Acta Politica Polonica nr 2/2018 (44) | www.wnus.edu.pl/ap | DOI: 10.18276/ap.2018.44-03 | 29–39

Cybersecurity as a challenge for modern state and society

Marek Górka
dr

Politechnika Koszalińska, Wydział Humanistyczny
e-mail: marek_gorka(at)wp.pl

Keywords security policy, cyber security, cyberspace, cyber power, cyber conflict

Abstract The Internet makes social and political life more dynamic by increasing the access to information, facilitating political discussion, development of social networking and offering alternative and convenient areas of political involvement. This work focuses on analyzing the political structure of the Internet. An emphasis is put on understanding the theoretical connection between technology and politics. It is also an attempt at answering the question, is World Wide Web the answer to the needs of socio-political potential? How can the Internet have a negative influence on political life? So, in order to understand contemporary events, one needs to understand the specificity of cyberspace, which consists both of continuation and new quality of identity and values for the users.

Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa

Słowa kluczowe polityka bezpieczeństwa, cyberbezpieczeństwo, cyberprzestrzeń, cyber power, cyber konflikt

Abstrakt Internet dynamizuje życie społeczne i polityczne poprzez zwiększenie dostępu do informacji, ułatwia dyskusje polityczne, rozwój sieci społecznościowych oraz oferuje alternatywne i dogodne miejsca do zaangażowania politycznego. Praca skupia się na analizie struktury politycznej Internetu. Położony zostaje akcent na zrozumienie teoretycznych relacji między technologią i polityką. To także próba odpowiedzi na pytanie o to, czy Internet odpowiada na zaistniałe potrzeby społeczno-polityczne, oraz o to, czy istnienie Internetu może mieć negatywny wpływ na życie polityczne. Aby zrozumieć współczesne wydarzenia, należy zrozumieć specyfikę cyberprzestrzeni, która stanowi z jednej strony kontynuację rzeczywistości, a z drugiej daje nową tożsamość uczestnikom życia społecznego.

Introduction

In an information era, all the key sectors of human activity, such as: politics, economy, business, public finance, transport, infrastructure, postal service, telecommunications, medicine and science are strictly dependent on IT. A crucial example is social media which can immediately influence the values, ideas and behaviors of large social groups. Due to the social media's global character, governments have virtually no control over what content is spread in cyberspace, and its censoring is quite limited to a certain country (apart from a total ban on the Internet country-wide). In practice, the Internet offers unlimited ways of distributing various ideologies and views which are connected with democratic changes of social relations and human rights.

The development of IT causes everyday life to be more dependent on it, and that leads to new challenges and threats in cyberspace. It is an ideal place for new, secret warfare and conflict. With no proper regulations, the aggressors stay anonymous freely in cyberspace, and that is where crime feels most comfortable while attacking various public organizations and individuals.

State security has been challenged deeply by the IT revolution. Securing and supervising data over cyberspace allows deterrence of cyber attacks which could harm the critical IT infrastructure of state.

Cyber threats to the critical IT infrastructure of state constitute a growing problem for both the governing bodies and the citizens. ICT is ubiquitous in many communication devices, which depend on each other. Therefore, weakening one element may negatively influence the others. Cyber attacks might include: denial-of-service attack (DoS attack), data theft and data manipulation. These could severely damage state security, economy and the level of social conditions of many citizens. Traditionally, cyber threats are seen as harmful to the communications systems or to the authorities.

The topic of cyberspace within political sciences, sociology or state security is an area of research to many. The researchers emphasize its negative consequences for the society which is becoming more and more addicted to the so-called web apps. Here, the work of Peter Trim and David Upton, *Cyber Security Culture. Counteracting Cyber Threats through Organizational Learning and Training* becomes quite essential (Trim, Upton, 2016).

Although the Internet is omnipresent and vital for the state, there are many processes and phenomena to understand, especially in the fields of international relations or the authorities and the information age. These have been presented in Madeline Carr's *US Power and the Internet in International Relations. The Irony of the Information Age* (Carr, 2016).

