soft usage of cyberspace	
Goal	*Tools*
• Manipulate public opinion in order to make the public exert pressure on decision-makers. In consequence, it will influence their decisions. • Undermine the credibility of the state and its government. • Escalate disputes among allies. • Increase tensions within society.	– providing false or manipulated information in the information sphere (use of trolls, blogs etc.) – controlled leaks of information that discredit the rival (often using information that was stolen previously) – spreading propaganda that supports specific narratives (use of trolls, blogs etc.)

[3] What must be underlined however is the fact that for Nye persuasion had positive connotation, here in context of information warfare it may serve for hostile purposes.

[4] This distinction reflects the difference in how Western countries and countries like Russia see actions conducted in cyberspace. Western countries mainly claim that cyberattacks are aimed at information infrastructure, while Russia perceives them as a danger to the information content.

• Achieve information superiority	– cyberespionage campaigns
• Create political reality in the rival country	Manipulating election processes through: – manipulating facts, spreading propaganda to affect the candidates, – vote rigging, – undermining trust for election processes
Hard usage of cyberspace	
Goal	*Tools*
• Cause a crisis situation	– cyberattacks that paralyze the functioning of critical infrastructure – cyberattacks that destroy the critical infrastructure
• Amplify military force in a networked battlefield	– weakening enemy's information systems through cyberattacks (often before taking conventional actions)

Source: author's own elaboration.

Attractiveness of Actions Conducted in Cyberspace

Cyberspace provides numerous opportunities and benefits for non-state and state actors who want to influence an opponent by interfering in its information sphere (Ciborowski 1999). Consequently, an increasing number of actors abandon conventional means and reach for cyber tools in order to achieve their goals. The key advantages deriving from the use of cyberspace are as follows:

- Cost reduction – conducting actions in cyberspace is relatively inexpensive. Thanks to that, not only state actors, but also non-state actors can take part in activities that lead to serious and often global consequences.
- Political deniability – using cyberspace can engender far fewer political and punitive consequences, especially when an attacker denies responsibility for certain acts. Cyberspace offers numerous possibilities to anonymize actions, use proxy actors, manipulate or falsify identity. That way, operations that truly influence a victim can be conducted almost without consequences.
- Extensive outreach – cyberspace enables disseminating information to a very broad audience in a very short time. Moreover, due to the new technologies, almost everyone can become a broadcaster by producing and extensively promoting his or her own content. Before the "cyber era", access to this kind of possibilities was limited to traditional, often state-controlled media. Internet

content can be easily manipulated and its message, once diffused in cyberspace, is almost impossible to verify or to correct.

- Asymmetry enhancement – as stated above, cyber tools are easy to acquire and use. At the same time, the most advanced countries increasingly rely on new technologies, becoming more and more vulnerable to cyberattacks. Consequently, using cyberspace to weaken an opponent may become a window of opportunity to damage a stronger rival. That way, an entity with a smaller potential may still play a significant role in the conflict. This is relevant not only from the point of view of state-to-state rivalry but also from the perspective of non-state actors' empowerment.

Are CEE Countries under Cyberthreats?

One may argue that cyberthreats are equally relevant for every country in the world and there is nothing special in the situation of the CEE countries. However, cyberattacks may play a significantly more important role with regard to countries located in this particular part of Europe. The CEE region is under a great threat of cyber aggression due to at least several reasons.

It should be stressed that the usage of information warfare in a broad sense – and conducting activities in cyberspace in particular – is never the goal itself (Ciborowski, 1999, p. 87). These measures are always undertaken as a tool enabling the achievement of a greater aim. Whether it is a political, economic or military goal, there are always support actions leading to the final goal. The CEE region is currently under visible geopolitical tensions. The conflict in Ukraine has actively proved that political rivalry and historical reminiscences are still vivid and influence the regional security environment. This part of Europe is therefore on the front line of potential turbulences. There is political context that can mobilize the use of cyberspace. The interested parties will use various tools to exploit these tensions, but it is highly probable that information-based actions will be used in the first place.

Due to the political circumstances, a conventional clash between Russia and CEE countries is not the most likely form of conflict. Open military collision would be too risky for all the stakeholders. CEE countries are member states of NATO and any decision to launch a military attack on a large scale would have hazardous consequences for the aggressor. Therefore, it is very probable that the interested parties will look for different tools allowing them to achieve their goals. It would probably take the form of hybrid actions with a considerable usage of cyber tools. Before talking about cyber actions undertaken as part of a hybrid strategy, it is useful to analyse the traditional elements of a hybrid conflict, whose main characteristics are the following (Komunikat, 2016):

- It is conducted below the threshold of war;

- It is focused on provoking chaotic situations and political, military, economic and social destabilization;
- It is conducted by state and non-state actors;
- It takes advantage of the opponent's weakest points.

