DOI: 10.17951/teka.2018.13.2.27-47

# THE PROBLEM OF CYBER ATTACKS ON THE CRITICAL INFRASTRUCTURE OF THE STATE IN THE ENERGY SECTOR. THE CASE OF TURKEY[1]

Kinga Smoleń
Maria Curie-Skłodowska University
ORCID ID: https://orcid.org/0000-0003-2564-5190
kinga.smolen@poczta.umcs.lublin.pl

**Abstract**: The cognitive aim of this paper is to analyze the problem of cyber attacks on the critical infrastructure of the state in the energy sector. In this context, Turkey is presented as a case study. This state acts as a "transport corridor" for hydrocarbons and therefore has a strong position on the international market of energy resources. Thus, the cyber attacks on its critical infrastructure have serious consequences not only for the development of this state and its security, but also for the geopolitical system in the Near East and the distribution of powers in the aforementioned international market of hydrocarbons. The following research assumptions are set for the need of the undertaken problem. Firstly, cyberspace poses a potential source of threats for the security of the state. It happens due to the fact that it is a kind of "space" which "escapes" from the control of state security authorities, which increases the probability of cyber attacks on the critical infrastructure of the state, etc. Secondly, in the conditions of cyberspace there is a change in the significance of the components of power in the international relations. The increase in the scale and the number of cyber attacks confirms the fact that nowadays the ability to protect effectively against the attacks in cyberspace and highly developed information technology indicates the position of the state and its possibility to influence the international system. Thirdly, the term "security" is broadened in a subjective and objective manner due to the process of globalisation and the withdrawal from perceiving the security from the perspective of the military threats as it was during the Cold War. Currently, security refers to lots of areas of the social life and the sources of its threats are of political, economic, military, social, ecological, demographical and energetic character. Thus, the energy security has become one of the autonomous dimensions in the structure of the largely perceived security.

**Keywords**: cyber attack, Turkey, critical infrastructure, security of state, cyberspace, energy security

[1] The author created this scientific article as part of the research project No. 2011/03/N/HS5/03773 entitled "The geostrategic location of Turkey after the Cold War", funded by the National Science Centre in Cracow.

## INTRODUCTION

The late Westphalian reality is characterised by the pluralism and hybridity of the subjective and objective scope as well as the increasing complexity of the social environment [Pietraś 2015: 65–97]. This resulted in the creation of the space with new qualitative traits which functions – as Marek Pietraś points out – "on the edge" of the state and the international system [Pietraś 2013: 129]. This space does not exist between the above-mentioned levels – it "overlaps" these levels to some extent and includes the activities, processes and cross-border phenomena generated largely by the activity of the non-state actors. The creation of an additional supraterritorial "space", together with its dimensions, e.g. in the form of cyberspace, led to serious qualitative changes in the international system. One of the most significant ones is related to the fact that the sovereign national states lost their exclusive ability to create and steer this system. Since the Peace of Westphalia, such states used to build their position and potential mostly on the basis of the armed forces and vast territory which was ruled and controlled exclusively by them. Thereby, cyberspace should be understood as a new kind of "space" and the activities taken herein may pose a potential source of threat to the security of the state.

The cognitive aim of this paper is to analyze the problem of cyber attacks on the critical infrastructure of the state in the energy sector. In this context, Turkey is presented as a case study. This state acts as a "transport corridor" for hydrocarbons and therefore has a strong position on the international market of energy resources. Thus, the cyber attacks on its critical infrastructure have serious consequences not only for the development of this state and its security, but also for the geopolitical system in the Near East and the distribution of powers in the aforementioned international market of hydrocarbons. The following research assumptions are set for the need of the undertaken problem. Firstly, cyberspace poses a potential source of threats for the security of the state. It happens due to the fact that it is a kind of "space" which "escapes" from the control of state security authorities, which increases the probability of cyber attacks on the critical infrastructure of the state, etc. Secondly, in the conditions of cyberspace there is a change in the significance of the components of power in the international relations. The increase in the scale and the number of cyber attacks confirms the fact that nowadays the ability to protect effectively against the attacks in cyberspace and highly developed information technology indicates the position of the state and its possibility to influence the international system. Thirdly, the term "security" is broadened in a subjective and objective manner due to the process of globalisation and the withdrawal from perceiving the security from the perspective of the military threats as it was during the Cold War. Currently, security refers to lots of areas of the social life and the sources of its threats are of political, economic, military, social, ecological, demographical and energetic character. Thus, the energy security has become one of the autonomous dimensions in the structure of the largely perceived security. Taking into account the undertaken research aim and adopted research hypotheses, the article defines the threats to state security in cyberspace and the special nature of cyber attacks on the critical infrastructure of the state in the energy sector, including the case of Turkey. The article presents the impact of cyber attacks on the energy security of the state and its reactions to this kind of threat.

## 1. THE NATURE OF THREATS TO STATE SECURITY IN CYBERSPACE

Hyperpolyarchity, pluralism and hybridity of the subjective and objective scope as well as the increasing complexity of the social environment expressed among others in the processes of globalisation contributed – in the time of the late Westphalian international system – to the creation of an additional supraterritorial "space" with new qualitative traits. The aforementioned "space" is defined in the source literature as transnational and is a complex "construct" of the specific sphere of the social reality [Mojska 2013: 339].

As a result of a very dynamic development of the technological factor and popularisation of the so-called new means of communication, especially the Internet, the creation of a new dimension of space took place – the creation of cyberspace as part of the transnational space. This new kind of the social "space" acts as a kind of a virtual reflection of the international environment, although it is an egalitarian and immaterial construct. Therefore, one deals with the "duality", hybridity, which results in the simultaneous functioning of the traditional space, interpreted in the territorial categories and geographical distances, and along with this one, a new space deprived of place, geographical distances and borders.

In the source literature, there is no common definition of cyberspace.[2] This term was first used in 1982 by William Gibson who used it in his science-fiction novel *Burning Chrome*. Two years later, Gibson defined cyberspace in his novel *Neuromancer*. The definition was as follows:

> […] A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts […]. A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data [Gibson 2009: 59].

[2] The name *cyberspace* comes from the Greek term *kybernetes* which means the *steersman*, *manager*, *guide*. To put it simple, the cybernetics is a knowledge about steering, controlling and communicating. This interdisciplinary science is applicable in such fields as: automatics, communication theories as well as conveying and transformation of information in the systematically perceived machines, entities, society [Berdel-Dudzińska 2012: 19].

This definition uses the literary language which is different than the language of the scientific discourse. Despite this fact, it clearly indicates some elements which are distinctive for this specific dimension of space. To the most vital ones belong the following: the transnational character, complexity, lack of geographical distances and the impossibility to refer the physical measures to the space perceived territorially, combining the resources into one [Wasilewski 2013: 226].

