Numer 1(6)/2018

SECURITY REVIEW

Numer 1(6)/2018

Wydanie specjalne

Wydział Administracji i Nauk Społecznych

Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie

ISSN 2543-6694

SECURITY REVIEW

NUMER 1(6)/2018

Drodzy czytelnicy,

Witam serdecznie na łamach numeru specjalnego kwartalnika „Security Review", specjalnego dlatego, że swoje artykuły prezentują w nim doktoranci Wojskowej Akademii Technicznej oraz członkowie Koła Naukowego Bezpieczeństwa Narodowego WAT.

W numerze tym znajdziemy dwa artykuły w języku angielskim, jeden w języku polskim oraz recenzję książki „Bezpieczeństwo energetyczne i ochrona klimatu w drugiej dekadzie XXI wieku. Energia - Środowisko - Klimat".

Szczególną uwagę czytelników zwracam na informację zamieszczoną w kwartalniku a dotyczącą nowo powstałej idei pod nazwą Baza Ludzi Nauki Służb Mundurowych. Dzięki inicjatywie i zaangażowaniu osobistemu dr Radosława Wiśniewskiego oraz jego zespołowi, stworzona została baza osób, które przez szereg lat pełniły i nadal pełnią służbę w różnego rodzaju służbach mundurowych, ale również zajmowali się i zajmują do chwili obecnej nauką.

Mam nadzieję, że wydawanie co jakiś czas numerów specjalnych naszego kwartalnika stanie się dobrą tradycją a jednocześnie okazją do publikacji pracowników naukowych poszczególnych uczelni wyższych kształcących w zakresie szeroko pojętego bezpieczeństwa.

Szanowni Państwo to już szósty numer naszego czasopisma, ale mimo tego jego tworzenie spotyka się co jakiś czas z różnymi trudnościami. Ostatnimi czasy powstał poważny problem związany z wykonywaniem korekty naszych numerów, jednak dzięki pomocy udzielonej przez Panią Prorektor ds. nauki Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie i okazanego przez nią wsparcia mogliśmy ruszyć dalej i wydać kolejny numer kwartalnika.

Zapraszam do lektury i zachęcam również do publikacji na jego łamach. Przed państwem szósty numer czasopisma. Życzę interesującej lektury.

W imieniu Rady Naukowej
i Zespołu Redakcyjnego
gen. bryg. rez. dr inż. Tomasz Bąk

W TYM NUMERZE:

Ensuring safety in the age of widespread technology S. 3
Sylwester Pniak

Unconventional threats in civil aviation S. 9
Kamil Gefert

Problematyka definiowania dowodzenia S. 14
Szymon Kochanowski

Recenzja książki *Bezpieczeństwo energetyczne i ochrona klimatu w drugiej dekadzie XXI wieku. Energia—Środowisko—Klimat* S. 24
Anna Kardasz

ENSURING SAFETY IN THE AGE OF WIDESPREAD TECHNOLOGY

Sylwester Pniak

Abstract

In the era of dynamic technological development and the coupling of most technologies directly with the unit, one can assume that an increasing discord between the conviction and uncertainty of the situation in which the community is observed. In this work the author points out that conscious society has a sense of constant observation. Population wanting to protect their own privacy, faces a difficult choice - whether to keep up with the times, entrusting part of their own privacy, or to limit the use of new technologies, thus remaining more anonymous.

Keywords: liquid surveillance, individual security, privacy protection

Introduction

State security creates a dialectical relationship with numerous threats. On the one hand, the evolving technological progress is the driving force of security construction, but on the other hand it creates new threats. In order to maintain the right level of security, it is necessary to take security measures covering many areas, including military, political, economic and public spheres. These considerations focus on activities that enter the public sphere and are directly related to the introduction of new technological solutions.

The topic of the work was chosen due to the expanding penetration of technology into social life. The multitude of devices in private use poses a risk of unconsciously providing information which is then collected through the used devices for further processing. In addition, the desire to maintain the highest level of security forces the state to apply modern control solutions.

Focusing on the security of information society, it is worth paying attention to the sources of current information exchange, as well as the ways of its transmission. The countless modern devices available to their users enable continuous communication with a global network. A worrying observation is that nowadays there are many more devices connected to the Internet than there are users. Such a situation may make us to "slaves" of new technologies. The constant use of technological innovations and direct integration of private life and new devices mean that our activities depend mostly on the access to new solutions as well as on the Internet (Pniak, 2017, p. 253).

The phenomenon of constant surveillance

The term "constant surveillance" put forward by Zygmunt Bauman reflects today's times that form the background elements of the reality in a labile way. It can be said that constant surveillance is a kind of infiltration adapted to the changing realities of everyday life. The society makes any possible effort to eliminate the sense of fear; however, each such interfer-

ence creates further threats or finally increases the level of anxiety (Bauman, Lyon, 2013, pp. 79 -110).

Our unstable times make the appearance of some threats more likely. One example in this category are asymmetrical threats. The evolution of asymmetrical threats shows more and more possibilities of technological adaptations to cause personal, material and economic damage as well as directly impact authorities and communities. That situation motivates us to shape and develop technologies adequately to the escalating threats – not only those which have already occurred, but also those which may occur in the future.

Not surprisingly, to ensure an adequate level of security, new scanning devices, detectors, biometric fingerprint or iris readers appear at airports. RFID chips (RFID, *Radio-frequency identification* – a technique that allows reading and, in some cases, writing information in the system. There are many types of chips; depending on the design, it is possible to read labels at a distance of several dozen centimeters to more than one hundred meters away from the reader's antenna. The label reading system allows identification of many items at the same time in the scan field) which can be found in modern passports are becoming a common solution. An individual who is a direct user of new devices is concerned about the possibility of them belonging to the risk group as a result of incorrect analysis of personality parameters, or about being disallowed entry to a target zone or deprived of the right to leave.

Since the whole society wants to feel safe, the problem of ensuring safety concerns everyone. However, there is no way to keep pace with the development of new technologies, we can only assimilate to them (Lyon, Dec 2010, pp. 325-338). One may get the impression that the part of the society who are engaged in technological innovations cope well with their adaptation in everyday life. That impression, however, may lead to hasty conclusions. Closer observation shows that even people who are heavily involved in technological progress may have difficulties finding their place or status in an automated world.

Zygmunt Bauman, in an interview with David Lyon, interprets and discusses the above problem on the example of a two-edged sword. He recognizes technology as the key feature of modernity, saying that the improvement, development and implementation of techniques that change our reality is currently a priority. Taking into consideration the nature of a two-edged sword, it is necessary to draw attention to the fact that such a sword can cut on both sides. It can be used to eliminate current problems, but a strong, violent and chaotic use of it can also cause some side effects. It is known that in targeting certain goals – assuming the goals fall within legal norms and fairness – the sword can still harm some accidental victims. The effectiveness of our activities depends on the concentration on selected objects. As a rule, relations with many other objects are created through a network of interrelations resulting in a situation which is not included in the previously considered proceedings. It is necessary to take into account that any actions taken, in addition to the targeted goals, may also bring unplanned consequences. Therefore, when undertaking certain activities, it is necessary to accept the risk associated with them (Bauman, Lyon, 2013, pp. 139-140).

The public got used to and even attached to the new technologies, so the appearance of a new device in a city does not impress many. On the one hand, the technological revolution initiated at the end of the 20th century gave freedom to humanity (through the possibility of continuous communication within a global network), but on the other, limited the possibilities of free and anonymous social life. The global unification of new infiltration technologies can be indicated as a significant phenomenon affecting the sense of security. An individual familiar with the current methods of surveillance is aware of the devices that can be encountered when travelling travel around the world. At the same time, such a person is certain that in the

case of an unfortunate turn of events there is a way to assert his or her arguments or enforce the law against undesirable situations.

Operators of the said devices have constant access to up-to-date information. Their training allows to properly analyze events and take actions against any possibility of an arising threat. Assuming that knowledge gives power, the fact of having information on as many citizens (or simply people staying at a given place) as possible results not so much in proper interpretation of the situation, but rather gives an opportunity to use the data afterwards. Information gathered in one place facilitates analysis of the collected data, either an immediate or a postponed one. Keeping a finger on the pulse of events, the probability of detecting a threat and limiting its negative effects increases.

The question that arises is whether society is actually in possession of new technologies that ensure security, or whether it is being forced to submit to them in order to follow accepted patterns and at the same time not to "step out of line". The surveillance technologies are increasingly penetrating our lives. Mobile phones, initially not associated with this concept, today have acquired unprecedented possibilities of infiltrating their users. An analogous situation can be observed in relation to personal computers and related networks of global reach. A part of our society forgot what life used to be like in the past. The innovativeness of new technologies has allowed us to make our lives diametrically easier, directly (by relieving human work through robots) and indirectly (by sending and receiving text messages on a regular basis, shortening the distance between the sender and the recipient, or providing continuous access to the latest information). On the other hand, new technologies have created both a certain distance among the society and a sense of distrust towards those who use technology, as well as a feeling of uncertainty and inaccessibility of the activities performed. Nowadays, these changes cease to be a theory and become a fact.

A desire for security

Surveillance technologies have seized the world. It can be noticed that society does not see anything wrong with that, because technology popularization has become a social norm found everywhere. For many people, the use of new technologies is a private matter. The situation is different when you consider surveillance technologies. Some of them are characterized by confidentiality of use (i.e. eavesdropping/tapping, transmitters, hidden cameras), and others are encountered at every step of everyday life (i.e. cameras, scanners, metal sensors, card readers with chips, biometric readers). The presented division does not depend on the object of surveillance; the observed person may be aware of being watched or perform daily activities without the awareness of being observed. Much depends on the technology used and its openness, the purpose of infiltrating the individual, as well as the place of observation. Regardless of the method of surveillance, there are few security options available or people cannot protect themselves against it at all.

Thus, paradoxically, the society is restless about a lustful will to remain calm . By shaping systemic norms and social order, we interpret reality as casuistic and postulate a desire to reform it.

