SAFETY&DEFENSE

2020
ISSN: 2450-551X
Volume 6 Issue 2

Centrum
Rzeczoznawstwa
Budowlanego

SAFETY AND DEFENSE

Volume 6 Issue 2 (2020)

"Science for Knowledge, Knowledge for Safety & Defense"

ISSN:2450-551X

Table of Contents

Dear Readers,

We are publishing the next issue of "Safety & Defense." On this occasion, I would also like to emphasize that we continue to make every effort to ensure that our journal gains an increasing number of readers, authors, and reviewers. Our efforts, apart from proquality activities, have recently focused on extending the journal presence in international journal databases. I am pleased to inform that our endeavors have brought tangible results because this year we have been included in one of the most important open source journal database, namely the Directory of Open Access Journals – DOAJ. I would like to point out that these small successes were achieved despite the difficult pandemic situation caused by the Covid-19 virus. We hope that this difficult situation will mobilize us to work even harder, which will facilitate the acceleration of the development of "Safety & Defense" in 2021.

We will do our best to ensure that the journal becomes more and more recognizable among academics in the country and abroad. In this regard, we realize that the basis for gaining universal recognition in the world of science are constructive conclusions formulated by the authors of articles published in "Safety & Defense." Based on the postulates and opinions formulated by the authors of the papers published in the current issue, it can be noticed that in many cases our thinking about safety requires a significant reevaluation and sometimes even rejection of already established patterns of operation and stereotypical solutions, which have often become obsolete in consequence of the changes that occurred in the security environment.

Therefore, we hope that "Safety & Defense" will become an important and valued discussion forum where the most important issues of national and international security are considered and discussed.

In the current issue of "Safety & Defense," we present twelve peer-reviewed articles presenting theoretical and empirical scientific considerations that focus on various areas of security. Despite the noticeable diversity of the subject matter, it is possible to identify several trends that have dominated these scientific analyzes. I am thinking especially about the problems related to cybersecurity.

Two articles – "Asian Cyber Security Standards" and "Cybersecurity – One of the Greatest Challenges for Civil Aviation in the 21st Century" correspond to this trend. The first one is in length presents theoretical scientific considerations referring to the issue of cybersecurity threats, the basis of which are domestic security standards introduced by China. Stemming from the analysis is the conclusion that in the last few years alone the Chinese government has implemented around 300 new national cybersecurity standards. These standards cover a variety of information and communication technology (ICT) services as well as products including software, routers, switches and firewalls. Taking into consideration the author's conclusions, it can be noted that such national standardization may pose a serious threat, especially to Western companies that are trying to develop their operations in China. The second article focuses on cybersecurity challenges in air transport. They relate to cybercrime issues occurring in ground handling, aircraft design and production, flight continuity, maintenance, and operation of air carriers. This is due to the fact that the efficient functioning of these areas is largely based on information technologies, including computers, telephones, and the Internet, for which we can diagnose a wide range of threats – from viruses and theft of personal data, to the takeover of the aircraft by cybercriminals. In order to increase the effectiveness of counteracting such threats, aviation organizations employ specific procedures

that broaden the scope of currently existing countermeasures.

The subject of safety and security in air transport is correlated with scientific considerations relating to the identification of air terrorism threats and the assessment of the effects of their occurrence on the functioning of air transport as a global transport sector. Another article deals with the issue of protecting air transport against acts of unlawful interference. In this regard, the authors postulate that aviation security covers the issues of flight safety and aviation protection against acts of unlawful interference. This is particularly important with regard to the security of aircraft and the security of civil airports. The authors of the paper try to answer the following question and research problem: in what direction should the current solutions in the field of air transport safety be improved in order to effectively prevent acts of unlawful interference in the future?

Next paper refers to the subject of protection. It focuses on the protection of individuals in the light of the 2016/679EU Regulation. The emphasis here is placed on the principles of personal data processing and the free flow of this kind of data.

NASA space laser communication system is the subject of the next paper. The topic has been analyzed through the prism of improving the safety of air operations. The authors suggest that two-way space communication is an essential condition for maintaining contact with space missions. This applies to both manned and unmanned ships. Due to constant progress of space technologies, such issues are subject to constant development. With this perspective in mind, the attention was paid to the development of optical space communication, which will ensure fast data transfer, increase throughput, and ensure resistance to typical cyber threats, including jamming, spoofing, and meaconing. Based on the analyzes carried out in the paper, it can be concluded that the implementation of laser optical communication will contribute to increasing the level of safety of air and space operations and will enable a wider exploration of outer space. High expectations are related to the implemented project of the LCRD laser communication transmitter, which is currently being tested by NASA.

Another publication discusses Poland's accession to the NATO as a means for strengthening security in the international arena. The presented research focuses on various kinds of determinants, i.e., technological, organizational, political, and ideological.

The considerations related to the security of Poland are presented in the next article, the content of which relates to the use of unmanned aerial systems in relation to crisis management after 2007. The paper outlines the conceptual framework and organization of crisis management in Poland and analyzes the capabilities of various categories of unmanned aerial systems regarding specific crisis management requirements. Additionally, the current use of unmanned aerial vehicles for crisis management was assessed as well as the prospects of using unmanned aerial systems in crisis management in Poland.

The subject of subsequent articles relates directly to military security. The first one deals with the complexities of the art of war, in particular the role and significance of irregular activities as a form of effective military operations. The paper refers also the 2010 NATO Strategic Concept, which places great emphasis on effective principles and forms of conducting operations against insurgents (COIN). The article accentuates that COIN operations can be the most versatile tool used to combat guerrilla groups.

The next article focuses on the contemporary situation and the future of field artillery. The considerations presented in this paper demonstrate the role and importance of artillery on the modern battlefield. Moreover, the article provides the description of the current state of this type of weaponry. A very interesting part the study is an original attempt to define the directions of the development of artillery capabilities. In this matter, attention was turned to increasing the range of fire systems, implementing multisensor ammunition for active search for tar-

gets, and introducing technologically advanced automated command and fire control vehicles into the army.

In the following paper there are very interesting considerations on hypersonic weapons presented from the point of view of the challenges they create for anti-aircraft fire command and control systems. Based on the conclusions, it can be stated that the highly developed capabilities of hypersonic weapons require a thorough modernization and the acquisition of anti-aircraft defense systems designed to counter these new types of air targets. In addition to the modernization of fire control systems, the fire command and control systems should be simultaneously developed. This is due to the necessity to ensure the efficiency of the decision-making process as well as uninterrupted and effective cooperation with national and allied elements of air reconnaissance and air defense, including the elements of missile defense, which are predestined to combat hypersonic weapons.

The current issue of "Safety & Defense" is concluded by a research paper that focuses on the proposal to calculate the effectiveness of air defense. In this regard, a proprietary model (algorithm) for calculating the air defense effectiveness was proposed. It enables to determine the degree of implementation of the task by the anti-aircraft defense forces in combat conditions. The article presents an innovative approach to the assessment of the effectiveness of air defense, which is based on methods and algorithms (mathematical formulas) that facilitate a reliable assessment of the possibility of performing a task by the air defense system in the case of an enemy air attack.

We hope that you will find the current issue interesting the and it will be a good read.

We would like to wish a great new year to all readers, author, reviewers, and supporters of "Safety and Defense". May the upcoming 2021 be filled with success and full of new achievements. Happy New Year.

Adam Radomyski
Safety & Defense
Editor in Cheif

SAFETY&DEFENSE
ISSN 2450-551X

Irregular Warfare and Modern Defense – Counterinsurgency Operations

Irmina DENYSIUK

War Studies University, Warsaw, Poland,
i.denysiuk@akademia.mil.pl, ORCID: 0000-0002-1154-5167

DOI: https://doi.org/10.37105/sd.71

Abstract
Nowadays, there are a lot of dangers, not only those related to the military. Particular attention should be paid to the threat of guerrilla activity. Therefore, the aim of this article is to indicate the essence of contemporary guerrilla operations in conflicts, and their methods of operation that allow them to achieve their goals. It was also assumed that the modern crisis response operations, and especially COIN (counterinsurgency) operations, constitute a comprehensive approach to counteracting guerrilla activity.
This article uses theoretical methods. Using the analysis and synthesis of materials and studies, the most important conclusions were pointed out.
The leading role in prevention insurgency activities lies with the United Nations, the North Atlantic Treaty Organization and their crisis response operations. In the Strategic Concept NATO 2010 specialists are putting more attention to conducting counterinsurgency operations (COIN). COIN operations are nowadays the most comprehensive tool for combating guerrilla activity, which mainly hits the civilian population. The concepts of using the assumptions of anti-Partisan operations should be implemented on a full scale, including in the armed forces of the Republic of Poland.
Particular attention should be paid to the threat of the guerrilla activity in conflicts. These problems are complex and they deal with many aspects (social, economic, cultural, political and many others). Moreover the partisans activities are irregular and they are often targeted at civilians. This article indicates the methods and techniques used by insurgents in the fight against the state / government. Reference has also been made to the activities that inhibit their activity - complex counterinsurgency operations.

Keywords: defense, insurgency, counterinsurgency operations (COIN), modern warfare, irregular warfare

1. The idea of modern insurgent activities

Many conflicts and crises are characterized by a high degree of irregularity. Insurgent activities use the methods and forms of irregular combat to achieve the goals. The phenomenon of globalization and universal access to information means that the insurgents can also use the latest technology to fight. Nowadays, it is very important to gain and develop the ability of COIN, which should be taken from the past experience of counterinsurgency, and also from the presence of coalition forces in Afghanistan, operating in the first four years of the war (2002–2006). From the analyzes of insurgency activities in this country are relevant. It appeared that the main objectives of their attacks are primarily the structure of the state and the civilian population then – attacks on the intervening forces (Jones, S.G. (2008). p. 53, Denysiuk, I. (2015). *Ewaluacja...,* p. 173, Marszałek, M., Denysiuk, I. (2011). *Koncepcja...*, pp. 28–37).

Guerrilla activities are defined as organized, often ideologically motivated actions taken by irregular groups whose aim is to change the political balance of power in the region or to prevent such change. On the other hand, insurgent actions focus on the abuse or violence of civilians. Such actions are part of irregular activity which is defined as the use or threat of using force by an irregular groups. Often irregular activities are ideologically or criminally (under the influence of warlords) motivated to do or not to do something. That is a challenge for the management of their rebellion against the legitimate authority (AJP 3-4.4. (2011). p. 2-15.).

Currently, experts point out the close connections between rebellion and terrorism and criminal activities. Any rebellion creates favorable conditions for terrorist and criminal groups. The environment is in fact unstable, weakened, often characterized by a large submission of society. However, insurgents seek ways and terrorist methods to support the achievement of their assumed objectives.

Such complex activities of an irregular character threaten all aspects of society, from the political and economic to legal and organizational functioning of the authorities and government state (AJP 3-4.4. (2011). p. 2-16). There are possibilities that guerillas could have endless influence on civilians. On the other hand, three main capabilities should be noted, which are used in their fight. They are mentioned in detail in the Allied Counterinsurgency Operations Doctrine AJP 3-4.4 as: intellectual, physical and moral (AJP 3-4.4. (2011). pp. 2-17–2-19).

The intellectual abilities of guerrilla groups means developing their own doctrine of action, based on the Islamic law, religious or traditional customs. It is also important for these groups to recruit their followers who will be ready to practice their assumptions recorded in the doctrine. It cannot be excluded that the intellectual manifestation of insurgents activities is based on the past experience, not only their own actions, but also those which are today the basis of classical ideas of irregular actions, and other resources available on the web even if they are interpreted by the strategy of NATO and other organizations and states (USA) (AJP 3-4.4. (2011). p. 2-17).

This aspect of insurgent activities is also reflected in the creative use of information and informative technology to achieve more extensive knowledge. The guerrillas, by using contemporary technology, refer to the instruments of propaganda by controlling behavior of local community. They undermine the legitimacy of local authorities and penetrate other countries in search of external support for their activities among groups of emigrants. The key element of these activities is to appeal to a common cultural circle and ideology.

The another group of capability – defined as physical, is the most primitive way,

but is the most popular and simple in practice. The activity of insurgent groups is generally unable to overcome the force of their opponents and therefore, they use asymmetric methods. The groups of insurgents take the enemy by surprise at a critical time and place, gaining advantage over not only tactically but also mentally. The guerrillas do not look for ways of winning in direct combat. Their long-term strategy is such that they can just survive and cause the greatest loss for their opponents.

Physical abilities give the largest range of possibilities and they are closely interrelated with each other, so you can distinguish among them:

— Mental interaction – which is a special tool of fighting between weaker and a stronger, sometimes with the use of primitive techniques. Mental interaction causes not only physical destruction, but it also intensifies panic. Insurgents choose their targets in the urban environments, and focuses on the civilian population. They expect to win renown in the media.
— Formal and informal methods of financial supporting their actions – constitute the power of the guerrilla movement all over the world and obtain the support of charitable organizations, non-governmental and private sponsors, as well as business people.
— Structuralization – creating a vast criminal network which will join not only the rebels, but also terrorists and activists together, not necessarily taking the form of a hierarchical relationship. This indicates that they are independent, and highly mobile, which ensures their anonymity. The insurgent groups, particularly those operating in an urban environment, have the opportunity to influence on the local community, providing them with protection, financial, logistical and mental support.

The last group of insurgent abilities is their motivational techniques often by using measures of social persuasion and/or controlling both the civilian population and individual citizens. The motivation is a complex process, but usually refers to the cultural context. The rebels promise society physical, material and spiritual safety in return for their subordination to them. The insurgents proclaim the need for change in the status quo of the state, by offering their own alternative government. The motivation the community takes different forms, which rebel groups want to keep in a state of instability and injustice to increase dependency and subordination of the civilian population. Currently, the rebels operate in Afghanistan, Iraq and African countries where so-called civil wars take place. Partisan activities are also visible in contemporary internal crises, including in Syria and Ukraine.

2. Insurgent activities and strategies of action

To achieve their goals, insurgents need an ability which was described in the first section of this article. In addition, experts point out that the insurgents use the following five instruments described as:

— violence (violent actions may take different forms, including military action, terrorism and riots),
— national and international propaganda,
— social support for a society,
— social and political activism,
— international relations (cooperation with other terrorist groups and other actors) (AJP 3-4.4. (2011). Annex B, p. B-1).

Today, insurgents have developed different methods to achieve their goals. These methods take the form of well-established strategies now. In Annex B, experts emphasize that insurgents used following strategic models of their activities. That could be distinguished as:

— conspiratorial,
— military-focused,
— urban approach,
— protracted popular warfare,
— identity-focused,
— composite and alliances (AJP 3-4.4. (2011). Annex A, pp. A-1–A-6).

The number and variety of these strategies emphasize a complex and comprehensive approach to insurgent activities (Smith, M.L.R., Jones, D.M. (2015). p. 1424–1425).

Firstly – the conspiratorial approach – involves a rebellion and the situation, in which a few leaders or militants are trying to take over control of government structures. Normally, such insurgents stay in secret for as long as possible and they emerge as soon as their success is almost at hand. The conspiratorial approach is usually created with a small and secretive group of forces.

The military-focused approach tries to create revolutionary possibilities of achieving their goals. By applying military force, insurgents try to fight for independence or secession. Normally, they can use conventional forces. In the complex environment of operations, they try to employ armed elements to support their seize power. This support can be created with urban or/and rural society. The authors of AJP 3.4.4. say that "this approach was applied in the 60s and 70s and it is currently used in some parts of Sub-Saharan Africa" (AJP 3-4.4. (2011). Annex A, p. A-1).

The next – urban approach – is focused on urban terrorism as a long-term activity which is taken by small and independent groups that do not need the support of the common people. This creates that countering them is very difficult. However, insurgents can gain popular support in certain times and areas, especially when there is a close relationship with religion, family or social groups. In urban society, the activities of insurgents and their impact on a population can be more effective.

The protected popular warfare is an approach of insurgents, where decisive combat is intentionally avoided. The main goal in this strategy is seizing political power in a given region. The examples of this approach are those found in the Republic of China or Vietnam in the 20th century. For example, Mao Zedong created a theory of war which contained a civil-military approach. The complex Mao Zedong's strategy included three phases: latent strategic defensive, strategic balance and strategic offensive.

The identity-focused approach is created on the basis of common identity of clan, tribe, religious or/and ethnic structure. It should be very strongly noted that this approach is most popular among contemporary insurgents. The operations conducted by them would be in the future based on the civil-military actions, more civil – less military. It is very important to get public support, and this is the easiest way to build it just referring to common values.

The composite strategy is the most extensive operation strategy which can be used by insurgents. Nowadays, insurgents use different ways and methods. They know that the best strategy is to take advantage of the moment. These also rely on experiences, not only their own. This approaches assume that there can be many different groups with competing interests in the operational environment.

Contemporary insurgent groups look for ways to maximize its survivability and to establish their own influences in a given state. This is very complicated for counterinsurgency operations. Both the soldiers and the experts (also NATO planners) must understand this type of insurgent strategy to win. Victory must be based on the analysis of all the factors (Marszałek, M. (ed.). (2013). *Zintegrowany...*, p. 42, Denysiuk I., 2015. pp. 85–106).

Today, insurgencies develop very complex scenarios of actions. There are many actors in the operations environment. It is very hard to clearly separate the two opposing sites: insurgents and forces of opposition. It is crucial that all sites in operation are not uniformed. It is not also easy to distinguish

them from others: "among these actors are militias, warlords, organized crime, drug dealers, private security companies, NGOs[1], the media, multinational companies, and foreign countries with strategic interests in the area" (AJP 3-4.4. (2011). Annex A, p. A-6).

The nature of contemporary insurgencies is complex. The experts emphasize that different groups of insurgents, also in different countries, can cooperate. There is the possibility of insurgents sharing their experiences. Fighters can take part in other wars. They can also train each other or only give logistic or financial support. It can be stated that today's insurgencies are characterized by an ability to adapt their strategies and rules of action to contemporary challenges of war.

The threats posed by new insurgencies affect countries, which are stricken by the rebellion and other (third) countries. Summarizing, it should be emphasized that there are many types of insurgencies which have different strategies and forms. Modern insurgency is the result of globalization (Jackson, P. (2019), pp. 1-3). Nowadays, insurgents use a new technology like the GPS. They often take a sort of terrorism actions or use tools to impact on society, for example propaganda. They have connections with criminal groups which support their actions in financial and ideological ways. The most comfortable environment for their operations is in the urban area.

We can also name the main motivation methods which are used by insurgents (AJP 3-4.4. (2011). Annex C, pp. C-1–C-2):

— persuasion,
— coercion,
— provoking disproportionate reaction,
— foreign support,
— apolitical motivation.

These motivation methods are the main reasons why insurgent movements are not seen as criminal.

3. Modern counterinsurgency operations

The counterinsurgency action theory has been developed since the mid-twentieth century and its main representatives are: David Galula and Roger Trinqier. The strategists have created the foundation of counterinsurgency operations based on their own experience gained during the war in Algeria. The study highlights the general assumptions of counterinsurgency operations and their history. Such operations were conducted, among others, in Indochina, Vietnam (Galula, D. (2006). Trinquier, R. (2006)).

The form of actions which could effectively counter the activities of the rebels are the operations against insurgents (COIN – counterinsurgency operations) as a process to respond to crises and conflicts outside the NATO treaty area. This form of fighting counter guerrilla groups, known as "operation other than a war", is therefore desirable.

Counterinsurgency operations are a relatively new tool, particularly in comparison with the older guerilla warfare, are used in non-military activities. The irregular actions are already well established in theory and practice. However, the counterinsurgency operations (COIN) are still developing. It is therefore important to develop the ability of COIN, which is now emphasized in the New Strategic Concept For the Defense and Security of The Members of the North Atlantic Treaty Organization – "Active Engagement, Modern Defense".

[1] Non-Governmental Organizations – added by author (I.D.).

As already mentioned, "New Strategic Concept ..." experts said that to be more effective across the spectrum of emergency response activities, we should develop abilities such as military abilities required to conduct expeditionary operations, with particular emphasis on counterinsurgency operations, stabilization operations and reconstruction operations (*Active Engagement, Modern Defence*. (2010), point 25). On the other hand, the U.S. Army Gen. George W. Casey Jr. said, that the armed forces of this country need the ability of counterinsurgency operations, containing of both offensive, defensive and stability actions (Caramone, J. (2010)). Taking into account the activity guerrillas, it is considered that COIN operations should be used and applied in practice not only optional, as one of many possibilities, but they must become an element of necessary actions.

Counterinsurgency operations (COIN) is separated from a set of military operations different from war implemented the stabilization phase, which should be understood as complex, multi-functional and multi-faceted projects, including both military operations conducted by coalition forces targeted against guerrillas and the process of state-building to support and help people (Ucko, D.H. (2009)). COIN includes psychological and information operations, intelligence and support to the local community (Marszałek, M., Denysiuk, I. (2013). *Elementy...,* pp. 12–16).

Counterinsurgency operations are aimed at all hostile groups in any state where they are needed. In the records of the "Department of Defense Dictionary of Military and Associated Terms" COIN is military, paramilitary, political, economic, psychological action taken against insurgents (AJP 1-02. (2001). p. 105). COIN operations are comprehensive civilian and military efforts covering a wide range of activities from fighting with guerrillas to ensure security of the civilian population (Read more: Ruff-Stahl, H.J. (2015). pp. 137–148).

The essence of COIN operations is connected by joint effort of the host countries, international agencies, different other organizations and forces of coalition (JP 3-24. *(*2009). p. X). It is also pointed out today that victory in war is largely based on the work with the local community, recognizing indigenous government and its security forces (if any). It is a critical value for the success of COIN (Jones, S.G. (2008), pp. 7–25, Denysiuk, I. (2015), pp. 207-210). The suppression of acting guerrillas depends on the preparation and modernization of the armed forces of intervening. The success will be depend on understanding the nature of local conflicts, the community's needs and the ability of guerrillas. The key to success in the fight against the insurgency is cooperation with society that knows the area of operations, knows the clans, and is able to move in the environment of operation. The local society can contribute to the activities of the coalition partners by providing them with relevant information, including the location of shelters and trails the guerrillas (Marszałek, M. (ed.). (2013). p. 11, Denysiuk, I. (2015), pp. 89–93).

The fundamental strategy of COIN gives assistance in maintaining the legitimate authority and minimizes attacks of guerrilla groups, mainly by trying to isolate those groups, and thus reduces the possibility of impacting them. The COIN effort can repel enemy attacks through the development of a defense system of the failed state (Marszałek, M., Denysiuk, I. (2013). *Elementy...,* pp. 17–19).[2]

Counterinsurgency operations act on two levels:

— political – as an attempt to reach a peace agreement, assuming that the dispute was created at the level of ideological and cultural, or from a sense of injustice,

[2] It is the process of Security Sector Reform (SSR).

— and military – the use of force to enforce the desired behavior. Hence, there is a real need for cooperation on these two levels (Marszałek, M., Denysiuk, I. (2011). *Koncepcja...,* p .13, Galula, D. (2017). p. 17).

There is a claim that COIN operations depend on: the simultaneous conducting offensive operations (against guerrillas, for example, to take control of at least one area which was previously controlled by the guerrillas), defense (protecting the civilian population, which manifests itself in taking control in major population centers) and stabilization.

There are different theories of COIN operations: today recognized as historic methods: carrot and stick, fight for the hearts and minds and transformation (Marszałek, M., Denysiuk, I. (2011). *Koncepcja...,* p. 13). The first refers to the correct choice of the system of rewards and punishments, which in practice are applied to manipulate a population. The second i way leads to gaining the confidence of the civilian population. The third is the most extensive approach to COIN, including the practical implementation of such projects as: the transformation of political and economic, and building a better future.

However, the new solutions to prevent insurgent actions are sought today. The nature of guerrilla warfare, which had been many times emphasizing, is difficult and complex. Therefore, the planned approach to COIN operations should include synchronized, multi-faceted activities, including civil-military cooperation, based on a foundation of information and psychological operations (JP 3-24. (2009). p. X-1).

A fundamental role of COIN operations is their information operations. They are addressed to two audiences: civilian and insurgents. Society is informed of the need to demonstrate their support for an operation. The aim is to increase awareness of the population that the coalition forces (U.S. forces) are conducting activities directed exclusively against the rebels (partisans). The messages sent to the rebels urges them to stop irregular activities.

The existence of many methods to achieve success in COIN operations was assumed, wherein these methods are not mutually exclusive and may be used simultaneously. The only criterion for selecting specific strategies for COIN operations is the degree of its adequacy to the needs and conditions in the area of operations. It is necessary to conduct an interview in the local community and select the appropriate strategy. Nowadays, there are three main strategies of counterinsurgency operations:

1 clear-hold-build,

2 combined action,

3 limited support (JP 3-24. (2009). pp. X-2–X-14, *The U.S. Army and Marine Corps Counterinsurgency Field Manual.* (2007). p. 174, Marszałek, M. Denysiuk, I. (2011). *Koncepcja...,* pp. 92–103).

The correct choice of strategy is implemented at the level of the operational planning process. It was pointed out that effective planning COIN operations requires a focus on both combat and non-combat activities. It is also important to distinguish the goals of both personal (detection and elimination the guerrillas) and non-personal (detection hiding places, Information operations).

Choosing the right strategy for COIN operations is based on the level of operations planning. Operational goals are set accordingly for each field of COIN operations, according to the so-called logical lines of operations (LLO) and at every level of activity. Both planning and management of the COIN operation is very complex and requires the involvement of many resources, ranging from intelligence activities, obtaining information (also HUMINT) about the enemy, its leaders, commanders, external support, bases, finances, media and local authorities. (degree of rule of law, democratization, development of security forces and basic government institutions and agencies, degree of provision of relevant services to society, de-

gree of economic development). All these elements combine the operations environment and information operations as the foundation of all COIN projects. The success of COIN is largely based on the use of strategic communication tools, including psychological operations (PSYOP), information activities (IOs), in the form of action counter - ideology, counter-sanctuary, counter – motivation of partisans or propaganda. In order to combat insurgent actions, one must understand the values of their ideology or religion. In addition, COIN efforts must understand the environment and culture of insurgent movements. This allows us to successfully carry out activities under such operations as: counteracting radical ideology, motivating partisans, also motivated by religion. For the purposes of the COIN operation, key recipients, leaders, and authorities are identified in order to know who to reach with information. In COIN operations, the world should be viewed from a local perspective. Comprehensive efforts made by a group of specialists, the media, finance, business and other consultants, including psychologists, are key. (Paul, Ch., Clarke, C.P., Grill, B. (2010). pp. 56–57, Denysiuk, I. (2014)).

In current forms of conducting military operations, including COIN, disinformation is extremely important (both propaganda and so-called fake news - although so far there are no reliable research results indicating the long-term effectiveness of their use). (Świerczak, M. (2018). p. 210).

Disinformation is an extremely complex method of operational work, which is a way of influencing the current or potential opponent, enemy special services or specific groups or social strata in foreign states, but sometimes also one's own country. It is a deliberate transfer of false information to the opponent, using means and methods of operational work in order to mislead him and obtain planned results that are beneficial for him (Polmar, N., Allen, T.B. (2000). p. 151., Lewandowski, H. (2000). p. 81–82.).

COIN strategies should be designed to protect the population against insurgent violence as well as strengthen the legitimacy and potential of government institutions. Therefore, since 2000 in COIN operations, the leading role has been played by groups of theoreticians and practitioners who, with their work, support the success of COIN operations based on information they obtain from civil sources (HUMINT) or through intelligence (SIGINT).