One of the mostly known and commonly cited definitions of cyberspace is the one formulated by the United States Department of Defense. It states that cyberspace is:

> […] the global domain of the information society which consists of the interdependent networks created by the infrastructure of the Information Technology (IT) and data saved in them, including the Internet, telecommunication networks, computer systems and processors and controllers embedded in them [Wasilewski 2013: 227].

In contrary to the first definition, the one created by the United States Department of Defense concentrates on the technological elements of cyberspace, among others, the Internet.

A similar attitude to this kind of transnational space is adopted by the European Commission, which understands cyberspace as a virtual space, in which the data processed electronically by PCs from all over the world circulates [Wasilewski 2013: 229]. The basis of the aforementioned definition is the perception of cyberspace as a sum of systematically put files, data, Internet websites, which are accessible through the teleinformation systems. It is worth noting that the definition emphasizes the supraterritorial character of cyberspace.

Apart from emphasizing the aforementioned technological component, some definitions of cyberspace put special attention to the social relations which refers thereby to the anthropogenic factor. It can be found among others in the paper of the Ministry of the Interior and Administration from 2010 which defines cyberspace as: “The [digital] space of processing and exchanging information [created] by the systems and teleinformation networks along with the connections between them and the relations with the users” [*Rządowy Program Ochrony…* 2010]. It is worth noting that in the source literature, *cyberspace* is understood as “a tool, subject or an environment of criminal activity” [Siwicki 2013: 18] which poses a threat to the security of states and non-state entities. Tomasz Aleksandrowicz and Krzysztof Liedel describe it as a new battle environment, which is a field for activities of a military, secret service, sabotage, criminal and hooligan nature [Aleksandrowicz, Liedel 2014: 11]. The analysis of the parts of components emphasized in the aforementioned definitions confirms the assumption which states that it is a kind of “space” that poses a source of threat to the security of the state. On the one side, there are elements constituting cyberspace which are decisive in this context, such as lack of territoriality, horizontal character of the network structure without the centralized place of power, existing beyond sectors. On the other side, there are the following phenomena happening as part of it: bifurcation of the subjective structure, demonopolization of the state power, change of the significance in the power components, "virtual" competition between states. Cyberspace is distinguished by a kind of a "lack of territoriality" and a "non-spatialness", which means that it is deprived of the geographical parameter and all the restrictions related to it [Aleksandrowicz, Liedel 2014: 35]. In this "space", the boundaries are limited to the level of the internetisation and the level of development of the technological factor. The aforementioned distinctive features indicate among others the asynchronicity of communication which takes place in an unreal time; the lack of corporeality which means the lack of necessity to be in the space physically and anonymity. The possibility for the user to remain anonymous does not result from the nature of cyberspace – as Marek Madej points out – but from its construct, the scale and complexity of connections building it [Madej 2007: 331] as well as the lack of the obligatory requirement to authorize the access to the system [*ibid*.]. The so-called petrifaction of cyberspace [Madej 2009: 32–33] takes place. In cyberspace, there are interdependencies based on partnership which means that every user may use the generally available Internet and after installing a proper free software he or she may also use the resources of the so-called "deep web" [Bógdał-Brzezińska, Gawrycki 2003: 38].

The aforementioned anonymity of the activities in the Internet simplifies transferring data on a bigger scale as well as undertaking measures which are related to the new areas of human life, functioning of the state and the societies. Some of these activities are illegal, i.e. cybercrime, cyberterrorism, hacktivism, hacking, cyber spying, military use of cyberspace. On this basis, one can distinguish the third distinctive feature of the cyberspace in the form of the transsectority. In cyberspace, the scope of the activities is constantly being broadened and includes the activities with the political, economic, social, cultural, technological and military character. The infringement of any of these dimensions may pose a threat to the effective functioning to the public administration authorities, institutions and companies, and thus, the state security [Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym… 2007]. The scale and the kind of new challenges that arise in the Internet very quickly cause the state's vulnerability to new threats, mostly of the asymmetrical character. Analogically, in response to them, the state is forced to reach for non-military security instruments while the military instruments are restricted. It is related to the changes that take place internationally along with the shaping of the late Westphalian international system [Pietraś 2003].

With respect to the asymmetrical threats mentioned above, it should be emphasized that in the virtual space, the forces of state entities balance the ones of non-state entities. This phenomenon is generated by the nature of the space which is non-territoriality [Madej 2007: 339]. There is a decline of factors which increase the potential of entities in the real world, such as numerous army, modern weapons, demographic factor, etc. while the values desired in the web are gaining significance, i.e. investment possibilities, ability to protect against cyber attacks, access to new technologies, highly qualified IT experts. Thereby, the change of power components takes place. In this context, cyberspace as an area of action and holding conflicts can be seen as a kind of *force equalizer* [Madej 2007: 339].

The situation in which various kinds of non-state entities start their activity in cyberspace on a bigger scale may lead to a conclusion that in cyberspace there was a withdrawal from the state-centred attitude – which was distinctive for the late Westphalian international system – according to which the national state is the main and the most important user of international relations. The state with its population, marked by the territorial boundaries and the sovereign authorities does not apply to cyberspace. What results from the lack of territoriality of this "space". Taking into account the fact that in cyberspace the non-state entities constantly gain significance, the bifurcation of the subjective structure of the system and the dynamic demonopolisation of the state power take place in cyberspace. The lowest level is constituted by individual Internet users; the higher level – by institutions, organizations (also organized criminal groups and terrorist organizations), companies, corporations and international organizations, which make use of a couple of computers connected in a network or all IT networks. The highest level is covered by administration structures which use the advanced IT infrastructure, authorities and services acting within the state and the international system conceived as a whole [Madej, Terlikowski 2009: 9].

Broadening the subjective structure within cyberspace does not make it safer or more predictable. This results from the nature of the "space" in which the lack of the centralized power is noticeable. The possibility to organize the network vertically was replaced in case of cyberspace by the horizontal system. These phenomena indicate the existence of anarchy, also in the virtual space. As a result, the space lacks one entity capable of controlling and providing security. Instead, there is a pluralism of norms which provide the relative order and the cooperation of the state and non-state entities for the sake of providing mutual security.

Similarly to the real international system, also in cyberspace – along with the cooperative activities for providing security – there is the competition between the national states regarding the expanding or sustaining the spheres of influence. Thus, the analyzed kind of "space" may be regarded as a new, modern form of geopolitics. The example is the case of Estonia which became a victim of the attack in cyberspace in April 2007, carried out probably by the Russian Federation. The tendency mentioned above is seen also in the case of the cyber attacks on the critical infrastructure of Turkey and Iran.