The observation tools are not just urban network cameras, infrared cameras or other optical devices. Police officers, governments, law enforcement agencies and corporations also control and observe; they use everyday objects to monitor our behavior. A perfect example of that are cell phones which track our every move through transmission towers and satellites. It can be said that an individual is traced by his or her own mobile phone. Even while in a pocket, it con-

stantly maps the route of its owner. In addition, most of the devices used by society, from a magnetic card used to open the door, through a gateway on the highway, to search engines, leave an electronic trace. Modern technologies are able to capture that trace, assign it to a given individual and follow it to the source.

The effective use of the collected information is shaped by a technique called resource exploration, which consists in gathering details from everyday life of the society by governments and other enterprises (Kobyliński, Pospieszny, 2015, pp. 67-79). That helps create data banks which contain information about the criminal records of individuals, their education, current place of residence, medical information; there is even a possibility to check their activities on the previous day. The information which is not openly available and which a person does not want to make public, is collected in the form of innumerable pieces of digital data, which together form a predicted digital image of a given person. Governments use such sets of information to create profiles of people, matching their behavior to patterns of social activity. Enterprises create behavioral profiles to increase product sales.

Such analysis of the collected information shows that people are extremely predictable. For example, knowing what an individual was doing at a given time for the last thirty days, it can be guessed what the person will do at the same time next day. And knowing what the person will be doing at a given time of the day, the analyzing party can use that information in any possible way, likely taking its own benefits into account.

An important element of the above interpretation of constant surveillance is the fact that the described data resources can be accessed by a limited number of people with a specific status and authorization by a government or other institutions to view those resources.

At the time of emergence of new infiltration technologies, constant surveillance is gaining more and more importance. Access to modern technology is spreading, and its development can be beneficial for users as well as producers, administrators, operators and controlling persons. The need for access to new technologies will continue to grow, due to a desire to simplify the performance of everyday activities and minimize the time associated with the performance of professional tasks and further interpersonal relations.

It is necessary to draw attention to the fact that the element of time saving – thanks to new technology – translates to a maximization of the time used for technological solutions. People will not only make all their activities dependent on the devices they have, but they will also have to spend time on their maintenance, security and control. Thus, it is an apparent saving of time in one spectrum, at the expense of the other. Bearing in mind the fact that technologies affect not only the individual but also the society, a higher purpose (including maintenance of state security) intensifies the need to use them, despite the time devoted to the implementation of activities ensuring their efficient functioning.

Governments claim that the dangerous computerized world should be kept under surveillance. Experience of previous years shows that even complex monitoring network systems and espionage technologies cannot provide adequate standards of protection, or defense against terrorist activities. Nevertheless, continuous improvement of the existing solutions will allow proper technological implementation in the future.

New technologies – including face extraction systems, implants, iris scans, and RFID microchips – can help to track people who have committed a crime or are staying in a given country illegally. The downside of their application is the possibility of users' privacy being violated. It is the privacy that is the focus when considering the growing tension between the good of the individual and the security of all. Taking into consideration the acceleration of the development of new technologies, it can be said that in the future world of global surveillance

there will be no possibility to hide or conceal some of the data. It is possible to exclude yourself from some participation in the prescriptive scheme, i.e. limit or even opt out of using devices that promote a safe and comfortable life. But there arises the question of whether such an action would not exclude an individual from social life and let them perform their everyday activities without disturbing interpersonal relations? The answer to that question is not clear and wakes uncertainty of the approaching future.

Summary

New technologies have moved the boundary between private and public spheres. Many surveillance devices allow multi-directional infiltration of their users, which enables constant observation of the participants of digital life. It can be said that we are witnessing an ongoing revolution and the coming of a new technological era. When one recalls the previous comparison to a two-edged sword, it can be seen that some of the changes which have already been set in motion cannot be omitted or left undone or unfinished, even when they become a nuisance.

A similar situation occurred with the invention of trains, designed to bring comfort and speed of travel, or cars, which were supposed to give people privacy and independence of travelling. At the time of their creation, no one thought that the number of casualties in accidents would be so alarming. Whether through derailment, or through human mistake of directing trains to one track, catastrophes occurred. With cars, the main error factor was human error in the form of drivers.

Yet despite the dramatic statistics, no one came up with the idea to delegalize those means of transport. The situation is analogous to the use of mobile phones. No one forbids people to use them because they emit electromagnetic waves which may cause cancer. The realities indicate that there will be a similar warp with surveillance technologies. In this case, it is a matter of the profit and risk ratio. The profits of using new technologies are bewildering, so instead of giving up, humanity prefers to tame the risk involved.

The community should be taught the proper use of new technologies, which will allow the proper valuation of their functionality. The tasks of the developed solutions are to facilitate everyday life, provide a sense of security, create joy in using new devices, and help. A conscious society, having knowledge of what hazards it may be exposed to while using new devices, has the possibility to see the price it has to pay for the use of new technology. Everyday use of it changes the understanding of the private and personal sphere, and thus contributes to the change of our identity.

Bibliography:

1. Bauman Z., Lyon D. (2013). *Płynna inwigilacja rozmowy.* Kraków: Wydawnictwo Literackie.
2. Goban-Klas T., Sienkiewicz P. (1999). *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania.* Kraków: Wydawnictwo Fundacji Postępu Telekomunikacji.
3. Jabłoński W. (2006). *Kreowanie informacji. Media relations.* Warszawa: PWN.
4. Kałużny P. (2008). *Techniki inwigilacji, Co nam grozi i jak się bronić?* Warszawa: PWN.
5. Kobyliński A., Pospieszny P. (2015). *Zastosowanie technik eksploracji danych do estymacji pracochłonności projektów informatycznych*. Warszawa: Studia i Materiały Polskiego Stowarzyszenia Zarządzania Wiedza / Studies & Proceedings Polish Association for Knowledge Management. Issue 73, pp. 67-79.
6. Lyon D. (2010). *Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies*. International Political Sociology. Vol. 4 Issue 4, pp. 325-338.
7. Pniak S. (2017). *Cyberzagrożenia w ujęciu społeczeństwa informacyjnego*, (in:) Szetela M., Kaleta M., Piech K., Piech M. (eds.): *Zaplątani w sieci, Społeczeństwo wobec wyzwań nowych mediów.* Toruń: WSKSiM.
8. Wierzbołowski J. (1997). *Aksjologiczne i społeczne skutki przekształcenia informacji w zasób.* Warszawa.
9. Wnuk-Lipiński E. (2005). *Socjologia życia publicznego.* Warszawa: Scholar.
10. Zacher L. (2007). *Transformacje społeczeństw od informacji do wiedzy.* Warszawa: C.H. Beck.

UNCONVENTIONAL THREATS IN CIVIL AVIATION

Kamil Gefert

Abstract

Threats to civil aviation can be divided into conventional and unconventional. Their nature and effects are very diverse. Unconventional threats are less predictable and often bring equally severe consequences as the conventional ones, or sometimes even more severe. They include chemical, biological and radioactive agents, aircraft used as live missiles, and, in some cases, cyber weapons. The article shows that the problem of unconventional threats in civil aviation is significant, and its underestimation may bring tragic consequences.

Keywords: air terrorism, unconventional weapons, cyberterrorism

Introduction

Terrorist threats are a particular group of threats in civil aviation. The means used in terrorist attacks are very diverse. To try and classify them, they can be divided into conventional (explosives, firearms, etc.) and unconventional ones (chemical, biological and radioactive agents, aircrafts used as live missiles). The effects of the second group seem to be less predictable, which this article will attempt to show. The other aim of this work is to present the problem and raise the awareness of its existence and gravity.

In the case of various weapons that can become instruments of terror one can distinguish a group of unconventional weapons, i.e. such as are normally not used because of their long-term negative effects and for humanitarian reasons (Kamler, 2001). Unconventional weapons used in aviation terrorism include the use of an aircraft as an effective air-ground missile, which amplifies the effects of the attack, as it happened in September 2001 in the United States of America. Moreover, this group should obviously include atomic (in this case, mostly radioactive materials), biological and chemical weapons (ABC) (https://encyklopedia.pwn.pl/haslo/bron-abc;3880948.html). An attempt to classify the threats within those two groups encounters yet another issue: cyberterrorism. It is certainly not a weapon of mass destruction, but in the context of unconventional weapons the place of cyberterrorism is somewhat different. The definition of the word "unconventional" is, according to the dictionary, "going beyond conventions, incompatible with tradition" (https://sjp.pwn.pl/slowniki/niekonwencjonalny.html). Therefore it is necessary to prove in reference to the above definition that cyberterrorism in civil aviation goes indeed beyond the conventional, traditional solutions used in the fight against terrorism.

Chemical, biological and radioactive agents

When considering chemical, biological and radioactive agents, there are two ways of using them against civil aviation: on the ground (crowded terminals) or in the air (aircraft). Moreover, aviation can become an excellent carrier of pathogens in the case of biological weapons. It is also worth mentioning that explosives can be an effective addition to chemical, biological or radioactive agents. They facilitate the dispersing of toxic substances over a large area in a very short time. A very effective weapon that causes maximized effects is therefore a hybrid bomb

that kills in two manners. These are: a strong shock wave generating enormous pressure differences and resulting in mechanical body injuries (also by shards), and a poisonous substance that works effectively in the second phase of the attack, causing severe health damage or death. Depending on the type of substance, the effect of poisoning can be immediate or delayed from a few hours to several days (especially in the case of biological contamination). For the above reasons, when used against a group of people, a bomb made solely of explosives is always less harmful than the same bomb with the addition of highly poisonous chemical or biological material. Biological "silent bombs", whose containers and dispersers are not of explosive nature, are particularly dangerous (Glen, 2014, pp. 38-39). They might result in deliberate contamination of tap water, disperse the substance into the air, e.g. in a small space (on a plane), or introduce the substance into a building's air conditioning. There may be many more manners of their use. At one time, people feared the possibility of an epidemic of anthrax spread by using ordinary mail, where the dangerous bacteria would be placed in envelopes and addressed to various places, particularly to important state institutions (Osiński, 2003, http://pis.mswia.gov.pl/ftp/PIS/BIOTERRORYZM.doc).

Civil aviation might be used as an excellent carrier and distributor of biological weapons. Silent biological bombs in one or more contaminated aircrafts could remain undiscovered for several days. The use of extremely strong strains of dangerous bacteria or viruses would be most effective. Through the air channel, biological material could rapidly spread to all continents before anyone realized what was happening and how.