4. Summary

Nowadays, it is very important to gain and develop the ability of COIN. Many conflicts and crises are characterized by a high degree of irregularity. Today, the insurgents have developed different methods to achieve their goals. These methods have taken the form of well-established strategies. The number and variety of these strategies emphasize a complex and comprehensive approach to insurgent activities.

Contemporary insurgent groups look for ways to maximize their survivability and to achieve their own influences on the state. This is very complicated for counterinsurgency operations.

COIN operations are comprehensive civilian and military efforts covering a wide range of activities from fight with guerrillas to ensure security of the civilian population. The success of COIN will be depend on understanding the nature of local conflicts, the community's needs and the ability of guerrillas. The key to success in the fight against the insurgency is a cooperation with society that knows the area of operations, knows the clans, and is able to move in the environment of operation. It existence of many methods to achieve success in COIN operations was assumed. There are three main strategies of counterinsurgency operations: clear-hold-build, combined action, limited

support. The correct choice of strategy is implemented at the level of the operational planning process.

The suggestions contained in this article have helped us to formulate following conclusions:

— the internal conflicts, especially ethnic, religious and national, will become more frequent;
— those conflicts will be dominated by the rebels who are using irregular forms of fights;
— civilians are and they will be the most affected group;
— it is possible to react to these conflicts by NATO forces, the United Nations and coalitions of states;
— it is important to train the armed forces and adjust their ability to adapt to the irregular nature of threats;
— the most crucial matter is civilians support (fight for the hearts and minds) so that it will benefit them, not the rebels;
— counterinsurgency operations reduce the terrorism.

In addition, we have noted that:

— an appropriate way of responding are counterinsurgency operations, which include civil-military cooperation rather than military operations;
— the reaction should take place in many areas, not only military but political, social and economic as well;
— the training system of forces should be expanded, also in the Polish Armed Forces;
— the civilians' participation in the operations should be taken into account;
— these changes must be considered during the planning stage of COIN operations;
— an important element on which COIN operations are based are information operations, psychological ops and other operations as part of strategic communication.

In summary, we have to control the counterinsurgency actions in a methodical way, not just intuitively.

References

1. *Active Engagement, Modern Defence.* (2010). *Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organization* - Adopted by Heads of State and Government in Lisbon, Lisboa
2. AJP 1-02. (2001). *Department of Defense Dictionary of Military and Associated Terms*
3. AJP 3-4.4. Annex A – *Strategies of insurgency*
4. AJP 3-4.4. Annex B – *Insurgent activities for achieving their goals*
5. AJP 3-4.4. (2011). *Allied Joint Doctrine for Counterinsurgency (COIN)*, NATO Standardisation Agency
6. Caramone, J. (2010). *Casey says Army needs counterinsurgency capabilities,* "American Forces Press Service", Washington, Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=59067, 25.02.2012
7. Cohen, E., Crane, C., Horvath, J., Nagl, J. (2017). *Principles, Imperatives, and Paradoxes of Counterinsurgency*, [in:] Bett, R.K (ed.), *Conflict After the Cold War. Arguments on Causes of War and Peace,* New York: Imprint Routledge. DOI: https://doi.org/10.4324/9781315231372
8. Crane-Seeber, J. (2011). *Everyday Counterinsurgency, "International Political Sociology",* Vol. 5, Issue 4, pp. 450–453, DOI: https://doi.org/10.1111/j.1749-5687.2011.00145_3.x
9. Denysiuk, I. (2015). *Ewaluacja operacji przeciwpartyzanckich*, rozprawa doktorska, Warszawa: AON

10. Denysiuk, I. (2014). *Modelowanie kryteriów sukcesu operacji przeciwpartyzanckich*, praca naukowo-badawcza , nr III.1.1.0., Warszawa: AON
11. Galula, D. (2006). *Counterinsurgency Warfare. Theory and Practice*, PSI Classics of the Counterinsurgency Era, Praeger Security International, Westport, Connecticut, London
12. Galula, D. (2017). *Insurgeny and Counterinsurgncy* [in:] Bett, R.K (ed.), *Conflict After the Cold War. Arguments on Causes of War and Peace,* New York: Imprint Routledge. DOI: https://doi.org/10.4324/9781315231372
13. Gompert, D.C., Gordon IV, J., Grissom, A., Frelinger, D.R., Jones, S.G., Libicki, M.C.,, O'Connell, E., Lawson, B.S., Hunter, R.E. (2008). *War by other Means. Building Complete and Balanced Capabilities for Counterinsurgency*, RAND Counterinsurgency Study – Final Report, Santa Monica: Rand Corporation
14. Jackson, P. (2019). *Intelligence in a modern insurgency: the case of the Maoist insurgency in Nepal,* "INTELLIGENCE AND NATIONAL SECURITY", https://doi.org/10.1080/02684527.2019.1589677, DOI: 10.1080/02684527.2019.1589677
15. Jones, S.G. (2008). *Counterinsurgency in Afghanistan,* RAND Counterinsurgency Study, Vol.4, RAND Corporation
16. JP 3-24. *(*2009). *Counterinsurgency Operations*, Joint Chiefs of Staff
17. Lewandowski, H. (2000). *Podstęp, inspiracja i dezinformacja w działalności służb specjalnych*, Warszawa
18. Marszałek, M., Denysiuk, I. (2011). *Koncepcja użycia sił zbrojnych w wojnach nieregularnych*, praca naukowo-badawcza nr III.5.1.0, Warszawa: AON
19. Marszałek, M., Denysiuk, I. (2013). *Elementy wsparcia procesu stabilizacji i odbudowy państw*, „Zeszyty Naukowe", no 4(9)
20. Marszałek, M. (ed.). (2013*). Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne*, Projekt badawczo-rozwojowy w zakresie obronności i bezpieczeństwa państwa finansowany ze środków Narodowego Centrum Badań i Rozwoju, Warszawa
21. Paul, Ch., Clarke, C.P., Grill, B. (2010). *Victory has a thousand fathers. Sources of Success in Counterinsurgency*, RAND Corporations
22. Pechenkina, A.O., Bennett, D.S. (2017), *Violent and Non-Violent Strategies of Counterinsurgency*, "Journal of Artificial Societies and Social Simulation", Vol 20, Issue, SimSoc Consortium, DOI: 10.18564/jasss.3540
23. Polmar, N., Allen, T.B. (2000). *Księga szpiegów. Encyklopedia*, Warszawa
24. Ruff-Stahl, H.J. (2015). *Human Factors im Krieg: Ist COIN eine taktische Antwort auf ein strategisches Problem?,* [in] Schroeder, R., Hansen, S. (ed.) *Stabilisierungseinsätze als gesamtstaatliche Aufgabe, Erfahrungen und Lehren aus dem deutschen Afghanistaneinsatz zwischen Staatsaufbau und Aufstandsbewältigung (COIN)*, DOI: https://doi.org/10.5771/9783845249018-137
25. Smith, M.L.R., Jones, D.M. (2015). *The political impossibility of modern counterinsurgency: strategic problems, puzzles and paradoxes, International Affairs*, Vol 91, Issue 6, https://doi.org/10.1111/1468-2346.12467
26. Świerczak, M. (2018). *System matrioszek, czyli dezinformacja doskonała. Wstęp do zagadnienia,* „PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO" no 19
27. *The U.S. Army and Marine Corps Counterinsurgency Field Manual. (2007).* Chicago and London: The University of Chicago Press

28. Trinquier, R. (2006). *Modern Warfare. A French View of Counterinsurgency*, PSI Classics of Counterinsurgency Era, Praeger Security International, Westport, Connecticut. London
29. Ucko, D.H. (2009). *The New Counterinsurgency Era. Transforming the U.S. Military for Modern Wars*, Washington

SAFETY&DEFENSE
ISSN 2450-551X

Poland's Accession to NATO Considering "Partnership for Peace" and the U.S. Perspective

Tomasz GERGELEWICZ

Independent researcher, Ministry of National Defense, Warsaw, Poland;
t.gergelewicz@wp.pl , ORCID: 0000-0002-9145-5099

DOI: https://doi.org/10.37105/sd.81

Abstract

The accession of Poland to the group of NATO member states was undoubtedly one of the milestones in the modern history of the country and in the direction of strengthening security in the international arena. The whole process was conditioned by various types of determinants: technological, organizational, political and ideological (Kupiecki, 2016). Many publications have been dedicated to Poland's accession to NATO and its later role among the allied members. Nevertheless, there is a lack of particular studies in the professional literature that presents a detailed chronology of Polish pre-accession activities and the diverse opinions of the US administration regarding the enlargement of NATO with new member states recruiting from the former Warsaw Pact. This gap in available literature was a trigger for writing this article with the purpose to present the undertakings of Poland aimed at accession to NATO in the aspect of "Partnership for Peace" and the US point of view. In the research process, two basic methods were employed: analysis and synthesis. The method of analysis was used in relation to the verification of collected literature, normative acts and documents on international security. The method of synthesis was applied for conclusions. The undertaken research on the topic proved that without consistent actions and initiatives conducted by Poland in the international area and without the support of the US, joining NATO would be highly difficult or even impossible. At the same time, a detailed analysis highlighted that the accession of Poland to NATO was and still is mutually and beneficial for Warsaw and Washington.

Keywords: safety, NATO, alliance, Partnership for Peace, foreign policy

1. Introduction

Despite the fact that NATO is a multinational structure, from its beginning to present times, the US is the leader that engages the largest amount of assets and forces in the activities of the Alliance. The US is also a primary political decision maker on the international forum and many tasks dedicated to the NATO alliance are conducted according to the political interest of the US (Pacuła, 2007). In terms of seeking security and geopolitical stability, the prevailing option among Polish politicians was that it would be most favorable for Poland would be to seek security and military balance within the cooperation with the US. The reason was the difficult situation of Poland after leaving the Eastern Bloc. Poland was isolated on the international ground, which in the long run could have threatened the maintenance of external security. In this situation, Poland put a great effort into reaching the status of a NATO member state. Moreover, the justification for these efforts was the historical experience resulting from the geopolitical location of Poland in Europe, which implied German and Russian aspirations to subordinate Poland. As a result of this reason, the breakup of the Warsaw Pact as well as the Mutual Economic Assistance Council resulted in the urgent need to create new political-military guarantees for Poland based on new alliances. Finally, the option of establishing the security of Poland on the basis of the North Atlantic Alliance and close cooperation with the US was been chosen. The adopted concept assumed that it is the best option to maintain balance of military force in Europe and to prevent Russian political-military expansion again to Poland (Mozol, 2016).

2. Poland in the "Partnership for Peace" program

The main effort of seeking the opportunity to join NATO structures was focused on a dialogue on the membership of Poland in the "Partnership for Peace" program. Politically, "Partnership for Peace" was a defense agreement for the US cooperation with Central and Eastern European countries. The idea of the program was announced on 20 October 1993 by the US Secretary of Defense Les Aspina during a conference NATO Defense Ministers in Travemünde, Germany. "Partnership" was also a response to the readiness of Central and Eastern European countries, former members of the Warsaw Pact, to join the new Alliance (Okoński, 1995). Taking into consideration the fact that Russia did not resign from its influence in the countries of the former Eastern Bloc, it was beneficial to secure the interests of the US in Central and Eastern Europe liberated from the Soviet control. For this reason, countries such as Poland, the Czech Republic or Slovakia could have been supportive of the US in the struggle with Russia for military dominance. It seemed to be the best way to push the border of "western world" farther to the east.

Closer analysis of the "Partnership for Peace" program proved that it was a well-built cooperative bridge for the integration of NATO with other countries, especially from the perspective of international security. The program was attractive for these countries, because it offered an opportunity to:

1) support efforts for the transparency of national defense planning processes and development of defense budgets;
2) guarantee democratic control over the armed forces;
3) create ability and readiness to contribute to UN operations;
4) develop cooperation and military contacts with NATO in order to plan joint exercises that aimed at maintaining the capability of

"Partnership for Peace" members to conduct peace, search and rescue missions;
5) train and organize forces that in a long-term perspective will cooperate more efficiently with NATO forces.

From the legal perspective, assumptions of the "Partnership for Peace" were consistent with Article 10 of the Treaty,[1] which states: "*The Parties may, by unanimous agreement, invite any other European State in a position to further the principles of this Treaty and to contribute to the security of the North Atlantic area to accede to this Treaty. Any State so invited may become a Party to the Treaty by depositing its instrument of accession with the Government of the United States of America. The Government of the United States of America will inform each of the Parties of the deposit of each such instrument of accession"* (NATO, 2019).

The Treaty creates the possibility for the Alliance's enlargement by including new European member states that would be able to comply with the principles of the Treaty and to contribute to NATO security.

It should be noted that for these reasons, on 10 January 1994 in Brussels at the NATO "summit", there was an official proposal presented to the countries of Central and Eastern Europe that emerged after the collapse of the USSR to cooperate with the Alliance in the framework of the "Partnership for Peace". As a result, during a meeting with President Bill Clinton in Prague on 12 January 1994, the presidents of Poland, the Czech Republic, Slovakia and Hungary stated that they would make every effort to achieve the program requirements for the "Partnership".

Regarding the wish to unify with the West and to join NATO, on 2 February 1994 during a visit to NATO Headquarters in Brussels, Polish Prime Minister Waldemar Pawlak signed the "Partnership for Peace Framework Document". Next, on 5 July the same year, Poland agreed with NATO the individual "Partnership for Peace Programme" (www.bbn.gov.pl-kalendarium).

The initial participation of Poland was limited to:

1) the participation of military experts in specialist courses organized by NATO;
2) engaging military units and observers in joint training and exercises with the use of troops (LIVEX);
3) participation in combat, humanitarian missions as well as search and rescue operations.

In the longer perspective, cooperation within the "Partnership for Peace" was significantly expanded to include:

1) increasing transparency in defense planning and in work on the military budget by exchanging information and sharing expenses with NATO Headquarters;
2) ensuring democratic control over the armed forces through structural transformation, legislative changes and democratic procedures for operating the budget, in line with NATO norms;
3) maintaining capabilities and readiness to join the UN or CSCE peacekeeping operations;
4) the development of military cooperation with NATO aimed at organizing peace, search and rescue, humanitarian missions through:
   a) undertaking joint actions for the compatibility of command and control system – C2;
   b) creating a modern Polish air defense system;
   c) unified procedures in emergencies and high necessity levels;
   d) defense and logistic planning, including purchasing and delivery

1 The North Atlantic Treaty is an agreement concluded in Washington on 4 April 1949 based on the United Nations Charter. On the provisions of the Treaty, the North Atlantic Treaty Organization – NATO was established.

system, military infrastructure and standardization;
   e) trainings and research as well as the development of military technology.
5) Long-term development of the armed forces and preparing them to cooperate with joint forces, adjusting the C2 system, communication, logistics, armament and education to NATO standards.

For the needs of the "Partnership for Peace" program, the Polish party declared its readiness to provide training centers and military training grounds, as well as the attachment of a battalion and several smaller specialist units for joint use in future operations.

Poland's implementation of the assumptions for the "Partnership for Peace" included three main forms of cooperation:

1) expert level consultations, exchange of experience and information;
2) participation of military units and observers in trainings and exercises in peacekeeping, search and rescue and humanitarian operations.
3) participation of security experts in courses, trainings and studies organized by specialist NATO centers (NATO, 1994).

One of the first examples of cooperation was the joint military exercise codenamed "Bridge of Cooperation", conducted from 12 to 16 September 1994 in Biedrusko near Poznań, in which military units from thirteen Allied member states and partner countries participated (Hansen, 1995).

In conclusion, it should be recognized that the "Partnership for Peace" was undoubtedly a fundamental premise for Poland's accession to NATO and played a significant role in the process of expanding NATO itself. At the same time, the first contacts of Polish soldiers with NATO soldiers revealed essential differences in the functioning of military structures, elements of C2, knowledge of NATO nomenclature, and most of all the technological distance in military equipment and assets.

Despite this disparity, Polish representatives assured the US that even though there are visible technical, logistic and training imperfections, Poland expresses the readiness to become an active member and equal NATO partner.

3. The American point of view on new NATO members

At the NATO Summit of Heads of States and Governments on 8 July 1997 in Madrid, it was decided to invite Poland, the Czech Republic and Hungary to talk about NATO membership. The decision was included in the "Madrid Declaration on Euro-Atlantic Security and Cooperation". The Declaration assumed that the goal of the Alliance was to sign the "Accession Protocol" during the next session of the North Atlantic Council on 16 December of the same year and to finalize the ratification process enabling the invited states to join NATO by April 1999 (Madrid Declaration, 1997).

After the summit, representatives of Poland held a meeting with US President Bill Clinton in Warsaw. During the meeting, participants proposed the idea of consolidating Europe, among others, by expanding the NATO Alliance. Former participants of the Warsaw Pact also expressed their request to the US for support in the process of accessing NATO. During the meeting, Polish representatives argued that this would consolidate Europe and create a united continent. They also declared that in return, Poland would support the US in European policy (Kupiecki, 2019).

Advocates of the expansion of NATO claimed that through partnership with Poland, the US would build a solid anti-Russian dam. What is more, they convinced that cooperation with Poland will counterbalance European hegemons such as Germany and France, opponents of the US in the fight for dominance and influences in Europe (*Encyclopedia Britannica*). Nevertheless, it has to be recalled that the

American political scene was divided into two "new membership access" camps. Despite the favorable position of President Bill Clinton, not all representatives of his administration agreed on the enlargement of NATO with new member states. Opponents stated that the expansion of NATO would disturb US relations with Russia. According to the Deputy Secretary of State for European Affairs Ronald Asmus, the only right solution in this matter should have been to choose negotiations as the main cooperative tool in building up the relationship between US and Russia (Asmus, 2002). Furthermore, Ronald Asmus claimed that any actions aimed at expanding the scope of NATO that would not be agreed and settled with Russia, would result in a backstop in the relations between US and Russia that would be difficult to estimate and rebuild (Asmus, 2008b). A good example of a negative approach to NATO candidates may also be a petition written by Susan Eisenhower addressed to Bill Clinton, which called for blocking further accession processes. It was a part of a wide-scale campaign called "No to NATO Expansion Tour" organized by the lobby group, which was, among others, associated with Neo-Nazi group "Cato Institute" (Kupiecki, 2019a).

At the same time, it was offered to the Central and Eastern Europe to evolve broader cooperation under the "Partnership for Peace" program and to open the gates of the European Union to these countries, instead of expanding NATO. There was also a clear message for the US to improve relations with Russia instead of supporting former Eastern Bloc countries in their strivings for the membership. It was pointed out that the US should seek solutions that would encourage Russia to assume the role of America's partner, and even ally in the further perspective (Asmus, 2008a).

Despite opposition, President Bill Clinton did not remain alone in his opinion, and his course of action remained unchanged. There were voices highlighting the fact that NATO enlargement is the necessary condition for the further functioning of the entire organization. The US conducted an analysis of Poland's readiness to join NATO structures. At the request of the US Congress Research Office the report determining the state of the Polish army was prepared. The report gave a positive opinion on Poland's preparation for the military operational capability, but undermined the ability to provide civilian control over the army (Zalewski, 2002).

Finally, the approval of Poland's aspirations to join NATO prevailed. Among other reasons, it was underlined that Poland played significant role in the overthrow of the communist system and it should be rewarded with a solid American support.

4. The end of the Warsaw Pact and a new opening for Poland

The year 1991 brought to Poland many changes in its political and military situation. It was stated at the forum that after the dissolution of the Warsaw Pact on 31 March 1991, Poland in the field of military and political affairs was definitely oriented towards the West (Kaczmarek, and Skrzyp, 2003).

On 23 May 1991, the Minister of National Defense visited the NATO Headquarters to reveal the course of Polish foreign policy. On 3 July 1991, the President of Poland paid a visit to Brussels, where he made a statement on Poland's support for NATO policy. In 1992, Poland officially re-confirmed the aspirations for membership in NATO (MON, 2017). On 11-12 March 1992, NATO Secretary General Manfred Wörner announced that the road to NATO is open. A month later, the first meeting of the NATO Military Committee was held, attended by defense ministers and chiefs of staff of Central and Eastern European countries. On 1 September 1993, President Lech Wałęsa in a letter to the Secretary General of NATO made a statement that membership in the allied structures is the

highest priority of Polish foreign policy (www.bbn.gov.pl-kalendarium).

After official announcements, Poland started implementing particular changes regarding the area of armament and equipment, which had to be strictly adapted to high NATO standards and norms. It was necessary to shift to a new communication system and C2. It was also necessary to restructure the organizational scheme of the army following the NATO pattern, which means that there was a high demand to achieve compatibility and interoperability of the Polish armed forces with Western armies. It was also necessary to ensure civilian control over the army, which meant civilian leadership at the Ministry of National Defense, subordination of the General Staff to the civil defense minister, and parliamentary control over the armed forces.

All of these projects were difficult to meet because of the high costs and the "curtain", which Poland was separated for many years from the modern way of conducting military operations and access to high-tech military technologies. Despite the existing difficulties, accession procedures gradually were implemented. Worth mentioning is the fact that all the "NATO-matching" efforts were provided along with diplomatic persuasions aimed at obtaining the consent of the Alliance for Poland to finally join NATO (Kaczmarek, and Skrzyp, 2003).

On 16 February 1995, the House of Representatives of the US Congress adopted a resolution on the "Revival of National Security" providing the enlargement of NATO including Poland, the Czech Republic, Slovakia and Hungary (Congress, 1995).

After the Alliance proposed to Poland an engagement into individual dialogue, on 4 April 1996 the Polish government submitted to NATO the "Individual Discussion Document" presenting Poland's positions for the enlargement of the Alliance, a vision of the European security architecture and the prospective role of NATO in the future.

The first meeting of the individual Poland-NATO dialogue was held in Brussels on 7 May 1996. In addition to individual meetings, there were two joint sessions of a dialogue between NATO and countries participating in the "Partnership for Peace" program. In his speech on 22 October 1996 in Detroit, President Bill Clinton for the first time specified the date of NATO enlargement. He announced that the first new members from Central and Eastern Europe should be admitted to the Alliance in 1999 (www.bbn.gov.pl-kalendarium).

5. Access dialogue with success

In 1997, four sessions of accession dialogue were held. The first one was carried out on 16 September 1997 and the second on 29 September being mainly dedicated to defense aspects. The third session of the dialogue was held on 9 October and was entirely devoted to financial matters, particularly to Poland's participation in the financing of Allied activities. On 23 October 1997, the last fourth meeting of accession talks was held at NATO Headquarters in Brussels.

On 10 November 1997, Polish Minister of Foreign Affairs Bronisław Geremek sent a letter to the Secretary General of NATO in which Poland officially accepted the amount of contributions to the civil and military budget of the Alliance and the "NATO Security Investment Program" (act.nato.int-NSIP in nutshell). Four days later, Bronisław Geremek officially presented a letter to the Secretary General of NATO, confirming Poland's readiness to accept the obligations related to NATO membership and expressing the Poland's will to join the North Atlantic Treaty.

On 25 November 1997, Polish Prime Minister Jerzy Buzek paid an official visit to Brussels and held a meeting with the Secretary General of NATO Javier Solana and the Secretary General of the Western European Union Jose Cutileiro. On 16 December 1997 in Brussels, NATO foreign ministers signed the "Accession Protocols"

for Poland, the Czech Republic and Hungary. Finally, the transfer of ratification instruments to the US government - the depositary of the Washington Treaty, was considered as the completion of the ratification procedure. The Secretary General of NATO, Javier Solana issued formal invitations to Poland, the Czech Republic and Hungary for accession to the North Atlantic Treaty. On 17th February 1999 the Polish Parliament adopted the act on the ratification of the North Atlantic Treaty, and the day after, the President of Poland Aleksander Kwaśniewski signed the act (www.bbn.gov.pl-kalendarium, www.sejm.gov.pl).[2]

On 12 March 1999, in the city of Independence, in the Missouri state,, the Polish Minister of foreign affairs Bronisław Geremek handed over to the US Secretary of State, Madeleine Albright, the act of Poland's accession to the North Atlantic Treaty.

From that moment, Poland formally became a party to the Treaty - a member of the North Atlantic Alliance. The same day, at Piłsudski Square in Warsaw, the President of Poland Aleksander Kwaśniewski and other leading representatives of the state authorities participated in the ceremony of raising the NATO flag (Pawlikowska, 2006).

6. Conclusions

The described analysis carried out in the field of the Polish-American relations in light of the involvement leading up to Poland's achievement of the status of a State Party in the NATO Alliance, proved rationality and effectiveness. For this reason, the pre-accession path may be of interest to representatives of various disciplines: political science, security, law and history. Particularly in the area of security science, it is possible to reflect on the process of political transformation that was supposed to lead to strengthening the position of Poland on the international arena and by this means, to guarantee the security of its borders. In the scope of the conducted research, it can be concluded that the government and politicians perceived the necessity to improve the security of Poland through the accession process that at the final stage would enable Poland to join NATO. Furthermore, as a strategic partner for national security, it was decided to rely on the power of the United States of America. Undoubtedly, the United States had the worldwide potential that gave the legitimacy to support and defend countries that were seeking security as well as political and social stability in the new European order.

Nevertheless, the matter of NATO enlargement by new member states, including the accession of Poland, occurred to be more complicated than expected. For the political reasons, it is highly important to underline the fact that there was a bipolar attitude among US politicians in the field of Poland's accession. For many key players on the American scene, opening the possibility for former satellite states to become a NATO member state would increase the tense American relations with Russia. Due to that factor, some political environments in the US strived to undermine the accession process with the prime aim to sustain dialogue with Russia. What is more, it is important to highlight that the accession process, apart from its political dimension, mostly required overcoming difficulties resulting from the lack of compatibility between the Polish armed forces and NATO forces in a very vast military context. The Soviet curtain caused the backstop of Poland in the international military area; thus, it was a great challenge to acquire operational capability and inter-state interoperability. Nonetheless, despite all the difficulties, the efforts regarding the accession were finally crowned with success. From the perspective

2 The Act of 17 February 1999 r. on the ratification of the North Atlantic Treaty, issued in Washington on 4 April 1949 r. (Journal of Laws 1999 no. 13, item 111).

of the past, the aspiration of Poland to NATO should be considered as justified. Looking back over the pages of history and analyzing the geopolitical situation in Europe nowadays, one would state that Polish relations with Russia have not changed a lot for decades. The political and military activities of Russia, especially taking into consideration the conflict on the Ukraine, proves that Russian political-military course still poses a threat to the countries of the region. From the Russian perspective, the vision of the Central Europe seems to stay unchanged with the supremacy of "Russian Bear" over the former satellite states and without the US engagement manifested in this part of the world. That supposedly would be the hierarchy and the order acceptable for the Russian head of state.

Fortunately, the accession process was successfully finished and Poland acquired one of the most important elements in the security puzzle, the strong Alliance. For the time being, the Polish armed forces are not fully prepared to face external military threats on their own, which is why NATO is perceived as the "security umbrella" expanded over Poland. The close cooperation with the US Army, joint exercises, American soldiers' presence on the Polish land, is an important deterrence factor in the international politics. However, the process of army transformation is still ongoing and although the pace of changes is visible, there is still a lot of space for improvement to achieve full interoperability with the armies of other NATO members.