The third, vital for the analysis presented in this article, work is a book by Julian Richards: *Cyber-War. The Anatomy of the Global Security Threat* (Richards, 2016). It shows a critical view on current debates about the probability and possible results of a cyber war. From the author's sociopolitical point of view, he believes that there is no sign of a destructive character of cyber war, but it might be the case with future conflicts.

Brian Mazanec and Bradley Thayer continue the topic in their *Deterring Cyber Warfare. Bolstering Strategic Stability in Cyberspace* (Mazanec, Thayer, 2016), pointing to the fact that

Internet attack deterrence is one of the most important topics discussed among many countries, but it is also the most problematic one.

This article aims at introducing certain behaviors and their effects concerning the Internet and the state, as well as private entities. It also describes the dynamics and nature of cyberspace conflict. A few thoughts on the functioning of modern state and its citizens in cyberspace are also presented. It also aims at organizing the selected concerns on judging and categorizing cyber threats.

1. Cyberspace

Today, more than half of population is active politically, economically or culturally in cyberspace. The Internet has become one of the most basic areas of a society's activity. Although cyberspace is not new to modern world, many countries still need to reorganize their institutions with regard to cyber threats. Unlike natural environments, such as: air, land, water or space, cyberspace is a man-made environment and is global in its nature.

The notion of cyberspace is very wide. It appears that this term could be of greatest challenge to analyze and interpret. The word „cyber" relates to IT and communications, and thus also to all the fields of human activity, including: economy, society, education, culture, entertainment, and knowledge. It is also this space which is constantly expanding and evolving because of inventiveness and participation of its users (Deibert, Rohozinski, 2010, p.15–32). The key in defining „cyberspace" lies in National Security Presidential Directive 54, which states that it is the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries, and is understood as virtual environment for interaction between people (Cybersecurity Policy, 2008). Following this thinking, one might notice the need of emphasizing interpersonal relations. Cyberspace needs not only the hardware and the software, but also human behaviors caught in digital format. Those interactions constitute a rich collection of both positive and negative aspects of human nature, which range from cyber auto-creation and self expressing to criminal activities, including terrorist attacks and possibly cyber conflict. The main features of cyberspace are: no boundaries, dynamic processes and anonymity of its users. Public institutions present in cyberspace are susceptible to cyber attacks, which may be organized by individuals, groups of attackers or even hostile countries. So, having the boundless nature of cyberspace in mind, it can be concluded that the aggressors might vary.

2. Cyberspace and the state

In a globalized world, a fast and secure communications system is not a luxury, but a factor determining competitiveness. Many countries invest large sums of money to widen their digital infrastructure, and the citizens welcome that with great enthusiasm. More frequently, governments use modern technology to communicate with the citizens. The problem lies in the question of doing so without the risk of being attacked by cybercriminals. Potential threats grow with the

level of social dependence on this new infrastructure. It is quite problematic, because most of competitive tendering is made via the Internet.

Cyber threats recently have become more serious. Some of the countries and international organizations are aware of establishing some policy and politics concerning cybersecurity. The very nature of the content present in cyberspace might shed some light on possible threats.

The problems multiply equally fast to the emerging possibilities of real cyber attacks which may damage e.g. a company's financial system severely. Such attacks aim at getting ransom from a company so it does not lose its data bases or the access to them.

In some instances the world introduces new technology so fast that people might not be able to realize its effects on public security in time. Cybersecurity, thus, has become a priority to most countries in the world. Cyber threats weakened the traditional forms of political power. To answer that, countries make efforts to govern the processes which occur in cyberspace (Vacca, 2011, p. 159–176). These efforts are directed towards a tighter integration of cybersecurity within a broader national security plan. It means closer cooperation between the state and its organizations and, therefore, ability of adapting to dynamic technological changes in a more integrated world of communication (Borandi, 2009, p. 51–56).

A big challenge to cybersecurity is reforming the current politics model, so that the government agencies would share some of their power with given entities (Brantly, 2014, p. 132–155). The security policy, including cybersecurity, deals with all entities which use the global IT infrastructure. Today the cooperation between the state and the private sector is not just one of the ways, but a basic way of functioning in the public sphere. It also enables implementation of innovations into the public security area as well. As the private sector is gaining importance in cybercrime, it is crucial for this sector to cooperate with public entities.