Toxic chemical weapons can be divided into the following types (Glen, 2014, p. 38-39):

- pervasive, disrupting the functions of all body cells (hydrogen cyanide),
- paralytic-convulsive, affecting the central nervous system and causing disturbances in the transmission of nerve impulses (sarin),
- suffocative, affecting the respiratory system (phosgene),
- blister agents, causing burns on contact with the skin (mustard gas),
- irritating, strongly affecting mainly mucous membranes, i.e. eyes, nerve endings in the upper respiratory tract (bromoacetone, adamsite),
- psychotoxic, acting in a manner similar to drugs (LSD-25).

There are also toxic weapons which destroy crops and substances (as napalm or termite), burn rapidly in high temperatures (without explosion), and are effective against vehicles and buildings (ibidem, p. 39).

The group of radioactive agents includes "dirty bombs". That is a hybrid bomb which consists of an explosive (which acts as a disperser) and, most importantly, a radioactive substance in the form of dust, powder or an aqueous suspension. A dirty bomb may contain various types of radioactive isotopes commonly used in various industrial sectors. Theoretically, it is quite easy to obtain access to the isotopes of cobalt-60 and cesium-137. The most dangerous, however, could be strontium-90, which accumulates in bones, and iodine-131, accumulating in the thyroid. It is also worth mentioning that cesium and strontium have a very long half-life, which means that the contaminated area would have to be closed for decades. Highly radioactive isotopes would be the best choice for constructing a dirty load (even small amounts of the substances have high toxic potential). This suggests the idea of using spent nuclear fuel, which possesses such properties (Bąk, Wolska, 2011, p. 51-52). An explosion of a sufficiently large and/or effective (in terms of radioactive power) dirty bomb in a terminal or inside a flying aircraft would cause extensives and long-lasting negative effects.

Means of air transport

Undoubtedly, the most sophisticated unconventional weapons are aircrafts themselves, used as missiles. The advantage of that "weapon" is the fact that a successful takeover of a plane guarantees almost certain success of the attack. It results in the death of not only passengers and crew, but also the people at whom the plane is aimed, as it was on September 11, 2001 (Chwalba, 2011). It is that date that marks a new era of terrorism and gives a new dimension to suicide attacks. Until then, plane hijacking had been used for extortion. Hostages were taken to force authorities to fulfill the demands of terrorists. After September 11, 2001, it was clear that the moment a plane was taken over, practically nothing could be done to protect the passengers from death, not to mention the object which the hijacked plane targeted. An aircraft is a significant target in itself, but it may also be a tool which, due to its dimensions, amplifies the effects of the attack. It can be used as a missile not only as a result of its takeover by terrorists. The best example of that is from 2009 when a suicide terrorist attempted to detonate charges on a cruise plane when it was flying over a densely populated area of Detroit (Bosacki, http://wiadomosci.gazeta.pl/wiadomosci/1,114881,7400071,Nieudany_zamach_w_samolocie_do_Detroit.html). Fortunately, the charge had ignited instead of exploding and thus a catastrophe was avoided.

According to statistics, 4.2 billion passengers were transported by air in 2006. It is estimated that by 2025 the number will double. The biggest passenger airplanes can take up to 853 people on board (Airbus A380), and the vast majority of planes can take over 180 people. The figures in combination with the delicate transport system of civil aviation show that the risk of assault on an aircraft is significant (Glen, 2014, p. 45).

Cyberterrorism

Cyberterrorism is a new form of terrorist activity. In simple terms, it is as a combination of terrorism and cyberspace – a terrorist attack used strictly against software, computer systems, information and electronic data. It is also necessary to distinguish cyberterrorism from computer crime, which aims at gaining advantage in a specific field or obtaining material benefits (Białoskórski, 2010, pp. 59-60). A cyberterrorist attack may result in human deaths, injuries, interruptions in communication, financial losses or e.g. power outages. The benefit of cyberterrorism for the perpetrators lies in the fact that it does not require large financial expenditure and is safe for the terrorist while it may cause difficulties the consequences of which are hard to eliminate. In aviation, a cyberterrorist attack may be directed against the electronic and IT infrastructure of airports or an aircraft. The disruption of navigational equipment could cause serious threat to security and even lead to a plane crash. Cyberattacks can be divided into IT and electronic attacks. The former involve processing digital data and implanting cryptic malicious software. It can take the forms of viruses, worms, trojans, logic bombs, etc. The latter lie in the use of electromagnetic energy to disrupt or damage electronic infrastructure and equipment (Glen, 2014, p. 45). Understandably, cyberterrorism takes advantage primarily of any shortcomings and gaps in information systems.

In fact, the only limitations in the field of cyberterrorism are set by the level of skills, cunning and determination. One can try to protect oneself against attacks, but the world of cyberspace is so extensive and complicated that the only thing that can be done is constantly searching for and eliminating gaps in security systems to decrease their number (Verton, 2004).

The effects of terrorists using cybernetic tools in civil aviation can be very serious.

A brief description of events of 2011-2015 caused by the activity of just one man demonstrates how many dangers from hackers and potential terrorists are lurking over civil aviation (Weise, http://www.usatoday.com/story/tech/2015/05/17/hacker-sideways-chris-roberts-fbi-united/27492409/). Fortunately, the aim of those incidents was to show goodwill and detect serious flaws in aircraft systems. However, they were not authorized by any security services or airlines, which angered the US authorities. Chris Roberts, IT specialist and founder of the company "One World Labs", proved that one could easily break into aircraft systems by connecting their own electronic equipment to audiovisual devices. He had done so up to 20 times in four years in different planes in the USA. He discovered critical security gaps that allowed him to manipulate some of the aircraft systems available only to pilots. He could influence the course, engine operation and other parameters of the flight. All that he needed were his computer skills and a laptop on board. It turned out that the systems of many modern aircrafts commonly used by airlines around the world (Boeing and Airbus) were linked to the passenger entertainment system and the only separation were some primitive firewalls. Roberts repeatedly accessed the aircraft systems, but only in such a way as to check the effectiveness of his actions without endangering the whole flight. Chris Roberts's company dealt with security in IT networks and he insisted that his actions were aimed at improving security by detecting systemic vulnerabilities. He was detained by the FBI in early 2015 and was informed that his actions were a federal crime. His discoveries raised deep concern, for they demonstrated that every IT expert skilled at security systems was able to cause a plane crash using a computer. In the era of the development of cyberterrorism, special attention must be paid to that issue to prevent anyone from outside the cockpit from accessing the instruments and mechanisms of the aircraft.

Conclusions

Returning to the hypothesis that unconventional threats in civil aviation cause less predictable results, it can be stated that the hypothesis is true. Hybrid bombs can be an example of that. Normal bombs using only explosive charges become a much more dangerous and unpredictable weapon when enhanced with chemical, biological, or radioactive agents. The mere use of deadly pathogens as a weapon distributed in a natural way through the use of air transport channels can cause death or serious illness not of several or several dozen people, but even of several thousand, and in extreme pandemic cases, hundreds of thousands. An aircraft used as a weapon in itself poses a greater danger than the mere use of weapons on board to kill passengers and crew or to lead to a spontaneous crash. Well-organized action, seizure of aircraft and its use as a guided missile can cause incomparably greater damage. The above-mentioned attacks of September 11, 2001 in the USA are a clear example. Nearly 3,000 people were killed in an attack that involved the use of four aircrafts (Kean et al, 2004). The average casualty number is about 750 victims per one aircraft missile. Such a number of victims would certainly have been unachievable if the attack had not been fully controlled by the terrorists.

The threat of using unconventional measures against civil aviation is clearly an important issue. This is demonstrated by the above analyzed case of unauthorized access to aircraft systems by Chris Roberts. He exposed the gaps in civil aviation security which could potentially lead to bold, massive and effective acts of terrorism with the use of cybertools. The detection of such intentions in a passenger-terrorist would be almost impossible. It is difficult to believe that civil aviation had such an enormous weak spot, taking into account the fact that the repeated actions of Roberts were not discovered for several years and would probably have re-

mained so, if he had not himself admitted to his experiments.

Is it possible to say that cyberterrorism in civil aviation belongs to unconventional threats? That cannot be defined clearly. However, the author tends toward the theory that in this respect, cyberterrorism can be considered both conventional and unconventional. Since firewalls and barriers protecting (to a greater or lesser extent) against such forms of criminal activity are constantly developing, the definition of unconventionality (as going beyond the typical patterns) is not fully specified.

However, cyberterrorism is sometimes largely underestimated, belittled, or simply not considered in some security systems. Taking into account the unpredictability of potential negative effects of cyberattacks, one can conclude that they have a certain element of unconventionality. It should always be remembered that civil aviation is a very complex and delicate organism. The disturbance of security is highly probable and easily achievable if any means of security has even the smallest flaw, and the effects of the wrong people using those flaws are overwhelming. For these reasons, civil aviation will always be an attractive target for terrorists, with cunning and determination being their strongest side.

Bibliography

1. Bąk, T., Wolska, E. (2013). *Terroryzm. Słownik*. Kraków: Dytko-Media.
2. Białoskórski, R. (2010). *Wyzwania i zagrożenia bezpieczeństwa XXI wieku*. Warszawa: Wydawnictwo Wyższej Szkoły Cła i Logistyki.
3. Bosacki, M. *Nieudany zamach w samolocie do Detroit*, http://wiadomosci.gazeta.pl/wiadomosci/1,114881,7400071,Nieudany_zamach_w_samolocie_do_Detroit.html.
4. Chwalba, A. (2011). *Historia powszechna. 1989-2011*. Warszawa: Wydawnictwo Naukowe PWN.
5. https://encyklopedia.pwn.pl/haslo/bron-abc;3880948.html.
6. https://sjp.pwn.pl/slowniki/niekonwencjonalny.html.
7. Glen, A. (2014). *Terroryzm lotniczy – istota zjawiska, organizacja przeciwdziałania*. Warszawa: Wydawnictwo Akademii Obrony Narodowej.
8. Kamler, M. (2001). *Wojsko, wojna, broń*. Warszawa: Wydawnictwo Naukowe PWN.
9. Kean, T. H. (2004). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*.
10. Osiński, R. (2003). *Bioterroryzm*. Bydgoszcz: Państwowy Inspektor Sanitarny MSWiA, http://pis.mswia.gov.pl/ftp/PIS/BIOTERRORYZM.doc.
11. Verton, D. (2004). *Black Ice – niewidzialna groźba cyberterroryzmu*. Gliwice: Wydawnictwo Helion.
12. Weise, E. http://www.usatoday.com/story/tech/2015/05/17/hacker-sideways-chris-roberts-fbi-united/27492409/.