## 2. SPECIFICITY OF CYBER ATTACKS ON THE CRITICAL INFRASTRUCTURE IN THE ENERGY SECTOR

There is not a single and conclusive definition of a cyber attack to be found in the literature. Instead, various researchers emphasize various elements of this phenomenon. Klaus-Peter Saalbach, for instance, considers cyber attack to be an "attack on computers, information, networks, and systems dependent on computers" [Saalbach 2013: 3–4], whereas the U.S. Army deems it to be "a hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions" [Lakomy 2015: 122]. Experts from the U.S. National Research Council, in turn, have adopted a wider approach, which takes into account the strategic importance of information, whereby a cyber attack is a "deliberate action to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programmes resident in or transiting these systems or networks" [Hathaway et al. 2012: 825]. For the Shanghai Cooperation Organization, the interpretation of a cyber attack is even broader, as it also includes any psychological operation on the Internet [Hathaway et al. 2012: 822–826].

The denotations of cyber attacks provided above underscore only its selected elements, most used methods, and attack objectives, which makes them either too general or too strict. Determining the specificity of a cyber attack requires a broader approach with regard to the following four criteria: their source, or the legal and political status and the organization level of the perpetrators, as well as their motivation, operational methods, techniques, and measures, along with the consequences and objects of attack [Kjaerland 2005; 2006: 124].

An attempt to indicate the sources of cyber attacks should involve dividing them in respect of the legal and political status of the perpetrators. The first group consists of subjects of international law which have the international legal capacity, enabling them to establish and maintain relations with other entities, to conclude international agreements, to be a member of international organizations, to participate in international trade, to press claims against other parties to international relations and enforce them peacefully, to comply with the rules of international law and the agreements concluded, as well as to be held responsible for their own actions and the actions taken by their officials [Kondrakiewicz 2006: 67]. These conditions are met by such entities as countries and international organizations. The second group includes, e.g. terrorist organizations, organised crime groups, other extremist groupings, and natural persons, without the status of a subject of international law or international legal capacity.

The degree of organization of entities which commit cyber attacks should be analysed in respect of their hierarchical system and the nature of the structure [Czermiński, Grzybowski, Ficoń 1999: 42–43]. Entities with a low level of organization do not have an internal hierarchy or organizational structure, or it may prove insignificant. The character of relations within these entities is informal.

This is the case in small groups such as hackers, hacktivists, or cyber criminals. Natural persons also have a low level of organization. Countries, international organizations, organised crime groups, and terrorist organizations, on the other hand, demonstrate a clearly defined hierarchy and a developed organizational structure (formal or informal), hence a high level of organization of these entities.

Motives of perpetrators are also of importance, since they imply their objectives and thus determine the specific nature of cyber attacks they commit. The grounds may be of political, military, religious, economic, social, and individual nature. A cyber attack is intended to promote their ideology and religious values, strengthen their position in the international system, support the implementation of particular military operations, enable them to steal technology and acquire financial benefits, expose a social problem, or develop their own skills [Lakomy 2015: 136].

As to the operational methods, i.e. techniques and measures used in cyber attacks, it should be clarified that techniques denote ways to access secured computer data, whereas measures stand for tools [Lakomy 2015: 123]. The most commonly employed operational methods include:[3] malicious software (computer viruses, worms, Trojans, rootkits, tracking programmes, adware, browser hijackers, ransomware, scareware), denial of service (DoS), network attacks, social engineering attacks, password attacks, material operations, gathering information about the computer vulnerability, and exploiting software vulnerabilities and user errors.

Out of all the types of malicious software employed, computer viruses are one of the most common and most severe cyber attack methods. A virus is attached to a programme file able to copy itself and infect system files without user's knowledge [Lakomy 2015: 124]. It attacks only selected file types and does so only once. Its goal is to modify the data of the victim. Symptoms of infection may be minor and delayed [Johansson 1994]. Viruses propagate, e.g. through any computer network, the Internet, or data carriers. Worms constitute self-replicating programmes which spread via networks. They do not need to be connected to the existing files, neither do they require user activity. Their aim is to infect the entire network infrastructure. They often install a backdoor in order to remotely control the infected computer [Lakomy 2015: 125]. The third category of malicious programmes consists of Trojans. A Trojan horse is "a programme in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage" [Lakomy 2015: 126]. It performs undesirable actions, such as deleting files, reformatting the hard disk, transferring data to the creator, etc. [Bógdał-Brzezińska, Gawrycki 2003: 149]. It uses the so-called backdoors which provide remote data access. It will not self-replicate as it is based on the creator's programme. Another type

[3] In this paper, only the basic information on methods of operations used in cyber attacks is presented. The detailed analysis will apply to methods used in case of a cyber attack on the critical infrastructure of Turkey.

of malicious software found in the literature are rootkits, whose aim is to obtain and maintain access and control of the system which allows the intruder to use it in any way [Lakomy 2015: 126]. Since there already are programmes combining the features of worms and Trojans, some experts are in favour of extending the malware classification by spyware, adware, i.e. unsolicited advertising on the screen, browser hijackers which introduce unwanted modifications to the browser settings, ransomware which blocks certain computer functions until the user makes a cash payment, as well as scareware, i.e. programmes designed to cause fear [Lakomy 2015: 127].

Apart from the malicious software, another destructive operational method of cyber attacks is denial of service (DoS). It is aimed at blocking a computer or a particular service from use by consuming all available resources [Lakomy 2015: 130]. Network attacks, on the other hand, involve manipulating the data which control the transmission of packets. A popular technique employed in those attacks is IP spoofing, which allows for obtaining illegal access to a network by imitating the IP address of an authorised computer [Lakomy 2015: 130]. A phenomenon which has been observed increasingly often is social engineering attacks, where access to information is obtained by surveillance, exploration of working environment and exerting a psychological pressure on the system user [Liderman 2009: 45]. One of the measures used for this purpose is phishing, i.e. impersonating a particular individual or institution in order to obtain sensitive information such as user logins, passwords, and even bank accounts. The victim provides these data upon reading a specially crafted e-mail, opening a file with a malicious code, or being directed to an infected website. Another type of undesirable actions are password attacks or user compromise, where computer or account passwords are determined by the means of the user's personal data, or through the so-called dictionary attacks, where glossary terms are used as potential passwords, or by entering random sequences of characters at an enormously high speed [Lakomy 2015: 131]. A particular type of attacks are material activities, including the use of electromagnetic pulse (EMP) weapons and Van Eck phreaking, which involves intercepting telecommunication signals and digital data saved in the computer memory through monitoring its electromagnetic field [Lakomy 2015: 132]. This allows for acquiring information located on the computer screen without having to break into the system. Many cyber attacks would not have any chance of success without the non-invasive method of collecting information about the vulnerability of a computer. From the perspective of the cyber attack architect, it may also be of importance to locate errors in software (e.g. in the OS code) and mistakes made by computer users (e.g. incorrect configuration of the computer or its applications) [Lakomy 2015: 132].