In other words, the cybersecurity level depends on the level at which the government encourages private entities to take part in security-related initiatives and on the flexibility as far as the public and private entities are concerned. Cybersecurity management can be interpreted as a form of a dialog between organizations and may greatly help to protect against cyber threats. However, this model of cooperation within government bodies and between government agencies and the public sector has not been yet properly spread among the authorities.

Summing up, cybersecurity is a challenge incorporated into cooperation between various state entities and institutions; private companies and NGOs; on an international level and globally. It has become a priority to the EU and NATO which began legal transactions as far as cybersecurity is concerned.

2.1. Politics – power

The world in the 21st century becomes more and more dependent on information, IT and communication. Most of today's governments try to take actions in order to be ready to face the new challenges that cyberspace may bring. The life of an average citizen, the national economy and virtually every country is currently dependent on the stability and security of cyberspace.

It appears that easy access to IT and communication is one of the conditions of functioning as a proper, modern society.

The popularity of cyberspace is so great that is changes the reality and, in some way, it determines and shapes current models of governing. Thus, the notion of *cyberdemocracy* emerged. It is defined by its authors as a basic rule governing the most of issues concerning the connections between IT and democratic processes that deal with the civil service or the elections (Jensen, Danziger, Venkatesh, 2007, p. 39–50).

It is worth thinking about the influence of IT on democracy quality. It appears that cyberspace allows to form a transnational and global public space in which people discuss civil rights and civil liberties. This is where social networking plays a major role, because it activates and brings different social groups or protesters together, thus giving the incentive to start democratic processes, just as it could be observed in the Middle East and North Africa countries. Generally, the chances cyberdemocracy offers are great as far as the citizen participation and transparency are concerned, but new technologies have also downsides, such as cybercrime and cyberterrorism. In a globalized and unified reality, politics or economy is dependent on technology not only in terms of communications and PR, but also finances. A good example are presidential elections in the US, where all the candidates visit Silicon Valley to raise funds for their needs. One cannot overestimate the value of IT for modern democracy.

2.2. Internet surveillance

Democratic values become, under certain circumstances, an obstacle to ensure cybersecurity. In extreme cases, those who control cybersecurity are authoritarian states which monitor the Internet in order to block access to certain websites (Simpson, Murphy, 2014, p. 189–191). The way in which elements of cybersecurity management work together (mostly between the state and private entities) determines the ruling model in a country. The pluralist character of cyberspace gives the freedom of speech, but whenever any democratic values become thus endangered, it is the time when democracy should yield to security. A good example is the unethical and illegal disclosure of confidential U.S. documents by Edward Snowden, a former NSA employee. The leaked documents revealed the numerous global surveillance programs, many run by the NSA and the Five Eyes Intelligence Alliance with the cooperation of telecommunication companies and European governments. In answer to cyber conflict among the governments, many negative consequences may occur – ideas of introducing laws that limit civil rights and liberties, which may lead to violence. Apart from physical damage and financial loss, the very possibility of future cyber threats may lead to social mistrust and unwillingness to work with new technologies. The loss of social trust may result in large social and economic unrest in a modern country.

2.3. The society

The fast growth of IT and communications in every aspect of a society's existence, combined with dependence on cyberspace, forged the modern society and added to its well-being. The society builds its future based on technology that is very vulnerable. Global expansion of social

networking, such as Facebook or Twitter, took over everyday life but also created a problem which might be difficult to deal with. Trojans, worms and viruses are installed onto computers and mobile devices in order to take them over and gain access to bank account passwords, Facebook account passwords, private e-mails and addresses. However, it is not only the loophole in a system or the user's mistake that needs to be present in order for hacking to take place. Stealing credit card details, data or identity theft, bank fraud, spamming and blackmail are only a few examples which prove that criminals have a wide range of tools. To make a crime successful, two of the above mentioned factors need to take place at one time. Today, social networking and the amount of information exposed through it, result in a weaker human nature, which leads to temptation. Any criminal today, with a little time spent on the Internet, can gather much information about his potential victim. The idea is to make the victim believe that the message he or she is getting is credible, so it is sent by a member of the family or a friend. Its aim is to build up trust and then steal personal data (Oates, 2001, p. 92–96).