References:

1. *Act of 17 February 1999 r. on the ratification of the North Atlantic Treaty*, issued in Washington on 4 April 1949 r. (Journal of Laws 1999 no. 13, item 111).
2. Apanowicz, J. (2002). *Metodologia Ogólna*. Gdynia: Bernardinum.
3. *Asmus, R. (2008). Europe's eastern promise: Rethinking NATO and EU enlargement. Washington: Council on Foreign Relations.*
4. *Asmus, R. (2008). NATO Enlargement and Effectiveness, Testimony Before the Senate Foreign Relations Committee. Available online https://www.foreign.senate.gov/publications/download/testimony-of-ronald-d-asmus-re-nato-enlargement-and-effectiveness, 13.05.2020.*
5. Asmus, R. (2002). *NATO – otwarcie drzwi*, Warszawa: MUZA SA.
6. Congress. (1995). *National Security Revitalization Act*. Retrieved from https://www.congress.gov/congressional-report/104th-congress/house-report/18/2 (1995-1996), 16.05.2020.
7. Encyclopedia Britannica. *20th-century international relations, The Role of NATO*, Available online https://www.britannica.com/topic/20th-century-international-relations-2085155/The-role-of-NATO, 13.05.2020.
8. Hansen, H. (1995). *Training and Exercises for Partnership for Peace*. Part One, XIIth NATO Workshop On Political-Military Decision Making, Dresden, Germany. Available online https://www.csdr.org/95Book/95Workshop.htm, 7.05.2020.
9. Kaczmarek, J., Skrzyp, J. (2003). *NATO*. Wrocław: atla 2.
10. Kupiecki, R. (2019). *NATO w polskiej perspektywie 1989-2019*. Warszawa: Polski Instytut Spraw Międzynarodowych.
11. Kupiecki, R. (2019). *Okiem Stratega i dyplomaty: Stosunki polsko-amerykańskie po 1918 r*. Warszawa: Wydawnictwo Naukowe Scholar.
12. Kupiecki, R. (2016). *Organizacja Traktatu Północnoatlantyckiego*. Warszawa: Ministerstwo Spraw Zagranicznych.

13. Ministerstwo Obrony Narodowej (MON), (2019). *Trochę historii*. Retrieved from https://archiwum2019.mon.gov.pl/polska-w-nato/droga-do-nato/troche-historii-02017-06-28/, 02.05.2020.
14. Mozol, (2016). *28th June 1991. Disintegration of the MEAC and dissolution of the Warsaw Pact*. Retrieved from http://mozol.pl/28-czerwca-1991-rozpad-rwpg-i-rozwiazanie-ukladu-warszawskiego, 22.05.2020.
15. NATO, (1997). *Madrid Declaration on Euro-Atlantic Security and Cooperation*. 8.07.1997. Available online https://www.nato.int/cps/en/natohq/official_texts_25460.htm?mode=pressrelease, 3.04.2020.
16. NATO, (2020). *NSIP in Nutshell*. Retrieved from https://act.nato.int/images/stories/structure/nsip/nsip_nutshell_1.pdf, 24.05.2020.
17. NATO. (1994). *Partnership for Peace: Framework Document*. Retrieved from https://www.nato.int/cps/en/natolive/official_texts_24469.htm, 25.04.2020.
18. NATO. (1949). *The North Atlantic Treaty*. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=p, 25.04.2020.
19. Okoński, Z. (1995). *Partnership for Peace: An Essential Element of the European Security System*. Part Four, XIIth NATO Workshop On Political-Military Decision Making, Dresden, Germany. Available online https://www.csdr.org/95Book/95Workshop.htm, 7.05.2020.
20. Pacuła, P. (2007) US w organizacjach międzynarodowych. *Kwartalnik Bezpieczeństwo Narodowe. 5(6)*. pp. 239-242.
21. Pawlikowska, I. (2006). *Koncepcje bezpieczeństwa państw Europy Środkowej po 1989 roku*. Toruń: Mado.
22. Sejm RP, (2019). *20th Anniversary of Poland's NATO membership. The role of the Sejm in the accession process*. Retrieved from http://www.sejm.gov.pl/Sejm8.nsf/komunikat.xsp?documentId=088D84288D0A16D1C12583BA00326C4D, 20.04.2020.

SAFETY&DEFENSE
ISSN 2450-551X

Asian Cyber Security Standards

Mateusz J. KUCZABSKI

War Studies University, Warsaw, Poland;
m.kuczabski@akademia.mil.pl, ORCID: 0000-0001-9952-1188

DOI: https://doi.org/10.37105/sd.75

Abstract

The scientific considerations outlined in this article address the threat to the cyber security quality system arising from unclear security standards implemented by China. Over the past few years, the Chinese government has imposed almost 300 new national cyber security standards. These norms cover a variety of information and communication technology (ICT) services as well as products, including soft-ware, routers, switches and firewalls. This standardization increases the threat to the cybersecurity quality system, and the more the US places pressure on the west-ern world for Chinese companies investing outside China and on western firms trading in China, the more difficult the situation becomes. The aim of this assessment is to identify these threats, which are also difficulties encountered by West-ern companies trying to develop their operations in China in order to minimize them. The study was compiled as an analysis of Chinese cybersecurity standardization policy documents and their confrontation with the practice of foreign businesses and as an analysis of international reports and standardization documents on cybersecurity. The theoretical investigative methods used in this paper are: syn-thesis, analysis, abstraction and generalization.

Keywords: cybersecurity, safety standards, cyberspace, commercial defense, IT infrastructure.

1. Introduction

Seconded European Standardization Expert in China (SESEC) is a project co-funded by the European Commission (EC), the Secretariat of the European Free Trade Association (EFTA) and the three European Standardization Organizations (CEN, CENELEC and ETSI). Since 2006, three SESEC projects have been implemented in

China, SESEC I (2006-2009), SESEC II (2009-2012) and SESEC III (2014-2017). In April 2018, SESEC IV was officially launched in Beijing for 36 months. The SESEC project supports the strategic objectives of the European Union, EFTA and European Standardization Organizations (ESOs). The SESEC project aims to:

- Promoting European and international standards in China;
- Improve contacts with different levels of Chinese administration, industry and standards bodies;
- Improve the visibility and understanding of the European Standardization System (ESS) in China;
- Collecting intelligence, regulatory and standardization information (Xu, 2018).

Despite the many efforts to bring the requirements in the area of standardization closer between foreign countries and China, Chinese cyber security standards create a set of diverse challenges for companies outside China in the area of security. The Chinese government may use the standards to put pressure on companies to undergo "invasive" product reviews, where sensitive intellectual property (IP) and source code (even if there is no clear indication of disclosure) may be required for verification and testing. In order to meet certain standards, foreign companies may be required to redesign products for the Chinese market if they do not comply with their domestic (Chinese) standards. In March 2018, The Office of the U.S. Trade Representative (USTR) issued a report on the discrimination and intellectual property (IP) challenges faced by U.S. companies operating in China, for which the Chinese market is particularly difficult. The difficulties are aggravated by the tightened US trade policy towards China. Retaliation with the use of standards, or rather the ambiguity of regulations, encourages discrimination against American and other foreign (western) entities. Chinese domestic standards build a competitive advantage for Chinese operators for two reasons:

- First, Chinese companies do not need to fear, unlike foreign companies, the obligation to provide sensitive information to the government as a condition for meeting standards.
- Second, Chinese companies may consider Chinese companies more secure on the basis of unclear criteria in the standards only because they are local and perceived to be more "controllable" and not influenced by foreign governments (something that China suspects foreign technology, whether true or not).

Although officially most standards are considered "recommended" (optional standards), in practice, for many entities may mean that they are required to meet them as necessary for doing business in China. This is the case when standards are listed as requirements for public or government procurement. In addition to government customers, some Chinese customers are not allowed to buy from suppliers who are not certified in accordance with certain standards.[1]

The standards are also becoming mandatory (obligatory) in combination with additional provisions that relate to these standards.[2] The government can audit companies for standards, even if the standards are not officially required. This, from a sales perspective, can generate significant costs for companies.

[1] This can be troublesome, because often the requirements vary greatly from company to company or product to product. There were cases in which contracts with customers were not concluded because, for example, the product did not have a specific certificate, and such a certificate was required.

[2] This practice is also valid in other countries. If appointments are made, e.g. in official documents, the standardization requirements become obligatory.

The ICT Market in China report reports that in 2014, the Ministry of Industry and Information Technology (MIIT) and Shanghai's municipal government jointly released a policy that opens opportunities in telecommunications for foreign companies in China in the (Shanghai) Pilot Free Trade Zone. The government's explanation of this new policy stated that foreign companies shareholding of information service business (app stores and data storing and forwarding) is no longer limited. The shareholding of online data processing and e-commerce was increased up to 55%. Furthermore, businesses in call centers, multi-party communication, internet access services, and virtual private networks (VPNs) were opened to foreign companies without shareholding restrictions. Other ICT sector regulations depend on the industry itself; for instance, in the software and hardware sectors, regulations are based on content and usage. For example, on 1 May 2015, the Local Administration for Industry & Commerce (AIC) and the Municipal Commission of Transport launched an investigation of Uber's Guangzhou office (and later its Chengdu office), as the Guangzhou province considers car-hire services that use private drivers illegal. They are therefore investigating Uber for allegedly operating a taxi service without the appropriate license (Yi Fan et al., 2017).

The Chinese use very vague, ambiguous language in the standards. This practice is assessed by experts as a way of reducing problems arising from relations with the World Trade Organization (WTO). At the same time, the ambiguities in the standards allow the Chinese government maximum flexibility and freedom to apply burdensome regulations to foreign entities, in particular when it considers it appropriate. Beijing may also rely on the fact that most standards are directive-based to avoid discretion. More than 1,000 Chinese standards (not only cyber security standards) previously submitted to the WTO were lowered from requirements for national standards to recommendations (in 2017 alone).

As the bilateral tensions between the US and China intensify, the standards associated with the new system of cyber security reviews are likely to be one of the first tools China can use to retaliate against US companies in a trade war. They offer the Chinese government the opportunity to delay the certification or issuance of licenses needed to gain market access, which may result in the closure of companies that may already have been "successful" in China. As a result, Beijing could use the standards to shift the basic requirements for foreign companies operating in China in a way that would have a long-term effect on short-term tensions in bilateral or multilateral relations.

2. Creating Cybersecurity Standards in China

In August 2016, a law on cybersecurity was published. A year before its entry into force, a group of three government agencies involved in the work on cybersecurity the standards issued an opinion which stressed the key role that standards should play in making President Xi Jinping's vision of building Chinese power in cyberspace a reality. The statement also describes how standards will support the implementation of the Cybersecurity Act (08.2016). In parallel, work continued and in November 2017, the National People's Congress issued a standardization law, which was last updated in 1988.[3] The new law codifies the recommendations of Chinese leaders to modernize China's standards system to keep pace with industrial and technological developments (USITC, 2010).

Chinese national standards are understood as policy instruments, and as a form of regulation that sets out requirements that

[3] Amendment of the law last updated in 1988.

can be used to control companies or used as a basis for testing and certification[4] (Ding, and Triolo, and Sacks, 2018). The Chinese government underlines its willingness to play a greater role in standard-setting in particular in areas such as 5G, which are international protocols or guidelines on design and interoperability. Some of these standards are required as a precondition for market access or sales - as indicated in public procurement lists. These standards have the letters "GB" at the front, which means "national standard" or "guobiao" (国 标). Others are recommended, but not formally binding, with the term "GB/T", which are "recommended" standards or guobiao/tuijian (国 标 / 推荐).

Even if standards are not officially required, companies may still be controlled by regulators and may require compliance with these standards in practice when:

- they are listed as public or government procurement requirements and
- when customers do not buy (do not conclude contracts) without a specific certificate.

The second requirement varies considerably depending on the sector or business segment. There are cases where contracts with customers are not finalized, because the product lacks a specific certificate. It is emphasized that failure to comply even with the recommended standards can result in high sales costs in China. Standards are also becoming required in conjunction with regulations that relate to these standards. The government can audit companies for standards, even if the standards are not officially required. As a result, compliance with the standards may be necessary to do business in China, even if the standards are only "recommended".

In China, all required standards must go through a process that will be officially approved. This is not an easy process in the Chinese political and legal bureaucracy. Moreover, Beijing must disclose the required national standards to the World Trade Organization (WTO) internationally. In fact, in 2017 the government downgraded more than 1,000 Chinese standards, not only from the set of cyber security standards Technical Committees ISO/TC260 (TC260) previously submitted to the WTO, from the required national standards to recommendations. As many as 396 mandatory national standards have been abolished and 1077 mandatory national standards have been converted into recommended national standards (Sacks, and Li, 2018).

The TC260 is not entitled to issue the required standards. There is, however, "circumvention" - the TC260 standards become de facto required when they are combined with specific legislation. In this way, they do not have to go through long agreements between the agencies. As a result, companies often have to apply even recommended standards to succeed on the Chinese market. In this way, they do not have to go through long agreements between the agencies. As a result, companies often have to apply even recommended standards to succeed in the Chinese market. Failure to do so can create enormous regulatory and political risks. This risk may increase if Beijing searches for ways to punish U.S. companies for the growing trade tensions in 2019 and 2020 (and perhaps even further into the future, with the unknown long-term effects of protectionism).

[4] Internationally, the Chinese government also stressed the importance of playing a greater role in standard setting (for example in areas such as 5G), which are international protocols or guidelines on design and interoperability. See: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table /online access [21.06.2020].

3. Foreign companies and the formation of Chinese cyber security standards

In 2016, China saw an important breakthrough in the field of standardization for foreign companies. To help develop China's cyber security standards, TC260 invited foreign participants to join the committee. This step was important in the end as foreign companies now take part in some discussions and are at least partly up to date. However, in general, their influence remains limited, it is local companies and the TC260 Secretariat who lead the core work[5] (Dou, and King, 2016). There are currently 16 foreign companies in these working groups that are members of the TC260. The structure of the foreign companies is shown in Figure 1.

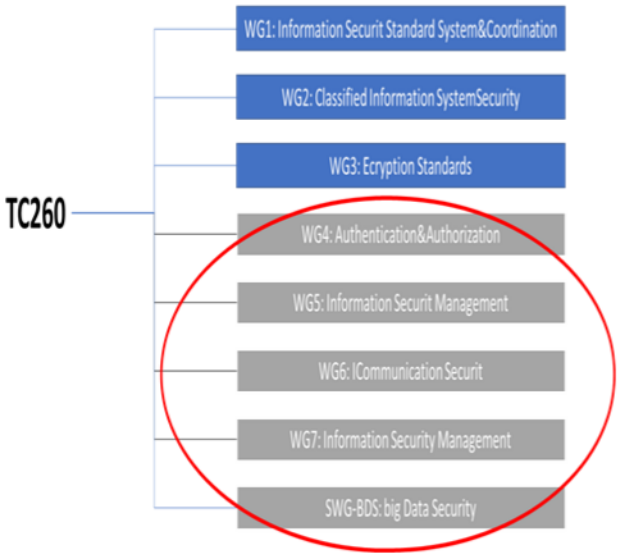


Figure 1. Structure of foreign companies in ISO/TC260. Own work.

According to participants, the Technical Committees ISO/ TC260 only accepts comments from foreign members that do not constitute real obstacles to the TC260. When comments from foreign members cause a conflict with the TC260's plans or interests of domestic companies, TC260 has applied a strategy of transferring the problem to one of the working groups closed to foreign participation. This approach was evident in the misunderstanding that emerged around the international standard interoperability initiative, the Trusted Platform Module (TPM). Chinese proprietary versions of the TPM standard required certain cryptographic algorithms for security tasks, such as verification, to be based on Chinese technology (USITC, 2010). When the WG7 voting which includes foreign members - stopped the initiative, TC260 addressed this problem in WG3 (encryption standards), which does not accept foreign members. The TC260 is likely to become even less sensitive to contributions from foreign members given the negative dynamics of cooperation between the US and China. Participation in the TC260 may help foreign companies gain political support from the government, but their presence may become increasingly symbolic.

4. Multi-level security program (MLPS)

The Ministry of Public Security has published a draft of a new version of the Multi-Level Protection Scheme (MLPS)[6] (called

[5] Microsoft has also been invited to join this committee to take an active part in developing the rules. The TC260 originally had 48 members and was expanded in January to 81 members, mainly Chinese officials and representatives of Chinese technology companies. The committee's seven working groups focus on encryption, large data and other cybersecurity issues. Earlier this month, 46 trade associations sent a joint letter to Chinese Prime Minister Li Keqiang, saying that the draft Cyber Security Bill, which will increase government monitoring and the data on fines will be stored locally, will "weaken security and separate China from the global digital economy" https://mspoweruser.com/china-invites-microsoft-to-join-technical-committee-260-tc260-to-draft-cybersecurity-rules/ online access [21.06.2020].

[6] The draft Regulation updating the original 2007 program is based on the new principles set out in the Cyber Security Act.

MLPS 2.0)[7]. According to the original MLPS plan, it ranks among the 1-5 ICT networks and systems that make up the Chinese Critical Information Infrastructures (CII) based on national security, and level 5 is considered to be the most sensitive. Level 3 or higher triggered a set of regulatory requirements for ICT products and services sold to this CII, including local IP products in China, shipping to government testing laboratories for certification and compliance with encryption rules prohibiting foreign encryption technology. A higher MLPS ranking meant that companies would be subject to enhanced monitoring by MLPS systems.

These factors have created barriers to market access as well as security risks for foreign companies. One of the most confusing but important issues in the new regulatory regime for cyber security is what exactly CII means. Under the Cyber Security Act, entities considered as CII have to face a package of new requirements. However, the government has not yet issued an official definition of CII or explained how these rules work with the existing MLPS. Currently, it seems that there are two parallel regulatory regimes for CII: one under the original MLPS and the other under the new regime set out in the Cyber Security Act. The government has not clarified the relationship between the two regulations; moreover, two government agencies, the Ministry of Public Security and Civil Aviation Administration of China (MPS and CAAC) have so-called overlapping jurisdiction over CII. MLPS 2.0 is likely to create greater regulatory control over foreign technology, although MLPS 2.0 seems to relax the original regime as it simplifies Chinese local IP requirements at level 3 and above. However, in parallel, MLPS 2.0 may increase control in other areas. For example, the document would potentially cover ICT products that were previously outside the scope of the MLPS, extending the program to cover all network operators, and not just those from CII or government agencies. According to MLPS 1.0, industries such as manufacturing or retail would not fall under the scope of the MLPS because they are not defined as CII. However, according to the draft MLPS 2.0 will cover any industry with an ICT infrastructure, through an unclear category called "network operators", which may include anyone using an ICT system. This seems to indicate that MLPS 2.0 also focuses on cloud computing, mobile internet and big data (Sacks, and Li, 2018).

Another challenge is that MLPS 2.0 may lower the threshold for the Grade 3 status, meaning that more companies (both Chinese and foreign) will be subject to enhanced monitoring by MPS, third-party certification and national encryption requirements.[8] In general, MLPS 2.0 is moving towards more government controls and audits instead of self-reporting by companies (Xiaomeng et.al., 2018). Standards play a key role in supporting the MLPS as they are used as a reference. They are used for testing, evaluation and classification against technical requirements at each level. Table 1 below illustrates the general structure of standards forming the existing MLPS (Sacks, and Li, 2018). The MLPS core standard ("Information Security Technology - The Basis for Cyber Security - Protection Classification: Part 1: General Security Requirements - The Basis for Other Standards") requires the provision of source code when a company at level 3 or above commissions the execution or development of software. MLPS standards related to access control may also favor local Chinese companies that have robust censorship (control) systems. One standard calls for censor-

[7] See: Seconded European Standardization Expert in China, https://www.sesec.eu/tag/cyber-security-digital-identity/, Ministry of Public Security Material on "Regulation of network security level protection (draft for comment)", Public Notice of Comments, http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html, [3.05.209].

[8] Expert analysis suggests that Chinese companies are likely to have fewer problems with these requirements in return: How Chinese Cybersecurity Standards Impact Doing Business in China.

ship and filtering of content at critical network nodes to control access. In this way, censorship of digital content could constitute a barrier to market access.

In a trade war scenario, the MLPS standards also provide Beijing with sufficient tools to take punitive measures against foreign companies on the basis of unclear approval rules. Network and system security management requires the authorization and approval of all connections to external networks, with regular inspections for violations. Other types of approvals that are not clear enough are needed in areas such as "design of security plan", which requires the approval of security plans and supporting documents.

Table 1.
General structure of standards forming the MLPS

Status of level	Requirements areas	Parts of Individual Standards
1	Standards on general requirements of multi-level protection scheme	INFORMATION SECURITY TECHNOLOGY **Baseline for Cybersecurity Classified Protection** Part 1: Security General Requirements Part 2: Security Special Requirements for Could Computing Part 3: Special Security Requirements for the Mobile Interconnection **General Requirements for Classified Protection of Cybersecurity Information Security Technology** Part 5: Special Security Requirements for Industrial Control System
2	Standards on design requirements of multilevel protection scheme	INFORMATION SECURITY TECHNOLOGY **Technical Requirements of security Design for Cybersecurity Classified Protection** Part 1: General Security Design Requirements
		Technical Requirements of Security Design for Network Security Classified Protection Part 2: Cloud Computing Security Requirements **Technical Requirements of Security Design for Network Security Classified Protection** Part 3: Security Requirements for the Mobile Internet Things Part 4: Security Requirements for Internet Things Part 5: Security Requirements of Industrial Control
3	Standards on testing and evaluation of multilevel protection scheme	**INFORMATION SECURITY TECHNOLOGY Evaluation Requirements for Cybersecurity Classified Protection** Part 1: Security General Requirements **Testing and Evaluation Requirements for Protection Network Security** Part 2: Testing and Evaluation Requirements Cloud Computing Security **Evaluation Requirements for Security Classified Protection** Part 3: Special Security Requirements for the Mobile Internet of Things Part 4: Special Security Requirements for Internet Things information Part 5: Industrial Control System Security Extension Requirements

Source: based on Introduction of the Framework of the Series of Standards on Cybersecurity Multi-Level Protection Scheme by Ma Li from MPS MLPS Evaluation Center. http://www.djbh.net/webdev/web/AcademicianColumnAction.do?p=getYszl&id=8a8182565deefd0d015e799ea2040094, in Sacks, and Li, 2018.

Foreign companies are not clear about the new rules, yet they are already under pressure from the Chinese government to meet increasingly onerous requirements.

Since the entry into force of the Cyber Security Act, much of the enforcement action against companies has focused on MLPS violations. This trend underlines the growing risk for companies related to the MLPS, officials are focusing in particular on this program to show progress in the implementation of the Cyber Security Act.

5. Cyber Protection of Critical Information Infrastructure (CII)

Under the Cyber Security Act, there is an intense debate on the relationship between the Multi-Level Protection Scheme (MLPS) and the new Critical Information Infrastructure (CII). The problem is unresolved as it is unknown which sectors are subject to CII. A characteristic feature of the Cyber Act is the burdensome requirements imposed on entities that are deemed to belong to critical infrastructure. Under the law, CII operators must only use network products and services that have undergone a vaguely defined review of the national security process (also known as a "black box" review). This includes the storage of certain data, regular security assessments and procedures, such as on-site testing.

In the draft regulation in May 2017, the scope for CII was presented. Under the Cyber Security Act, covering sectors such as energy, finance, transport and others, meeting the general criteria set out in Article 18, according to which: "The network infrastructure and information systems operated or managed by entities which, if destroyed, rendered inoperative or caused a data leak, could seriously harm national security, the national economy, the livelihoods of the population and the public interest shall be included in the scope of CII protection" (CII Security Protection Regulations, 2017). The development of Critical Information Infrastructure Protection Regulation standards is extremely slow.

The draft CII Protection Regulation suggests that standards will play an important role in clarifying unclear concepts, in particular as regards critical infrastructure itself. For example, the baseline standard issued on 11 June 2018 has little help in narrowing the definition of CII, using the expression "including but not limited to". Another standard contains a section that deals with the obligation to comply (base standard) with the MLPS for CII operators. It is concluded that some actors in CII areas, such as network infrastructure, big data, clouds and IoT, should take security measures according to the MLPS class. In pursuing the implementation of the MLPS 2.0 regime, it is noted that a competitive parallel CII protection regime is being developed. The draft CII Regulation refers to the regulatory authorities responsible for the different sectors, which should identify CII within their sector at all times.[9] As a result, foreign companies may be subject to uneven enforcement, as government stakeholders have wide discretionary powers to ring-fence competing regulatory systems and ensure priority.

6. Personal data and protection of sensitive data

The Cyber Security Act and its accompanying standard, known as the Personal Data Security Specification, set out the general principles for user consent and what companies should do to collect, store, process and transmit personal data. Beijing views the protection of personal data against fraud or

[9] "National sectoral controlling or supervision departments will, according to the CII identification guidelines, organize the identification of CII within those sectors and those areas, and report the identification results according to procedure," https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/ [21.06.2020].

misappropriation by companies or criminals as an essential element of cyber security.

However, this approach may imply a completely different understanding of data privacy from the Western concept and may be guided by different considerations (Xiaomeng, Manyi, Sacks, 2018). MLPS 2.0 even emphasizes the importance of protecting personal data through seven separate articles. Network operators who illegally allow a leak or sell or make it available without authorization will be punished. In practice, enforcement may be uneven and politically discredited because of unclear, undefined regulatory zones. The government has no other criteria for assessing how companies are to process personal data in addition to the specifications and unclear rules in the Cyber Security Act. In the future, the legislator may develop a separate national privacy law, but during this period the specification offers only general principles on this issue, which in effect means that it can be interpreted as required if officials want to enforce it.

The conflict between the specification and the Cyber Security Act also creates opportunities for law enforcement by ad hoc authorities. Regulators may penalize the company for collecting personal data without explicit consent (required under the Cyber Security Act), despite specifications allowing for implicit consent in some cases. That fact prevents transforming businesses and other forms of transactions from a centralized, human-based to a shared, algorithm-based trust model, which enables a new risk management paradigm (Drljevic et al., 2020).

7. Encryption

In accordance with generally applicable rules, the foremost short-term *technical* option recommended for ensuring data security and privacy is encryption (Schuster et al., 2017). In 2016, Beijing launched the world's first quantum satellite, “Micius”, which teleported pairs of entangled photons to Earth in 2017. This achievement will probably allow China to create the world's first quantum satellite network. In 2017, China also established the first long-distance quantum ground connection between Beijing and Shanghai, approximately 2000 kilometers long. In the future, it will probably be connected to the quantum satellite network.

These scientific achievements are groundbreaking initiatives that can protect Chinese government communications from foreign observations, at least until post-quantum cryptanalysis becomes a functional reality. For the development of quantum technologies, American companies from the private sector are important, including Google, IBM, Intel and Microsoft, which have been conducting quantum research for almost ten years (Kuczabski, 2019). In this context, it is not surprising that vague areas in the Chinese encryption regulatory system give authorities wide discretion to enforce requirements.

Moreover, the rules on what exactly foreign companies have to do to incorporate encryption into their products, as well as the use of encryption in their own communications, are currently undergoing major changes. The encryption bill has been under review for a long time. When enacted and enforced, the law may be interpreted as requiring the use of only pre-approved national encryption products (Luo, 2017). The grey market has been a concern for foreign industry for years, and the Chinese government considers that enforcement would be too costly for foreign companies, which have to stay in the market. The only exception in the current Regulation allows companies to apply for approval to use commercial encryption products produced abroad.