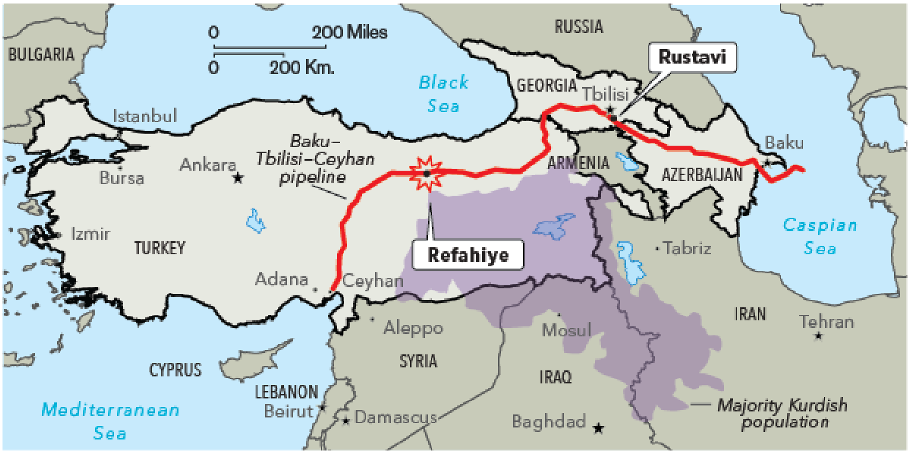
Cyber attacks have the following consequences: permanent or temporary loss of the ability to perform tasks, damaged infrastructure, casualties, leaks of commercial, financial, or classified information regarding the state or a specific undertaking, reactions in the media or propaganda reactions [Marczak 2014: 154].

In the case of attacks intended to infiltrate the internal network of an organization or aimed at data theft, unauthorised entities acquire classified data or information of strategic importance for the development of a business or the State security. Cyber attacks of destructive nature cause such consequences as destruction of information resources of the targeted entity (country, enterprise, natural person), disruption of industrial systems, paralysis of other sectors dependent on network communication, etc. [Marczak 2014: 151–152].

The effects of cyber attacks may be analysed in relation to the objects at which they are aimed, which primarily entails critical infrastructure. In a broad approach, there are eight components of infrastructure: telecommunications (telephone lines, satellites, and commercial, military, academic, and medical computer networks, etc.), energy grid (production, transport, and distribution of energy, transport and storage of the raw materials required for its production), production, storage, and transport of crude oil and natural gas (pipelines, vessels, road and rail transport), banking and financial system (available instruments for financial operations), transport (air, rail, sea, and road transport, inland waterways, all in relation to persons and goods, the whole system of logistical support), water supply (water intakes, water tanks, waterworks, filtering systems and water purification systems, water provision systems), emergency services, as well as systems which provide for the continuation of the authority and public services [Bógdał-Brzezińska, Gawrycki 2003: 134–135].

### 2.1. CYBER ATTACK ON CRITICAL ENERGY INFRASTRUCTURE OF TURKEY

The explosion of the Baku–Tbilisi–Ceyhan oil pipeline (BTC) occurred on August 6, 2008 at 23.00, yet the pipeline staff became aware of it only forty minutes later. The subsequent investigation revealed that the offender had exploited the vulnerability of one of the safety mechanism components. Every kilometre of the oil pipeline was equipped with camera monitoring, oil pressure flow sensors, and fire alarms. The parameters read by those appliances were transferred to the pipeline control centre by means of a wireless network and by the emergency satellite connection in case of communication issues. From the analysis of the attack it may be seen that the computer responsible for collecting diagnostic data underwent misconfiguration. The perpetrators most likely also suppressed satellite communications, which explains why the sensors did not report the parameters *via* the alternative communication channel [Kozak 2016]. Moreover, 60 hours of footage were deleted from the recorder discs. The only recovered image came from an infrared camera connected to a separate network. The recording showed two men in special forces uniforms carrying laptops along the pipeline a few days before the explosion. Examination of system logs from oil pipeline computers confirmed a time correlation between that event and the moment when the ICT infrastructure was being scanned. The initial attack vector was the communication software used by the monitoring camera. Upon obtaining the access to the computer operation network, the perpetrators gained entry onto the internal network of the oil pipeline and subsequently installed a backdoor on one of the computers running a Windows OS. Consequently, they were able to take over the controllers of the individual valves and in this way manipulate the values corresponding to the pressure level in particular sections of the oil pipeline. As a result, they caused a leak and an explosion on one of the object valve stations [Kozak 2016].



Map 1. Baku–Tbilisi–Ceyhan pipeline (BTC)

Source: Bloomberg research

As a consequence of the Baku–Tbilisi–Ceyhan fire, its majority shareholder, the British company BP, announced that its daily financial losses amounted to five million dollars [Kozak 2016]. The company also lost 30,000 barrels of crude oil [Konieczny 2015]. Yet the effects of the cyber attack on the oil pipeline in question need to be analysed in a broader, not only financial perspective.

Beside the Baku–Tbilisi–Erzurum gas pipeline (BTE), the Baku–Tbilisi–Ceyhan gas pipeline is one of the key energy investments of the Republic of Turkey. It was in November 1999 in Istanbul that the decision to create this transfer route was made. In accordance with the agreement between Turkey, Azerbaijan and Georgia, the oil extracted in Azerbaijan was to be transported by the Baku–Tbilisi–Ceyhan pipeline through the territory of Georgia to Turkey, circumventing Russian borders. The target flow level from Baku to the Ceyhan port in Turkey amounted to approximately one million barrels of crude oil per day. Its final destination was primarily Western Europe. The construction of the BTC oil pipeline, launched in September 2002, was entrusted to a consortium of the same name. Its majority shareholders were BP and SOCAR (the State Oil Company of Azerbaijan Republic), whereas the minority shareholders included Chevron (US), Statoil (Norway), and Eni (Italy). The construction cost of the oil pipeline was estimated at over four billion dollars. The profits from the transit fees predicted for Turkey at the maximum bandwidth of 50 million tonnes might reach approximately 300 million dollars on an annual basis [Piotrowski 2005: 99].