Creating one's public image before the Internet age usually took months or years and required a lot of work and energy. Today, in just a few hours, one can create a fresh, credible individual with no equivalent in real life (Roberts, Indermaur, Spiranovic, 2013, p. 315–328). It is thus amazing how much information people can put online. The influence of social engineering is devastating, because one can form bonds and build up trust without leaving any trace, and it is not about attacking any IT systems, but the aggression towards other people.

The information that is gathered through various applications and social networking is a source of knowledge about the victim's family, friends and workmates. Such a set of data can become highly malicious when used by wrong people.

3. Cyber War

Compared to conventional warfare, cyber conflict appears to be a relatively cheap form of struggle between countries. What is more, actions in cyberspace can be initiated from virtually any place on Earth and do not require large amounts of weapons or army, only access to a computer and to the Internet. A possible cyber conflict is one of today's greatest challenges in the areas of military, political, economic and social security of a country.

Although exact borderlines of cyber war have not been identified yet and are still questioned by some researchers, a more broad definition can be formed: a conflict taking place in cyberspace, with the use of IT and communications in order to destroy the resources and IT infrastructure of the enemy (Rid, 2012, p. 5–32).

Richard Clarke, in his book entitled *Cyber Warfare*, defines cyber war as hacking into computers or computer networks of another country in order to destroy the enemy's resources (Clarke, 2012, p. 33–68). „The Economist" describes cyber war as the fifth domain of warfare, after land, sea, air and space (The Economist, 2010).

Assuming that cyberspace is an alternate environment where countries can compete, one may conclude that escalation of conflict at that level leads to serious damage in nearly all domains of

public sphere. This fact allows one to use the notion of „cyber warfare". E-environment makes new possibilities of having military impact. New technologies allowed to make weapons more efficient. Intelligence has been improved and it determines one's superiority on the battlefield. Cyberspace, thus, has become a source of information with a strategic meaning (Thomas, 2014, p. 370–393). The very first phases of war include gathering precise information. Today the ability to gather, use, store and process information is the major proof of military power (Ormrod, Turnbull, 2016, p. 270–298). Communications and information technologies adapted by the military and paramilitary forces lead to revolutionary changes in warfare. They multiply the speed of data processing which makes complex decision making easier and creates new tactics for the armed forces. They also add to the military potential of e-warfare systems, which can damage or destroy the enemy's military and civilian computer networks more effectively. Some experts believe that this „invisible weapon" may end a conflict before it can even break out. In this context, one can conclude that having IT weaponry provides military benefits and is probably highly competitive as far as conventional weapon is concerned. Those two types of weapons are currently the major argument in pressure politics. E-weaponry is gradually becoming one of the main elements of military potential within modern countries. Today, many developed countries such as: the U.S., China or Russia intensively prepare for e-warfare.

It can be assumed that less technologically developed countries also pursue the said e-war solutions. It is highly probable as e-weapons have certain advantages for both sides of conflict. Firstly, their use and spread is fast and low-cost, thus making it available to many. Furthermore, it can be designed, constructed and employed without the notice of public opinion. So, it is difficult to charge any particular entity (which is usually a foreign regime) which aims at causing local or global unrest (Peterson, 2013, p. 120–124). Summing up, cyber war involves using computers to destabilize a hostile or competitive country by means of attacks on its communications systems. There are four main notions that define cyber war: the first one is the asymmetric character of conflict, thus its cheap and destructive factor; the second is low detectability, so there is no immediate retaliation; the third one is difficulty of defending a country when being attacked in e-war, so most of the countries (which is logical) want to attack first. The fourth deals with classified data on means of cyber war and any agreements concerning weapons control are difficult to implement. In other words, cyber war means more military possibilities (Junio, 2013, p. 125–133).