PROBLEMATYKA DEFINIOWANIA DOWODZENIA

Szymon Kochanowski

Abstract

The issue of defining a command

The article present a problem with the common understanding of the definition „command" mainly on the basis of Polish literature, but also aboard, in particular in the doctrinal documents of NATO. It also shows the differences between command and control, steering and management

Keywords: command, management, coordination, control

Wstęp

Od starożytności termin „dowodzenie" był kojarzony z wojskiem, siłami zbrojnymi, w których istniało stanowisko dowódcy, który za pomocą swojej charyzmy, umiejętności, posiadanych tytułów, kompetencji dowodził oddanymi mu podwładnymi.

W początkowych dziejach wojska były tworzone jedynie doraźnie, lecz wraz z wzrostem znaczenia państw, wprowadzeniu stałych oddziałów wojskowych, wzroście liczby żołnierzy w siłach zbrojnych, powiększeniu wachlarzu zadań, sposobie funkcjonowania zmieniało się również postrzeganie terminu „dowodzenie".

Obecnie bardzo dużo się mówi o dowódcach, dowodzeniu, stanowiskach dowodzenia, systemie i strukturze dowodzenia. Zawsze były i będą to tematy ciekawe, od których to tak naprawdę zależy nasze bezpieczeństwo. Odpowiednie pojmowanie terminu „dowodzenie" wydaje się zatem bardzo istotne. Szczególnie podczas wspólnych manewrów, ćwiczeń na szczeblu międzynarodowym, głównie w ramach NATO.

Celem niniejszego artykułu jest analiza terminu, definicji „dowodzenia", pokazanie problemu związanego z wyborem odpowiedniej definicji dowodzenia oraz wytypowanie tej najbardziej trafnej.

Obszar badań zatem będzie obejmować normy prawne oraz literaturę krajową, jak i zagraniczną regulującą pojmowanie definicji dowodzenia.

Analizując literaturę dotyczącą definicji „dowodzenia" postawiłem następującą **hipotezę** – Uważam, że ujednolicenie definicji „dowodzenia" jest bardzo trudne, ponieważ istnieje zbyt wiele różnych wersji definiowania tego terminu, lecz dzięki współpracy w ramach takich organizacji jak NATO ujednolicenie pojmowania „dowodzenia" jest bardzo możliwe.

Dana hipoteza zostanie zweryfikowana w trzech **problemach badawczych**: Jak odróżnić dowodzenie od sterowania, kierowania i zarządzania? Jak jest definiowane „dowodzenie" w Polsce? Jak jest definiowane „dowodzenie" w NATO?

1. Dowodzenie a sterowanie, kierowanie i zarządzanie

Wraz z rozwojem wielkości sił zbrojnych, instytucji, przedsiębiorstw skupiających dziesiątki, a nawet setki tysięcy ludzi, wykształciły się nowe sposoby i zasady zarządzania tak wielkimi tworami, organizacjami i organami pozwalającymi na ich sprawniejsze oraz efektywniejsze funkcjonowanie. Spowodowało to, że ponownie zaczęto analizować

i interpretować pojęcie „dowodzenia", poprzez interdyscyplinarne podejście, rozpatrując „dowodzenie" poprzez pryzmat sztuki wojennej, ale także poprzez teorię organizacji i zarządzania oraz funkcjonujących w niej terminów „sterowanie", „zarządzanie" i „kierowanie". To właśnie termin ,,kierowanie" jest kojarzony przede wszystkim z ludźmi, natomiast ,,zarządzanie" odnosi się do działalności organizacji, instytucji (Kręcikij, 2015, s. 10). Są one także często uzupełnione o przedmiot oddziaływania. Z tego powodu często funkcjonują określenia typu ,,kierowanie zespołem ludzkim" oraz ,,zarządzanie przedsiębiorstwem (spółką, firmą, uczelnią)" (Majewski, 2003, s. 6). Wyniki badań literatury wskazują jednak, że nawet te terminy są często używane zamiennie, gdyż mówi się np. o ,,zarządzaniu personelem" i ,,kierowaniu firmą". Tutaj termin ,,kierowanie" oznacza działanie na kogoś lub coś, aby powodowało ono czyjeś zachowanie zgodne z wolą kierownika. Natomiast w organizacji ,,kierowanie" kojarzy się z bezpośrednim kontaktem i stosunkiem przełożonego z jego podwładnymi (Kręcikij i Wołejszo, 2007, s. 12).

Nawet w Siłach Zbrojnych na najwyższym szczeblu dowodzenia, nie raz słyszymy, że Minister Obrony Narodowej ,,dowodzi" Siłami Zbrojnymi RP. Takie stwierdzenie jest powszechnie krytykowane przez większość naukowców, ponieważ rezerwują oni termin ,,dowodzenia" wyłącznie służbom mundurowym, a szczególnie wojsku. Nawet w Ustawie o urzędzie Ministra Obrony Narodowej przeczytamy, że ,,kieruje" on działem administracji rządowej: Obrona narodowa. W Konstytucji RP z 1997 r. również przeczytamy, że Siły Zbrojne są neutralne politycznie i podlegają cywilnej oraz demokratycznej kontroli, co było również jednym z wymogów przystąpienia do NATO.

Wyjaśniając więc szeroko rozumianą definicję ,,dowodzenia", staje się zasadne wyjaśnienie również powyższych terminów, ich cech oraz wzajemnych związków, które są do siebie bardzo podobne, a częściej różnią się jedynie zakresem, co sprawia, że są często stosowane zamiennie (Michniak, 2005, s. 13). Doszukując się samej etymologii terminu ,,kierowanie" i ,,zarządzanie" możemy zauważyć, że w języku angielskim słowo ,,management" jest dosłownie tłumaczone zamiennie na kierowanie, zarządzanie. W słowniku języka polskiego możemy zauważyć, że kierowanie oznacza: ,,zarządzać kimś, czymś, stać na czele czegoś lub wskazywać sposób postępowania" (https://sjp.pwn.pl/szukaj/kierowanie.html). Tutaj również widzimy, że kierowanie i zarządzanie są używane zamiennie, traktowane jako synonimy. Dodatkowo każdy z tych terminów posiada wiele różnych definicji, co stwarza jeszcze większy problem przy ich odróżnieniu.

Według Zbigniewa Ścibiorka to ,,**sterowanie**" jest pierwotnym terminem, od którego wywodzi się ,,zarządzanie" i ,,kierowanie". Jest ono definiowane jako ,,wszelkie celowe oddziaływanie jednego systemu na inny w celu otrzymania takich zmian przebiegu procesu zachodzącego w przedmiocie sterowania lub stanu sterowanego systemu w danej chwili, które uważa się za pożądane" (2000, s. 26).

„Kierowanie" najczęściej jest definiowane jako proces planowania, organizowania, motywowania i kontrolowania działalności członków organizacji oraz wykorzystania wszystkich innych jej zasobów dla osiągnięcia ustalonych celów (Ścibiorek, 2005, s. 50). Synteza wielu różnych definicji kierowania, (wg Michniaka) wskazuje, że aby o nim mówić muszą zostać spełnione następujące warunki (2005, s. 15):

- istnienie dwóch związanych z sobą modułów dynamicznych (kierującego i wykonawczych), tworzących razem system kierowania;
- występowanie między dwoma modułami sprzężeń jednokierunkowych lub dwukierunkowych;

- istnienie dla obydwu modułów stanowiących jeden system określonego celu kierowania, któremu podporządkowane jest działanie modułów;
- oddziaływanie modułu kierującego na elementy składowe modułów wykonawczych, powodując zmiany jego stanów zgodnych z celem kierowania.

Definicja zarządzania, obok definicji dowodzenia zdaje się jednym z bardziej rozbudowanych terminów, posiadających bardzo dużą ilość definicji. I tak „**zarządzanie"** definiowane jest jako: „ciąg działań będących funkcjami planowania, organizowania, pobudzania i kontroli, które uporządkowane są w określonych układach przebiegów organizacyjnych (zwykle informacyjno-decyzyjnych) i spełniane przez jednostki zarządzania oraz stanowiska kierownicze" (Stabryła i Trzciński, 1986, s. 132); „sprawne i skuteczne przekształcanie zasobów finansowych, ludzkich, informacyjnych, rzeczowych w złożone rezultaty" (Szczupaczyński, 2002, s. 11); „zestaw działań (obejmujący planowanie, organizowanie, podejmowanie decyzji, przewodzenie – kierowanie ludźmi i kontrolowanie) skierowanych na zasoby organizacji (finansowe, rzeczowe, ludzkie i informacyjne), wykonywanych z zamiarem osiągnięcia celów organizacji w sposób sprawny i skuteczny" (Griffin, 1996, s. 38); „działalność kierownicza polegająca na ustaleniu celów i ich realizacji w obrębie sformalizowanych struktur organizacyjnych systemu dowodzenia, a przede wszystkim w produkcji usług sztabowych, a także szkoleniu, itp." (Michniak, 2005, s. 18).

Analizując literaturę możemy zauważyć, że odróżnienie tych pojęć i wskazanie, które posiada szersze znaczenie wcale nie jest takie łatwe. Niektórzy uczeni wskazują, że kierowanie jest znaczeniowo szersze od zarządzania (np. Jan Zieleniewski), drudzy uważają, że kierowanie jest znaczeniowo węższe od pojęcia zarządzanie (np. Józef Penca, Tadeusz Pszczołowski), a jeszcze inni (np. Leszek Krzyżanowski) uważają, że pojęcie kierowanie jest zakresowo szersze od zarządzania oraz dowodzenia, ale jednocześnie nie przypisują zbyt dużej wagi do odróżniania tych terminów (Kręcikij i Lewandowski, 2015, s. 12).

Zauważyć można, że o tym, czy dana osoba dowodzi, kieruje czy zarządza daną organizacją, instytucją, przedsiębiorstwem zależy głównie od rodzaju danej organizacji, typu organu władzy, form i środków ingerencji w funkcjonowanie organizacji oraz posiadanych kompetencji (Kręcikij i Lewandowski, 2015, s. 12).