The draft law also includes unclear requirements for decryption in terms of national security (a provision also found in the Chinese Counter-Terrorism Act), on-site inspections to access data and seize equipment and an overview of national security for certain types of encryption products and services (Sacks, and Li, 2018). A statutory regulation would significantly strengthen the ex-

ecutive powers of the Chinese state cryptographic administration through enhanced government oversight and access to China's first uniform encryption system (Luo, 2017). As the rules for this new system are still being developed, they can easily become another retaliatory tool of the so-called 'backdoor' against foreign contraband. There are still serious gaps between the existing rules and the standards that create the aforementioned 'grey areas' that the authorities may interpret freely. For example, there are no standards that set out the details of the implementation of anti-terrorism legislation obliging companies to provide "technical assistance" to the government (which may mean decryption) to support national security investigations. There are also no standards related to encryption in the CII sectors - perhaps because the very meaning of CII is changing - even though it is a central point in the Cyber Security Act. Ambiguous rules in this area give authorities enough room for ad hoc enforcement of requirements and the possibility of wide discretion. Although many Chinese encryption standards adopt international standards, these include modifications to the use of algorithms approved by the Chinese encryption management departments. Examples include standards related to data integrity, digital signature and identity authentication. It is also important that government authorities have a wide discretion as to what they require companies to do in the process of performing an inspection related to encryption requirements.

With regard to the security standard, the test requirements for cryptographic modules state that "the burden of proof shall lie with the controlled company. If there is any uncertainty or ambiguity, inspectors should ask the inspected company to provide additional information" (ISO/IEC 24759 : 2017). Thus, encryption standards related to CII in particular will be an important area for observation in the coming years, especially as the Chinese administration is trying to define exactly what falls under this often-contested category.

8. Conclusion

Cyber security standards will be a key element in technical and commercial relations between China and abroad, especially in the US, as most US ICT companies are trying to enter the Chinese market or are already there. As the US takes an increasingly confrontational stance towards Beijing, the US must recognize the consequences of this as a cost to US companies, which concerns not only the form of reciprocal tariffs but also the perception and impediments to trade.

Currently, there are still many uncertainties. It is unclear what exactly the government is trying to protect under the hundreds of newly created standards. It is not clear how companies will be controlled. A positive development would be to make the processes to which foreign companies should adhere more transparent in order to avoid arbitrary audits. Undoubtedly, however, cyber security standards in China are an important and growing factor shaping the operating environment for foreign companies. This is important for any company that relies on an ICT infrastructure, including sectors dominated by public, government or private commercial entities. The standards provide authorities with "unclear" regulatory tools that can pose security risks, increase costs and underline the importance of total control.

These challenges will intensify as the trade war between the United States and China escalates, albeit in a difficult to quantify manner. The standards support new types of cyber-security reviews. Foreign companies need to have a clear picture of the layered and sometimes ambiguous regulatory nature to be able to use it to communicate their negotiating positions with Chinese partners and the government. Understanding the practical effects of standards, especially the avalanche of new cyber security standards can change the unfavorable status quo and can help prepare strategies for foreign companies. Unclear, and imprecise language in the standards and laws is often used to refer to different interests in the Chinese

system. Foreign companies and governments should recognize where debates take place and try to cooperate with interest groups similar to their own. Especially when the relationship between regulatory control and business interests in China is discussed, especially as many private Chinese companies expect to expand into global markets. The fact that Chinese global companies also benefit from Beijing's acceptance of more international standards is not insignificant.

In March 2019, annual meetings of the National Chinese People's Congress were held, which in the Chinese political system corresponds to parliament. These events are known in China as lianghui(会), i.e. "two meetings" because the People's Political Consultative Conference of China, which functions as an advisory body, also takes place simultaneously. The report that followed the deliberations contained references to the tense situation of the "trade war" with the USA and a call for internal consolidation and solidarity towards global challenges.

The set course of action is to counteract the deepening economic and social problems and to mitigate international tensions. In the Prime Minister of China's annual report, there is no reference to the strategy "Made in China 2025" although new regulations and laws serve to implement this strategy. The most important event of last year's National Chinese People's Congress, from the point of view of its international implications, was the announcement of a new law regulating foreign investments in China (Chinese Prime Minister Report, Xinhuanet, 2019). Although the new law appeared, its general nature may allow the government to continue its interference and unequal treatment of foreign entities in the Chinese market.

All political declarations and actions also affect standardization regulations. At the time of the detailed analysis from October 2018 to June 2019, the regulatory documents were not yet published, and the beginning of 2020s did not bring any changes in this respect.

References

1. *Critical Information Infrastructure Security Protection Regulations, July 2017.* http://www.cac.gov.cn/2017-07/11/m_1121294220.htm, *transl. by Graham Webster, Paul Triolo and Rogier Creemers* http://www.chinacopyrightandmedia. wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/, 21.06.2020.
2. Ding, J., and Triolo, P., and Sacks, S. (2018), *Chinese Interests Take a Big Seat at The AI Governance Table* http://www.newamerica.org/cybersecurity-initiative/ digichina / blog / chinese-interests-take-big-seat-ai-governance-table/, 21.06.2020.
3. Dou, E., and King, R. (2016), *China Sets New Tone in Drafting Cybersecurity Rules Allows Microsoft, Cisco, other foreign tech companies joint influential Technical Committee 260.* https://www.wsj.com/articles/china-moves-to-ease-foreign-concerns-on-cybersecurity-controls-1472132575, 21.06.2020.
4. Drljevic, N., and Aranda, A., and Stantchev V. (2020), Perspectives on risks and standards that affect the requirements engineering of blockchain technology, Computer Standards & Interfaces, Volume 69, pp. 10-17, DOI: 10.1016/j.csi.2019.103409.
5. ISO/IEC 24759:2017 (E), *Security Test Requirements for Cryptographic Modules* http://www.sis.se/api/document/preview/921732/, 21.06.2020.
6. Kezhi, Z. (2019) *Regulation of network security level protection Ministry of Public Security Material Report (Report No. n49)* Beijing: Public Notice of Comments.
7. Keqiang, L. (2019). *Highlights of 2019 Government Work Report* (Report No. 5.03.19). Beijing: China.org.cn.
8. Kuczabski, M. (2019). Środowisko przyszłej wojny stymulowane technologiami – wyzwania i zagrożenia. In R.

Bielawski, and J. Solarz, and D. Miszewski (Eds.), *Współczesne i przyszłe zagrożenia bezpieczeństwa cz. I* (pp. 175-196). Warszawa: Akademia Sztuki Wojennej.
9. Luo, Y. (2017), China Revises Proposals on Regulation of Commercial Encryption. Covington. https: //www.inideprivacy.com/, 21.06.2020.
10. Sacks, S., and Li, M. *How Chinese Cybersecurity Standards Impact Doing Business In China.* Retrieved from http://www.csis.org /analysis/how-chinese-cybersecurity-standards-impact-doing-business-china/, 21.06.2020.
11. Schuster, S., and Berg, M., and Larrucea X., and Slewe, T., and Kostic, P. (2017). Mass surveillance and technological policy options: Improving security of private communications. *Computer Standards & Interfaces, Volume 50,* pp. 76-82, DOI: 10.1016/j.csi.2016.09.011.
12. *USITC Publication 4199 (amended) November 2010.* http://www.usitc.gov /publications/332/pub4199.pdf, 21.06.2020.
13. Xiaomeng, L., and Triolo, P., and Samm, S., and Creemers, R., and Webster, G. *Progress, Pauses, and Power Shifts in China's Cybersecurity Law Regime.* http://www.newamerica.org/cybersecurity-initiative/digichina/blog/progress-pauses-power-shifts-chinas-cybersecurity-law-regime, 21.06.2020.
14. Xiaomeng, L., and Manyi, L., and Sacks S. (2018). *CSIS Report: What the Facebook Scandal Means in a Land without Facebook: A Look at China's Burgeoning Data Protection Regime (Report No. 04.25.2018).* Washington: CSIS.
15. Xu, B. (2018). *SESEC IV China Cybersecurity Standardization* (*Report SESEC IV No. 1.2018).* Beijing: China Cybersecurity News.
16. Yi Fan, Y., and Lu, M. C., and Luo, H. H., and Sung, Ch. (2017), Standardisation and Trade Barriere Issues Regarding the ICT Market in China: A Study of the Wi-Fi Industry, *Journal of Computers, Volume 28,* pp. 35-42 DOI: 10.3966/199115592017062803004.

SAFETY&DEFENSE
ISSN 2450-551X

Cybersecurity – One of the Greatest Challenges for Civil Aviation in the 21st Century

Małgorzata ŻMIGRODZKA

Military University of Aviation, Dęblin, Poland;
m.zmigrodzka@law.mil.pl, ORCID: 0000-0003-3896-0819

DOI: https://doi.org/10.37105/sd.73

Abstract

In every aspect of aviation's operations, from ground handling, aircraft designing and production, ensuring the continuity of flights, technical service, to air carriers, there is a possibility that cybercrime may occur. Ubiquitous computers, telephones, and internet carry the risk of various types of threats – from simple viruses, to personal data theft, to taking over of an aircraft by cybercriminals. The aim of the paper is to describe the main cyberthreats in the area of civil aviation. The theoretical analysis of the available source materials and empirical usage of security procedures in aviation organizations served as the main research methods that have been utilized in the analysis of the cybersecurity problem. The author's extensive professional experience in the aviation sector, especially in the field of quality and security, provided the possibility to verify and understand these vital problems for the aviation industry.

Keywords: cybersecurity, cyberthreat, risk, security, threat.

1. Introduction

Currently, a smartphone, laptop, or computer pose a threat on board an airplane. Cyber and mobile transformation, i.e., that what drives the revolution in aviation, constitutes a significant challenge. Growing automatization brings forth a larger risk of cyberattacks, because the more there are complex systems, the possibility that someone unauthorized, like hackers, can break in those systems is greater. Those systems can be used by criminal groups seeking political and financial benefits. For years, humanity saw the main threat in weapons. It seemed

that the systems and procedures were secured. However, at the beginning of the 21st century, in times of new technologies, we have to change the way of thinking. Most systems in aviation are automatized and based on the Global Navigation Satellite System (GNSS), especially on Global Positioning System (GPS), through which the autopilot of a flying aircraft may be interrupted, and the course or the destination changed (Compa, Rajchel, 2011).

2. Characteristics of cybercrime in the modern world

Technological capabilities of the 21st century galvanized the development of new criminal trends. These new technologies and phenomena should be understood and properly defined. Cyberspace is a complex notion and is usually linked to internal and external computer networks used for data transmission. Cyberspace is related to cybernetics, i.e., science dealing with the processes of control, transmission, and transformation of information. It consists of communication and information systems, links between them, and the relations with the users (BBN, 2015).

The language of the cyber world, which is difficult to understand, poses certain limitations for the average citizen. The data made available by not fully aware users of the information systems can be easily taken over and used for various purposes. Even the process of purchasing a plane ticket on the internet creates the opportunity for crime to be committed. A notion directly linked to cyberspace is cyberterrorism that takes place in it. It is a form of terrorism that came to being and was developed along with the technological development and globalization of information systems.

According to the 2019 KPMG report, 84% of the analyzed organizations see the largest threat in lone hackers (Fig. 1.). A real threat for the safety of aviation organizations is posed also by organized criminal or cyberterrorist groups, and disgruntled or bribed employees. Kids having access to various IT tools are able to break into booking systems, among other things. It is often done just for laughs.

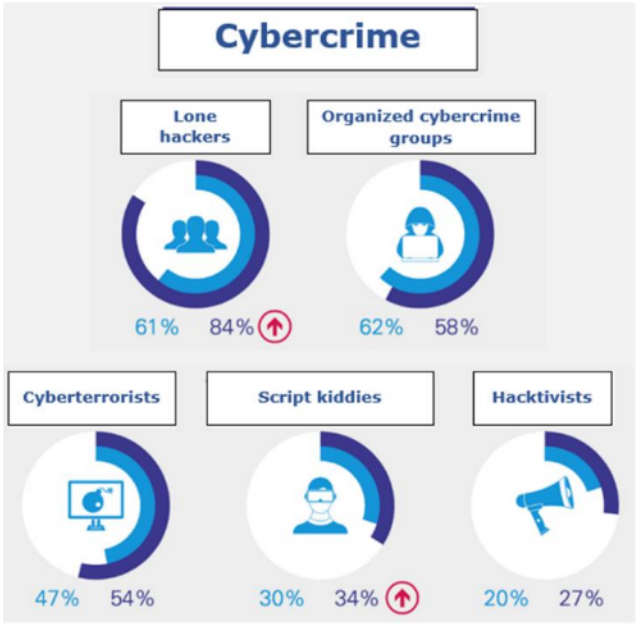


Figure 1. The perceived threat sources. Source: KPMG, 2019.

Taking into account the spectrum of the variety of possible attacks, it is necessary to describe a given phenomenon in more detail. Cyberterrorism is identified with unlawful actions targeting important communication and information systems in a way that the threat of carry them out enables reaching particular objectives or goals. People trained for these terrorist acts are not only schooled ideologically, but also have IT skills.

Figure 2. Visualization of interlinked systems in civil aviation that shows several potential paths of cyberattacks. Source: Vereinigung Cockpit, 2017.

Aviation is particularly vulnerable to all forms of terrorist attacks, and due to technological development to attacks in cyberspace as well. Among the possible threats, there are attacks with the use of malicious software, theft, modification or destruction of data, blocking access, and socio-technical attacks, i.a., phishing (Goodman, 2015). The aviation sector is mainly at risk due to cyberterrorist attacks, because it operates with a large amount of computer equipment, massive amount of data, which are transmitted every minute between electronic devices. Moreover, there is an arising necessity to rely on IT systems that are inevitable for the functioning of aviation today. Airports, airlines, navigation systems, flying an aircraft can become a target of a cyberattack. Even factories that manufacture components used for constructing airplanes can be attacked by cyberterrorist, which may lead to various, chiefly negative consequences for the whole aviation sector (ICAO, 2019).

3. The human factor and cybercrime

The internet is a generally accessible tool that offers its users many possibilities – from communication and acquiring knowledge, to enjoying shopping, medical, tourist, and other services. The growing threat of attacks that utilize shortcomings of the human mind make the human factor key in cybersecurity (Pisarek, Ščurek, 2017).

The 2019 ENISA report "Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity" informs that during last 25 years, actions meant to increase IT security have focused mainly on the technological security of systems and equipment. The role of the human being in the security systems was limited by procedures and sanctions (ENISA, 2019). Such an approach was responsible for the low level of social awareness regarding cyberattack prevention. However, it is well known that lack of education in that area generates a lack of understanding of the essence of cyberthreats. Therefore, enhancing the awareness of cyberspace is very important. Consequent implementation of secure global network services into everyday practices is equally vital. The need for deploying proper educational programs for employees from the private and public sectors is necessary because only through regular courses and training the state of cybersecurity may be improved.

In their research on cybersecurity, Mancuso (2014), Porctor and Chen (2015), Horowitz and Lucero (2016), and Heiges (2015) used a scenario which simulated the manipulation of the navigation system that presented false points on course (Gontar, et al., 2018). The main goal of the experiment was to learn what security requirements would be useful. The analysis of the human factor showed pilots' needs during a cyberattack, as well as their concerns regarding making inappropriate decisions. The biggest problem turned out to be the fact that during a cyberattack, pilots are uncertain (ICAO, 2015). In situations of technical malfunctions, pilots often act in accordance to procedures in order to solve them. In such a situation, pilots are also able to predict the behavior of the aircraft (e.g., if a hydraulic system is leaking). Pilots, acting in accordance with instructions, know that in a situation when hydraulic pressure is too low they would get a warning signalizing the malfunction. Moreover, pilots (depending on the aircraft) can get information from the aircraft system of how a particular malfunction will influence the aircraft's performance. Such situations are subject to training during simulator practices. It is worse during a cyberattack because pilots do not know whether the signals are trustworthy, or they can be unclear whether the system was attacked. Pilots, in such a situation, could be disoriented and not know if the problem could be solved by means of the established procedures. Following procedures, in such situations, can be

utilized by potential attackers to manipulate the pilots' behavior (Gontar, et al., 2018).

Potential cyberterrorist attacks aim at finding and making use of gaps and errors occurring in the security systems and shortcomings of human character that manifest itself in recklessness, laziness, or lack of imagination. The effects of cyberattacks may be the same as in the case of a terrorist attack – they have the potential of threatening of the lives of air transport users or their health, the destruction of airport infrastructure, or loss of important data for the aviation sector. Undoubtedly, the functioning of aviation is based on public trust, which can be irreversibly undermined by the occurrence of cyberattacks. This is why, , the aviation industry will face challenges to keep the public's trust in cyberspace in upcoming future. Solving these problems is crucial for the safe functioning of air transport.

4. Cybersecurity programs in Poland and the European Union

The European Union's actions regarding security in cyberspace are divided into two thematic areas. One of them is focused entirely on counteracting cyberattacks, while the second aims at maintaining the protection of critical infrastructure, IT critical infrastructure, and security of the network and information (Kańciak, 2013). According to that division between security and counteraction, the EU's programs and strategies have been prepared. There are, however, certain problems of a formal nature that have led to the lack of a common approach among the EU's institutions regarding those problems.

Security constitutes a fundamental air system and is a main goal of the EU's policy in the area of aviation and IT (Balcerzak, et al., 2019). Issues related to, i.a., the protection of critical infrastructure, personal data, and the environment are closely related to aviation security. Therefore, it is necessary that the EU's directives are implemented into national regulation frameworks. These documents are:

- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection;
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union;
- Personal Data Protection Act of 10 May 2018;
- National Cybersecurity System Act of 5 July 2018;
- Ministry of Digitization Regulation of 10 September 2018 on the organizational and technological conditions for the entities providing services in the area of cybersecurity and internal organizational structures of the key services provides responsible for cybersecurity;
- Council of Ministers Regulation of 11 September 2018 regarding the list of key services and materiality thresholds of the effects of distorting events for providing key services;
- Ministry of Digitization Regulation of 20 September 2018 on the criteria of a breach of the security or integrity of the network or telecommunication services that have a significant impact on the operation of network or services;
- Ministry of Digitization Regulation of 20 September 2018 on a model form for the communication of information about security breaches or the integrity of telecommunications networks or services that have a significant impact on the operation of networks or services;
- Council of Ministers Regulation of 16 October 2018 on the documentation of cybersecurity of the IT systems used for providing key services.

The national cybersecurity policy framework of the Republic of Poland was established by a Council of Ministers' resolution. It has a direct bearing on government administration bodies. After being adopted, at

the initiative of the Council of Ministers, as the regulations of the national law, they, in an indirect way, affect other bodies of public administration. These regulations in particular refer to (Ministry of Digitization, 2017):

- The goals regarding computerized systems security;
- The main bodies engaged in implementation of the national framework of computerized systems security;
- The management framework facilitating the goals of national framework regarding computerized systems security;
- The need for preventing and reacting to incidents and recovery to the nominal state after disruption, including the rules of cooperation between the public and private sectors;
- The approach to risk assessment;
- The types of approaches to educational, information, and training programs regarding cybersecurity;
- The actions related to research and development plans in the scope of computerized systems security;
- The approach to international cooperation regarding cybersecurity.

Taking into account the development of the information society, electronic administration and digital economy, and the threats of cyberspace, the structures of the national protection of cyberspace have to be strengthened. Quickly changing methods of committing crimes require carrying our research in the area of counterfeiting cybercrimes, the results of which will provide support to law enforcement bodies (Żmigrodzka, 2011).

The body responsible for preventing hacker attacks is the Computer Security Incident Response Team (CSIRT GOV), whose key tasks focus on information exchange and knowledge sharing. The cyber emergency response center is a unit that monitors and reacts 24 hours a day and seven days a week.

Aviation is in the process of integration with the national system of cybersecurity, just as the power and financial sectors did previously. The main goal is to ensure the security of aviation operations in Poland by implementing all security procedures according to aviation law regulations.

Cybersecurity is not limited to IT but, above all, it consists in information. It is important not to marginalize even the smallest signs, because thanks to currently accessible technology, even a minor strange detail in the information or data may lead to significant losses, and thus it should be taken into account. Conclusions should be drawn from that information and then given over to other sectors and institutions because attacks can be multisectoral; they do not have to be direct.

5. Examples of risks and threats of cyberattacks in aviation

The whole development of aviation is based, to a considerable extent, on access to modern technologies, especially information technologies. All of the elements of the aviation sector should be aware of the risk that stems from using computer networks, and without which aviation activity could not exist. Recent incidents have shown that there is a growing interest in cyberspace among people who are willing to disrupt the functioning of aviation. In 2011, hackers were able to gain access to the radio frequencies used by British air traffic controllers, and give false information to the pilots and send a false signal about the danger. In the same year, a break into the internet network of one of the airlines was reported, in consequence of which the hackers gained access to confidential information about customers, their credit cards, flight plans, and data bases of that airline. The threat of cyberterrorism seems to be even more dangerous, because one just needs a computer with the internet access to carry out an attack. The cyberterrorists' knowledge and access they have to relatively cheap equipment makes them often feel that they are untraceable and unpunishable for creating real threat to the air transport users. Already at the level of providing software and operational systems

for the aviation sector, one should expect from the suppliers to provide updates on an ongoing basis, as well as to solve security related problems with the software they supply. Designing one piece of software for a particular company or institution from the aviation industry seems to be an ideal solution. It should not be available for other industries.

Enhancement of security may also consist in running applications as part of the so-called isolated areas, which limits undesirable software interactions. When it is accompanied by regularly updated anti-virus system, it decreases the risk of damages caused by cyberattacks. It should be obvious that the equipment dedicated to professional tasks cannot be used for private purposes. All data should be encrypted and properly secured. Especially sensitive systems should be cut off from the internet. A good example here is the fact of separation of the onboard entertainment system from other systems of the aircraft. Another important issue is data transfer, which ought to be performed only with the use of a secured, encrypted channel, and minimal internet connections. It should be noted that cyberattacks may go unnoticed even for a longer period of time. Therefore, there is a need for inspecting the accumulated data. Employees of various organizations of the aviation sector have to be aware that cybercrime threats may occur. Therefore, employers should organize specialized courses for their employees, which would include issues regarding how to increase employees' awareness of the security gaps in the data processing systems and how those systems could be attacked. The employees' skills should be also expanded by learning characteristic features of cyberattacks, so every one of them would be able to quickly recognize them and initiate limitation of its effects.

Higher risk related to cyberattacks in aviation occurs in the following areas (Żmigrodzka, 2011):

- Monitoring aircraft in airspace;
- Various IT software used by aircraft producers and operators;
- Activities related to operation of aircraft and support of people using the aircraft;
- Software that requires more secure programming so it would be ready to repulse every unpredictable cyberattack automatically;
- Securing against cyberattacks the equipment used for gathering and storage of important data;
- Management and control aiming at the deployment of proper security policies by the most important people in aviation organizations. Defining the process of risk management related to one's own organization and cooperating entities;
- Air traffic services that would profit from the implementation of monitoring systems and verifying the data they transmit;
- Access control with the use of the proper protocols and procedures, and limiting the access to particular sectors.

The main tasks of aviation organizations include, above all, the development and implementation of legal norms, procedures, and technological solutions enhancing security and development of aviation (Compa, 2017), as well as the following (Żmigrodzka, Kostur-Balcerzak, 2018):

- Licensing and Certifying;
- Carrying out audits, checks, and inspections;
- Carrying out scientific research, and development activities;
- Preparation of bills, normative documents, and manuals;
- Organizing courses and scientific conferences;
- Organizing civil-military cooperation at the national and international levels (Zajas, 2015).

An effective cybersecurity program should include using management structures based on international sectorial standards and guidelines in order to cover all necessary aspects.

One of the many issues related to prevention, and also to a certain degree, combating cyberterrorism is securing computerized

systems. EASA estimates that every year there are 1,000 cyberattacks on aviation systems globally (PA, 2018).

Despite the aviation industry lobby's belief that the systems aircraft are equipped with cannot be overtaken by hackers, researchers of the security market demonstrate the opposite. For example, at a conference in Greenberg (2013), Hugo Teso showed that he was able to manipulate the ACARS system used to address and report on aviation communication with the use of his smartphone running on Android. Ruben Santamarta, a security specialist, reveled in his research paper that he was able to take control of SATCOM radio telephones, which allowed him to conclude that the "current status of the products IOActive analyzed makes it almost impossible to guarantee the integrity of thousands of SATCOM devices" (Santamarta, 2014, p. 25).

In recent years, the number of cyberthreats related to airports has grown significantly, e.g.:

- Passport control systems at the departure terminals of Atatürk and Sabiha Gökçen airports in Istanbul were closed because of a cyberattack, which resulted in the passengers having to wait for hours in lines and light delays (2013) (PA, 2018);
- The resource planning system of a company managing airports in India was taken over, which resulted in losing personal employees data of 75 American airports. The break in was carried out by a organized hacker group financed by the state (2014) (PA, 2018);
- At Warsaw Frederic Chopin Airport there was a break in into the schedule planning system that caused grounding ten aircraft and delaying sever others. The hacker attack resulted in suspending flights that affected 1,500 passengers, and the teleinformation department was paralyzed for a few hours. Due to the breakdown, the Polish airlines LOT cancelled both domestic (from Warsaw to Kraków, Wrocław, Rzeszów, and Gdańsk) and international flights – to Dusseldorf, Hamburg, and Copenhagen (2015) (WP, 2015);
- Adata theft occurred at the Turkish Directorate General of Civil Aviation. The attack was discovered by a cybersecurity analyst working for Lockheed Martin, who noticed that hackers took control of two ICAO servers. Malicious software was installed on those servers and the software could be disseminated further by authorized government and aviation organizations employees. The hackers used the so-called water hole method, which gets its name from the way predators wait around their prey close to water holes. They used it to create the possibility of breaking into the server visited by their potential victims and install malware, which was ten downloaded by people logging in the ICAO server (2016) (Bounaoui, 2019).
- The Vietnam Airlines' webpage and information screens in Hanoi and Ho Chi Minh City airports were attacked by hackers, resulting in all systems connected to the internet being turned off, and all operations being carried out manually. The hackers obtained the data of 400,000 passengers (2016) (Bounaoui, 2019).
- There was an outbreak of ransomware that attacked systems, which resulted in the attacked organizations having to pay off hackers for getting data back. LATAM Airlines had their data decrypted by WannaCry and The Boryspil International Airport in Ukraine lost access to its systems because of ransomware called NotPetya. These cyberattacks did not target aviation, but caused a break in providing airport services (2017) (Bounaoui, 2019).
- The data from the transactions processed through a webpage and mobile application of a British carrier were taken over. The hackers gained access to credit cards numbers, their expiration dates, and CVV numbers. Such information make it possible for the cybercriminals to break into the customers' accounts and collect personal data. However, the passport and travel arrangements data were not targeted by the hackers (2018) (Górski, 2018).