Massive competition and conflict of interests of many entities and groups make it hard to establish a law system within international space that would define which actions could be treated as cyber crime. Of course, there are other circumstances hindering international cooperation with regard to e-crime. The developed countries make great profits within cyberspace and surely would not like to lose them.

One of the major problems is that there are no international agreements with regard to spread, development and using e-weapons in military context. So, there appear some questions within the public opinion and the authorities: when and to what extent e-weapons can be used? What circumstances justify their use? How to use highly dangerous computer viruses which could cause local or global ecological or socio-economic disaster? How not to become a victim of one's

own weapon? Can the use of e-weapons cause a conventional conflict? To what extent can cyber attack justify retaliation? A partial answer to the above might be found in creating norms and rules concerning e-weapons and also integration of international agreements between countries which can form a framework for functioning of political entities.

From the institutional and technical point of view, there are many difficulties in implementing international law during cyber operations. In reality, the international society demands something more than bilateral agreements which do not work in case of breach. Some countries took safety measures in the form of national cybersecurity strategies in order to minimize the damages caused by cyber attacks. Those measures are only partially effective.

There are no bilateral or multilateral international agreements which would define cyber attack in a simple way and give solutions on what sanctions it should impose. Also, there is a visible lack of cooperation between entities in terms of controlling, processing and sharing information which might be helpful in tracking cyber aggressors (Choucri, Madnick, Ferwerda, 2013, p. 96–121).

Another difficult fact is a situation in which some countries, namely the U.S. and Russia, act in a way which cannot be differentiated from terrorist attacks. In such case, choosing methods of counteracting becomes a problem. A combination of anonymity and operating at the same time from two countries or non-governmental entities plus the difficulties with telling the difference between military and unlawful actions is highly problematic. Every cyber incident is hard to describe, so there are no entities that are fully responsible.

What is more, the uncertainty combined with lack of agreement between the political players creates the risk of unrest and misinterpreting of some facts. Therefore, identifying of the wrongdoer is crucial when dealing with cyber crime, cyber terrorism and cyber war. One has to bear in mind that the attacker might be an individual or a group of people or a certain political entity.

3.1. Asymmetric War

The war in cyberspace is asymmetric in nature, because the technology offers unauthorized users the possibilities of taking control over, e.g., management systems in a given public sector. As a result, financial, economic or political systems become endangered. In this case, the hostile entities or organizations gain advantage over public institutions (Schroefl, Kaufman, 2014, p. 862–880). An illustration of such a case is the cyber attack carried out by the Anonymous – a group of hackers – on about 400 000 Turkish websites with the „.tr" domain. The attack was launched due to the accusations of Turkish government of buying oil and thus supporting ISIS. The Anonymous threatened Turkey with more cyber attacks unless the country stopped supporting ISIS (Summers, 2015). A country's political course may be determined by such entities and their actions. A rapid technological boom made boundaries between public and private goals disappear on the Internet. The enemy can cripple a country by destabilizing financial markets and not necessarily the areas strictly connected with the state (e.g. the army or the government). So, the main job of a country is to secure its interests as well as its citizens.

3.2. Cyber attacks and computer viruses

The growth of computer viruses, as well as anti-viruses, is, metaphorically speaking, another arms race between political entities. The news on supermalware, such as *Stuxnet* and *Flame* shows the advanced level of both programs. Undoubtedly, they also point to their authors in intelligence agencies of developed countries. This malware was probably designed by the U.S. and Israel in order to sabotage Iran's nuclear program and shows its superior level of development over any other malware or virus so far deployed. Both *Stuxnet* and *Flame* are hard to spot on a computer. *Flame* can record audio, screenshots, keyboard activity and network traffic. The program also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth-enabled devices (Messmer, 2012).

In a situation where the most powerful countries in the world develop computer viruses, it is worth giving a thought what security level those countries have. Can those malicious programs spread secretly and infect more systems or will they be used by terrorists in the future?