Three days after the BTC attack, the war between the Russian Federation and Georgia broke out. One of the first attacks was aimed at a section of the oil pipeline near the town of Rustavi. Kurdistan Workers' Party (PKK) later claimed responsibility for the attack [Smoleń 2012: 272–286], although some experts point out that the Kurds would not be able to carry out such an undertaking on their own. Given the fact that Russia had opposed the construction of the oil pipeline from the very beginning,[4] its participation in this cyber attack cannot be excluded. In December 2014, Bloomberg stated the cyber attack was driven by Russians [Maciążek 2014].

For the purpose of classifying the Baku–Tbilisi–Ceyhan cyber attack under the four criteria described above, it should be noted that it is not possible to clearly identify the source of this attack. There is certain probability that the Kurdistan Workers' Party is responsible for it. This grouping supports the aspirations for the national independence of the Kurds, but due to its use of extremist methods, it is considered a terrorist organization by a part of the international community, including the European Union and the United States. It has, therefore, no legal capacity under international law, nor is it a subject of it. In the case of the Russian Federation, i.e. the other alleged instigator or perpetrator of the pipeline cyber attack, it is the opposite. Russia is a subject of international law as a country and has such legal capacity. Furthermore, the level of organization of both entities suspected of committing the attack is remarkably high, with a clearly defined internal hierarchy and a developed internal structure. As to the motivations of the potential perpetrators, members of the Kurdistan Workers' Party might have intended to weaken the political and economic situation in the Republic of Turkey,

[4] The concept of transporting the energy resources through the so-called Caucasian-Turkish corridor was supported by the United States and the European Union. On the one hand, the East-West axis increased the influences of the United States in the Caucasian region and the integration of this part of the world with the global economy and the international system. On the other hand, it led to the isolation of Iran, which is in line with the will of the US leaders. It also posed a threat to Russian influences in the Caucasian region and in the Central Asia. It weakened the monopoly of its concerns: Gazprom and Transbieft in terms of the control of transporting routes of resources from the Caspian region. Thus, it limited the participation of Russia as a distributor in the energy market among the European countries. In this way, it created the chance for the diversification of supply sources of natural gas and led to the independence of the European Union from Russian supplies. Due to these threats, the Russian Federation opposed the concept of the so-called Caucasian-Turkish corridor. As an alternative route, Russia proposed the pipeline which connects the oil fields in Kazakhstan with the port in Novorossiysk in Russia and the project of the Burgas–Alexandroupoli pipeline, through which the oil from Russia and Kazakhstan would be transported to Bulgaria and Greece. The undisturbed transit of natural gas to Europe would be provided for the Russian Federation by the Blue Stream pipeline.

whose authorities had opposed the idea of a Kurdish country for years, hence the probability of political inspiration of their actions. It could also have been a political motive, reinforced with the economic factor, that made the pipeline attack seem desirable from the perspective of the interests of Russia in the region of the Caspian Sea, particularly in the context of Russian aspirations to maintain control of the routes of raw material transport in the area and its subsequent distribution to Europe.

In conclusion, the cyber attack on the Baku–Tbilisi–Ceyhan pipeline presented above was the first action of this sort worldwide aimed against critical infrastructure. It was 2 years later that the Iranian nuclear facilities were attacked by the special forces of Israel and the United States with the use of malicious software called Stuxnet, which was widely analysed and publicised.

## 3. IMPACT OF CYBER ATTACKS ON ENERGY SECURITY OF A COUNTRY

Energy is a factor which determines many areas of social life due to its trans-sectoral nature [Attila 2012]. It is of key importance for the economy and for development processes, for social life and consumption processes, for politics, and for governance, and thus it constitutes a crucial factor behind a country's power, defence, impact, and geopolitical schemes in the field of contemporary international relations. It is the source of prosperity, a determinant of technological innovation and competitiveness of the economies of particular countries [Pascual, Elkind 2010: 1].

Since the end of the Cold War, the economic importance of energy has been also interpreted politically, forming the widespread belief that possessing adequate energy resources is compulsory for the economic and political power of a country. Energy has therefore become an instrument for influencing the behaviour of other countries. At the same time, numerous states have seen a rise in their vulnerability to and propensity for various problems concerning the access to energy carriers as a result of the fluctuations on the market of raw energy materials or exploitations in this respect, i.e. when those materials are used as a tool for achieving political objectives and exerting pressure [Özcan 2013]. Given the systematic growth in energy consumption on the one hand, and its politicisation on the other hand, energy has consequently evolved into a vital factor behind social life, processes of economic development, as well as national and international security, with the last one becoming increasingly more significant [Flaherty, Filho 2013: 13].

In view of the multi-faceted value of energy described above, it may be concluded that it is now a strategic resource, along with raw energy materials [Gradziuk et al. 2003: 72]. Energy and access to it has been recognized as a component of the contemporary, broadly understood security. On the one hand, increasing international interdependence and the dynamics of the globalisation processes in the post-Cold War era are expanding the subjective scope of security by extracting its new dimensions, which is reflected in the concept of comprehensive security. On the other hand, the personal scope of security is expanding as well. The so-called vertical deepening should be understood as including entities other than the state itself in the security analysis. The trends delineated above give rise to an increased complexity of risks, security, and action taken to ensure it. It is important that they also imply an autonomous nature of the energy aspect of security. It was, however, isolated from the notion of economic security relatively late, i.e. at the turn of the 20th and 21st century.

It is essential to outline the multidimensional nature of security and its requirements, as well as the nature of energy security [Żukrowska 2011: 397; Pascual, Elkind 2010: 2] in order to properly determine the impact of cyber attacks on this aspect of security, namely from the perspective of the state. Along with the progress of the information revolution since the turn of the 20th and 21st century, there has been a steady increase in the importance of cyberspace as a source of challenges and threats to the security of the state. This is because this specific type of "space" has begun to be used as a convenient area for implementing measures considered to be harmful to national and international security [Lakomy 2015: 103]. This is confirmed by numerous reports, i.e. the report published by the analysts of Kaspersky Lab in 2013, which shows that up to 91% of companies have detected attacks on their systems this year. 50% of undesirable actions in cyberspace have been aimed at the energy sector, while the control systems in the energy sector were the target of 30% of such activities [Malko, Wojciechowski 2015].

These statistics confirm that cyber attacks on critical infrastructure pose an increasingly more serious challenge to the security of the state [Bania 2012: 286; Aleksandrowicz, Liedel 2014: 11]. Their consequences are to be considered in two dimensions, i.e. direct and indirect. The direct consequence of a cyber attack is either the total destruction or disruption of the energy infrastructure of a given state, with the first blocking the access to raw energy materials on a permanent or a long-term basis (if there are no diverse supply sources), and the latter temporarily limiting its availability. Regardless of the scale of damage, there are rare situations of casualties, as well as financial costs associated with the reconstruction or the construction of new infrastructure, or trade disruption.