6. Conclusions

In conclusion, threats to aviation security, especially frequent cyberattacks are one of the most important issues in the 21st century. Without proper training on the protection of IT infrastructure and making society aware of the danger, there is no possibility of ensuring security in aviation. The most common cases, as the research shows, are related to hackers' cyberattacks. Common strategy and policies to secure new technologies against undesirable access is key. Every computerized system connected to the internet or network can become a target, even aircrafts, which have been demonstrated in the paper. This is why, it is important to work out security procedures and common standards of using available, technologies created for aviation. Of course, while having regard to cultural differences, it has to be said, that it is a real challenge but, as it is the case with other security procedures, aviation security procedures have to be followed very restrictively.

References

1. Balcerzak, T., et al. (2019).Cybersecurity in civil aviation. In E. Dynia, and S. Kubas (Eds.), Bezpieczeństwo w międzynarodowym i krajowym prawie lotniczym i kosmicznym (pp.57-78). Rzeszów: Wydawnictwo Uniwersytetu Rzeszowskiego.
2. BBN [Biuro Bezpieczeństwa Narodowego] (2015). Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej z dnia 22 stycznia 2015 roku. Warszawa.
3. Bounaoui, S. (2019). Międzynarodowa Organizacja Lotnictwa Cywilnego padła ofiarą hakerów. RMF24, 08.03.2019. Retrieved from https://www.rmf24.pl/fakty/swiat/news-miedzynarodowa-organizacja-lotnictwa-cywilnego-padla-ofiara-,nId,2873380?fbclid=IwAR1qmuHK8XtIQm9nKywky0jOYAR01_2uMc_IwixJFkJoiY2QwxT6Ma5z_Cs, 10.04.2020.
4. Compa, T. (2017). Międzynarodowe organizacje lotnicze w systemie bezpieczeństwa transportu lotniczego. Dęblin: Wydawnictwo Wyższej Szkoły Oficerskiej Sił Powietrznych.
5. Compa, T., and Rajchel J. (2011). Podstawy nawigacji lotniczej. Dęblin: Wyższa Oficerska Szkoła Sił Powietrznych.
6. ENISA [European Union Agency for Network and Information Security] (2019). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. Retrieved from https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity, 19.03.2020.
7. Gontar P., et al. (2018). Are pilots prepared for a cyber-attack? A human factors approach to the experimental evaluation of pilots' behavior , Journal of Air Transport Management, 69, 26-37. DOI: https://doi.org/10.1016/j.jairtraman.2018.01.004.
8. Goodman, M. (2015). Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do about It. London: Corgi Books.
9. Górski, S. (2018). Atak hakerów na British Airways. Wyciekły dane kart kredytowych 380 tys. klientów. PCWorld, 07.09.2018. Retrieved from https://www.pcworld.pl/news/Atak-hakerow-na-British-Airways-Wyciekly-dane-kart-kredytowych-380-tys-klientow,410833.html.10.04.2020.
10. ICAO (2015). Podręcznik zarządzania bezpieczeństwem (SMM) (Doc. 9859 AN/474). Retrieved from http://edziennik.ulc.gov.pl/api/DU_ULC/2015/64/oryginal/Zalacznik1.pdf, 22.03.2020.
11. ICAO (2019). Security and Facilitation Strategic Objective: Aviation Cybersecurity Strategy. Retrieved from

https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf, 18.04.2020.
12. Kańciak, A. (2013). Problematyka cyberprzestępczości w Unii Europejskiej. Przegląd Bezpieczeństwa Wewnętrznego, 8(5), 109-120.
13. KPMG (2019). Barometr cyberbezpieczeństwa: W obronie przed cyberatakami. Retrieved from https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/04/pl-Raport-KPMG-Barometr-Cyberbezpieczenstwa-W-obronie-przed-cyberatakami.pdf, 22.04.2020.
14. Ministry of Digitization (2017). Krajowe ramy polityki cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022. Warszawa: Ministerswo Cyfryzacji. Retrieved from https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/0bbc7a32-64df-b45e-b08c-dac59415f109, 12.04.2020.
15. PA (2018). Overcome the Silent Threat: Building Cyber Resilience in Airports. Retrieved from https://www.nsr-org.no/getfile.php/1310858-1532343127/Dokumenter/Eksterne%20publikasjoner/PA_Airport%20Cyber%20Security%20Report.pdf, 12.04.2020.
16. Pisarek, J., and Ščurek, R. (2017). Determination of the Human Factor in Air, Land and Marine Traffic. Saarbrücken: Lambert Academy Publishing.
17. Santamarta, R. (2014). SATCOM Terminals: Hacking by Air, Sea, and Land. IOActive Security Services. Retrieved from https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf, 10.04.2020.
18. Vereinigung Cockpit (2017). SafeSKY 2017. Retrieved from https://www.vcockpit.de/fileadmin/dokumente/presse/2017/Brosch%C3%BCre_SafeSKY2017_Onlineversion.pdf, 07.04.2020.
19. WP (2015). Systemy LOT narzędziem hakera. Wirtualna Polska, 29.09.2015. Retrieved from https://tech.wp.pl/systemy-lot-narzedziem-hakera-6034789869351553a, 10.04.2020.
20. Zajas, S. (2015). Międzynarodowe i krajowe organizacje lotnicze. Warszawa: Akademia Obrony Narodowej.
21. Żmigrodzka, M. (2011). Terroryzm powietrzny i środki jego zwalczania. In A. Kozera, et al. (Eds.), Polaków portret niedokończony: Studia z zakresu historii, prawa, politologii (pp. 360-373). Kraków: Wydawnictwo Naukowe Uniwersytetu Pedagogicznego w Krakowie.
22. Żmigrodzka, M., and Kostur-Balcerzak K. (2018). Measuring the Power of VR Education. In Transport Means 2018. Proceedings Of The 22nd International Scientific Conference: PART III (pp. 1459 -1463). Kaunas: Kaunas University of Technology.

SAFETY&DEFENSE
ISSN 2450-551X

Unmanned Aircraft Systems in Crisis Management in Poland After 2007

Wojciech Krasiński

Siedlce University of Natural Sciences and Humanities, Siedlce, Poland
wojciech.krasinski@lipsko.eu, ORCID: 0000-0003-4041-2598

DOI: https://doi.org/10.37105/sd.79

Abstract
This article discusses the employment of unmanned aircraft systems in crisis management in Poland after 2007. The conceptual framework and organization of crisis management in Poland is presented as an introduction to further discussion. This article then analyses capabilities of various categories of unmanned aircraft systems taking into account specific requirements of crisis management. This article also points at preliminary lessons learned from employment of unmanned aircraft systems for crisis management in Poland in recent years. Due attention is paid to missions and the organization of employment of unmanned aircraft systems in crisis management operations. Perspectives of employing unmanned aircraft systems in crisis management are presented in the final part of the article.

Keywords: unmanned aircraft systems, crisis management, safety, Poland.

1. Introduction

Unmanned aircraft systems offer unique capabilities to crisis management as they increase the safety of rescue teams and the effectiveness of overall response to crisis situations. Unmanned aircraft systems have traditionally contributed to situational awareness by surveillance missions, but the scope of their employment in crisis management is expanding nowadays. Unmanned aircraft

systems have been used for crisis management in Poland for a few years now. With technology evolving rapidly, and the accumulation of preliminary observations, it is good time to explore the topic as it is timely and directly related to the safety of citizens. The article introduces conceptual framework of crisis management in Poland and discusses the capabilities of unmanned aircraft systems in the context of requirements related to crisis management. Preliminary lessons learned from unmanned aerial vehicles' employment in crisis management in Poland are presented and serve as a point of departure for discussion on the future of the use of such systems in crisis management.
This article aims at a preliminary assessment of unmanned aircraft systems' employment in crisis management in Poland after 2007. The topic is new in Poland. While there is plenty of research on crisis management in Poland, only a few research papers have been devoted to the employment of unmanned aircraft systems in crisis management in Poland. However, there are no monographic scientific analyses in the field of lessons observed yet. Research papers published in Polish after 2016 focus almost exclusively on the employment of unmanned aircraft systems in firefighting operations. The employment of such systems in crisis management in Poland has been mentioned in official press releases, internet news and publicly available documents related to crisis management. Therefore, a preliminary analysis and assessment of the employment of unmanned aircraft systems in crisis management in Poland seems desirable and may be viewed as a departure point to further research in this field.

2. Conceptual framework for crisis management in Poland

Political changes in Poland in the 1990s meant that more and more importance was attached to non-military threats. The experience of the 1997 "millennial" flood and adoption of the Act on the State of Natural Disaster in 2002 provided basic assumptions for the conceptual and legal framework related to crisis management in Poland. Poland's accession to NATO in 1999 and the European Union in 2004 accelerated the implementation of new solutions within the crisis management system in Poland that were needed for an effective response to non-military threats. Finally, the most comprehensive regulations in the field of crisis management entered into force with the adoption of the law on crisis management in 2007. A 'crisis situation' has been defined in Poland as a phenomenon adversely affecting the level of people's safety, constituting a threat to the property of considerable size or to the environment, and causing significant restrictions in the operations of public administration. The act on crisis management that was adopted in April 2007 defines crisis management as the activity of public administration authorities that constitutes an element of managing the national security management system. In accordance with the act regulations, crisis management activities consist of: preventing crisis situations, preparing to take control over them by way of planned activities, responding in the case of emergencies, removing their effects and reconstructing resources and critical infrastructure (RCB, 2020). In 2013, the comprehensive risk assessment for crisis management was completed and implemented into crisis management plans in Poland. It provided a catalogue of natural and man-made hazards, and assessed their possible impact through the lens of the probability of occurrence and severity of consequences. Since

that time, flooding has been constantly assessed as one of the most frequent natural hazard that results in serious consequences for citizens, property and environment (RCB, 2013). Hurricanes and extremely high temperatures causing fires have been more frequent in recent years, requiring more attention within crisis management system. The crisis management system in Poland is characterized by a vertical structure of management by public administration. The span of management stretches down from the Prime Minister, through individual ministers, voivodship governors, and county mayors down to commune heads and city presidents. The Ministry of the Interior and Administration plays a major role in crisis management system as it supervises the activities of, among others, the Police, Border Guard, State Fire Service, and National Civil Defense. Crisis management in Poland is based on the principle of primacy of the territorial system. It means that the response to crisis situations is based on the territorial division of the state into municipalities, counties and voivodships up to the territory of the country. Depending on the scale of the crisis, the authority in charge for crisis response is the commune head (mayor, president), county mayor, the voivodship governor or the Prime Minister. Depending on the needs related to crisis response, the voivodship governors may request the support of the Armed Forces of the Republic of Poland. The routine response to crisis situations in Poland is the primary responsibility of the entities of the National Firefighting and Rescue System, Police, units of the State Medical Rescue Service, the Border Guard and other competent state offices, agencies, inspections, guards and services (Sienkiewicz-Małyjurek, and Krynojewski, 2010). The National Firefighting and Rescue System has been organized mainly on the basis of the State Fire Service and, to a lesser extent, volunteer fire brigades (Włodarski, 2018). The mission of the State Fire Service related directly to crisis management is to protect life, health, property, and the environment against fires, natural disasters or other local threats (Michailiuk, 2015). The leading role of the State Fire Service in crisis management in Poland is primarily due to the specialized equipment, knowledge, experience and skills that the servicemen of this formation have at their disposal (Gromek, 2017).

3. Unmanned aircraft systems' capabilities and crisis management

Public perception of unmanned aircraft systems is tied strongly to "drones" and focuses almost solely on the aerial vehicle. That is not true in terms of the complexity of unmanned aircraft systems employment or capabilities which they offer for crisis management. The term unmanned aircraft systems is much broader than unmanned aerial vehicles. It is defined as a system whose components include the unmanned aircraft, the supporting network and all equipment and personnel necessary to control the unmanned aircraft. Unmanned aircraft systems include remotely piloted aircraft, as well as ground control and support components. The lack of crew onboard such aircraft offers unique capabilities for crisis management, as it keeps rescue personnel safe outside the danger zone. Unmanned aircrafts may be smaller and cheaper to perform the same mission as a manned platform as they do not need to carry a human onboard or meet strict safety certification requirements. As unmanned aircraft systems operate within close vicinity of the crisis response action area, they may be more responsive than manned aircraft and stay longer in the air. Unmanned systems are also less vulnerable to limitations in visibility, which limit take off, operations and landings of manned aircraft (Cieślak et al., 2014). For crisis management purposes, the missions of un-

manned aircraft systems are similar to piloted platforms. Unmanned systems are best suited for intelligence, surveillance and reconnaissance missions (Urząd Lotnictwa Cywilnego, 2013). They are a proven asset for search and rescue operations both during crisis situation and under normal conditions (Półka, et al., 2017). As such systems are equipped with daylight and thermal observation systems, and some of them even with radars, they may be used for both a wide area surveillance and pin-point detection of a broad spectrum of objects of interests to crisis management authorities and rescue teams. The key capability of unmanned aircraft systems for intelligence, surveillance and reconnaissance missions is tied to a near real-time transmission of imagery to ground stations, both point to point or in a broadcast mode. Thanks to that, data obtained by unmanned aircraft systems may be exploited in a timely manner by rescue teams and contribute to situational awareness at higher echelons of crisis management command and control. The spectrum of unmanned aircraft system tasks is related to a specific type of natural disasters or manmade catastrophes. During flooding surveillance aircraft systems can provide a real-time overview of the spread of floods, water levels at levees, and associated potential hazards for rescuers and surrounding communities (Kostur et al., 2019) . Similar actions can be taken with unmanned aircraft systems in the event of fires and search and rescue operations. The COVID 19 pandemic has proved that unmanned aircraft systems may also be used for measuring body temperature from a distance, as well as tracking and identifying people who do not comply with certain sanitary restrictions. Unmanned aircraft systems equipped with loudspeakers can be used for alerting the population about threats. This may improve evacuation efforts and improve communication between crisis management authorities and the community. Mini unmanned aircraft systems, especially vertical takeoff and landing systems may be used in urban areas affected by floods or even inside facilities that have suffered a construction collapse. In case of NCBR events, unmanned aircraft systems may be used to measure contamination, locate leaks of toxic substances, monitor areas of particularly dangerous industrial plants and check radiation around borders adjacent to nuclear power plants (Tuśnio, and Nowak, 2016). Larger unmanned aircraft systems may be employed for transportation missions. They may carry specialized rescue equipment appropriate to the mission being carried out. It is possible for unmanned aircraft systems to carry a rescue container for people effected by natural disasters such as floods or hurricanes, and to deliver the aid precisely. Thus such systems will be capable of reducing the time of providing a person in need with preliminary assistance before the rescue teams arrive at the scene (Borkowski, 2018). Possible payloads of unmanned aircraft systems may include first aid kits, medicines, medical equipment or personal protective equipment. Unmanned systems may deliver such supplies to hard-to-reach and particularly dangerous places without exposing rescue teams to unnecessary safety risk. It is also possible to use unmanned aircrafts to assist in decontamination in the event of an epidemic. The use of unmanned aircraft systems also has its economic justification. Although purchasing such systems seems expensive at the beginning, operating them is much cheaper than manned aircraft operations. Small unmanned aircraft systems are relatively easy to operate and the training costs are low. Finally, they may be easily integrated with rescue teams at lowest levels providing them with organic surveillance and reconnaissance capabilities. The loss of an aerial vehicle during crisis management operations does not bear serious consequences and by no means may be compared with a loss of a manned aircraft.

4. Lessons observed

Recent years have seen more and more frequently increasingly extreme natural hazards, such as flooding, hurricanes or fires. The scale of natural disasters usually precluded effective conduct of crisis management, to include rescue operations, by local territorial self government authorities. Due to the scale of disasters and short warning time, the authorities needed external support from both civilian rescue services and military forces. The flood of May and June 2010 on the Wisła, Odra and Warta rivers directly impacted two percent of Poland's territory and required several thousands of rescue professionals to deal with disaster. The storms of August 11 and 12, 2017 were accompanied by the hurricane of the century, that instantly caused losses in several voivodships along three hundred kilometers wide swath of multi-cell line thunderstorms. Climate change, with higher average temperatures and decreasing precipitation have increased the risk of wild fires in forests and on pastures across Poland. An example may be the fire of 2020 in the Biebrzanski National Park, in which more than 52 square kilometers of grass and peatlands burnt. The effects of the fire were increased by prolonged droughts. Finally, the COVID 19 pandemic challenged Polish law enforcement, crisis management authorities and rescue teams with a number of issues. The need for effective enforcement of quarantine, restrictions of movement or gathering serve just as example. All those situations prove the importance of employing unmanned aircraft systems in crisis management. The State Fire Service in Poland started operating first unmanned aircraft systems that could be employed in crisis management in 2011 thanks to the support of the European Union's funds. Until the end of 2015, the State Fire Service had only eight unmanned aircraft systems. This changed in 2019 with large scale purchases of dedicated unmanned aircraft systems. The State Fire Service acquired fifteen Yuneec Typhon H520 and eleven DJI Matrice 200 systems. Both systems are equipped with daylight cameras, and the DJIs also carry infrared cameras. The systems are capable of real life transmission of imagery to ground control stations (InfoSecuritu24, 2019). In 2019, the Police bought thirty eight DJI Matrice 210v2 and DJI Matrice 200v2. unmanned aircraft systems for PLN 5.6 million (BRD24, 2019). Prior to the COVID 19 pandemic, the unmanned aircraft systems supported routine operations of the State Fire Service and the Police. Some lessons about unmanned aircraft systems' capabilities were gathered during crisis management exercise. In 2018, exercises were carried out using unmanned aircraft systems based on the scenario of a potential flood related situation in Wroclaw with elevated water levels on the Odra River (Straż Wrocław, 2018). Between 2018 and 2020, the State Fire Service used unmanned aircraft systems to locate fire sources, contaminated spots on the water surface, obtain spatial data in the event of a flood, and to search for missing people in debris. Real life employment of unmanned aircraft systems in crisis management took place in March and April 2020. Territorial Defense Forces used FlyEye unmanned aircraft systems to monitor fires in the Biebrzanski National Park. Broad area airborne surveillance proved critical in a swampy terrain that was hard to access by ground firefighting units. Unmanned aircraft systems equipped with infrared cameras provided timely and precise data for the commanders of the firefighting teams services. They were also employed at night, when they successfully located fire outlets, and assisted the movement of firefighting units (Radar, 2020). Since March 2020, the governmental and territorial self government authorities have used unmanned aircraft systems for crisis management activities related to COVID 19 pandemics. The Police have been using such systems for monitoring wide areas and to

augment ground patrolling. The Polish Air Navigation Services Agency initiated the coordination of the possible employment of privately owned aircraft systems to monitor the situation related to the COVID 19 pandemic. More than 750 operators willing to help responded. The capabilities of Poland's produced unmanned aircraft systems were demonstrated to governmental and territorial self government at the beginning of the disease outbreak. The Flytronic company offered the support of its unmanned aircraft systems to assist response to the COVID 19 pandemic. The FlyEye systems developed by Flytronic demonstrated the establishment of a voice communication and video transmission system for all crisis management services, which might be employed in observing hard-to-reach areas requiring surveillance in connection with COVID 19 disease. In addition, FlyEye MED, an unmanned system that provides support to all medical services capable of delivering medicines and other medical supplies over a distance of up to 50 kilometers, was presented (Świat Dronów, 2020a). The state Police along with municipal guards have been using unmanned aircraft systems to monitor public spaces. Aerial surveillance were used among other cities including Bydgoszcz, Lublin, Kraków, Szczecin, Siemianowice Śląskie and Zielona Góra (Świat Dronów, 2020b). The unmanned aircraft systems assistance to law enforcement and public order services have proved efficient and invaluable. On 29 April 2020, the first autonomous flight of Polish Hermes V8MT unmanned aircraft system with a transport module took place in Warsaw. It was the first such flight in Europe. Samples for COVID 19 testing were transported between two hospitals in Warsaw. The flight proved capability of the unmanned aircraft systems to replace ambulance vehicles in such a service and free them for transporting patients. Unmanned aircraft systems made several rounds between Warsaw hospitals and the tests were successful (Spartaqs, 2020). In May 2020, preparations were made in Sosnowiec to use unmanned aircraft systems to disinfect bus stops in the city (Cyfrowa, 2020).

5. The future of unmanned aircraft systems' employment in crisis management in Poland

The growing commercial sector of unmanned aircraft systems in Poland, including both producers and service providers, allows for rather optimistic foresight related to the employment of such systems in crisis management. In recent years, the Polish Development Fund in cooperation with the Ministry of Infrastructure, the Polish Air Navigation Services Agency and the Civil Aviation Office has been implementing a program that is to support the development of the unmanned aircraft system production in Poland. Poland is one of the regional leaders in developing infrastructure that allows managing unmanned aircraft systems traffic management throughout the national airspace with the use of the PansaUTM system and respective legal regulations tailored specifically for unmanned systems (PANSA, 2020). According to the announcement of the Minister of Infrastructure of 2019 and the standards developed by the Polish Air Navigation Services Agency, Poland has introduced one of the first regulations in the world that allows for flexible unmanned flights, i.e. Beyond Visual Line Of Sight (BVLOS) and fully automatic flights of unmanned aircraft systems. With such technological and procedural solutions in place, there is a growing potential for the employment of unmanned aircraft systems as part of crisis management efforts. Enabling BVLOS flights of unmanned systems will, in the long term, improve broad area surveillance. It will greatly increase situational awareness and safety of ground rescue teams during fires, flooding or chemical, biological, radiation, nuclear (CBRN) events (Salmoral,

et al., 2020). BVLOS operations will speed up assistance to people in need, especially in hard-to-reach places and increase the safety of rescue teams. In the future, the Police plans to use unmanned aircraft systems to detect illegal firing of grasses leading to fires (Świat Dronów, 2020c). With almost no experience of using unmanned aircraft systems for aerial delivery so far, one may expect dynamic increase in such tasks for unmanned aircraft systems in crisis management in Poland in near future. Following the experience of other countries, such as France, Iran, Spain and Greece, unmanned aircraft systems may be used for helping to supply life-saving equipment to people in need. They may also resupply rescue teams. It is too early to discuss the scope of the use of unmanned aircraft systems in pandemic scenarios in Poland. Depending on results of trials in Sosnowiec, we may see increasing use of unmanned systems for disinfection of public infrastructure in cities. It is technically feasible to measure the body temperature of people and use unmanned aircraft systems to enforce sanitary regimes (Cyfrowa, 2020). So, it seems fair to argue that law enforcement and rescue services along with crisis management authorities will be tempted to use this capability more often. In the future, the challenge for the employment of unmanned aircraft systems in crisis management will be tied to increasing automation of their operations to reduce number of people needed to operate them. With broad area surveillance capability limited to unmanned aircraft systems of the Armed Forces of the Republic of Poland and the Border Guard, it will be necessary to improve civil-military cooperation and inter-agency coordination to make the best of their employment in civilian led crisis response actions. A community of about twenty thousand professional private operators of unmanned aircraft systems in Poland needs due attention to integrate them into crisis management along with state rescue services. Although use of privately owned "drones" may be of assistance in crisis management, one must be cautious about appropriate level of training of volunteer operators of unmanned aircraft systems and safety during rescue operations.

6. Conclusions

Natural disasters have been occurring in Poland more and more frequently in recent years. Such threats to society's safety requires timely and effective response through crisis management operations. Unmanned aircraft systems offer unique capabilities that may be useful in crisis management. They may be employed for broad area surveillance of natural disasters and execution of tasks in hazardous places. Unmanned aircraft systems reduce the danger to life and health of rescue personnel involved in crisis management operations. The use of unmanned aircraft systems in crisis management in Poland has just started. Until now, unmanned aircraft systems have been used for monitoring threats. However, taking into account even preliminary observations and lessons in the field of employment of unmanned aircraft systems in crisis management, it can be seen that these are tools with high potential. In the coming years, unmanned aircraft systems may replace manned aircraft in a number of tasks related to crisis management. While it is too early to propose specific solutions that need improvement, the issue of the deconfliction and integration of unmanned aircraft systems in crisis management will grow in importance. With the development of visions of unmanned aircraft systems' employment in crisis management, it is also important to create very precise rules and procedures that will enable the best use of the potential that those systems bring to rescue efforts.

References

1. Borkowski, R., (2018). Bezpieczeństwo. Teoria i praktyka. Ratownictwo i medycyna katastrof w reagowaniu kryzysowym, Kwartalnik Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, No. 2 (XXXI), p. 125.
2. BRD24, Polska policja kupiła dorny za blisko 6 mln zł. 19.12.2019. http://www.brd24.pl/spoleczenstwo/polataja-nad-kierowcami-polska-policja-kupila-drony-za-blisko-6-mln-zl/, 30.05.2020.
3. Cieślak, E., Zieliński, T., Grenda, B., Rosłan, G., Żyłka, D., Kuptel, A., Markiewicz, T., Marud, W., (2014). Operacyjne aspekty rozwoju i wykorzystania bezzałogowych systemów powietrznych w Polsce, Akademia Obrony Narodowej, p. 10.
4. Duszczyk, M., Cyfrowa rp.pl, Polski latający termometr pomoże w walce z koronawirusem, 26.04.2020. https://cyfrowa.rp.pl/technologie/46341-latajacy-termometr-pomoze-w-walce-z-wirusem, 31.05.2020.
5. Duszczyk, M., Cyfrowa rp.pl, Pandemia przyśpieszyła rewolucję w przestrzeni powietrznej w naszym kraju. Drony będą przewozić testy na Covid-19, dezynfekować przystanki autobusowe czy... mierzyć temperature przechodniów. 26.04.2020. https://cyfrowa.rp.pl/technologie/46341-latajacy-termometr-pomoze-w-walce-z-wirusem, 31.05.2020.
6. Gromek, P., (2017). Państwowa Straż Pożarna a zarządzanie kryzysowe. Ujęcie strukturalne, Zeszyty Naukowe Szkoły Głównej Służby Pożarniczej w Warszawie, No 63/3/2017, p. 32.
7. Kostur, K., Żmigordzka M., Balcerzak T., Bezzałogowe statki powietrzne w ochronie przeciwpożarowej. (2019). https://www.eu-med.net/rev/rednma/36/aerial-vehicles.html, 31.05.2020, p. 42-43 , 58-60.
8. Kozubal, M., Radar Wojsko Polskie, Bezzałogowce szukają źródeł ognia. 23.04.2020. https://www.rp.pl/RADAR-Wojsko-Polskie/304239939-Bezzalogowce-szukaja-zrodel-ognia.html, 28.04.2020.
9. Michailiuk, B., (2015). Miejsce ochrony ludności i ratownictwa w systemie bezpieczeństwa narodowego Rzeczypospolitej Polskiej, „Zeszyty Naukowe WSEI", seria: Administracja, No 5 (1), p. 285.
10. Mieszała, T., Straż Wrocław, Ćwiczenia taktyczno-bojowe ,,ODRA-2018". (2018). http://straz.wroclaw.pl/cwiczenia-taktyczno-bojowe-odra-2018/, 29.04.2020.
11. Pansa, PansaUTM. https://www.pansa.pl/pansautm/, 26.05.2020.
12. Półka, M., Ptak, Sz., Kuziora, Ł., The use of UAV's for search and rescue operations. (2017). https://www.sciencedirect.com/science/article/pii/S1877705817326759, 01.06.2020. DOI: https://doi.org/10.1016/j.proeng.2017.06.129, p. 2.
13. Rachwalska, M., InfoSecurity24, Do kogo trafią strażackie drony?. 4.06.2019. https://www.infosecurity24.pl/komenda-glowna-psp-rozdziela-drony, 27.04.2020.
14. RCB, Act of 26 April 2007 on Crisis Management. https://rcb.gov.pl/wp-content/uploads/WERYF_-ACT_Crisis_Management_English-1.pdf, 31.05.2020.
15. Salmoral, G., Rvias Cascado, M., Muthusamy, M., Butler, D., Menon, P.P., Leinster, P., Guidelines for the Use of Unmanned Aerial Systems in Flood Emergency Response. (2020). https://www.mdpi.com/2073-4441/12/2/521/htm, 01.06.2020. DOI: https://doi.org/10.3390/w12020521, pp. 2 - 17.
16. Sienkiewicz-Małyjurek, K., Krynojewski, F. R., (2010). Zarządzanie kryzysowe w administracji publicznej. Wydanie II, Difin SA Warszawa, p. 51.