3.3. Stereotypes about cyber conflict

In source literature one can frequently find a statement about cyber war being asymmetric in nature, because the tools needed for cyber war are cheap and easily accessible. It is not always the case, though. Their design takes much time and effort. Poor preparations may end in a failure for the cyber aggressor (Rid, McBurney, 2012, p. 6–13). Furthermore, cyber attacks are effective only when combined with conventional weapons. Such an offensive of a weaker country is reasonable only when aided with conventional weaponry. Even if e-weapons were to be used, it would be rather improbable, because an answer to such a cyber attack would be conventional weapons of a stronger country destroying their aggressor's infrastructure. This explains why it is so unlikely for countries such as Somalia or Tajikistan to perform cyber attacks on the U.S. No matter the damages their cyber attacks would cause in the U.S., the American answer would be devastating for those countries. When starting a cyber war, the aggressors must be aware of the consequences they might have to face. Even a military power which uses cyber weapons cannot be absolutely sure of their strength, because the risk of a backfire is quite high.

Some countries or organizations choose to use the cyber loophole and not get involved in the expensive processes of resolving conflicts. In this context, the access to e-weapons might in fact help weaker countries to fight the stronger ones. Paradoxically, under some circumstances, the possibility of cyber war might be useful as a deterrent which could scare the potential, traditional enemies off. This phenomenon is similar to the nuclear war threat, which was enough to stop the escalation of the conflict during the Cold War and which helped in peace talks during the Cuban Missile Crisis in 1962. It has to be mentioned that there are many stereotypes about cyberspace. One will agree that cyber war is harmful in its nature to the international security and to the world peace, but the belief that social networking is harmful to dictators is not entirely true. It

appears that appropriately controlled IT can serve as another means of spreading certain ideas for different regimes.

Commencing cyber attacks is not easy, because their origins are usually unknown. This makes counteracting quite difficult. An effective deterrent should be credible. Joseph S. Nye, a strategist with Harvard University, believes that the main discouraging aspect is money. Making the attacker's identity public might also be another one. Deterrence might also depend on the way an attacked superpower uses its cyber weapons in the future. It would be a clear warning that a given country is ready and willing to act (Nye, 2011, p. 25–50).

Conclusion

It is hard to overestimate the role which computer systems play in maintaining modern economies. However, it is easy to imagine what would happen if communications satellites or main financial systems databases were damaged. Although most of the cyber threats come from the developed countries, it has to be mentioned that the threats might come from anarchist organizations and terrorists.

Cybersecurity experts share two contradictory beliefs: one says that with reasonable preventive measures, huge cyber disasters are unlikely (Isenberg, 1999, p. 7); the other says that cyber terrorists are able to bring the world economy down (Burton, 2015, p. 297–319). It is difficult to tell who is right in this debate, but it seems that both scenarios are probable. Everything, apparently, depends on social education with regard to cybersecurity, and also on preserving those basic skills of using analog devices or traditional tools in case of a digital apocalypse. It should be emphasized, though, that both cybersecurity and economic stability of a country are a delicate and complex matter and many public institutions, responsible for the functioning of the above, do not always keep pace with the changes in those areas.

References

Borandi, T. (2009). Introduction to Secure Global Collaboration. *Information Security Journal. A Global Perspective*, *2* (18), 51–56. DOI: 1080/19393550902791473.

Brantly, A.F. (2014). The Cyber Losers. *Democracy and Security*, *2* (10), 132–155. DOI: 10.1080/17419166.2014.890520.

Burton, J. (2015). NATO's Cyber Defence. Strategic Challenges and Institutional Adaptation. *Defence Studies*, *4* (15), 297–319. DOI: 10.1080/14702436.2015.1108108.

Carr, M. (2016). *US Power and the Internet in International Relations. The Irony of the Information Age*. New York: Palgrave Macmillan.

Choucri, N., Madnick, S., Ferwerda, J. (2013). Institutions for Cyber Security. International Responses and Global Imperatives. *Information Technology for Development*, *2* (20), 96–121. DOI: 10.1080/02681102.2013.836699.

Clarke, R.A. (2012). *Cyber War. The Next Threat to National Security and What to Do About It*. New York: Ecco Press.

The Economist (2010). *Cyberwar. The Threat from the Internet*. Pobrane z: http://www.economist.com/leaders/2010/07/01/cyberwar (12.08.2016).