2. Definicja dowodzenia w Polsce

Istnieje wiele definicji dowodzenia, które znacznie różnią się od siebie zawartością treści. Jest to konsekwencją przede wszystkim czasów, w których zostały napisane, zadań i sposobu funkcjonowania jakie posiadały dane instytucje (jak np. siły zbrojne), różnych potrzeb podmiotów tworzących treść badanego pojęcia, potrzeb i preferencji autorów oraz aspektów, w których były rozpatrywane: psychologicznych, społecznych, technologicznych czy prakseologicznych.

Dla pokazania różnicy w definiowaniu **dowodzenia** na początku przedstawiłem dwie definicje dowodzenia (w ujęciu szerokim i węższym) z drugiej połowy XIX wieku, **przedstawionej przez J. Orzechowskiego**.

Pierwsza definicja – **w ujęciu szerokim** – przedstawia dowodzenie wojskami jako całokształt działań dowódców i ich organów dowodzenia w zakresie przygotowania oraz prowadzenia działań bojowych, szkolenia, wychowania i zarządzani jednostkami wojskowymi jako oddziałami gospodarczymi (Orzechowski, 1974, s. 21).

Druga definicja – **w ujęciu węższym** – przedstawia dowodzenie jako proces kierowania

walką (kierowania wojskami), działalność dowódcy i jego organów dowodzenia, zorganizowanych i nastawionych na osiągnięcie określonego celu, jakim jest pokonanie i zniszczenie przeciwnika (Orzechowski, 1974, s. 21).

Warto także zwrócić uwagę na **definicję dowodzenia** przedstawiane przez innych autorów z tamtych lat. I tak np. definicja dowodzenia w węższym ujęciu przedstawioną przez **F. Wiśniewskiego**. Napisał on, że ,,dowodzenie to kierowanie procesem walki (kierowanie wojskami), a więc działalność dowódcy i jego organu dowodzenia, zorganizowaną i nastawioną na osiągniecie określonego (wynikającego z istoty i sensu konfliktu zbrojnego) celu: pokonanie i zniszczenie przeciwnika" (1965). Widać, że definicje dowodzenia przedstawione przez obu autorów są niemal identyczne.

Jeszcze wcześniej **Antoni Aponowicz** określił dowodzenie jako ,,działalność dowódcy jednostki wojskowej polegającą na wszechstronnym przygotowaniu podwładnych do walki i na kierowaniu nimi w walce" (1961, s. 72).

Władysław Mróz natomiast zdefiniował **dowodzenie** jako ,,podstawową formę kierowania wojskami, opartą na uprawnieniach do kompleksowego kształtowania wszystkich elementów gotowości bojowej w odniesieniu do pośrednio i bezpośrednio podporządkowanych żołnierzy, a więc przygotowania ich do działania i kierowania nimi podczas wykonywania zadań bojowych" (1978, s. 13).

W **Leksykonie wiedzy wojskowej** z 1979 r. przeczytamy, że **dowodzenie** to ,,całokształt celowej, zaplanowanej działalności dowódcy i sztabów, realizowanej w obrębie określonego systemu kierowania, zapewniającej wysoką gotowość bojową wojsk i ich właściwe przygotowanie do efektywnego osiągnięcia celów walki, bitwy, wojny, operacji" (s. 13).

W **Regulaminie pracy organów dowodzenia w Siłach Zbrojnych RP, dowodzenie** jest określone jako ,,działalność dowódcy (szefa), której celem jest wykonanie zadania poprzez utrzymanie wojsk (sił) w ciągłej gotowości i zdolności bojowej, przygotowanie działań zbrojnych oraz kierowanie nimi" (1996, s. 5).

Po zakończeniu Zimnej Wojny, Rozpadzie Układu Warszawskiego, upadku bloku komunistycznego, wprowadzenia nowych rządów demokratycznych i zaprzestaniu traktowania wojska jedynie jako machiny wojennej, ale także jako organu, który może pomóc ogółu społeczności np. w realizacji zadań z zakresu zarządzania kryzysowego zmieniło się także postrzeganie i definiowanie ,,dowodzenia".

Obecna **definicja dowodzenia** (**wg J. Michniaka**) w szerszym ujęciu powstała na bazie integracji wielu innych definicji. Mówi ona, że dowodzenie to podstawowa forma kierowania wojskami, oparta na uprawnieniach do kompleksowego kształtowania wszystkich elementów gotowości oraz zdolności bojowych w odniesieniu do bezpośrednio i pośrednio podległych żołnierzy, przygotowania ich w czasie pokoju do realizacji wszelkiego rodzaju działań i do kierowania nimi w okresie pokoju, wojny i kryzysu (2003, s. 1).

Przez niektórych autorów **dowodzenie** jest definiowane jako ,,szczególna forma kierowania, dotycząca uzbrojonych zespołów ludzi, funkcjonująca w surowych warunkach pola walki i dyscypliny wojskowej, obliczu zjawisk wywołujących najwyższe napięcie ludzkich sił duchowych i fizycznych" (Zabłocki i Miodek, s. 43).

Bardziej **rozbudowaną definicję dowodzenia** wprowadził **Ryszard Kuriata**. Uznał on dowodzenie za ,,szczególny ze względu na zakres, rodzaj kierowania polegający na projektowaniu i zorganizowanym oddziaływaniu informacyjno-decyzyjnym, ze sprzężeniem zwrotnym realizowanym przez dowódcę i inne organa dowodzenia, na podległy potencjał bojowy w czasie poprzedzającym walkę zbrojną i podczas jej trwania, zmierzający do jak najlepszego przygotowania tego potencjału do walki, utrzymania go w gotowości bojowej odpowiedniej do sytua-

cji i wykorzystania do odniesienia zwycięstwa nad przeciwnikiem przez spowodowanie jego uległości lub rozbicie go w walce zbrojnej" (2004, s. 18).

W **Regulaminie działań wojsk lądowych** możemy przeczytać, że dowodzenie to „działalność dowódcy, który narzuca swoją wolę i zamiary podwładnym. Jest wspomagany przez swój sztab, planuje, organizuje, koordynuje i ukierunkowuje działania podległych mu wojsk przez użycie standardowych procedur działania i wszelkich dostępnych środków przekazywania informacji" (Dowództwo Wojsk Lądowych, 2008, s. 271).

Z przytoczonych definicji widać, że głównym celem dowodzenia w tamtych czasach było przygotowanie wojska, podwładnych do walki, operacji i pokonanie, zniszczenie przeciwnika, co wynikało głównie zapewne z ciężkich czasów XIX i XX wieku, w których potyczki, bitwy, wojny stanowiły niemalże normę życia codziennego. Jedynie definicja dowodzenia w szerszym ujęciu J. Orzechowskiego z tamtych lat zdaje się bardziej adekwatna do dzisiejszych czasów, w których dowódca nie skupia się już wyłącznie na prowadzeniu wojny, ale także na całokształcie działań szkoleniowych, administracyjnych, wychowawczych mających za zadanie utrzymanie w ciągłej gotowości i zdolności bojowej armii do wykonywania powierzonych, aktualnych i przyszłych zadań.

Obecnie za opracowanie definicji „dowodzenia" i nie tylko odpowiada w Polsce oraz w ramach Sił Zbrojnych - Wojskowe Centrum Normalizacji, Jakości i Kodyfikacji (WCNJK), którego głównym zadaniem jest ujednolicanie terminologii w resorcie obrony narodowej, które mają zwiększyć zdolności naszego wojska do współdziałania w środowisku wielonarodowym podczas wspólnych misji i operacji. Zadanie to jest realizowane głównie poprzez aktualizowanie i publikowanie polskiej wersji „Słownika terminów i definicji NATO AAP-6" oraz opiniowanie polskich norm terminologicznych: Norm Obronnych (NO), podręczników normalizacji obronnej (PDNO), a także słowników specjalistycznych poszczególnych rodzajów wojsk, rodzajów sił zbrojnych i rodzajów działalności wojskowej (http://wcnjk.wp.mil.pl/pl/30.html).

Najbardziej aktualnym dokumentem zawierającym wojskowe definicje w Siłach Zbrojnych jest ***Wykaz haseł terminologicznych stosowanych w obowiązujących resortowych dokumentach normalizacyjnych NO i PDNO wyszczególnionych w Decyzji Nr 86/MON Ministra Obrony Narodowej*** *z dnia 23.03.2015 r.* W dokumencie tym dowodzenie jest definiowane jako (http://wcnjk.wp.mil.pl/plik/file/N_20151029_Terminy_2015.pdf):

- „Kierowanie, koordynowanie i sprawowanie kontroli nad formacjami wojskowymi przez uprawnioną osobę spośród stanu osobowego sił zbrojnych";
- „Władza nadana osobie (dowódcy) wyznaczonej spośród składu osobowego sił zbrojnych w celu kierowania, koordynacji i dowodzenia wyodrębnionymi elementami tych sił";
- „Proces decyzyjno-informacyjny, poprzez który dowódca narzuca swoją wolę i zamiary podwładnym oraz w ramach którego wspomagany przez swój sztab planuje, organizuje, koordynuje i ukierunkowuje działania podległych mu wojsk przez użycie standardowych procedur działania oraz wszelkich dostępnych środków przekazywania informacji".

Jak widać istnieje wiele definicji dowodzenia. Nawet w najbardziej aktualnych dokumentach sił zbrojnych podaje się więcej niż dwie definicje tego terminu. Sprawia to problem w ujednoliceniu tego pojęcia, jego uniwersalizacji i jednakowego stosowania we wszystkich instytucjach na terenie naszego kraju. Nawet po przystąpieniu w 1999 r. do NATO powstało jeszcze wiele różnych definicji „dowodzenia". Jednak zagłębiając się w definiowanie terminu „dowodzenia" poza granicami naszego państwa zobaczymy, że nie jest

to tylko nasz problem, ale borykają się z nim również nasi sąsiedzi, partnerzy, sprzymierzeńcy – kraje członkowskie NATO, jak i zobaczymy, że w samych dokumentach natowskich problem jest podobny.