17. Spartaqs, Zagraniczne media o locie transportowym Dronoida HERMES V8MT pomiędzy warszawskimi szpitalami. 28.05.2020. http://spartaqs.com/media-o-nas-cat/zagraniczne-media-o-locie-transportowym-dronoida-hermes-v8mt-pomiedzy-warszawskimi-szpitalami/, 31.05.2020.
18. Świat Dronów, Systemy bezzałogowe grupy WB w walce z koronawirusem. (2.04.2020a). http://www.swiatdronow.pl/systemy-bezzalogowe-grupy-wb-w-walce-z-koronawirusem, 29.04.2020.
19. Tuśnio, N., Nowak, A., (2016). Bezzałogowe statki powietrzne w działaniach Państwowej Straży Pożarnej – propozycja dedykowana dla Państwowej Straży Pożarnej. Zeszyty Naukowe SGSP 2016, no 58 (vol. 1)/2/2016, pp. 119-120.
20. Urząd Lotnictwa Cywilnego. (2013). Zespół do spraw bezzałogowych statków powietrznych, Bezzałogowe statki powietrzne w Polsce. Warszawa, p. 2.
21. Włodarski, A. J., (2018). Współdziałania międzyorganizacyjne w ochronie ludności (ujęcie retrospektywne). Szkoła Główna Służby Pożarniczej, p. 66.

SAFETY&DEFENSE
ISSN 2450-551X

NASA Space Laser Communications System: Towards Safety of Aerospace Operations

Radosław BIELAWSKI[1*], Aleksandra RADOMSKA[2]

[1] War Studies University, Warsaw, Poland; r.bielawski@akademia.mil.pl,
ORCID: 0000-0002-5701-4476
[2] Military University of Technology, Warsaw, Poland; aleksandra.radomska@wat.edu.pl,
ORCID: 0000-0003-4486-8437
* Corresponding author

DOI: https://doi.org/10.37105/sd.85

Abstract

Bidirectional space communication is a fundamental prerequisite for maintaining contact with objects performing missions in space, whether manned and unmanned. Until recently, it relied solely on the propagation of electromagnetic waves (the radio) using frequency bands dedicated for objects outside the Earth's atmosphere. However, modern space technologies are subject to ongoing development as they are being fitted with advanced communication systems. Given the constant enhancement of our technological capabilities, the traditional radio-based communication shows a glaring inadequacy and contributes to the widening of a gap between this and the high technology of on-board devices installed on modern spacecrafts. The technology that complies with the up-to-date requirements of space communication is optical space communication. It is expected to provide for high-speed data transfer and increase the bandwidth several times, while ensuring immunity to common cyber threats, including jamming, spoofing and meaconing. The deployment of laser-based optical communication will not only contribute to increasing the air and space operation safety levels, but also enable deep space exploration. To this end, NASA's Laser Communications Relay Demonstration Project (LCRD) is currently undergoing development and testing. This chapter undertakes to characterize the emerging technology with respect to its operating principles, the future scope of applications and involvement in currently conducted experiments. The results from the analysis are presented in the form of scenarios outlining possible applications of laser communication.

Keywords: Laser Communication Relay Demonstration, optical space communication, outer space, security, space security

1. Introduction

Since the dawn of civilizations, space has been in the keen interest of philosophers, scientists, mathematicians and astronomers alike. In ancient times, celestial bodies such as stars and planets were the objects of observations and discourses attempting to understand how they influence the lives of people. Space was the source of continuing fascination, and yet it had for long remained in the realm of the fantastic and the unattainable for further investigation, not to mention its use. This changed no sooner than in the 20th century, following the rise of two powers – the United States and the Union of Soviet Socialist Republics, which were the first to have embarked on the space race – the race to dominate the extra-terrestrial. Initially, the space exploration aimed to investigate the conditions that were highly dissimilar to the ones found on the Earth and to launch artificial satellites. The space race became an important issue and a cultural reference in these countries; it had a marked influence on the national morale, paved the way for new ideological trends, but, predominantly, it became a major indicator of the military capabilities of the states and a marker of their technological advancement. Two events are regarded as the milestones of space exploration. The first event was the launch of the first artificial Earth satellite, Sputnik 1, and its placement in the orbit in 1957 (Polkowska, 2018). The second most important step was the landing of the manned mission on the moon, which took place in 1969. Over time, the competition between these and new contenders has evolved into cooperation – since outer space is the province of all mankind and cannot be regarded as belonging to any particular state or be subject to their control. Today, the near-Earth orbits accommodate artificial telecommunications satellites, space stations and various components of the present and developing global satellite navigation systems infrastructure. The systems provide the technological capabilities for locating objects on earth, water or in the air. On the other hand, the systems handle the communication with unmanned space flights, which are reaching increasingly remote regions of space, and in the future, this may include manned missions. Regardless of the type of object performing space flight, it is essential to maintain constant bidirectional communication to enable the transfer of data to Earth-bound centers. Given the long distances involved, it is critical that space communication should be highly reliable, continuous and resistant to electromagnetic, electronic or radio-frequency interference, whether as an intentional act or the result of natural space weather phenomena.

2. Modern space communication in the face of cyber threats

Outer space exploration has always been associated with launching objects that would deliver data from their research to centers on Earth. The communication systems of modern and future spacecrafts must, therefore, exhibit high reliability and resistance to interference, while ensuring uninterrupted data transmission over extended distances (Brandt-Pearce and Noshad, 2016). Accordingly, the bidirectional space communication networks are classified into three broad categories below (Figure 1).

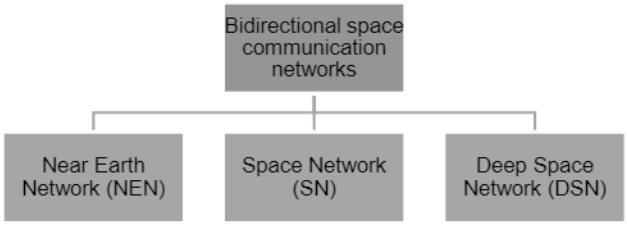


Figure 1. Classification of bidirectional space communication networks

The first scope of communications is managed by the Near Earth Network (NEN). The NEN infrastructure has two major components: the space and the earth segments. The space segment is composed of 14 satellite stations strewn across the Low Earth Orbit (LEO), the Geosynchronous Orbit (GEO), the highly elliptical orbit and the selenocentric orbit. The stations constituting the Near Earth Network include NASA-operated objects and commercial satellites. The other component of the NEN system is the ground segment comprising 25 antennas. The antennas' locations have been selected so as to provide the optimal coverage of the Earth: the stations are on several continents and at a considerable spacing. This configuration ensures constant and uninterrupted communication with the satellites, which, *nota bene*, constantly change their positions. The connection is established provided that the station is at a specified height directly above the receiving antennas (Dale, 2019). The Near Earth Network operates on a relatively small range, estimated at one thousand nautical miles, and it primarily handles the transmission of satellite data that provide telemetry and communication services to spacecrafts, command, ground tracking to a range of recipients, including national and international entities, governments and trade organizations, notwithstanding NASA. The unit in charge of NEN management is the Robert H. Goddard Space Flight Center, located in Greenbelt, USA.

The second system of communications in question is the Space Network – SN. It comprises an extensive technical infrastructure composed of several elements: the Tracking Data Relay Satellite (TDRS) – a constellation of geosynchronous satellites orbiting the Earth, satellites operating at an altitude of 73 kilometers in the Low Earth Orbit, the ground systems that form a relay system between the satellites, other ground objects and a high-speed broadband network connecting all the elements in a continuous cooperation. The range of uses of the Space Network is not limited to one task – its secondary tasks include: supporting telecommunication transmissions, testing, tracking, providing service and assuring required safety levels during unmanned space flights. In the future, SN is set to participate in the operation of manned flights to Mars. Currently, it delivers communication with astronauts performing space resupply flights, monitors their vital functions and space telemetry. The Space Network has substantially contributed to the exploration of orbital regions. The range of service of the SN has never been precisely defined due to the fact that its primary function consists in providing communication with objects in continuous motion; however, it may be described as operating on the orbital distance. As in the case with the NEN, it is the Robert H. Goddard Space Flight Center, located in Greenbelt, USA that is responsible for the supervision and management of SN operations.

The system for establishing and maintaining communication with objects and devices exploring the most remote sectors of outer space is the Deep Space Network (DSN). It is a system of 3 large terrestrial antennas (34-70 m in diameter) whose location facilitates communication with distant regions of the Solar System. According to calculations, the optimal spacing angle between the antennas in question, i.e. ensuring full signal coverage, is 120°. The antennas are situated in Madrid, Canberra and Goldstone, California, and thus, every satellite in space can at all times communicate with at least one station. The ground stations connect with satellites to initiate course corrections, provide software updates and introduce changes in the procedures of scientific observations carried out by these objects. Although the DSN range is not specified, it has

been designed to support only interplanetary missions, that is to deliver communication with rovers and probes exploring the Moon and Mars, as well as with objects sent to perform missions in the vicinity of the giant planets located in the most distant areas of the Solar System. The secondary role of the Deep Space Network is to support the other two networks: the Near Earth Network and the Space Network. The safety of DSN space operations is supervised by the Jet Propulsion Laboratory of the National Aeronautics and Space Administration (JPL NASA), located in Pasadena (California) in the United States.

To ensure that space communication is performed as intended, it was necessary to establish the uplink/downlink frequencies, i.e. the electromagnetic spectrum bands to be used by the systems (Table 1).

Table 1.

The traditional designation of the microwave radio bands for space communication

Band	Frequency [*f*]
L	1.5÷2.7 GHz
S	2.7÷3.5 GHz
C (downlink)	3.7÷4.2 GHz
C (uplink)	5.9÷6.4 GHz
X (downlink)	7.2÷7.7 GHz
X (uplink)	7.9÷8.3 GHz
K_u (downlink)	10.7÷12.75 GHz
K_u (uplink)	12.75÷14.5 GHz 17.3÷18.1 GHz
K_a (downlink)	18.1÷21.2 GHz
K_a (uplink)	27÷31 GHz
Q–V	36÷51 GHz

The classification of electromagnetic microwaves for space communication with satellite systems, given in Table 1, presents the traditional division of the spectrum and band designations. In modern and emerging space communication satellite systems, the frequency bands below 3 GHz are disregarded, which is a consequence of their excessive use and insufficient capacity, as well as of natural factors, such as the high impact of space radiation and the nature of the ionosphere, which is known to reflect and absorb electromagnetic waves. Currently, frequencies below 3 GHz provide for the mobile satellite networks, satellite telecommunication users and deep space research. The terms *downlink* and *uplink* designate the direction of communication, *i.e.* respectively, from the satellite to the Earth station receiver and from the Earth to the satellite system in space.

3. Space Laser Communications System

In the past, the limitations in communication between objects performing space flight and terrestrial observatories would frequently subject the scientific mission plans to revision. The conventional space communication systems employ the transmission of electromagnetic (radio) waves (Radio Frequency – RF) in specified frequency ranges. The problems in question primarily stem from the non-parallel progress of the communication technology and the rapid technological evolution of equipment and instrumentation fitted in modern space vehicles. Radio waves travel in space at a near-lightspeed velocity (in vacuum it is 299.792.458 m/s). Given the distances covered, there is an inherent substantial delay involved in space communication (e.g. an approximate time offset for a Moon rover is one second); the time delay increases with distance. This effect is exemplified by the Martian rover: in the most disadvantageous scenario of the planets' mutual position, the maximum delay time may reach up to approximately thirty minutes. The optical communication technology is expected to overcome the technological limitations of the existing electromagnetic-wave-based space communication. The new solution is expected to ensure considerably higher quality, thus effectively supporting future space flight missions. One of the key distinct advantages of optical communication consists in that it ensures data transmission speeds

of the order of a hundred times faster than the traditional RF systems at the same weight and power requirements of the equipment. Moreover, the new communication solution eliminates such underlying problems as microwave spectrum overload and allocation, limited bandwidth while providing higher security against cyber threats, which are rather common in radio communication. The new type of space communication network is set to be activated once the objects performing space flights are fitted with high-bandwidth instruments, such as hyperspectral cameras and instrumentation operating in high-resolution spectral, spatial and temporal modes. In the future, optical communication is envisaged to provide the technological capability for the establishment of a "virtual presence" on a remote planet or another celestial body within our solar system, enabling fast and reliable space communication.

In essence, optical communication is the transfer of data by means of an optical waveguide. Fiber optics uses the spectrum of the light, not the radio waves, to transfer information in a specific medium, which is in this case, between the space communications center on Earth and a space probe). Concerning its applications in telecommunication, it should be taken into consideration that data transmission in optical fibers occurs as a result of lightwave modulation that is caused by a semiconductor laser (LD) or a light-emitting diode (LED). A characteristic feature of fiber optic technology is that it is highly resistant to electromagnetic interference, as it does not emit an external electromagnetic field that would cover a certain extensive area (Furch et al., 2002). In such a special kind of telecommunications (Drzewiecki, 2015) as bidirectional space communication, it is necessary to clearly distinguish between the classic use of optical fiber in terrestrial and space applications. The technology in question employs photon propagation from the transmitter (Wu et al., 2019) to the receiver that is carried out through a waveguide; the latter could be a properly adapted optical fiber structure constituting a closed-loop glass-fiber system for data transmission. In the case of space communication, however, which makes use of a laser beam directed at a specified receiver target, it is the Earth's atmosphere that becomes the medium. Therefore, the created network is apparently an open-loop system based solely on the emission of light waves. This allows the use of unlimited bandwidth and reduces the risk of radio interference.
The results from the preliminary analyses of the capabilities of optical techniques in bidirectional space communication, originally developed for the United States Department of Defense (DoD) and NASA itself, have encouraged the space agency to put it to further testing, under the working title – Laser Communication Relay Demonstration (LCRD). During the demonstration, the laser communication relay has been employing the existing technical infrastructure to set up a bidirectional space communication network. The procedure that is being followed is expected to allow the researchers to gain operational experience while maintaining an optimal cost variant. The tests are scheduled to extend over the period of at least two years (to be completed no sooner than in 2021), over which time high-speed optical communication will be provided in the operational environment. The LCRD tests are intended to show whether the optical communication possesses the potential to meet the growing demand of NASA and other agencies for high data transmission rates and, secondly, whether it is suitable for low-power and low-mass spacecraft systems. The LCRD architecture is further assumed to serve as a platform for testing advanced communication tools, including adaptive optics (Wang et al., 2019), symbol coding, data link layer protocols and network layer protocols. The double optical link to be incorporated in the LCRD system will handle optical communication, enable the presentation of the new generation space relay system capabilities and provide early operational support for low-altitude orbit (LEO) terminals. An important step in the testing plan is to verify the effect that the Earth's atmosphere has on the laser space communication system and to create new atmospheric models. LCRD is likely to

provide the spur for the development of optical communication technology for space and near-Earth systems while boosting the efficiency of the industrial sector to produce cost-effective communication systems and components for terrestrial and space applications.

With respect to the design of the Laser Communications Relay Demonstration, it is composed of two major segments: the flight segment and the ground segment. The former segment houses the flight payload and the high-bandwidth Radio Frequency transceiver, both fitted on the spacecraft. For tests, the LCRD payload will be flown in the geosynchronous orbit on the Space Test Program Satellite-6 (STPSat-6). The payload will be composed of the Space Switching Unit (SSU) and Optical Space Terminals (OST). The SSU is the central controller of the LCRD payload, whose core functions are to receive and relay the incoming data according to physical layer frame, process commands, collect and transmit flight payload telemetry data. In addition, the LCRD system is equipped with an optical module for collecting and transmitting laser signals, a Pulse Position Modulation (PPM) transmitter and Differential Phase Shift Keying (DPSK) for uplink and downlink directions. The modem handles the operation of high-speed electronics with the Pointing, Acquisition and Tracking (PAT) algorithm and thermal control in space. It is also equipped with rudimentary calibration (Chen et al., 2019) and testing tools, such as the built-in test (BIT) for internal modem or flight payload loopback checks. With respect to the high-frequency radio terminals that constitute the second component of the LCRD flight segment, they communicate in the Ka wave band. In the uplink direction, the HBRF terminal supports one or two users with a maximum data transmission rate of 32 Mb/s each. On the downlink, the terminal accommodates the transfer from one user with an effective data transfer rate of up to 622 Mb/s; alternatively, the bandwidth may be split, in which case, the transfer rate of the order of 311 Mb/s is allocated to each user. The HBRF terminal forwards combined data packs in either direction: to (return link) or from (forward link) both optical space terminals. Finally, given that the HBRF terminal remains permanently connected to the SSU, it is possible to switch between the transmissions through optical and RF links (NASA 2017, pp. 4, 6–8) with no interruption in communication.

The ground segment of LCRD is composed of two core components – two networked ground stations, i.e. Optical Ground Station 1 – OGS-1 and Optical Ground Station 2 – OGS-2 located in California and Hawaii. The optical ground stations are systems composed of an Optical Telescope Assembly, a Ground Modem, a Coder-Decoder (CODEC), a User Services Gateway (USG), an Atmospheric Channel Monitoring System (ACM) and User Element Simulators (UMS) that comprise a User Mission Operations Center Simulator (User MOC) and a User Platform Simulator (UPS). The differences between OGS-1 and OGS-2 are revealed when their technical architectures are compared in detail. OGS-1 is a 1-meter optical telescope with an adjacent room for transmitting and receiving optics, whereas OGS-2 is installed in an approx. 5.5-metre dome equipped with a 60-cm receive aperture and a 15-cm transmit aperture. The receiving systems of each telescope rely on adaptive optics to collect efficient light at the wavelength of the forward link to a single-mode waveguide, which is subsequently directed to the terrestrial modem and CODEC. Both OGS-1 and OGS-2 utilize the uplink channel (Du et al., 2018) to send a reference beam for the optical space terminal to adjust the pointing direction. The ground modem of the stations modulates the signal on the uplink direction and demodulates it on the downlink, however, while in OGS-1 both Pulse Position Modulation (PPM) and Differential Phase Shift Key (DPSK) modulation is enabled, OGS-2 only enables the latter. Furthermore, as for the coder/decoder function, before modulation, the signal is subjected to Forward Error Correction (FEC) on the uplink and the flight payload data can be integrated (interleaving) with

user service data, if necessary. Upon encoding and interleaving, the data is labelled with a correct logical path identifier (the "unique word") and a physical layer frame. Thus, the prepared uplink data is multiplexed into a single stream and directed to the ground modem. The received return data and payload telemetry data are subsequently decoded by the CODEC on the downlink. Multiple terrestrial users of space infrastructures exchange data with flight payload over a laser link within the user services gateway. User Element Simulators connect to service gates thus enabling data transmission and reception for all services desired by a particular user. The reverse link transmissions are forwarded to particular CODEC channels and distributed on the downlink to User Mission Operations Centers or LMOC. The user services gateways also process protocols for space or terrestrial transport within the provided user service. For presentation and testing purposes, LCRD uses two types of simulators: the User MOC Simulator (UMS) and the User Platform Simulator (UPS). By connecting to the LCRD via USG, the UMS enables the transmission and reception of data via the optical link. It is also an important element from the perspective of planning future services and receiving relevant data, giving a range of prospective possibilities for multiple user applications. The last component of the system is the Atmospheric Channel Monitoring, which collects current weather forecast data for analysis at a specific place and time. Weather observation is a vital element of the infrastructure due to the dangers and other impacts of weather conditions on optical links during experiments. The acquired data will remain available to researchers only for the duration of the system testing period, it can be thus assumed that this component will be withdrawn afterwards. The system will provide data regarding:

- Weather – temperature, humidity, atmospheric pressure, wind velocity and direction;
- Atmospheric transmittance;
- Daytime sky radiance;
- Strength of optical turbulence at the ground layer;
- Atmospheric coherence length during daytime;
- Cloud coverage;
- Atmospheric coherence length along the downlink path (during experiments);
- Downlink signal irradiance.

The radio communication system is the second cardinal component of the terrestrial segment of the laser space communications transmissions. It is composed of the RF Ground Station (RF GS) (Dreischer et al., 2009), a New-Mexico-based operations control center that is a part of the LCRD Mission Operations Center (LMOC) and a Maryland-based LMOC Extension – LMOC-E, i.e. an additional facility for monitoring LCRD operations and experiments. The capabilities and the function of the RF ground station are the same as of CODEC, i.e. it provides the user gateway and simulator (UMS and UPS) in optical space communication laser relay systems, and, therefore, it provides radio communication in support of the same user services and experiments. Numerous auxiliary elements are included in the LCRD RF ground station: antennas, amplifiers, transmitters, receivers and other processing equipment required to combine the LCRD high-frequency data stream with CODEC. A system playing an essential function in coordinating all activities related to safe operation is the LCRD Mission Operations Center (LMOC). Connected via ground networks to all radio and optical stations supporting LCRD missions, LMOC enables integrated mission scheduling, telemetry data acquisition, storage and analysis, centralized monitoring of operations, service management, remote monitoring of ground stations and experimental operations. The LMOC extension will support the LCRD testing process, ensuring at least a suitable level of space communication and security. Its capabilities provide invaluable insight into planning and monitoring of experiment operations, which in turn enables the assessment of the LCRD link performance during testing and analysis

of weather factors and their effect on the system's uninterrupted functioning (NASA, 2017). The diagram below (Figure 2) illustrates the general principle of the system operation and its key elements.

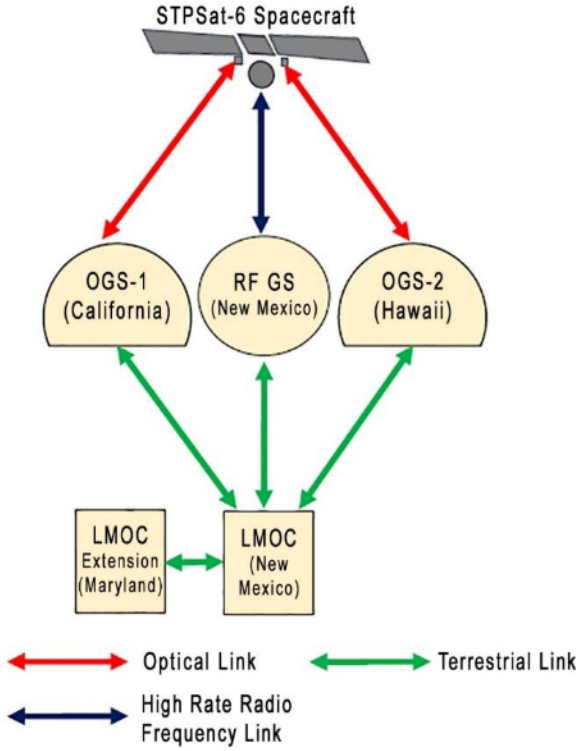


Figure 2. The main architecture of the Laser Communication Relay Demonstration (NASA 2017, p. 6).

Given the presented technical structure of the entire LCRD system, the forecasted purpose of laser communication, the opportunities it creates with respect to improving the current radio-based space communication, the primary objectives of LCRD testing are as follows (NASA 2017, p. 5):

- demonstrating the potential of bidirectional optical communication between the flight segment relay on the GEO orbit and the Earth-bound facilities;
- performance testing of the novelty communication system in various atmospheric or space weather conditions;
- developing operational procedures and evaluating its potential for future space missions;
- laser space communication technology transfer to the space industry (Strauch, 2015);
- ensuring GEO's capability for testing and demonstrating suitable relay standards for optical communication.

The National Aeronautics and Space Administration has planned the first phase of LCRD tests, which are set to last two years (tests to end in 2021). While the tests are expected to verify the points above, the agency has not excluded additional experiments should the need arise. The supplementary tests can be requested by parties involved in the laser communications relay demonstration project or external to it, this includes individuals or institutions from NASA, other government agencies, academia or the space industry. This open approach to testing is dictated by the desire to adapt the functional characteristics of the LCRD program to the needs of various optical communication users.

The laser communication relay demonstration is not the first attempt to replace radio waves with the optical technology in space communication, as the first successfully tested technology was the Lunar Laser Communications Demonstration (LLCD), by the European Space Agency – ESA. The tests confirmed the capability of the solution in question, which provided record data transmission speed over the optical link between the Earth and the LLCD (Lunar Lasercom Space Terminal – LLST) located on the satellite of NASA's Lunar Atmosphere Environment Explorer (LADEE) placed on the lunar orbit. The downlink transmission was shown to handle data at a speed of 622 Mb/s and, in the uplink direction, at a 20 Mb/s rate. The operational capabilities of the LLCD architecture support a range of conditions and multiple ground terminals of various designs and capabilities, limited contact times, energy, as well as thermal and viewing conditions (Khatri et al., 2015).

4. Results from experiments and potential LCRD application case stories

While the use of solutions based on optical techniques in various sectors of telecommunication has been relatively common for years, in space communications, it is an absolute novelty. The provision of space optical communication services to users presents numerous technical challenges related to the development and placement of dedicated infrastructure in the GEO orbit. In addition, it is vital to account for the atmospheric and space weather conditions, which could have a negative effect on the technical devices. Nevertheless, unlike in the case with the conventional radio communication, these conditions will not affect the transmission, reception and storage of data, nor the bandwidth or performance of the optical link. Therefore, prior to becoming fully operative, the laser space communication system will be subjected to various test and experiment scenarios developed with the participation of its future stakeholders. The implemented testing procedure ensures that the system's operational capabilities can be developed along with testing so as to respond to the needs of its various users. At the current stage of development, the optical links are expected to be predominantly utilized by research centers and private businesses involved in the space industry. In this respect, the following part of this section moves on to describe two experiments that could be performed as part of the LCRD testing. The reader should note that the capabilities of the laser space communication relay are by no means limited to scientific and commercial purposes. The laser relay technology will be subjected to a variety of tests aimed to establish a range of its potential applications in space. In the initial stages, the testing objectives are likely to focus on determining the performance rates, thus providing an estimate of the system capabilities and the scope of service that it can provide at the present time. Additional tests will, in turn, serve to set the direction for the future development of the technology with a view to optimizing the optical communication systems and improving the level of service provided. Relay providers will be presented with an opportunity to determine the effectiveness of their pre-developed operational procedures and establish the necessary improvements to be introduced in the future with a view to future full automation of laser space communication system.

The first scenario (Figure 3) concerns providing the service to multiple users. In the diagram, the communication configuration with a space probe via relay providers is given on the left. On the right-hand side, there is the simulated configuration of the LCRD experiment. In this test, OGS-1 employs its UPS to simulate the function of a user spacecraft, exchanging data with one of the on-board space terminals via an optical link. OGS-2 functions as a second user spacecraft. The LCRD flight segment then tracks several simulated objects – spacecraft – with a single relay, exchanging data via radio transmission between the HBRF terminal and the ground station. Due to the great bandwidth, it is capable of supporting up to approximately 20 users and track their space objects with no interference or time delays.