All these elements of a hybrid strategy can be conducted with the use of cyber tools and can cause serious harm to the victims, without risking an open conflict. As argued before, cyber actions – soft and hard – are ideal tools for conducting a conflict below the threshold of war. Weakening an opponent by launching effective, large-scale cyberattacks on critical infrastructure is a very effective *modus operandi*. For example, a direct cyberattack on an electrical system could temporarily paralyse the functioning of the entire targeted state and its citizens. An example of this kind of cyberattack was observed during the conflict in Ukraine when in December 2015, Ukrainian energy companies were hacked, resulting in 103 cities being cut off electricity for several hours ("USA oskarża…", 2016). A large attack of this kind can lead to chaos, financial losses and a decline in the citizens' trust in their government. Finally, it may diminish the state's reputation in the international arena. In consequence, the victim state will concentrate on stabilising its internal situation. In a weaker position, it may be discouraged from taking action at the international level. Cyberattacks can be easily carried out using proxy actors – for instance, hired groups of hackers. They would conduct the planned actions without acknowledging the attacker's identity[5].

Cyberattacks on Ukraine are the most recent, however not the only ones that have occurred in Europe in the recent past. The cyberattacks on Estonia from 2007 and on Georgia from 2008 are further examples. Cyberattacks on Estonia first took place when Tallinn authorities decided to remove the statue of the Bronze Soldier of Tallinn commemorating the Soviet soldiers. This situation caused political tensions with the Russian Federation (Kozłowski, 2014, pp. 238–239). Cyberattacks on Georgia followed the war with Russia over two disputed provinces: South Ossetia and Abkhazia in 2008 (Kozłowski, 2014, pp. 238–239). It seems that cyberattacks have often been used during conflicts involving countries formerly under Soviet control. Again – information warfare conducted in cyberspace with the involvement of nation states needs political context. Tensions in the CEE region are very visible.

Cyberattacks on critical infrastructure, according to the typology presented in the article, are known as hard cyberattacks. But in order to influence modern states, including CEE countries, also soft tactics can be deployed. Soft tactics often aim to influence

[5] This is called an attribution dilemma. Some solutions how to solve it can be found in the great text by J. Healey Beyond Attribution: Seeking National Responsibility for Cyber Attacks (Healey, 2011).

the political reality, so the society and decision-makers will take strategic decisions in line with the attacker's intention. The example of the US presidential elections has demonstrated that an external actor can use the power of cyberspace to try to influence a democratic election process. The official report prepared by three US security agencies – the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency concluded that Russia ordered a hacking campaign to improve one candidate's chances of election (Intelligence Community Assessment, 2017). Once an operation like this becomes successful and the preferable candidate is elected, it is much easier to execute one's owns goals and strategies. This scenario could be used against European countries – also in the CEE region. Circumstances support the choice of this strategy. It would be extremely beneficial for countries like the Russian Federation to cooperate with political leaders who do not want pro-NATO policies and who do not engage in the eastern policy – especially when the conflict on the eastern border of Europe is vivid.

It is interesting to notice that the group of hackers accused of interfering in the US elections, named as APT 28, was active and conducted espionage campaigns also in Poland and other CEE countries (APT28:…, 2014). It is clear that the CEE governments are in the field of interest of groups that may be interested in gaining strategic information. Recently, both the Ministry of Foreign Affairs of the Republic of Poland (Ferfecki, 2017) and the Ministry of Foreign Affairs of the Czech Republic (Muller, 2017) were attacked again as part of a massive cyberespionage campaign. Cyberespionage campaigns play a very important role in the process aimed at influencing others. Stolen information can be used for various purposes. For example, it can be leaked to the public and influence public opinion – especially in the election period.

Besides influencing the internal political scene, soft actions can also be used to cause turbulences between allies and to diminish the position and international engagement of the CEE countries. Influencing the perception, and consequently, the behaviour of the victim with the use of cyberspace is easy achievable. Cyberspace enables the massive sharing of simplified, very often attractively formulated emotional content with an unlimited number of recipients in a very short period of time. Disinformation, manipulation, trolling, and leaking information – these are the perfect tools for destabilising societies, introducing social tensions, and causing disputes. In this situation, societies can be very easily manipulated or even steered. In a nutshell, it is the perfect way to influence the rival and defeat him without even having to fight. Cyber actions aimed at perception have already been observed. For example, abundant information appeared on the Internet in February stating that Bundeswehr soldiers had raped a girl in Lithuania (The Diplomat, NATO, 2017). It was soon discovered that the news was fake and some officials, also from Germany, stated that

it was an attempt to manipulate people's emotions, discredit NATO troops and cause turbulences between allies (The Diplomat, NATO…, 2017). Before the news was emended, it had managed to spread all over the Internet. With the increasing presence of NATO troops in the CEE region, this problem may increase.