3. Definicja dowodzenia w NATO

Analizując hierarchię źródeł prawa w Polsce, można łatwo zauważyć, że pierwsze miejsce w hierarchii zajmuje Konstytucja RP z 2 kwietnia 1997 r., a na drugiej pozycji znajdują się Ratyfikowane umowy międzynarodowe wymagające ich wprowadzenia wcześniejszą zgodą w formie ustawy (są to umowy dotyczące pokoju, sojuszy, układów politycznych, wojskowych czy członkostwa w organizacji międzynarodowej). Dopiero po nich, na 3 miejscu znajdują się Ustawy i Rozporządzenia z mocą ustaw. Do tego, jeżeli wynika to z ratyfikowanej umowy międzynarodowej przez RP, umowy tworzące organizację międzynarodowe i prawo przez nie stanowione mają pierwszeństwo w przypadku kolizji z ustawami (*Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r.*, art. 87, 89, 91). Oznacza to, że decyzje i dyrektywy wydawane przez NATO mają pierwszeństwo nad polskimi ustawami, decyzjami czy zarządzeniami w przypadku kolizji, niezgodności. Jednak ani w Konstytucji, ani w Traktacie Waszyngtońskim, nie znajdziemy definicji „dowodzenia". Natomiast już w dyrektywach wydawanych przez NATO sytuacja definiowania dowodzenia ulega zmianie.

Dyrektywy te są sporządzane przez Komitet Wojskowy, który składa się z 29 szefów obrony państw członkowskich przy współpracy z: Dowódcami Sił Sojuszniczych ds. Transformacji i Operacji, Międzynarodowym Sztabem Wojskowym, w którego skład wchodzi ok. 600 ekspertów wojskowych i pracowników cywilnych oraz Biurem Standaryzacji NATO (NSO). Biuro to natomiast współpracuje z Europejską Organizacją Normalizacyjną, Międzynarodowymi Organizacjami Normalizacyjnymi oraz polskim Wojskowym Centrum Normalizacji, Jakości i Kodyfikacji. Organem decyzyjnym, co do wprowadzenia dyrektyw jest Rada Północno-Atlantycka (https://www.nato.int/ims/docu/mc-brochure-for-mccs-poland-07.pdf; https://www.nato.int/cps/en/natohq/topics_124879.htm).

W Sojuszu Północnoatlantyckim funkcjonuje ***AAP-6(2014) – Słownik Terminów i Definicji NATO***, który jest uzgodniony przez wszystkie państwa członkowskie i corocznie aktualizowany. Wg tego słownika „**dowodzenie** to władza nadana osobie spośród stanu osobowego sił zbrojnych do kierowania, koordynacji i sprawowania kontroli nad formacjami wojskowymi" (NATO Standardization Office, 2014, s. 98, źródło: http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6PL.pdf).

W natowskiej ***Doktrynie Operacji Połączonych – AJP-01(E),*** która również jest obowiązująca dla wszystkich państw członkowskich możemy przeczytać, że termin „dowodzenie" *(command)* bardzo często występuje wraz z terminem „kontrola" *(control)*. Terminy te nie są synonimami, lecz mają ścisły związek. W tej doktrynie **dowodzenie** jest definiowane jako: „władza nadana dla jednostki w siłach zbrojnych do kierowania, koordynacji i kontroli sił zbrojnych. To jest jak dowódca narzuca swoją wolę i intencje na podwładnych do osiągnięcia poszczególnych celów. Obejmuje to władzę i odpowiedzialność za wykorzystanie i użycie podległych sił do wypełnienia ich zadań. **Kierownictwo** jest zdefiniowane jako cel do osiągnięcia, działania jakie należy podjąć oraz zasoby i procedury do osiągnięcia tych celów. „**Koordynacja** jest harmonizacją i prowadzeniem przydzielonych sił do osiągnięcia celów". **Kontrola** natomiast jest definiowana jako „władza sprawowana przez dowódcę nad częścią działalności podległych organizacji lub innych organizacji, które normalnie nie znajdują się pod jego dowództwem i obejmuje odpowiedzialność za wprowadzenie rozkazów lub dyrektyw" (NATO

Standarization Office, 2017, s. 72-73).

Również w **regulaminie NATO - *„ATP 35(B) Doktrynie wojsk lądowych"*,** który posługuje się ujednoliconą terminologią i odwołującym się do *Słownika Terminów i Definicji NATO,* przeczytamy, że **dowodzenie** to „proces, w ramach którego dowódca zmusza podwładnych do działania zgodnie ze swoją wolą i zamiarami. Obejmuje on władzę i odpowiedzialność za użycie podległych mu sił i środków do wykonania zadania". W tym dokumencie podobnie również zdefiniowano termin **kontroli**, pisząc, że jest to „proces, w którym dowódca przez swój sztab, organizuje, kieruje i koordynuje działania podległych mu sił poprzez użycie standardowych procedur działania i wszelkich dostępnych środków przekazywania informacji" (NATO Standarization Office, 2017, s. 15-16).

W tym miejscu warto jeszcze przytoczyć definicję dowodzenia z wybranych krajów członkowskich NATO, czyli Stanów Zjednoczonych Ameryki (USA) i Wielkiej Brytanii, które to tak naprawdę stanowią główne źródło i odniesienie do tworzenia definicji dowodzenia.

W **amerykańskim regulaminie *FM 101-5 Organizacja i praca sztabów* „dowodzenie"** *(command)* postrzegane jest jako „władza, którą dowódca sprawuje nad swymi podwładnymi z racji posiadanego stopnia lub zajmowanego stanowiska. Obejmuje ono prawo do odpowiedzialność za skuteczne użycie dostępnych środków oraz za planowanie, organizowanie, kierowanie, koordynowanie i kontrolowanie sił wojskowych w celu wykonania postawionego zadania". Dopiero „dowodzenie i kontrola" *(command and control)* uważane jest za „proces, poprzez który działania militarne są kierowane, koordynowane i kontrolowane" (Department of the Army, 1984, s. 1).

Natomiast w **angielskim dokumencie *ADP-2 Command*,** termin „**dowodzenie**" oznacza „władzę sprawowaną przez dowódcę w celu kierowania, koordynowania i kontrolowania działań sił wojskowych". Pojęcie „kontrola" *(control)* w tym dokumencie występuje oddzielnie i jest definiowane jako: „proces, poprzez który dowódca, wspomagany przez sztab, kieruje, organizuje i koordynuje działania podległych mu żołnierzy, bazując na wspólnej doktrynie i używając standardowych procedur oraz korzystając z systemów informacyjnych i środków łączności" (Prepared under the Director of the Chief of the General Staff, 1995, s. 2). Czyli widać tu podobnie jak wcześniej wyraźne rozdzielenie „dowodzenia" (*command)* i „kontroli" *(control).*

Z powyższego wynika, że **dowodzenie może być postrzegane w 2 płaszczyznach** (Kręcikij i Wołejszo, 2007, s. 16):

- **jako władza**, czyli prawa do wydawania rozkazów oraz odpowiedzialność za skutki ich wykonania;
- **jako proces** sprawowania dowodzenia przez dowódcę, przy pomocy podległego mu sztabu, realizując czynności związane z planowaniem, kierowaniem, organizacją i koordynacją działań podległych mu sił.

Analizując definicje „dowodzenia" w poszczególnych krajach natowskich, wydawanych i tworzonych przez narodowych autorów oraz obowiązujących w ich dokumentach normatywnych, wojskowych, a między tymi tworzonymi w dokumentach natowskich uwypukla się różnica w ich pojmowaniu, mimo tego, że w ich tworzeniu i wprowadzaniu biorą udział wszystkie kraje członkowskie.

Podsumowanie

Istnieje bardzo dużo definicji dowodzenia. Ich postrzeganie różni się od siebie znacząco. Różnice te widać szczególnie jaskrawie na przełomie XX i XXI wieku. Za zamiany w pojmowaniu terminu dowodzenia odpowiada głównie zmiana zadań i funkcjonowania sił zbrojnych, nowe interdyscyplinarne podejście do tego zagadnienia, rozwój teorii organizacji i zarządzania, przystąpienie do NATO i wymagań z tego wynikających (interoperacyjność; kompatybilność; współdziałanie; implementacja dokumentów, zasad, procedur).

To wszystko sprawiło, że wybór jednej najtrafniejszej definicji „dowodzenia" stał się bardzo trudny. Główną zagwozdką autorów zdaje się być pytanie, czy „dowodzenie" powinno obejmować swym zakresem „kontrolę"? A jeżeli nie, to czy można wtedy mówić, że „dowodzenie" jest procesem zamkniętym cyklem? Zastanawiać także może - czy definicja „dowodzenia" powinna być zastrzeżona jedynie dla wojska? Gdyż wyraźnie widać w próbach definiowania tego pojęcia, że mamy wyróżnioną jednostkę – dowódcę, której nadano pewną władzę w siłach zbrojnych. Widzimy także w tych definicjach, że dowódca może, a nawet powinien korzystać z pomocy sztabu do wypełnienia powierzonych mu zadań, a także postępować w sposób standardowy, przewidywalny, zgodny z procedurami i za pomocą wszystkich dostępnych środków.

Pomimo jednak tak wielu definicji dowodzenia można także zauważyć jej pewną systematyzację i uniwersalizm, cechy wspólne we wszystkich przytoczonych definicjach. Szczególnie dobrze jest to zauważalne w krajach należących do NATO i doktrynach wydawanych przez tę organizację międzynarodową, do której odniesienia zauważamy również w polskich aktach normatywnych. Szczególnie dużo podobieństwa w definiowaniu terminu „dowodzenia" możemy zauważyć w natowskiej *Doktrynie Operacji Połączonych, Słowniku Terminów i Definicji NATO, Doktrynie Wojsk Lądowych* oraz w polskim *Regulaminie działania Wojsk Lądowych* czy w *Wykazie haseł terminologicznych stosowanych w obowiązujących resortowych dokumentach normalizacyjnych NO i PDNO wyszczególnionych w Decyzji Nr 86/MON Ministra Obrony Narodowej,* a nawet w definicjach stosowanych w USA czy Wielkiej Brytanii.