Indirect consequences of cyber attacks are, however, much more severe. First of all, the affected state loses the supply chain continuity in respect of the particular raw material. With no alternative supply sources, its energy security is directly threatened. At this point, the state is at risk of becoming dependent on another, often stronger entity in the field of energy. Such relationship has financial (high costs of purchasing the raw material from a new source or a loss of income in the case of export), but above all geopolitical implications. This is the type of threat which Turkey faced following the attack on the Baku–Tbilisi–Ceyhan pipeline.

The highly probable participation of Russia was supposedly to provide it with control monopoly over the routes of hydrocarbon transit from the Caspian area. Temporarily disrupting the operation of the object would make Turkey lose its credibility as a reliable "transit" country and as a supplier of crude oil. This would also thwart its potential of influencing the events in the Caucasus and Caspian regions, which are zones of contention and competition for influence between Turkey and the Russian Federation.

It is therefore evident that national energy security is becoming "politicised". First, it is because energy carriers have become a tool for state entities to achieve their own political objectives. Secondly, they use them to exert an influence on other participants of international relations. Thirdly, energy is a subject of political decisions at the highest level. These circumstances may lead to changes in the international position of countries, and even in the importance of entire geopolitical regions in international relations [Misiągiewicz 2012].

The trends delineated above allow for the recognition of cyberspace as a new and modern form of geopolitics, as well as another arena for the international conflict and competition – the fifth one already, in addition to the air, land, sea, and space [*Department of Defense*… 2011].

## 4. THE REACTION OF THE STATE TO CYBER ATTACKS ON THE CRITICAL INFRASTRUCTURE IN THE ENERGY SECTOR

The activities of the state which are aimed at counteracting cyber attacks on the critical infrastructure in the energy sector should be carried out on two levels: inside the state and internationally. The multidimensional approach to the problem of cyber attacks is conditioned to a large extent by the character of cyberspace.

On the state level, the security of the energy sector is provided by the following activities: active defense, passive defense, improving the specific phases of defense, effective technological defense, professionalization of the sector of the fight against cybercrime. They should be completed by the international cooperation. Referring to the first activity, which is the active defense, it should be underlined that it is aimed at detecting, unmasking and then punishing the subject responsible for the attack. The preventive actions can be included as part of it [Szulc-Wałecka 2014: 289]. Due to the fact that especially detecting the author of the cyber attack requires a multidimensional and very eager involvement of the state, the authorities decide more often to defend passively, which consists in improving the safety elements that can possibly become the subject of the attack. According to experts, this strategy is insufficient. A more complex approach is required in this case. Improving the specific phases is another activity required due to the protection of the energy critical infrastructure against cyber attacks. It consists, first of all, of the prevention which means implementing safety elements as soon as in the design phase of the facility, controlling the human factor, legal bans. Secondly, it includes the incident management, mitigating incidents and minimizing damage caused by them. This is achieved, *inter alia*, by improving the alarm effectiveness, strengthening the system protection. Thirdly, managing the consequences of the attack is required among others by renewing the damaged objects [Szulc-Wałecka 2014: 290]. The other element of the defense strategy is the effective technological protection of the critical infrastructure by improving the existing solutions. Due to the fact that the shares in a large part of this kind of infrastructure are held by the private entities, it is necessary that the private entities cooperate constantly with the state based on the subsidiarity of the cooperation. Moreover, the constant exchange of information between them is required [Szulc-Wałecka 2014: 290]. The professionalization of the sector of the fight against the cybercrime consists in adapting the legislation to the changing threats and abilities of authorities which are responsible for the prosecution and trial of the cyber criminals. It occurs due to the involvement of IT specialists [Szulc-Wałecka 2014: 291]. Regardless of the activities carried out by the state as part of protecting its critical infrastructure against the cyber attacks, the involvement of many entities is necessary. The cooperation of the following is required: states and their services, IT specialists, non-profit organizations, interest groups and scientists, etc. [Kruczkowska 2011].

Along with the strategy to fight against cyber attacks individually implemented by the state, the international cooperation in this matter should be constantly developed. In this context, another important problem should be taken into consideration which is the lack of international legal and system regulations which refer to the rules of the fight and conflicts in cyberspace [Lee 2012]. This significant gap is conditioned to a large extent by, among others, the impossibility to create a common definition of cyberspace [Grzelak, Liedel 2012: 129], and to define the essence of threats which result from its specificity. The individual interests of particular states are essential in this context, because their lack of agreement hinders creating the common approach to the problem of cyber attacks. The tendency mentioned above may be seen, among others, in the debate over government's rights to infringe the right to privacy and controlling the Internet.

In the latter case, a substantial dissonance can be observed between the approaches of China and Russia, which allow the possibility of controlling the "web" by the state, and a part of the Western international society, which excludes it. As an example, both countries formulated entirely different priorities during the United Nations works on the security of state in cyberspace [Lakomy 2015: 350]. As a result, there was no consensus regarding the specific practical solutions. It is worth noting that among organizations of the UN system only the International Telecommunication Union managed to create valuable mechanisms of international cooperation regarding this matter. In this context, the following initiatives should be mentioned: Global Cybersecurity Agenda and International Multilateral Partnership Against Cyber Threats [Lakomy 2015: 351–365].

Some regional initiatives are started along with the activities of the universal character in the international system. The problem of the security of state in cyberspace may be found in regulations introduced by NATO, the Council of Europe, the European Union, Organisation for Economic Cooperation and Development, Shanghai Cooperation Organisation, etc. [Lakomy 2015: 365–404, 410–414; Bógdał-Brzezińska, Gawrycki 2003: 222–225, 227–244]. Among these regulations, the solutions of NATO are worth being mentioned. This organization created three areas of cooperation referring to energetics. One of these areas is the cooperation in terms of the protection of the critical infrastructure and the NATO Energy Security Centre of Excellence is responsible for this part. It is a kind of an analytical institution which offers the support for the members of NATO in creating analyses, recognizing the international system, implementing tests and tasks [Kister 2016]. The ministries of the member states: the Ministry of National Defence, the Ministry of Foreign Affairs and the Ministry of Interior cooperate with the Centre as well as the operators of energetic systems and scientists from all over the world.

After the 2016 Warsaw NATO Summit, Prime Ministers of the member states issued a statement with a point stating that they recommend to intensify the cooperation with the International Energy Agency and the European Union as well as to provide the efficient exchange of information, consultations, workshops and seminars regarding the critical infrastructure. According to the politicians, the energy security of the member states should be provided by, among others, security of supplies, diversification of energy sources, construction of interconnectors [Kister 2016].