Conclusions

We are neither living in a peaceful world nor in a peaceful region. An illusion of stability was created among others by the fact that the nature of conflicts has evolved. They are no longer as obvious as they were only a few years ago. The way societies function has changed, so has the way conflicts are conducted. This is the materialization of Alvin Toffler's conclusions included in the books entitled *The Third Wave* (Toffler, 2006) and *War and Anti-War: Survival at the Dawn of the 21st Century* (Toffler A. & Toffler H. 2006). Modern societies are built on information, and information is the main tool by which we interact. Since information is increasingly correlated with new technologies nowadays, cyberspace becomes the new dimension of rivalry between both state and non-state actors. The CEE region is currently, and unfortunately will be in the future, an area of great political tensions. Due to their characteristics analysed in the article, it is very likely that cyber activities, both soft and hard, will serve as the main tool of influence. These strategies may be very effective and lead to severe consequences. Decision-makers from the CEE region must be aware of this new type of threats and use all available resources to increase security.

References

"Apt28: A Window Into Russia's Cyber Espionage Operations?" (2014). *Fireeye*. Retrieved from: www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

Alberts, D.S. Garstka, J.J. Stein, F.P. (2000). *Network Centric Warfare: Developing and Leveraging Information Superiority.* CCRP Publication Series.

Libicki, M. (2012). *Crisis and Escalation in Cyberspace.* RAND Corporation.

Castells, M. (2008). *Społeczeństwo sieci*. Warszawa: Wydawnictwo Naukowe PWN.

Ciborowski, L. (1999). *Walka informacyjna*. Toruń: Wydawnictwo ECT.

European Security Strategy (2003). *Secure Europe In a Better World*. Brussels: Council of the European Union.

Ferfecki, W. (2017). "MSZ na celowniku rosyjskich hakerów". *Rzeczpospolita.* Retrieved from: www.rp.pl/Polityka/301299943-MSZ-na-celowniku-rosyjskich-hakerow.html.

Goban-Klas, T., & Sienkiewicz, P. (1999). *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*. Kraków: Wydawnictwo Fundacji Postępu Telekomunikacji.

Healey, J. (2011). "Beyond Attribution: Seeking National Responsibility for Cyber Attacks". Washington, DC: Atlantic Council.

Intelligence Community Assessment (2017). "Assessing Russian Activities and Intentions in Recent US Elections". *Senate.gov,* Retrieved from: www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf.

Komunikat do Parlamentu Europejskiego i Rady (2016). *Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej*. Brussels: the European Union.

Kozłowski, A. (2014). "Comparative Analysis Of Cyberattacks On Estonia, Georgia And Kyrgyzstan". *European Scientific Journal*, 3, pp. 237–245.

Kushner, D. (2013). "The Real Story of Stuxnet". *IEEE Spectrum*, Retrieved from: spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Kvochko, E. (2013). "Five ways technology can help the economy". *World Economic Forum*, Retrieved from: www.weforum.org/agenda/2013/04/five-ways-technology-can-help-the-economy/.

Kwiećka, R. (2001). *Informacja w walce zbrojnej*. Warszawa: Akademia Obrony Narodowej.

Muller, R. (2017). "Foreign state seen behind hack into Czech Foreign Ministry email", *Reuters.* Retrieved from: www.reuters.com/article/us-czech-cybercrime-idUSKBN15F1OS.

Nye, J.S. (2004). *Soft Power. The Means to Success In World Politics*, New York.

Rządowe Centrum Bezpieczeństwa (2013). *Narodowy Program Ochrony Infrastruktury Krytycznej*. Warszawa: RCB.

Singer, P.W. (2010). *Wired for War. The Robotic Revolution and Conflict in the 21st Century.* Penguin Books.

Toffler, A. (2006). *Trzecia Fala*. Poznań: Wydawnictwo Kurpisz S.A.

Toffler, A., & Toffler, H. (2006). *Wojna i antywojna. Jak przetrwać na progu XXI wieku?*. Poznań: Wydawnictwo Kurpisz S.A.

„USA oskarża Rosję o cyberatak na Ukrainę" (2016). *Rzeczpospolita*. Retrieved from: www.rp.pl/Konflikt-na-Ukrainie/160219754-USA-oskarza-Rosje-o-cyberatak-na-Ukraine.html.

Author

Dr Joanna Świątkowska

Pedagogical University of Kraków, Institute of Political Science. Contact details: ul. Św. Kingi 8/39, 30–528 Kraków, Poland; e-mail: joanna.swiatkowska@ik.org.pl.