Z przeprowadzonej analizy terminu „dowodzenia" to właśnie jej ujęcie zawarte w natowskiej *Doktrynie Operacji Połączonych – AJP-01(E)* z 2017 r. wydaje się najbardziej trafne i aktualne, uzgodnione przez wszystkie państwa członkowskie i organy tej organizacji. Wg niej **„dowodzenie" to władza nadana dla jednostki w siłach zbrojnych do kierowania, koordynacji i kontroli sił zbrojnych".** Czyli widzimy tu, że obecnie naukowcy uważają „dowodzenie" za znaczeniowo szersze niż „kierowanie", które to stanowi jedynie jedną z trzech głównych działalności jakimi zajmują się dowódcy. Dalsza część tej definicji - „**To jest jak dowódca narzuca swoją wolę i intencje na podwładnych do osiągnięcia poszczególnych celów. Obejmuje to władzę i odpowiedzialność za wykorzystanie i użycie podległych sił do wypełnienia ich zadań",** pokazuje, jak wiele wspólnego ma z najnowszymi polskimi normami (szczególnie z *Regulaminem działań wojsk lądowych* z 2008 r.), w których pierwsze zdanie definicji „dowodzenia" jest niemal takie same. Doktryna ta dodatkowo zawiera definicje kierowania, koordynacji i kontroli. **Kierownictwo** jest zdefiniowane jako „cel do osiągnięcia, działania jakie należy podjąć oraz zasoby i procedury do osiągnięcia tych celów". „**Koordynacja** jest harmonizacją i prowadzeniem przydzielonych sił do osiągnięcia celów". **Kontrola** natomiast jako „władza sprawowana przez dowódcę nad częścią działalności podległych organizacji lub innych organizacji, które normalnie nie znajdują się pod jego do-

wództwem i obejmuje odpowiedzialność za wprowadzenie rozkazów lub dyrektyw".

Uważam, że to właśnie ta definicja powinna być powszechnie stosowana, nauczana i rozpowszechniana. Została ona stworzona w ramach współpracy przez wszystkie kraje członkowskie NATO i w związku z tym powinna być stosowana na obszarze każdego z tych państw. Takie podejście i rozwiązanie (definiowanie) terminu „dowodzenia" ułatwi nauczanie, pojmowanie i stosowanie tego pojęcia w Polskich Siłach Zbrojnych podczas wykonywania codziennych zadań, ale także podczas prowadzenia międzynarodowych ćwiczeń i operacji, ciągłej wymiany danych między krajami.

Wszystkie przytoczone definicje sprawiają, że hipotezę, którą postawiłem we wstępie - „uważam, że ujednolicenie definicji dowodzenia jest bardzo trudne, ponieważ istnieje zbyt wiele różnych wersji definiowania tego terminu, lecz dzięki współpracy w ramach takich organizacji jak NATO ujednolicenie pojmowania definicji dowodzenia jest bardzo możliwe", uważam za zweryfikowaną przeze mnie pozytywnie.

Mam nadzieję, że dany artykuł przyczyni się do uniwersalizacji ww. definicji dowodzenia w naszym kraju i będzie stosowana przez wszystkich naukowców, jak i zwykłych obywateli interesujących się bezpieczeństwem i obronnością.

Bibliografia

1. *AAP-6(2014) Słownik Terminów i Definicji NATO zawierający wojskowe terminy i ich definicje stosowane w NATO.* (2014). Bruksela, NATO Standardization Office, s. 98, http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6PL.pdf (Dostęp: 12.12.17).
2. Aponowicz A. (1961). *Dowodzenie.* Warszawa: Wydawnictwo Ministerstwa Obrony Narodowej, s. 72.
3. *Army Doctrine Publication Volume 2 Command,* Prepared under the Director of the Chief of the General Staff, London, 1995, s. 2, http://ids.nic.in/UK%20Doctrine/18aa.pdf (Dostęp: 22.12.17).
4. Auerbach W. (1979). *Leksykon wiedzy wojskowej,* Laparus M. (red.), Warszawa: Wydawnictwo Ministerstwo Obrony Narodowej, s. 90.
5. Dowództwo Wojsk Lądowych. (2008). *Regulamin działań wojsk lądowych.* Warszawa, s. 271.
6. *FM 101-5 Staff Organization and Operations.* (1984). Washington, Department of the Army, s. 1.
7. Griffin R. W. (1996). *Podstawy zarządzania organizacjami.* Warszawa: Państwowe Wydawnictwo Naukowe, s. 38.
8. http://wcnjk.wp.mil.pl/pl/30.html (Dostęp: 30.12.17).
9. http://wcnjk.wp.mil.pl/plik/file/N_20151029_Terminy_2015.pdf (Dostęp: 30.12.17).
10. https://sjp.pwn.pl/szukaj/kierowanie.html (Dostęp: 28.12.17).
11. https://www.nato.int/cps/en/natohq/topics_124879.htm (Dostęp: 12.22.17).
12. https://www.nato.int/ims/docu/mc-brochure-for-mccs-poland-07.pdf
13. *Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r.,* art. 87, 89, 91.
14. Kręcikij J., Lewandowski J. (2015). *Organizacja dowodzenia na poziomie strategicznym i operacyjnym.* Kraków: Oficyna Wydawnicza AFM KAAFM, s. 10, 12.
15. Kręcikij J., Wołejszo J. (red.) (praca zbiorowa). (2007). *Podstawy dowodzenia.* Warszawa: Akademia Obrony Narodowej – Wydział Wydawniczy, s. 12, 15, 16.

16. Kuriata R. (2004). *Dowodzenie siłami powietrznymi.* Warszawa: Akademia Obrony Narodowej – Wydział Wydawniczy, s. 18.
17. Majewski T. (2003). *Kierownik – dowódca w organizacji, zadania, czynności, umiejętności.* Warszawa: Akademia Obrony Narodowej – Wydział Wydawniczy, s. 6.
18. Michniak J. (2003). *Dowodzenie w teorii i praktyce wojsk.* Warszawa: Akademia Obrony Narodowej – Wydział Wydawniczy, s. 1.
19. Michniak J. (2005). *Dowodzenie i łączność.* Warszawa: Akademia Obrony Narodowej – Wydział Wydawniczy, s. 13, 15, 18.
20. Mróz W. (1978). *Zakres kierowania i organizacji pracy dowódczej i sztabowej.* Warszawa: Sztab Generalny Wojska Polskiego, s. 13.
21. *NATO STANARD AJP-01 Allied Join Doctrine,* Edition E, Version 1. (2017). Brussels, NATO Standardization Office, s. 72-73, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/602225/doctrine_nato_allied_joint_doctrine_ajp_01.pdf (Dostęp: 23.12.17).
22. *Organizacja i zarządzanie.* Stabryła, Trzciński (red.) (1986). Warszawa: Państwowe Wydawnictwo Naukowe, s. 132.
23. Orzechowski J. (1974). *Dowodzenie i sztaby.* Warszawa: Wydawnictwo Ministerstwa Obrony Narodowej, s. 21.
24. Szczupaczyński J. (2002). *Anatomia zarządzania organizacjami.* Warszawa: Wyd. Międzynarodowa Szkoła Menadżerów, s. 11.
25. Sztab Generalny Wojska Polskiego. (1996). *Regulamin pracy organów dowodzenia Siłami Zbrojnymi RP.* Warszawa, s. 5.
26. Ścibiorek Z. (2000). *Kierowanie w przedsiębiorstwie.* Toruń: Wyd. Adam Marszałek, s. 26.
27. Ścibiorek Z. (2005). *Podejmowanie decyzji.* Warszawa: Wyd. Ulmak, s. 50.
28. Wiśniewski F. (1965). *Dowodzenie, a znawstwo zagadnień cybernetycznych.* Warszawa: Akademia Sztabu Generalnego.
29. Zabłocki, Miodek. *Dowodzenie w wymiarze powietrznym.* Warszawa, s. 43.

Recenzja książki *Bezpieczeństwo energetyczne i ochrona klimatu w drugiej dekadzie XXI wieku. Energia — Środowisko — Klimat*

Anna Kardasz

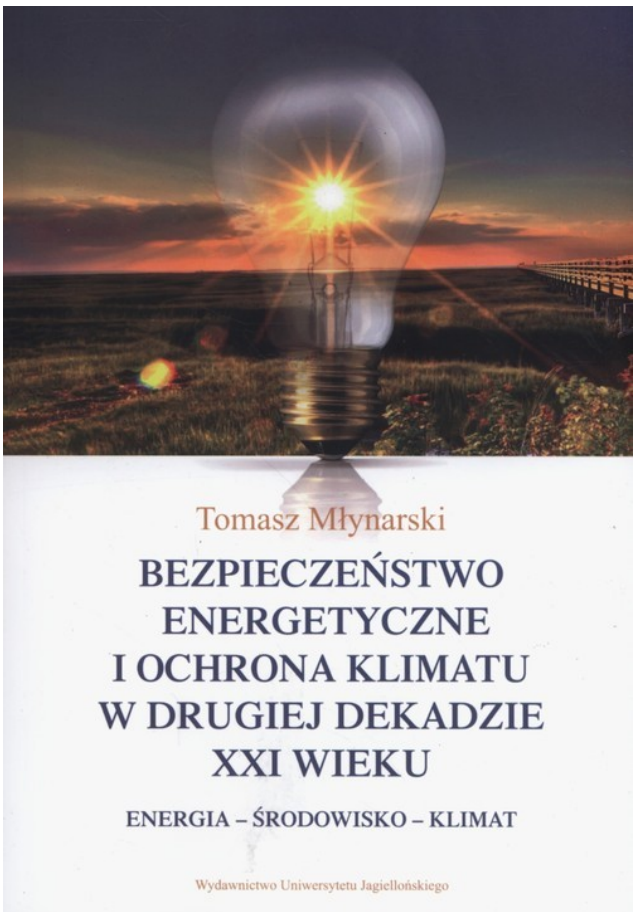
Book review: *Energy security and climate protection in the second decade of the 21st century. Energy - Environment - Climate*

Przedmiotem recenzji jest monografia Tomasza Młynarskiego zatytułowana *Bezpieczeństwo energetyczne i ochrona klimatu w drugiej dekadzie XXI wieku. Energia - Środowisko - Klimat.* Została wydana w 2017 roku przez Wydawnictwo Uniwersytetu Jagiellońskiego. Tomasz Młynarski jest politologiem, wykładowcą w Katedrze Stosunków Międzynarodowych i Polityki Zagranicznej w Instytucie Nauk Politycznych i Stosunków Międzynarodowych Uniwersytetu Jagiellońskiego. Zajmuje się zagadnieniami dotyczącymi współczesnej polityki zagranicznej i bezpieczeństwa Francji a także bezpieczeństwem energetycznym i polityką klimatyczną w Europie oraz międzynarodową ochroną środowiska. Jest autorem wielu monografii i artykułów, m.in.: *Francja w procesie uwspólnotowienia bezpieczeństwa energetycznego i polityki klimatycznej Unii Europejskiej* (2013), *Dylematy bezpieczeństwa energetycznego i polityki klimatycznej Unii Europejskiej w drugiej dekadzie XXI wieku* (2015), *Bezpieczeństwo energetyczne Polski a swoboda wyboru źródeł energii w kontekście unijnej polityki klimatyczno–energetycznej* (2016). Od sierpnia 2017 roku pełni funkcję ambasadora Polski we Francji.