Deibert, R.J., Rohozinski, R. (2010). Risking Security. Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, *1* (4), 15–32. DOI: 10.1111/j.1749-5687.2009.00088x.

Isenberg, D. (1999). *A Cyber Pearl Harbor? More Hype Than Threat*. Pobrane z: https://www.joc.com/cyber-pearl-harbor-more-hype-threat_19991227.html (12.058.2016).

Jensen, M.J., Danziger, J.N., Venkatesh, A. (2007). Civil Society and Cyber Society. The Role of the Internet in Community Associations and Democratic Politics. *The Information Society*, *1* (23), 39–50. DOI: 10.1080/01972240601057528.

Junio, T.J. (2013). How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate. *Journal of Strategic Studies*, *1* (36), 125–133.

Mazanec, B.M., Thayer, B. (2016*). Deterring Cyber Warfare. Bolstering Strategic Stability in Cyberspace*. New York: Palgrave Macmillan.

Messmer, E. (2012). *Stuxnet and Flame share code, development teams. Kaspersky Lab Says Early Version of Stuxnet Has a Flame Module*. Network World. Pobrane z: https://www.networkworld.com/article/2189257/security/stuxnet-and-flame-share-code--development-teams.html (12.08.2016).

Cybersecurity Policy (2008). National Security Directives George W. Bush Administration, 54. Pobrane z: https://fas.org/irp/offdocs/nspd/nspd-54.pdf (12.08.2016).

Nye, J.S. (2011). *The Future of Power*. New York: PublicAffairs.

Oates, B. (2001). Cyber Crime. How Technology Makes it Easy and What to Do About it. *Information Systems Management*, *3* (18), 92–96. DOI: 10.1201/1078/43196.18.3.20010601/31295.12.

Ormrod, D., Turnbull, B. (2016). The Cyber Conceptual Framework for Developing Military Doctrine. *Defence Studies*, *3* (16), 270-298. DOI: 10.1080/14702436.2016.1187568.

Peterson, D. (2013). Offensive Cyber Weapons: Construction, Development, and Employment. *Journal of Strategic Studies*, *1* (36), 120–124. DOI: 10.1080/01402390.2012.742014.

Richards, J. (2016). *Cyber-War. The Anatomy of the Global Security Threat*. New York: Palgrave Macmillan.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *1* (35), 5–32. DOI: 10.1080/01402390.2011.-608939.

Rid, T., McBurney, P. (2012). Cyber-Weapons. *The RUSI Journal*, *1* (157), 6–13. DOI: 10.1080/03071847.2012.664354.

Roberts, L.D., Indermaur, D., Spiranovic, C. (2013). Fear of Cyber-Identity Theft and Related Fraudulent Activity. *Psychiatry, Psychology and Law*, *3* (20), 315–328. DOI: 10.1080/13218719.2012.672275.

Schroefl, J., Kaufman, S.J. (2014). Hybrid Actors, Tactical Variety. Rethinking Asymmetric and Hybrid War. *Studies in Conflict & Terrorism*, *10* (37), 862–880. DOI: 10.1080/1057610X.2014.941435.

Simpson, B., Murphy, M. (2014). Cyber-Privacy or Cyber-Surveillance? Legal Responses to Fear in Cyberspace. *Information & Communications Technology Law*, *3* (23), 189–191. DOI: 10.1080/13600834.2014.978551.

Summers, Ch. (2015). *Hacking group Anonymous declares 'Cyber War' on Turkey for 'Supporting ISIS'.* Daily Star, 23 grudnia.

Thomas, T. (2014). Creating Cyber Strategists. Escaping the 'DIME' Mnemonic. *Defence Studies*, *4* (14), 370–393. DOI: 10.1080/14702436.2014.952522.

Trim, P., Upton, D. (2016). *Cyber Security Culture. Counteracting Cyber Threats through Organizational Learning and Training.* London–New York: Routledge.

Vacca, W.A. (2011). Military Culture and Cyber Security. *Global Politics and Strategy*, *6* (53), 159–176. DOI: 10.1080/00396338.2011.636520.