Regarding the defence strategy of the Republic of Turkey against the cyber attacks on the critical infrastructure, it is worth emphasizing that in the internal dimension it is consistent with the scheme presented above in terms of activities performed by the state in case of this kind of threat. In the multilateral dimension, Turkey is obliged to abide by the regulations of the international organizations that it belongs to. In this context, it is important to stress the particular cooperation – mostly due to the experiences – between this state and the NATO Energy Security Centre of Excellence. Regardless of these activities, the authorities of Turkey perform a range of other initiatives on an international scale. For instance, in May 2016, they announced the cooperation with the leaders of Georgia and Azerbaijan in the area of the cyber security and the protection of pipelines [Łomanowski 2016].

## CONCLUSIONS

To sum up, the presented analysis of the problem of cyber attacks on the critical infrastructure of the state indicates that cyberspace is now a source of serious challenges and threats to the security of state. They are implicated by the specific features of cyberspace, *inter alia*, the lack of a central authority centre and a non-spatial character. In terms of cyberspace, there is also a change in the importance of power components in the international relations. A flexible strategy of defence against cyber attacks, supported by international cooperation with many entities: other states, international organizations, IT specialists, business sector and

scientists, is decisive in the area of state position and the possibility of having the influence on the international system. Considering the fact that security now refers to many areas of social life and the sources of its threats are political, economic, military, social, ecological, demographic and energetic, there is a withdrawal of thinking about it only from the perspective of military threats, posed by other countries. The extension of its subjective and objective scope refers to all areas of social life. The energy security has become *ipso facto* one of the autonomous dimensions in the structure of broadly understood security.

**Tytuł:** Problem cyberataków na infrastrukturę krytyczną państwa w sektorze energetycznym. Przypadek Turcji

**Streszczenie**: Celem poznawczym niniejszego artykułu jest analiza problemu cyberataków na infrastrukturę krytyczną państwa w sektorze energetycznym. W ramach *case study* zaprezentowano przypadek Turcji. Państwo to ze względu na odgrywanie roli „korytarza tranzytowego" dla transportu węglowodorów posiada silną pozycją na międzynarodowym rynku surowców energetycznych, przez co cyberataki dokonywane na infrastrukturę krytyczną Turcji mają poważne konsekwencje nie tylko dla rozwoju tego państwa oraz jego bezpieczeństwa, lecz także układu geopolitycznego w regionie Bliskiego Wschodu i rozkładu sił na – wspomnianym powyżej – międzynarodowym rynku węglowodorów. Dla potrzeb podjętego problemu przyjęto następujące założenia badawcze. Po pierwsze, cyberprzestrzeń stanowi potencjalne źródło zagrożeń dla bezpieczeństwa państwa. Dzieje się tak, gdyż jest to rodzaj „przestrzeni", która „wymyka się" spod kontroli państwowych organów bezpieczeństwa. Zwiększa to prawdopodobieństwo cyberataków, m.in. na infrastrukturę krytyczną państwa. Po drugie, w warunkach cyberprzestrzeni dochodzi do zmiany ważności komponentów siły w stosunkach międzynarodowych. Wzrost skali i liczby cyberataków potwierdza, że o pozycji państwa i możliwości wywierania przez nie wpływu na system międzynarodowy decyduje obecnie skuteczna zdolność obrony przed atakami w cyberprzestrzeni oraz posiadanie wysoko rozwiniętej technologii informatycznej. Po trzecie, w warunkach procesów globalizacji i odejściu wraz z końcem zimnej wojny od myślenia o bezpieczeństwie z perspektywy zagrożeń wojskowych doszło do poszerzenia jego zakresu podmiotowego i przedmiotowego. Bezpieczeństwo dotyczy obecnie wielu obszarów życia społecznego, zaś źródła jego zagrożeń mają charakter: polityczny, gospodarczy, wojskowy, społeczny, ekologiczny, demograficzny, energetyczny. Tym samym bezpieczeństwo energetyczne stało się jednym z autonomicznych wymiarów w strukturze szeroko pojmowanego bezpieczeństwa.

**Słowa kluczowe**: cyberatak, Turcja, infrastruktura krytyczna, bezpieczeństwo państwa, cyberprzestrzeń, bezpieczeństwo energetyczne

## REFERENCES

1. Aleksandrowicz T.R., Liedel K. (2014), *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia*, [in:] K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Difin, Warszawa.
2. Attila F. (2012), *Energy Security from a Regional Perspective – the Concept of Regional Energy Security Complexes*, Budapest, www.etd.ceu.hu/2013/farkas_attila.pdf [access: 27.09.2017].
3. Bania R. (2012), *Wojny w cyberprzestrzeni – przypadek Iranu*, [in:] R. Bania, R. Zdulski (red.), *Bezpieczeństwo narodowe i międzynarodowe w regionie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*, UŁ, Łódź.
4. Berdel-Dudzińska M. (2012), *Pojęcie cyberprzestrzeni we współczesnym polski porządku prawnym*, „Przegląd Prawa Publicznego", nr 2.
5. Bloomberg research, https://www.google.com/search?q=baku+tbilisi+ceyhan&client=firefox-b-ab&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjZpOPdnP3fAhUxNOwKHTmWD1gQ_AUIDigB&biw=1366&bih=654#imgrc=2rPFNJbfZAnsUM [access: 21.12.2018].
6. Bógdał-Brzezińska A., Gawrycki M.F. (2003), *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Aspra, Warszawa.
7. Czermiński A., Grzybowski M., Ficoń K. (1999), *Podstawy organizacji i zarządzania*, WSAiB, Gdynia.
8. *Department of Defense Strategy for Operating in Cyberspace*, (2011), Department of Defense in the USA, July, https://www.hsdl.org/?view&did=489296 [access: 28.09.2017].
9. Flaherty Ch., Filho W. (2013), *Energy Security as a Subset of National Security*, [in:] W. Filho, V. Voudouris (eds.), *Global Energy Policy and Security*, Springer, London.
10. Gibson W. (2009), *Neuromancer*, Książnica, Katowice.
11. Gradziuk A., Lach W., Posel-Częścik E., Sochacka K. (2003), *Co to jest bezpieczeństwo energetyczne państwa?*, [in:] S. Dębski, B. Górka-Winter (red.), *Kryteria bezpieczeństwa międzynarodowego państwa*, PISM, Warszawa.
12. Grzelak M., Liedel K. (2012), *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe", nr 22.
13. Hathaway O.A., Crootof R., Levitz P., Nix H., Nowlan A., Perdue W., Spiegel J. (2012), *The law of cyber attack*, "California Law Review", vol. 100.
14. Johansson K. (1994), *Computer Viruses: The Technology and Evolution of an Artificial Life Form*, http://interactionstation.wdka.hro.nl/mediawiki/images/7/76/The_Technology_and_Evolution_of_an_Artificial_Life_Form.pdf [access: 16.09.2017].
15. Kister Ł. (2016), *W PSE skutecznie przeciwdziałamy cyberatakom*, „Biznes Alert", July 21, http://biznesalert.pl/pse-skutecznie-przeciwdzialamy-cyberatakom/ [access: 30.09.2017].
16. Kjaerland M. (2005), *A classification of computer security incidents based on reported attack data*, "Journal of Investigative Psychology and Offender Profiling", no. 2. DOI: https://doi.org/10.1002/jip.31.
17. Kjaerland M. (2006), *A taxonomy and comparison of computer security incidents from the commercial and government sectors*, "Computers & Security", no. 7. DOI: https://doi.org/10.1016/j.cose.2006.08.004.
18. Kondrakiewicz D. (2006), *Państwo*, [in:] M. Pietraś (red.), *Międzynarodowe stosunki polityczne*, UMCS, Lublin.
19. Konieczny P. (2015), *10 godzin bez prądu, czyli potężna awaria elektrowni w Turcji. Czy to cyberatak?*, „Niebezpiecznik", April 15, https://niebezpiecznik.pl/post/10-godzin-bez-pradu-czyli-potezna-awaria-elektrowni-w-turcji-czy-to-cyberatak [access: 25.09.2017].