Bezpieczeństwo ekologiczne należy do pozamilitarnych wymiarów bezpieczeństwa państwa natomiast problemy środowiskowe są uznawane za źródła wielu zagrożeń. Z uwagi na ich ponadnarodowy wymiar istnieje potrzeba międzynarodowej współpracy dotyczącej realizacji ujednoliconej i efektywnej polityki ekologicznej. Jednym z najważniejszych wyzwań XXI wieku jest ochrona środowiska i przeciwdziałanie zmianom klimatu. W tym miejscu polityka środowiskowa łączy się z polityką energetyczną, gdyż energetyka to sektor, który jest jednym z głównych emitentów gazu cieplarnianego w postaci dwutlenku węgla. Sposoby ograniczenia antropogenicznych emisji tego gazu są przedmiotem wieloletnich negocjacji na arenie międzynarodowej. Ma to swoje uzasadnienienie nie tylko przez wzgląd na problem ocieplenia klimatu spowodowany rosnącym stężeniem atmosferycznym szkodliwych gazów (z czym nie zgadza się nieliczna grupa naukowców) ale również zanieczyszczeniem powietrza. Zaproponowanym przez autora rozwiązaniem tej kwestii jest szeroko rozumiana transformacja energetyczna oparta przede wszystkim na ograniczeniu spalania paliw kopalnych i zastosowaniu alternatywnych źródeł energii. Tomasz Młynarski we wstępie swojej książki formułuje szereg założeń i pytań badawczych oraz określa metody badawcze. Zakończenie zawiera odpowiedzi na postawione hipotezy, prowadzące do konkretnych wniosków. Monografię cechuje układ analityczno-problemowy, co znacząco wpływa na jej atrakcyjność pod względem naukowym. Książka składa się z dwóch części, pierwsza z nich zawiera dwa rozdziały merytoryczne, natomiast w części drugiej znajduje się ich dziewięć. Monografia posiada wyodrębniony wstęp i zakończenie. Ponadto zamieszczony został wykaz najważniejszych skrótów, załączniki w postaci wykresów i tabel, spis rysunków, tabel i załączników oraz bibliografia. Rozdział pierwszy zatytułowany *Klimat – energia: bezpieczeństwo energetyczne w erze zmian klimatu* składa się z podrozdziałów, które dotyczą wielu zagadnień. Autor

zawarł w nich następujące kwestie: problem zmian klimatu w ujęciu neorealizmu oraz neoliberalnego instytucjonalizmu, związek między produkcją energii a emisją gazów cieplarnianych, genezę i ewolucję współpracy międzynarodowej w zakresie ochrony środowiska i klimatu oraz genezę, ewolucję i perspektywy dotyczące międzynarodowego reżimu zmian klimatu. Tutaj autor skupił się na przybliżeniu mechanizmów wspomagających redukcję emisji gazów cieplarnianych, w tym realizację postanowień protokołu z Kioto, opisie negocjacji klimatycznych w układzie post-Kioto i postanowień konferencji Klimatycznej Narodów Zjednoczonych COP21. Drugi rozdział to *Ochrona klimatu jako element bezpieczeństwa ekologicznego.* Kolejne podrozdziały poruszają takie zagadnienia jak: definicje pojęć i kategoryzacja zagrożeń związanych z bezpieczeństwem energetycznym, ekologicznym i bezpieczeństwem klimatu, przyczyny zmian klimatu i ich następstwa w różnych regionach świata. Na szczególną uwagę zasługuje tutaj tabela zawierająca prognozowany wpływ zmian klimatu w różnych częściach świata. Każdy z wymienionych przez autora rejonów jest w pewien sposób narażony na szereg negatywnych konsekwencji zmian klimatycznych, które mogłyby doprowadzić do nieodwracalnych zmian w ekosystemie planety, przyczyniając się tym samym do poważnych zagrożeń dla bezpieczeństwa ekologicznego jak i społeczno-gospodarczego. Ostatni z podrozdziałów dotyczy transformacji energetycznej, jej definicji, kierunków i atutów gospodarczych. Autor podkreśla jej znaczenie na rzecz ograniczenia negatywnego wpływu wytwarzania energii na środowisko. W ujęciu praktycznym oznaczałoby to szersze zastosowanie alternatywnych źródeł energii, rozwój przemysłu w oparciu o rozwiązania innowacyjne i nowe technologie. Transformacja energetyczna to proces długotrwały i wieloaspektowy, wymagający także zmian w podejściu społeczeństwa do użytkowania energii. Pozostałe rozdziały książki zawierają opis stanowisk i interesów państw, które w największym stopniu są odpowiedzialne za emisję gazów cieplarnianych. Są to: Unia Europejska, Stany Zjednoczone, Chiny, Indie, Rosja, Japonia, Australia, Meksyk, Korea Południowa, Kanada, wybrane kraje Grupy 77 np. Brazylia. Każde z opisanych krajów reprezentuje zróżnicowane poglądy na temat sposobów redukcji emisji gazów cieplarnianych do atmosfery, które wynikają z określonych interesów politycznych, gospodarczych oraz kwestii dotyczących bezpieczeństwa państwa.

Książka napisana jest językiem naukowym, aczkolwiek zrozumiałym dla czytelnika, który nie miał wcześniej do czynienia z taką problematyką. Przejrzysty układ oraz sprecyzowane tytuły rozdziałów i podrozdziałów umożliwiają łatwy i szybki dostęp do określonego zagadnienia. Książka posiada sporo pozycji bibliograficznych, w większości obcojęzycznych. Oprócz monografii i artykułów naukowych, autor korzystał również ze źródeł takich jak: raporty, analizy, ekspertyzy, deklaracje, traktaty międzynarodowe, rezolucje, przemówienia, komunikaty prasowe i materiały internetowe. Zamieszczone tabele, wykresy i schematy ułatwiają zrozumienie omawianych, często bardzo złożonych problemów. Wybór tak licznej i zróżnicowanej literatury jak i aktualnych danych statystycznych umożliwił autorowi przedstawienie problemu badawczego w szerokim ujęciu. Zamieszczone przez niego analizy i wyjaśnienia są niezwykle wartościowe w kontekście zrozumienia istoty ochrony klimatu i jej powiązań z polityką energetyczną państw świata. Książka ta jest cennym źródłem informacji nie tylko dla osób zainteresowanych zagadnieniem bezpieczeństwa energetycznego i ochrony klimatu, ekspertów i naukowców, ale również studentów.



Tomasz Młynarski

Bezpieczeństwo energetyczne
i ochrona klimatu w drugiej dekadzie XXI wieku.
Energia - Środowisko - Klimat

Wydawnictwo Uniwersytetu Jagiellońskiego
Kraków 2017
Liczba stron: 216
ISBN: 9788323342397

Naukowcy w mundurach
Zapraszają

Szanowni Państwo,

w imieniu własnym oraz koleżanek i kolegów skupionych w **Bazie Ludzi Nauki Służb Mundurowych** serdecznie zapraszamy do przyłączenia się do naszego projektu. Baza Ludzi Nauki Służb Mundurowych jest inicjatywą osób, które są aktywne naukowo i służą bądź służyły w polskich formacjach mundurowych. Celem powstania bazy jest integrowanie i rozwijanie „Naukowców w Mundurach" poprzez m.in.:

a) nawiązywanie kontaktów i budowanie kapitału relacji,

b) wymianę doświadczeń, spostrzeżeń, materiałów,

c) pomoc w rozwiązywaniu problemów naukowych i służbowych,

d) organizację konferencji, zjazdów, sympozjów,

e) tworzenie zespołów zadaniowych,

f) realizację projektów badawczych,

g) informowanie o organizowanych konferencjach krajowych i zagranicznych,

h) umieszczanie komunikatów i ogłoszeń,

i) promocję w środowisku służbowym i naukowym,

j) bezpośrednie dotarcie do uczelni, instytucji, organizacji biznesowych z ofertą realizacji wykładów/projektów/ekspertyz.

Mamy nadzieję, że szybko zwiększająca swoją objętość **Baza Ludzi Nauki Służb Mundurowych** będzie stanowiła docelowo swoistą platformę służącą wymianie wiedzy, doświadczeń oraz będzie zachęcać do tworzenia wspólnych projektów naukowo-badawczych. Zachęcamy Państwa do zapoznania się z Naszym projektem znajdującym się pod adresem internetowym:

www.naukowcywmundurze.pl

W przypadku zainteresowania i chęci przyłączenia się do Nas prosimy o kontakt poprzez formularz znajdujący się na naszej stronie internetowej. Chętnie pomożemy rozwiać wszelkie wątpliwości i postaramy się odpowiedzieć na nurtujące pytania.

Zespół prowadzący
Bazę Ludzi Nauki Służb Mundurowych

Czasopismo naukowe Security Review

Wyższa Szkoła Informatyki
i Zarządzania w Rzeszowie
Ul. Sucharskiego 2
35-225 Rzeszów

Redaktor Naczelna:
Ewa Wolska-Liśkiewicz
tel. 17 866 14 47
mail: wolska.eva@gmail.com

Redaktor Techniczny: Anna Kardasz
Korektor języka angielskiego:
Agnieszka Maria Gernand
Projekt okładki: Aleksandra Barć

www.securityreview.pl