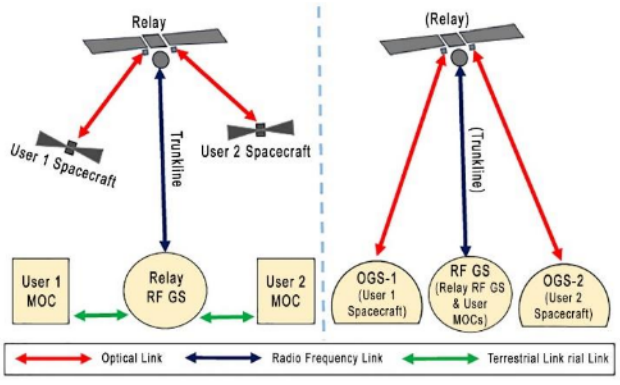


Figure 3. Example LCRD experiment configuration (depicted on the right) to simulate a scenario involving a relay provider supporting multiple user spacecrafts (depicted on the left) (NASA, 2017, p. 18).

The other potential scenario tests the functions important for flight segment relay providers supporting a single user spacecraft

(Figure 4); the simulated activity is the "station handover." The handover is presented on the left side of the diagram: the line connecting the optical terminal to the ground station is transferred between the ground stations. In the experiment (on the right), the RF ground station functions as a relay spacecraft, while the two remaining optical ground stations are free for the station handover. To simulate a user spacecraft, the ground radio station employs its UPS simulator to mock the data package of the links and their exchange with the flight segment using the HBRF terminal. The optical trunkline is established between the LCRD optical space terminal and the OGS-1 station, which also simulates the functions of User MOC. The handover procedure is initiated with the termination of the initial optical trunkline that becomes replaced by a new optical line between the same optical relay in the flight segment and the OGS-2 station. Having formed a new optical link, the OGS-2 station begins to function as a relay optical ground station and the user operations center simulator (User MOC). The use of electromagnetic links in this simulation (Wan et al., 2010) enables relay providers in the flight segment to determine the characteristics of the handover process. The tests could be modified to include a range of other conditions, e.g. a simultaneous transfer of data with multiple users or in the presence of adverse weather conditions – to test the handover process times. The results from the experiments would deliver reliable data enabling providers to calculate how far in advance station operators would need to prepare for station handover. To determine the effectiveness of handover needs prediction, the provider could establish a communication link and subsequently test the capacity for prediction when the connection will be severed by weather conditions (NASA 2017).

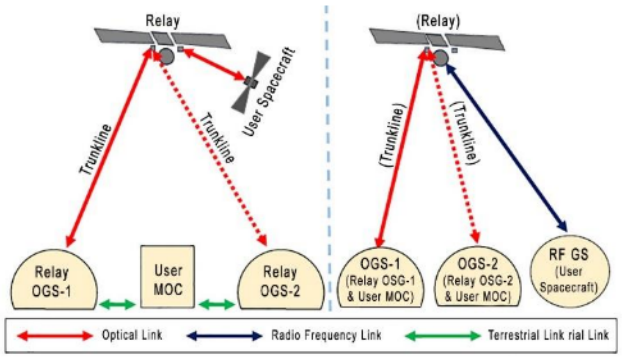


Figure 4. Example LCRD experiment configuration (depicted on the right) to simulate a scenario involving a relay provider executing station handovers (depicted on the left) (NASA, 2017, p. 19).

5. Conclusions

In the text, the Harvard referencing citation style should be used (Smith, 2017) or (Smith, and Bradley, 2017). In the case of more than three authors, write the surname of the first of them and add the abbreviation et al. (Bradley et al., 2017).

Several general conclusions emerge from the presented analysis of existing literature on the subject and the results from the author's own study:

- contemporary technologies providing communication with in-space objects employ the propagation of electromagnetic waves in various frequency bands. Space communication accomplished by radio is divided between three bidirectional networks that are used according to the distance between a given object and the Earth. In its current form and technical capabilities, the conventional communication is largely insufficient with respect to providing effective bidirectional communication with spacecrafts, which is a consequence of a widening gap between advanced space and communication technologies installed on spacecraft or satellites that are incompatible with radio communications;
- in view of the status quo, there emerges a need to replace the bidirectional radio space communications networks,

which appear to be headed for obsolescence, with a new type of communication that exhibits a higher future potential. Optical space communication, which uses a laser beam as an information carrier, is widely regarded to be the most likely successor to radio-based technologies. The laser beam in space communication provides higher bidirectional throughput for both uplink and downlink data, undisrupted communication with objects, lack of time delays and resistance to disturbances, which could result from e.g. space weather;

- optical space communication technical infrastructure will combine components of the existing radio-based systems and laser-beam propagation devices, which is expected to reduce the cost-intensity of the project;
- the development of optical space communication is predominantly aimed to provide technological support to future interplanetary space flight missions, organized by research centers and private enterprises involved in the space industry;
- to ensure that laser communications relay technology is compliant with the needs of various users, it is crucial to perform extensive and comprehensive testing of the entire system, which is currently in progress.

Acknowledgements

This work is financed through funds for scientific activity as part of the research task: Unmanned Aerial Apparatus in Provision of Safety and Security (task number: II.1.25.0).

References

1. Brandt-Pearce, M. and Noshad, M. (2016). Optical transmission. In S.K. Wilson et al. (Eds.), *Academic Press Library in Mobile and Wireless Communications* (pp. 661-687). Amsterdam: Elsevier. DOI: 10.1016/B978-0-12-398281-0.00017-X.
2. Chen, G. *et al.* (2019). Polarization properties of calibration reflector system in the polarization-modulated space laser communication. *Optics Communications*, *430*, pp. 311-317. DOI: 10.1016/j.optcom.2018.06.058.
3. Dreischer, T. *et al.* (2009). Integrated RF-optical TT&C for interplanetary telecomms. *Acta Astronautica*, *65(11-12)*, pp. 1772-1782. DOI: 10.1016/j.actaastro.2009.05.006.
4. Drzewiecki, D. (2015). Geopolitycal conditions of development cartography in safety communications. *Security and Defence Quarterly*, *7(2)*, pp. 49-70. DOI: 10.5604/23008741.1189284.
5. Du, B. *et al.* (2018). Laser communication based on a multi-channel single-photon detector. *Optics Communications*, *426*, pp. 89-93. DOI: 10.1016/j.optcom.2018.05.039.
6. Furch, B., et al. (2002). Optical Communications in Space – a challenge for Europe. *AEU - International Journal of Electronics and Communications*, *56(4)*, pp. 223-231. DOI: 10.1078/1434-8411-54100102.
7. Khatri, F.I. *et al.* (2015). Lunar Laser Communication Demonstration operations architecture. *Acta Astronautica*, *111*, pp. 77-83. DOI: 10.1016/j.actaastro.2015.01.023.
8. NASA (2017). *Laser Communications Relay Demonstration: Introduction for Experimenters*. Greenbelt: NASA.
9. Polkowska, M. (2018). Limitations in the airspace sovereignty of states in connection with space activity. *Security and Defence Quarterly*, *20(3)*, pp. 42-56. DOI: 10.5604/01.3001.0012.5151.
10. Strauch, A. (2015). Still All Quiet on the

Orbital Front? The Slow Proliferation of Anti-Satellite Weapons. *Obrana a Strategie, 14(2)*, pp. 61-72. DOI: 10.3849/1802-7199.14.2014.02.061-072.

11. Wan, L. et al. (2010). On-ground simulation of optical links for free-space laser communications. *Optik*, *121(3)*, pp. 263-267. DOI: 10.1016/j.ijleo.2008.07.002.
12. Wang, R. et al. (2019). Demonstration of horizontal free-space laser communication with the effect of the bandwidth of adaptive optics system. *Optics Communications*, *431*, pp. 167-173. DOI: 10.1016/j.optcom.2018.09.038.
13. Wu, J. et al. (2019). Condition for keeping polarization invariant on propagation in space-to-ground optical communication downlink. *Optics Communications*, *453*, p. 124410. DOI: 10.1016/j.optcom.2019.124410.

SAFETY&DEFENSE
ISSN 2450-551X

The Protection of Individuals in the light of EU Regulation 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data

Mirosław TOKARSKI
Military University of Aviation, Dęblin, Poland;
m.tokarski.mil.pl, ORCID: 0000-0003-1882-668X

DOI: https://doi.org/10.37105/sd.86

Abstract

The process of establishing normative acts in the European Union does not occur out of nowhere, but in the context of specific social needs. That was the case of the genesis of establishing legal regulations regarding the protection of personal data in the European Union. Socio-economic integration, which resulted from the functioning of internal market in the European Union, has led to a significant increase in cross-border transfers of personal data. It led to situation in which various economic operators or state institutions of the Member States have increasingly processed the personal data of the EU citizens. Within time, these data have become an equally valuable commodity - not to say even more valuable – compared to goods and services (Costa-Cabral, and Lynskey Orla, 2017, p. 11). Making use of personal data on a large scale especially by public and private entities, associations and companies over time has posed a threat to the security of personal data. This has made it necessary to introduce legal protection measures for personal data in the European Union that would eliminate the negative effects of any form of personal data processing. The purpose of this article is to evaluate legal regulations regarding legislative protection of personal data in the European Union against the background of EU Regulation 2016/679 of the European Parliament and the Council with respect to the protection of individuals due to processing personal data, its free movement and repealing Directive 95/46/EC (hereinafter referred to as Regulation 2016/679). Due to initially adopted purpose of the considerations there arose a problem which was formulated in the form of a question: Do the legal measures introduced by the Regulation constitute an effective tool for the protection of personal data in the event of a violation of the law by personal data administrators and entities while processing such data? The presented purpose of the considerations and the research problem determined the order of the analysis.

Keywords: Protection, Security, Personal data, European Union.

1. Introduction

Although discrepancies in the protection of personal data in individual countries of the European Union were a natural consequence of state independence and the sovereignty of national legislators, the persistence of such implemented procedures in the long run was a highly undesirable phenomenon. Not only did it weaken the feeling of legal security of natural persons whose data were processed, but above of all, it denoted uncertainty when referred to their legal situation. The meaning to ensure uniformity in the field of personal data security became therefore a value of significant social importance. A member of the European Union had the right to expect proper interpretation and application of regulations in a predictable and equal manner throughout the European Union area. On the other hand, the state authorities were obliged to shape the direction and the content of provisions in such a way that they could be brought as close as possible to the ideal of uniformity and consistency in the field of personal data protection. Therefore, it needs to be stressed that the collection and processing of citizens' personal data by various entities did not use to ensure their security, but often threatened their privacy (Robinson, et al., 2009, p. 1). In this situation, an attempt was made to introduce a stable and coherent framework for the protection of citizens' personal data throughout the Union and the legal mechanisms for its enforcement. This was expressed in Regulation 2016/679. It needs to be noted that according to Article 4 (1) of the Regulation, "personal data" denotes any information related to an identified or identifiable natural person they refer to. On the other hand, protection of personal data was defined as "a set of legal provisions aimed at protecting the rights, freedoms and interests of natural persons whose personal data can be collected, stored, processed, distributed, destroyed, etc." (Dove, 2018, p. 5). In this way, the protection of personal data has become one of the fundamental rights in the European Union. It should be noted that the effectiveness of legal norms in the field of personal data protection and the rights of the subjects is not determined by the mere introduction of normative provisions on personal data protection procedures, but it is also influenced by establishing effective mechanisms towards their enforcement (Pantlin et al., 2018). Even a brief analysis of the Regulation 2016/679 reveals that it plays a key role for people whose personal data are processed by the administrator and entities that further process personal data. It retains the main principles of personal data protection included in the Directive 95/46 / EC of 1995 (Directive, 1995) and it contains corrections referred to obedience and enforcement of these data over the area of the European Union. At this point, it should be clarified that according to the above-mentioned regulation, the "data administrator" is "a natural or legal person, public authority, agency or other body that either single acting or jointly with others determines the purposes and means of processing personal data" (Article 4, Act 7). Conversely, "the processor" means here a natural or legal person, public authority, an entity or other entity that processes personal data on behalf of the administrator (Article 4, Act8). In this context, normative solutions aimed at implementing the rights of citizens to protection of their personal data and the guarantees that processing such data will be carried out in accordance with the law prove to be significantly important. The protection of personal data introduced by the regulation applies to both private and public persons. At the same time, the legal regime of the regulation defined the rights of persons whose data are processed and it imposed obligations on personal data administrators and entities processing such data.

An extremely important solution of the mentioned regulation mentioned above was the introduction of legal protection measures for people whose personal data are being processed. In reference resources, legal measures are defined as: a procedural institution by means of which authorized entities may demand verification of legal status or actions performed in the course of proceedings by the body conducting such procedures (Przybysz, 2020). In that way, legal actions may be taken up by an individual and denote a possibility, not an obligation, to act in order to change the legal situation of a natural person. Such measures may become a tool to defend the interests of an individual; and, as a result, he or she becomes the subject not the object of any actions (Pierzchała, 2013, p. 123). Referring to the term "legal measures" found in Regulation 2016/679, two groups of legal measures can be distinguished where a natural person is entitled to make the use of them against the entity processing his/her personal data: legal protection measures in connection with implementation of operational programs using personal data and administrative legal protection measures in connection with violating personal data regulations. It should be noted that in addition to the indicated legal measures, the EU legislator introduced in its Regulation 2016/679 regulations on the liability of subjects contravening provisions on the protection of personal data. These regulations are further discussed below.

2. Principles of personal data processing

Confronting the legal articles referred to in Regulation 2016/679 with practical experience reveals that normative solutions towards the protection of personal data are increasingly being followed by administrators and subjects that process them. Nevertheless, a lot of controversy has arisen around this issue, concerning the principles of personal data protection and liability for their violations. Since ignorance of them may further lead to the imposition of financial sanctions on the administrator or the subject processing personal the data, it is worth mentioning them in their original form.

According to Art. 5 of the Regulation, the following rules apply to the processing of personal data:

1) processing should be lawful, fair and transparent for the data subject (González-Fuster, 2014, p. 102);
2) collecting data for further processing must result from a specific and legitimate purpose and adequate to it;
3) processing should comprise only up-to-date personal data, whereas outdated data should be deleted or put right;
4) processed personal data should be stored for no longer than it is necessary for the purpose of processing;
5) processing personal data should be secured against accidental loss, destruction or damage by appropriate technical or organizational measures.

The presented rules for the processing of personal data are accepted in related subject literature. As argued, negligence or conscious actions of the subjects during data processing has resulted in negative effects for those whose data had been processed. For this reason, it was necessary to introduce rules securing personal data contained in a data filing system in relation to their automated or manual processing (Comforte AG, 2018, p. 7).

It needs to be clearly emphasized that the right to protect personal data is not an absolute right: it should be perceived in its social function and balanced against other fundamental rights in the context of their proportionality. That results from Art. 89 of the Regulation, which allows for derogation from the main principle of personal data protection due to the need of processing it

for archival purposes in the public interest, scientific, historical or statistical research.

In the field references, it was emphasized that the indicated exceptions are allowed, provided that appropriate technical and organizational safety measures are introduced by the administrator and the subject processing such personal data (Ducato, 2020, p. 5).

It needs to be clarified that these are not the only restrictions on the protection of processed personal data. Namely, personal data protection is excluded from the regulation's jurisdiction due to activity related to national security and the processing of personal data by the Member States based on activities related to common foreign and security policy of the Union. The protection provided by the regulation also excludes personal data processing by a natural person within a purely personal or domestic activity, without any connection with a professional or commercial activity. It needs to be stressed that any personal or domestic activity should be understood as correspondence and the storage of addresses, maintaining social bonds and any Internet activity undertaken towards such activities. However, the provisions of the Regulation may apply to administrators or entities processing personal data if they make the means of processing personal data available either for personal or domestic purposes. In the light of the presented regulations, it can be concluded that the rules on personal data processing are undoubtedly the most prominent example of "federal EU law in the field of personal data security of natural persons (Lenaerts, and. Gutiérrez-Fons, 2010, p. 1631).

3. Subjectively and objective scope of personal data protection

Directive No.14 of Regulation 2016/679 indicates that protection concerning personal data processing should apply to natural persons, regardless of their nationality or place of residence. Also, the provision included in Article 8 Section 1 of the Charter of Fundamental Rights of the European Union (Official Journal, 2012) and Article 16 Section 1 of the Treaty on Functioning of the European Union (Official Journal, 2012) provide that every person has the right to the protection of his/her own personal data. Such legal articles become more significant as they create the principle of equality before the law when referring to personal data protection. It means that all natural persons whose personal data are processed should be treated equally, according to the same measure, without discriminating or favoring differences.

The Directive corresponds to its second counterpart of Regulation 2016/679, which requires that the legal articles on the protection of individuals with regard to processing of their personal data, regardless of their nationality, place of residence should not violate their fundamental rights, freedoms and the right to protection of personal data.

Considering this, actions undertaken by the administrator of personal data and subjects processing them should be conducted in such way so as not to cause negative effects in the sphere concerning the person whose data is processed, provided that he or she is a citizen of the European Union member country.

Directive No. 11 of Regulation 2016/679 states that this is the personal data which become the subject of legal protection with reference to natural persons. It does not apply to all data, but only these which allow identification of a natural person based on his name and surname, identification number, location data, online identifier or just factors determining physical, physiological, genetic, mental, economic, cultural or social identity of that person. In addition, it concerns personal data about the natural person who previously presented it to an administrator.

It should be emphasized that according to Article 4 Point 2 of the Regulation, processing of personal data denotes a wide scope. It either includes one or more operations performed with the use of personal data or personal data sets in an automated or manual manner. The range of processing such data may comprise: collecting, recording, organizing, storing, adapting or modifying, downloading, making use, revealing by sending, circulating or other ways of sharing, adjusting or combining, limiting, deleting or removing personal data.

In terms of the range of its impact, the protection of personal data processing has an extended territorial scope (Dove, 2018, p. 5). It includes activities carried out by the organizational unit of the administrator or the subject processing data within the territory of the Union and outside its borders. Such protection also applies to processing the personal data of people residing in the Union by the administrator or the subject converting information which is not officially established in the EU once the processing activities involve offering goods, services or monitoring their behavior in the territory of the Union. In addition, the protection extends to processing personal data by an administrator which is not established in the Union but in a place where the law of a Member State is applicable under public international law.

4. Legal protection measures related to personal data processing during the implementation of operational programs

Generally, processing personal data during the implementation of operational programs is directed towards original personal data. In order to avoid violating the security of the data mentioned above, the EU legislator allowed for possibility of processing personal deprived of elements which might identify its owner by means of "pseudonymization" or "anonymization". In the light of Article 4 Section 5 of the "pseudonymization" regulation, it is based on the concept of processing personal data in such way that it can no longer be attributed to the data subject without the use of any additional information. By contrast, "anonymization" refers to a technique that removes personal information from certain sets of data. However, if it occurs that following the processing of the data in connection with implementation of operational programs, a security breach has been found, a natural person then has the right to request: access to his personal data and rectification; the deletion or limitation of their processing; the transfer of personal data; an objection claim towards processing of personal data.

1) The right to access and rectify personal data allows for the possibility of posing to the administrator or the subject processing the data the question: what personal data are processed and where were they obtained, what is the purpose of processing, what is its legal basis and how long will the data be processed. Once the processed information is out of date, the person may request to update it.

2) The right to request the deletion or limitation of personal data processing becomes effective when further processing is no longer necessary to achieve the purpose indicated by the administrator or processor, or it was processed against the law. Restricting personal data processing may result in the administrator of personal data or the subject processing data being able to store such information. However, they are not only allowed to transfer data to other subjects, modify or delete it. Restricting the processing of personal data may be also implemented in the event of an objection against data processing until the objection is previously examined.

3) The right to withdraw consent to personal data processing may be implemented at any time, if the basis for data processing is the agreed consent. Withdrawing consent has the effect that current data being processed cannot be considered as an unlawful act. It has been pointed out in the field references that personal data processing may be performed on the basis of the approved consent of the data subject, therefore it is necessary to ensure that he or she makes a deliberate choice when referred to sharing personal data (Rubinstein, 2013, p. 78).

4) The right to transfer the data to another administrator is based on the concept of demanding the transfer of personal data from one administrator who previously owned such data to another appointed owner. The primary purpose of the data transfer regulation is to increase individuals' control over their personal data and to ensure that they play an active role in the data ecosystem (Graef, et al., 2918, p. 1365).

5) The right to file an objection referred to personal data processing becomes effective once the basis for data processing is the performance of the administrator's public tasks or its legitimate interests. The objection should result in ceasing personal data processing by the administrator, unless he/she demonstrates the existence of legitimate grounds for data processing which are superior to the interests, rights and freedoms of the data subject.

The presented legal protection measures in connection with the implementation of operational programs based on the use of personal data are generally available. This translates into possibility of using any of the discussed legal actions by a natural person, regardless his intellectual, physical or financial conditions.

5. Administrative and judicial remedies in connection with violation of the articles referring to personal data protection

As it was already mentioned in the introduction, European Union countries have recorded a massive amount processed personal data, commonly introduced even against the will of the people these data referred to. On the other hand, natural persons have become more and more aware of the use of their personal data for commercial purposes (Robinson et al., 2009, p. 7). In order to meet the needs of the personal data protection of natural persons, the EU legislator introduced Regulation 2016/679 which allowed for legal protection measures of administrative and judicial nature in relation to subjects violating rules on the protection of personal data. It needs to be pointed out that the term "infringement of provisions on personal data" denotes a broad meaning and it includes any action which contradicts the regulation along with the acts which allow for its implementing (Polanowski, and Lasek, 2018).

Thanks to the presented legislative procedure, the natural person whose personal data has been violated has the right to undertake legal protection in the form of: the right to file a complaint addressed to the supervisory body; the right to bring a lawsuit against a supervisory authority; the right to file a claim in court against the administrator or processing subject; the right to compensation.

1) The right to file a complaint addressed to the supervisory authority, in accordance with Art. 77 of the Regulation 2016/679 is allowed to any person in the Member State of his residence, place of work or place of committing the infringement, if he decides that processing his/her personal data is in conflict with the regulation discussed. It should be clarified that in the light of

Article 4 Point 21, the "supervisory authority" has the status of an independent public authority established by the Member State to protect fundamental rights and freedoms of natural persons with regard to personal data processing. Such a provision imposes an obligation on the supervisory body to inform the person making the complainant about the progress and effects on the examined case.

2) The right to legal protection in a court against a supervisory authority, in accordance with Art. 78 of Regulation 2016/679 is offered to any natural or legal person against the decision of the supervisory authority that concerns him. The right becomes effective in a situation where the supervisory authority has not dealt with the complaint or the petitioner has not been informed within a three month period about the progress or effects of his complaint, and the processing of personal data is still in conflict with the regulation. Proceedings against a supervisory authority shall be brought before the court of the Member State where the supervisory authority is established.

3) The right to legal protection before a court against the administrator or processor in accordance with Article 79 of Regulation 2016/679 is possessed by every data subject if he/she considers that his/her rights have been violated as a result of personal data processing. According to this regulation, proceedings taken up against the administrator or the personal data processor are initiated before the court of the Member State in which the administrator or the processor is established. It should be emphasized that the provision of Article 79 of Regulation 2016/679 also allows for the initiation of proceedings in the court of the Member State in which the aggrieved party is residing, unless the administrator or the processor are public authorities of the Member State using their powers.

4) Every natural person is entitled to compensation based on Article 82 of Regulation 2016/679, if he/she has suffered material or non-material damage as a result of violation of rules referred to personal data protection. The right to compensation is effective in the event of any loss suffered caused by the administrator or the data processor. According to this regulation, every administrator involved in the processing is liable for the loss caused by the processing. On the other hand, the processor is liable for any losses caused by processing only when obligations related to data processing were not fulfilled or he/she acted in way that is contrary to the instructions issued by the administrator. However, either the administrator or processing information entity shall be released from liability once they prove that they were not at fault for the circumstances that led to its initiation. When it occurs that more than one administrator or processor is involved in the processing of personal information, then all the sites involved become jointly and severally liable for the entire loss. If the administrator or the personal data subject has paid compensation for the entire damage caused, he has the right to request from the other administrators or processors who participated in the same processing scheme, partial compensation corresponding to the part of the damage the subjects were responsible for. Actions taken up for damages are sent to a court in a particular Member State.

It needs to be stressed that the starting point for any application of the presented legal protection measures was the specification of the subject of personal data protection and its scope in Regulation 2016/679. Providing the protection of personal data with a normative character has resulted in the possibility of introducing specific measures aimed at enforcing the lawful actions of administrators and entities processing personal data. They were

manifested in legal protection measures of an administrative and judicial nature in connection with the violation of the provisions on personal data. In this way, a natural person who has suffered a breach of his own personal data can effectively oppose entities that have violated the provisions on the protection of personal data.

6. Administrative fines

The Article No. 83 of the Regulation introduced a procedure for imposing administrative fines by the supervisory authority in the event of a breach of personal data security by the administrator or the data processing entity. He/she needs to bear in mind that Regulation 2016/679 does not apply to the processing information considered as anonymous, but only data relating to a specific natural person (Lindgren, 2015, p. 241). Moreover, the quoted regulation is ineffective against data which were previously agreed on for further processing by given consent of its owner.

However, if the processing of personal data is based on invalid consent, there is no legal basis for their processing by any entity (Helberger et al., 2917, p. 25). In consequence, illegal activity will result in imposing an obligation to pay an administrative fine. According to the Directive 2016/679, the administrative fee should be effective, proportionate and it should discourage from further infringement of violating the regulation.

According to Article 83 Section 2 of the Regulation, the administrative fine imposed may be independent or combined with legal measures taken by a supervisory authority against the administrator or data processing subject in the form of:

1) warning about the possible breach of personal data security during processing;
2) ordering the fulfillment of the data subject's request;
3) reminders in the event of violation of legal articles on data processing;
4) ordering the adjustment of the processed data to applicable legal articles;
5) ordering the administrator to notify the data subject about a breach of data protection;
6) introduce temporary or total restriction towards data processing, including given prohibition;
7) ordering the rectification, deletion of personal data, restriction of further processing and notification of these actions to recipients whose personal data have been revealed;
8) withdrawal of certification or ordering the certifying subject to withdraw certification or not to grant certification if the requirements are not met or they are no longer fulfilled;
9) ordering the suspension of data flow to a recipient in a third country or to an international organization.

The presented set of legal measures reveals that neglecting duties through unlawful data processing can be very severe. In the light of Article 83 Section 2 of the discussed Regulation, administrative fines may be imposed taking into account:

1) the nature, weight and duration of the violation, number of people who suffered the situation and the extent of the loss;
2) intentional or unintentional nature of the violation;
3) actions taken by the administrator or processor to minimize the loss suffered by the data subjects;
4) the degree of responsibility of the administrator or the subject processing personal data;
5) identified previous violations on the side of the administrator or the subject processing personal data.

Moreover, according to the applicable procedure, when imposing an administrative fine, a supervisory authority is obliged to take into account the following:

1) the degree of cooperation with the supervisory authority in order to remove violation and alleviate its possible negative effects;
2) categories of the personal data the violation concerned;
3) the way the supervisory authority learned about the breach;
4) financial benefits gained directly or indirectly in connection with the breach of personal data security.