20. Kozak A. (2016), *Cyberbezpieczeństwo przemysłowych systemów sterowania*, „Automatyka-Online.pl", February 9, http://automatykaonline.pl/Artykuly/Inne/Cyberbezpieczenstwo-przemyslowych-systemow-sterowania [access: 24.09.2017].
21. Kruczkowska D. (2011), *Cyberterroryzm znakiem naszych czasów*, „psz.pl", September 12, http://www.psz.pl/116-bezpieczenstwo/cyberterroryzm-znakiem-naszych-czasow [access: 28.09.2017].
22. Lakomy M. (2015), *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, UŚ, Katowice.
23. Lee D. (2012), *Flame: UN urges co-operation to prevent global cyberwar*, "BBC News", June 7, http://www.bbc.com/news/technology-18351995 [access: 28.09.2017].
24. Liderman K. (2009), *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa.
25. Łomanowski A. (2016), *Turcja tworzy antyrosyjski sojusz wojskowy*, „rp.pl", May 16, http://www.rp.pl/Dyplomacja/305169856-Turcja-tworzy-antyrosyjski-sojusz-wojskowy.html#ap-1 [access: 30.09.2017].
26. Maciążek P. (2014), *Rosja sięga po energoterroryzm. Kluczowe rurociągi zagrożone*, „Space24", December 12, http://www.space24.pl/167144,rosja-siega-po-energoterroryzm-kluczowe-rurociagi-zagrozone [access: 27.09.2017].
27. Madej M. (2007), *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, PISM, Warszawa.
28. Madej M. (2009), *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [in:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo informatyczne państwa*, PISM, Warszawa.
29. Madej M., Terlikowski M. (red.) (2009), *Bezpieczeństwo informatyczne państwa*, PISM, Warszawa.
30. Malko J., Wojciechowski H. (2015), *Sektor energetyczny i cyberbezpieczeństwo*, „Nowa Energia", nr 1.
31. Marczak P. (2014), *Cybertataki – narzędzia konfliktu w cyberprzestrzeni*, [in:] K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Difin, Warszawa.
32. Misiągiewicz J. (2012), *Geopolitics and energy security in the Caspian region*, "Teka Komisji Politologii i Stosunków Międzynarodowych", vol. 7.
33. Mojska K. (2013), *Korporacje transnarodowe jako podmioty instytucjonalizacji ochrony środowiska w przestrzeni transnarodowej*, [in:] E. Haliżak, M. Pietraś (red.), *Poziomy analizy stosunków międzynarodowych*, vol. 1, PTSM, Warszawa.
34. Özcan S. (2013), *Securitization of energy through the lenses of Copenhagen school*, [in:] *The 2013 Orlando International Conference*, 21–23 March, https://www.westeastinstitute.com/wp-content/uploads/2013/04/ORL13-155-Sezer-Ozcan-Full-Paper.pdf [access: 27.09.2017].
35. Pascual C., Elkind J. (2010), *Introduction*, [in:] C. Pascual, J. Elkind (eds.), *Energy Security. Economics, Politics, Strategies and Implications*, The Brookings Institution, Washington, D.C.
36. Pietraś M. (2003), *Bezpieczeństwo państwa w późnowestfalskim środowisku międzynarodowym*, [in:] S. Dębski, B. Górka-Winter (red.), *Kryteria bezpieczeństwa międzynarodowego państwa*, PISM, Warszawa.
37. Pietraś M. (2013), *Przestrzeń transnarodowa jako poziom analizy w nauce o stosunkach międzynarodowych*, [in:] E. Haliżak, M. Pietraś (red.), *Poziomy analizy stosunków międzynarodowych*, vol. 1, PTSM, Warszawa.

38. Pietraś M. (2015), *Przestrzeń badawcza nauki o stosunkach międzynarodowych*, „Politeja", nr 5(36). DOI: https://doi.org/10.12797/Politeja.12.2015.36.05.
39. Piotrowski M.A. (2005), *Polityka w sektorze naftowo-gazowym*, [in:] T. Bodio (red.), *Turkmenistan. Historia – polityka – społeczeństwo*, Elipsa, Warszawa.
40. *Rządowy Program Ochrony Cyberprzestrzeni na lata 2011–2016*, 2010, MSWiA, Warszawa.
41. Saalbach K. (2013), *Cyber War. Methods and Practice*, Universität Osnabrück, Osnabrück.
42. Siwicki M. (2013), *Cyberprzestępczość*, Beck, Warszawa.
43. Smoleń K. (2012), *Ekstremizm polityczny w Turcji. Analiza na przykładzie Partii Pracujących Kurdystanu*, [in:] A. Moroska-Bonkiewicz (red.), *Ekstremizm polityczny we współczesnym świecie*, DSWE, Wrocław.
44. Szulc-Wałecka E. (2014), *Znaczenie cyberterroryzmu we współczesnym świecie*, [in:] M. Marczewska-Rytko (red.), *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja)*, UMCS, Lublin.
45. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 Nr 89, poz. 590).
46. Wasilewski J. (2013), *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 9 (13).
47. Żukrowska K. (2011), *Bezpieczeństwo energetyczne*, [in:] K. Żukrowska (red.), *Bezpieczeństwo międzynarodowe. Przegląd aktualnego stanu*, SGH, Warszawa.