It should be noted that according to Article 83 Section 2 of Regulation 2016/679 also specifies the method of imposing the amount of an administrative fine. Based on that article, once an administrator or subject processing data intentionally or unintentionally infringes a few of the articles of this Regulation in the processing operation, the total amount of administrative fine may amount to EUR 20 million. Imposed financial sanctions for any indicated violations are deliberate. The lowest fine is equal up to EUR 10 million or 2% of the total annual turnover of the previous financial year and it applies to infringements of the provisions related to: obligations of the administrator and the subject processing the data, obligations of the certifying subject, obligations of the monitoring subject. In that case, the prerequisite for applying a penalty is administrative inconsistency, which is treated less severely than any direct violation of the privacy of the data subjects.

On the other hand, violation of the articles which might concern: basic principles of processing, including the conditions of consent, the rights of data subjects, the transfer of personal data to a recipient in a third country or an international organization, non-compliance with an order, temporary or final limitation of processing or suspension of data flow ordered by supervisory authorities – this all allows for imposing an administrative fine up to EUR 20,000,000. In the case of a company, it may amount up to 4% of its total annual worldwide turnover based on previous financial year record, however it is the higher one which is usually taken into consideration.

In the event of non-compliance with the order stated by a supervisory authority, an administrative fine is imposed at the amount of up to EUR 20,000,000, and referred to a company – it equals up to 4% of its total annual worldwide turnover based on the previous financial year's records, and it is the higher amount which is applied.

On the basis of the presented procedure of imposing administrative fines, there is no doubt that the protection of data of natural persons to whom they refer (Comforte AG, 2018, p. 1) becomes effective, as it provides for direct interference in the event of a violation of the articles of Regulation 2016/679. In that meaning, a personal data protection instrument aims at shaping the manner of using personal data by various types of entities in accordance with standards set by the EU legislator for all countries within the European Union.

It should be added that in a situation where the legal system of a Member State does not provide imposing administrative fines, then in accordance with the discussed regulation, application of the fine is requested by a competent supervisory authority and it is imposed by a competent state court. In that case, the same principle is applied which means that the imposed fine on the perpetrator must be effective, proportionate and dissuasive - against further violation of the law on personal data protection.

7. Conclusions

Summing up, this article focuses on the assessment of legal protection measures for personal data in the European Union against the background of Regulation (EU) 2016/679 of the European Parliament and of the Council. The conducted analysis allows for concluding that the problem formulated

in the form of a question: Do the legal measures introduced by the regulation constitute an effective tool towards protection of personal data in the event of violation the law by personal data administrators and other subjects during processing of such data and whether it has been positively solved.

First of all, referring to the problem question, it needs to express an opinion that the point of intersection between protection of personal data and legal regulations concerning legal protection measures enclosed within Regulation 2016/679 coincides with social expectations of the European Union citizens. In that way, the law goes beyond theoretical assumptions and is part of the procedural approach which assumes that enforcement is autonomous and independent of the will of administrators and other legal subjects regarding protection of personal data.

The model of administrative or judicial proceedings against subjects violating the articles referred to personal data protection is based on the assumption that there is a need to synchronize the procedures preventing violations of the law in all countries which are members of the European Union. In this context, it needs to be stated that specificity of the principles contained in Regulation 2016/679 makes that the incorporated system of personal data protection of natural persons is stable. In addition, it constitutes a detailed regulatory system that forces personal data administrators and subjects using such information to apply lawful practices in the field of personal data processing.

Thanks to provisions of Regulation 2016/679, processing personal data is based on a voluntary consent of the data owner. Thus, it enables eliminating consent to further data processing in an insidious manner. For example, it may be achieved by forcing confirmation of the addressee consent on the Internet system using the phrase "I agree" appearing on the computer screen, without the possibility of familiarizing with the content of the offer or advertisement. As a consequence of the agreed solutions, voluntary consent to processing personal data is required, which cannot be rescinded by the data processor itself (Hoofnagle, et al., 2019, p. 86). Thus, the personal data protection measures introduced by Regulation 2016/679 become an effective tool to fight entities violating its articles in a stateless sense. First of all, it has led to eliminating any normative gaps in the existing legal systems of the Member States in the field of personal data protection. Thanks to such kind of solution, there is coherence in the legal system in the field of personal data protection among the European Union member states. At the same time, the principles introduced constitute the basis for interpretation of provisions referred to protection of personal data contained in the regulation. Moreover, they enable us to refer to legal regulations based on articles regarding the prevention of unlawful acts of personal data processing when using legal remedies.

Providing a catalogue of legal measures in Regulation 2016/679 aimed at protection of personal data referring to natural persons in a situation in which a personal data administrator or any other subject processes information against legally binding articles is an extremely important normative solution. In that way, each natural person, in order to avoid the negative effects of unlawful data processing, may effectively demand that further processing to be stopped or demand that his/her identifying features be removed.

References

1. Charter of fundamental rights of the European Union (Official Journal of the European Union (C 326/391, 26.10.2012).
2. Costa-Cabral, F., Lynskey, O. (2017). Family ties: the intersection between

data protection and competition in EU Law. Common Market Law Review, Kluwer Law International, Available online http://eprints.lse.ac.uk/68470/.
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281, 23/11/1995).
4. Dove, E.S. (2018) The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era, *Journal of Law*, 46(4). pp. 1013-1030. DOI: 10.1177/1073110518822003
5. Ducato, R. (2020). Data protection, scientific research, and the role of information, *Computer Law & Security Review*, 37.DOI: https://doi.org/10.1016/j.clsr.2020.105412
6. González-Fuster, G. (2014) How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection, *IDP Revista de Internet Derecho y Política*, 19. DOI: 10.7238/idp.voi19.2424
7. Graef, I., Husovec M., Purtova N. (2018), Data Portability and Data Control: Lessons for an Emerging Concept in EU Law. *German Law Jurnal,* 19(6). DOI:https://doi.org/10.1017/S2071832200023075
8. Helberger, N., and Borgesius, F.Z. and Reyna, A. (2017), The perfect match? a closer look at the relationship between EU consumer law and data protection law, Commo*n Market Law Review*, 54(5).
9. Hoofnagle, Ch.J., and van der Sloot, B. and Borgesius, F.Z. (2019) The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28, pp. 65-98, Published online: 10 Feb 2019. DOI:10.1080/13600834.2019.1573501.
10. Lenaerts, K., and Gutiérrez-Fons J.A. (2010). The constitutional allocation of powers and general principles of EU law. Powers and general principles, *Common Market Law Review*, 47, pp 1629-1669.
11. Lindgren, P. (2016). GDPR Regulation Impact on Different Business Models and Businesses, *Journal of Multi Business Model Innovation and Technology*, 4(3). DOI: 10.13052/jmbmit2245-456X.434
12. Pantlin, N., Wiseman, C., Everett, M. (2018). Supply chain arrangements: The ABC to GDPR compliance - A spotlight on emerging market practice in supplier contracts in light of the GDPR*, Computer Law & Security Review*,34(4). DOI: https://doi.org/10.1016/j.clsr.2018.06.009
13. Pierzchała, E. (2013). *Standardy funkcjonowania administracyjnych środków prawnych w postępowaniu przed organami pomocy społecznej,* Wrocław: Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.
14. Polanowski, A. and Lasek, Ł. (2018), *Private enforcement under the GDPR*, newtech.law., https://translate.google.com/translate?hl=pl&sl=en&tl=pl&u=newtech.law (Access 2018.07.10).
15. Przybysz, P.M. (2012). Administracyjne środki prawne w postępowaniu egzekucyjnym w administracji, https://sip.lex.pl/komentarze-i-publikcje/monografie/administracyjne-środki-prawne-w-postepowaniu-egzekucyjnym-w-369243969 (Access 14.07.2020).
16. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Official Journal of the European Union L 119/1, 4.5.2016).
17. Robinson, N., Graux H., Botterman M., Valeri L. (2009*), Review of the European*

Data Protection Directive, RAND Corporation - Office of the Information Commissioner.
18. Rubinstein, I., Big Data: The End of Privacy or a New Beginning? (October 5, 2012). International Data Privacy Law (2013 Forthcoming), NYU School of Law, *Public Law Research Paper*, 12-56, Available at SSRN: https://ssrn.com/abstract=2157659 or http://dx.doi.org/10.2139/ssrn.2157659 Treaty on the Functioning of the European Union (Official Journal C 326, 26/10/2012, P. 0001 – 0390).
19. Three Key Risks and Opportunities of GDPR (2018), Comforte AG. https://www.comforte.com/resources-detail/news/whitepaper-three-key-risks-opportunities-of-gdpr/. (Access 20.08.2020).

SAFETY&DEFENSE
ISSN 2450-551X

Protection of Air Transport Against Acts of Unlawful Interference – What's Next?

Jacek NOWAK[1*], Jerzy ACHIMOWICZ[2], Krzysztof OGONOWSKI[3], Rafał BIERNACKI[4]

[1] Military University of Aviation, Dęblin, Poland; e-mail: jacek.nowak@law.mil.pl, ORCID: 0000-0002-4621-6670
[2] Independent researcher, Warsaw, Poland; e-mail: jachimow@gmail.com, ORCID: 0000-0001-6949-4051
[3] Military University of Aviation; Dęblin, Poland e-mail: k.ogonowski@law.mil.pl, ORCID: 0000-0002-6075-4571
[4] Lublin Airport, Lublin, Poland; e-mail: pyton9@op.pl, ORCID: 0000-0002-4004-4556
* Corresponding author

DOI: https://doi.org/10.37105/sd.89

Abstract

Air transport consists in moving people or goods by air. Aircrafts, known as the main means of air transport, can be divided into two categories: airplanes and helicopters. Such transport is the most modern and the most dynamically developing branch of transport. It is also considered to be the safest mode of transport, even though, for various reasons, aviation accidents still occur.
Security in aviation has various connotations. According to the International Civil Aviation Organization (ICAO), it is a state in which the possibility of damage to persons or property is minimized and is maintained as part of a continuous process of hazard identification and safety risk management at an acceptable level or below this acceptable level. Aviation security includes flight safety and aviation security against acts of unlawful interference. There is a significant difference between the meaning of "safety" and "security". The first of these concepts means preventing unintentional damage, while the second refers to the procedures undertaken in order to prevent deliberate damage resulting from an intentional act.

As it appears from the abovementioned information, the immovable part of aviation safety is aircraft protection, including the protection of civilian airports.
The aim of the article is to draw attention to the problems of air transport security, including the security of airports, related to the evolution of threats and the functioning of the airport security system.
The problem that the authors address is expressed in a question: in what directions should the current solutions in the field of air transport security be improved in order to effectively prevent acts of unlawful interference in the future?
Theoretical research methods, such as the analysis and synthesis of information contained in literature and source materials, inference, comparison, were used to develop the article.

Keywords: air transport, security, airport, security systems, technical security measures.

1. Introduction

It is widely believed that general aviation is one of the safest means of transport. The sense of security is quite relative, largely dependent on subjective feelings and difficult to describe in terms of procedures that ensure it.

Aviation safety has numerous connotations. According to the International Civil Aviation Organization (ICAO), it is a state in which the possibility of damage to persons or property is minimized and is maintained as part of a continuous process of identifying threats and managing safety risks at or below an acceptable level. More effective laws and procedures, resulting in a reduction of the number of incidents, increase the sense of security and, as a result, raise the number of passengers. This simple mental observation has become the basis of many efforts taken by airline companies, both those to deal with the transport of passengers and those to deal with the transport of goods. It also became the basis for research and analyses.

Aviation safety covers the problems of flight safety and aviation security against acts of unlawful interference. There is a significant difference in meaning between "safety" and "security". The first of these terms means avoiding unintentional damage, while the second means avoiding intentional and culpable damage.

The aim of the article is to draw attention to the problems of air transport security, including the security of airports, related to the evolution of threats and the functioning of the airport security system.

The problem that its authors want to highlight is expressed by the question: in what directions should the current solutions in the field of air transport security be improved in order to effectively prevent acts of unlawful interference in the future?

The authors of this article make the following assumption: the protection of aircrafts and airports should be viewed in a systemic way. This means that the authorities, ministries and state services that can provide information about a potential threat and be used to naturalize it, should operate in one coherent system dedicated to civil aviation security, according to previously established rules. Currently, the protection of airports should be dynamic, maneuverable and related to the protection of its operational zone.

The theoretical research methods, such as analysis and synthesis of information

contained in the literature and source materials, inference and comparison, were used to develop this article.
An important source of information for the authors of this article come from the participation in anti-terrorist exercises at Chopin Airport in Warsaw.

2. Protection of air transport and its contemporary threats

Security in the light of Annex 17 to the Chicago Convention is understood as a combination of measures, and human and material resources intended to protect international civil aviation against acts of unlawful interference. In the traditional approach, the security of civil aviation against acts of unlawful interference is to prevent sneaking objects and dangerous materials onboard which pose a threat to the safety of passengers and aviation infrastructure. The issues related to the protection of civil aviation are particularly visible at an airport. The infiltration of people and hazardous materials onto the grounds of the airport results from a breach in the protection system, which is highly unlikely, especially in the Member States of the European Union, where high common standards for the protection of airports are established. They are related to the applied procedures, training and technical devices used by the security services of the airport.

As a phenomenon, terrorism is still increasing in terms of its impact and the use of modern technological solutions. This characteristics is due to its ideas that do not follow any legal standards of the civilized world and which is constantly changing to awe and raise fear in the increasingly immunized society.

Currently, the Acts of Unlawful Interference in civil aviation are actions or attempts to undertake measures that threaten the safety of civil aviation, including, among others (Annex 17 to the Convention on International Civil Aviation, 1974):

- unlawful seizure of aircraft;
- destruction of aircraft in use;
- hostage-taking on board an aircraft or at airports;
- seizure of an aircraft, unlawful interference on the premises of an airport or an airport facility;
- bringing on board the aircraft or onto the airport area a weapon or a dangerous device or a material used for criminal purposes;
- using an aircraft during its operation in order to cause death, serious injury or serious damage to property or the environment;
- transfer of incorrect information aimed to endanger an aircraft during a flight or on the ground, including its passengers, crew, ground staff or the general public, at the airport or an aviation facility.

Taking into account the adopted solutions with regard to the protection of civil aviation, traditional hijacking of an aircraft appears to be extremely difficult (Evans, 1969). Nowadays attempted acts of unlawful interference, either at the airport or in its proximity, are most likely to occur.

Currently, there is no need for criminal groups to physically infiltrate the system of airport security. The same effects can be achieved by using, for example, the so-called cyberspace, or open space of communication via computers and computer memories operating worldwide. The widespread storage of information in computer systems turns cyberspace into an interesting target for possible terrorist operations. Thus, it is possible to effectively manipulate the information, or even generate fake information, which threatens the security of civil aviation.

It should be assumed that terrorists will also take action in the so-called operational sector of the airport. This is understood by airport facilities and the surrounding area, in which airport services and other entities provide assistance to an endangered aircraft within the of radius 8,000 m - in the case of a certified airport, and 3,000 m - in

the case of an airport with limited certification or an airport for exclusive use - from the airport reference point. This is a vast space, giving considerable freedom of action for possible terrorist groups. In the operational zone of the airport, various assets may be used as acts of unlawful interference, e.g. small arms, man-portable air defense systems, wide-area mines and unmanned aerial vehicles.

Another threat, known for centuries, is also worth mentioning, namely the war.

In the classic approach, warfare is understood as the use of military force in international relations against the territorial integrity and political independence of other countries. The nature of warfare is changing and the so-called hybrid warfare has the potential to change a quite stable country into an arena of the most intense armed conflict within a few months, if not days. The role of political, economic, information operations as well as the role of mobile military formations operating in a uniform information space is on the increase. The combination of conventional operations ranges from guerrilla operations (diversion, sabotage, terrorist acts) to operations in cyberspace and exerting economic pressure. It is increasingly difficult to separate war from terrorism and in the military aspect, the phenomenon of war is losing its exclusive national character.

3. Airport – a specific protected facility

The airport is a network of interrelated elements, forming a coherent and harmonious structure. Above all, it is characterized by complexity and a multi-level character. It consists of such elements as a passenger terminal, control tower, radio equipment, runways, depots, parking lots and access roads surrounding the airport area. In general, the airport can be divided into two areas:

- airside - an area where aircraft are handled and air operations are executed,
- landside - an area designed for passenger traffic (Compa, 2013).

When using the airport services, in the first place, we enter the terminal. This is the facility connecting the general public sector with the airport area. It is primarily intended to handle passengers. It is composed of specially detached airport buildings, providing service for passengers. On the grounds, there are restaurants, cafes, shops and other services. In terminals, there are also different types of recreation places, VIP zones and facilities for children. Terminals fall under two categories: domestic and international.

Domestic terminals are much smaller in size compared to the international ones, due to the fact that international terminals require additional space for arranging check-in and customs clearance as well as passport control. In addition, there are duty-free shops here. Bigger airports, due to a large flow of passengers and goods, have got several terminals divided by category, for example the way it is organized at Fryderyk Chopin Airport in Warsaw. It should be noted that most European countries and several non-European countries belong to the Schengen Area. This is the area where there is no border control at the internal borders within this area. Therefore, it was necessary to create separate areas: Schengen Area and Non-Schengen Area. In the "Schengen Area" passengers cross the generally available and restricted border zone without the necessity of going through a passport control. On the other hand, in the Non-Schengen Area each passenger is obliged to pass through the border crossing and undergo passport control.

Another important element facilitating the use of airport services is parking lots. Travelers beginning a longer trip can use a car park adjacent to an airport. They are usually paid as well as fenced, with 24/7 protection, and are located close to a terminal.

In the operational zone of an airport, aprons (Chicago Convention, 1944) are designated for various types of aircraft. The apron is a separate area at the airport tarmac for aircraft parking. Aprons are provided for passengers getting on and off a plane, loading and offloading of cargo, luggage or mail as well as aircraft servicing. The overall dimensions of an apron area are determined by the size of the airplanes expected to serve the aerodrome and to permit expeditious handling of airplane movements and the volume of traffic anticipated for the aerodrome. The dimensions of an apron are adapted to the aircraft size (min. wingspan) and derive directly from the airport reference code.

In addition, based on ICAO Annex 14, it is necessary to enclose an isolated apron, which might have become the subject of an act of unlawful interference, or due to other reasons it is necessary to isolate the aircraft from the normal activities of the airport. The apron should possibly be in the most remote part of the airport, no closer than 100 m from other parking positions, buildings or the general public area. It is also important that the apron location does not interfere with the aerodrome systems of supply installations such as gas, fuel, energy or telecommunications (Annex 14 to the Convention on International Civil Aviation, 1974).

Every modern airport possesses radio technical devices. These devices facilitate and enable the aircraft to perform flight operations. They indicate the parameters necessary for the proper performance of take-offs or landings especially in conditions of limited visibility. The devices need to be certified and are subject to periodic tests on the ground and in the air. They must have a continuous energy supply so as not to disrupt the continuity of their operation. Radio technical devices include radio navigation aids, radars and radio communication equipment.

The air traffic control tower is an important part of the airport. Its main function is to control the area of an airport and its airspace, as well as issuing commands and instructions relating to performed flight operations. It is usually a high structure towering over airport buildings, and also equipped with a glazed observation point, which enables an observation of aircraft maneuvers. The large international airports, air traffic control towers are open 24/7. Moreover, they are manned by several air traffic controllers, including technical maintenance and support personnel. They receive all the necessary information to be provided to pilots, including meteorological conditions, disruptions at the airport, delays and any other circumstances that affect the ability to perform procedures of flight operations. In addition, information is provided on the condition and suitability of navigation aids and lighting.

An integral part of an airport is various types of airport warehouses, composed of building complexes, halls localized at the airport or outside. In practice, larger airports make investments not just in ordinary warehouses, but in modern logistics centers that meet the requirements of the 21st century. In this way, the logistics center for Krakow Balice Airport was created, named The Krakow Airport Logistics Centre, localized approximately seven kilometers from the airport. These buildings are designed for the storage and distribution of cargo and light production, sharing regular warehouse space or one that is equipped with offices and social areas.

The warehouses located on the grounds of the airport additionally offer comprehensive services with regard to air cargo handling at the international airport. This service includes warehouse temporary storage and inspection of cargo safety (The service of conducting safety inspections is possible after the granting of Regulated Agent status by the Civil Aviation Authority (Regulation (EC) No 300/2008).

The additional elements of the airport infrastructure are all types of systems responsible for the functioning of the facility from the purely technical side, i.e. mainly such issues as the energy supply, sanitary and IT systems.

The energy system can be compared to the bloodstream of a living organism. All machines, equipment, light conveyor belts, navigational aids, alarm systems, monitoring systems and other are dependent on an energy supply. The system is vitally important since the quality of the electricity supply affects the security of the entire airport area. When designing the airport, it is important to ensure that the sources of energy supply are checked. Typically, several sources of energy are used for an uninterrupted power supply. The system should also be provided with an alternate power supply to ensure a safe execution of air operations and to transfer information both for pilots and airport workers, in the event of a failure. Power units which generate energy from the combustion of fuels or from alternative sources of renewable energy, such as solar or wind power are exploited for this purpose. Due to the significance of this system, it is necessary to use special protection, which minimize the risk for unwanted interference of third parties. The buildings contain the devices responsible for the transfer of energy are encoded. The power cables used for the delivery of energy to different parts of the airport are located underground, under the tarmac.

It is difficult to imagine the operation of an airport without any computer system or the use of network technology. The reliance on information technology has good and bad sides. On the one hand, it allows efficient management, on the other hand, the so-called cyberspace is the interest of criminal groups and even rogue states which are hostile to western democracy. The protection of airports also entails the protection of cyberspace that these ports use.

The qualities that may expose an airport to a terrorist attack include the following:

- a large area, which is extremely difficult to isolate and control;
- a large number of personnel;
- a massive flow of people and baggage from different destinations, steady and high concentration of people;
- dependence of air traffic safety on technology, safety equipment and power supply;
- storage of a massive amount of explosives and easiness of planting an explosive in the landside, which can be reached without passing through any control.

4. Airport security system

Rankings state that the largest airport in the world is King Fahd airport located in Saudi Arabia near the city of Ad-Dammam. The airport in question was built on a grand scale. It has a four-kilometer long runway and seven terminals (including one luxury Royal Terminal, designed to handle the Saudi royal family and their guests). The airport complex houses a mosque that can accommodate even two thousand worshippers. The airport comprises an astonishing 780 hectares surface area (Kubisa, 2017). By comparison, the surface area of London Heathrow Airport equals 1227 hectares and the largest Polish national airport Okęcie is an area of approximately 830 hectares. There is only one conclusion - the area that needs to be protected is vast and the task should be approached best through the prism of a security system.

One of the definitions describes the system as a deliberately defined set of elements and a set of linkages among them, which together determine the characteristics as a whole. Defining the system consists in extracting the elements of the system environment, significant couplings between system components and relevant system feedbacks with all its surroundings (Sillitto et al., 2017). The system of airport security is a deliberate link between the human being and technical assets.

Ensuring airport security is mostly the responsibility of Airport Security (Guard) Services. This security also comprises Border Guard, Police, Customs Service and the

operational services of the airport. The protection system is designed to prevent any act of unlawful interference on its territory.

The organization and functioning of the protection system of individual airports in Poland results from the implementation of the rules of international aviation law, including that of the EU, into national documents. One should bear in mind that the indicated documents are updated from time to time.

In the system of airport security, the following subsystems can be observed:

- the legal and organizational subsystem, including the division of an airport into zones;
- the technical subsystem;
- the subsystem of the security service personnel and other.

5. The legal and organizational subsystem

It is created by laws relating to civil aviation security, and their effects, namely issues relating to the organization of this protection. The records of these documents also enable a clear understanding of the basic concepts related to the protection of civil aviation. The following international documents are worth mentioning:

- The Annex 17 to the Convention on International Civil Aviation, "Protection of international civil aviation against acts of unlawful interference";
- Regulation of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002;
- Commission Regulation (EU) no 18/2010 of 8 January 2010, amending Regulation (EC) No 300/2008 of the European Parliament and of the Council as far as specifications for national quality control programmed in the field of civil aviation security;

The national documents include:

- Aviation Law Act of 2002, Part IX. Aviation Security;
- Regulation of the Minister of Transport, Construction and Maritime Economy of 31 July 2012. On the National Civil Aviation Security Program (Annex to the notice of the Minister of Infrastructure of 6 March 2018. / Item 631/);
- Regulation of the Minister of Transport, Construction and Maritime Economy of 25 July 2013 on the National Quality Control Program in the field of civil aviation security (Appendix to the notice of the Minister of Infrastructure and Construction dated 25 August 2016/ item 1497/);
- Regulation of the Minister of Transport, Construction and Maritime Economy of 20 September 2013 on the National Training Program in the field of civil aviation security (Appendix to the notice of the Minister of Infrastructure and Construction dated 27 October 2016/ item 1852/).

At the level of an airport, a program and a protection plan are developed, which obviously are classified documents.

The overall organization of protection at an airport is imposed by the National Civil Aviation Security Program. The contents of this document are the implementation of ICAO and EU documents, relating to civil aviation security.

Chapter 1 "General provisions" of this document indicates which institutions are to cooperate with each other in the implementation of the provisions of this document. In the opinion of the authors' team, this is a good solution because this cooperation is essential in the dynamically changing security environment

This article presents only some of the provisions of this document, those which are the most visible to people who use airport services. First of all, when entering the premises of an airport, a division into zones can be noticed, i.e.:

- (landslide) the general open public area, which is not part of the operational part of the airport;
- (airside) the operational part of the airport, which refers to the movement area of an airport, adjacent terrain and buildings or portions, to which access is restricted;
- security restricted area, which refers to the airside where, apart from restricted access, also other aviation security norms are applied;

The boundary between landside and airside shall be a physical obstruction that is clearly visible to the general public and which denies a person unauthorized access.

6. Security bodies (services) at airports

Polish Act of 22 August 1997 on the protection of people and property describes an airport as an area, an important object in the protection of economic interests of the state (Ustawa o ochronie osób i mienia, 1997). In accordance with the legislator, apart from the use of technical security assets, physical security in the form of Internal Security Services or Professional Uniformed Security Formations will also be used to protect an airport. These two forms constitute the Airport Security Service (ASS). The established service is the managing airport body, constituting the Internal Security Services and operating under the authorization of the competent Provincial Police Commander. In the event that it is outsourced to a business entity that provides services for the airport, as a Specialist Uniformed Security Formation, it must have an adequate concession, which specifies the scope and form of the provided services. Regardless of the type of organizations that can create ASS, they are composed of employees which are registered on a list of well-qualified security personnel (Biernacki, 2014).

ASS performs the following tasks in the field of airport management:

- conducting security check-ups;
- conducting access control to airport restricted areas;
- inspecting passes issued by the airport manager;
- detention and handover of a person (passenger) breaching the safety conditions at the airport to the Police or Border Guard.

By 15 January 2011, Border Guard was responsible for conducting security checks of passengers in domestic flights at Chopin Airport. After this period, this task was taken over by the Airport Security Service.

Other services which are involved in the protection of the airport are the Police, Border Guard and Customs Service. Due to the authorities possessed by the ASS, the service which in an emergency situation is linked with airport security, must cooperate closely with the ASS.

Compliance with stringent norms of airport security make the penetration of people and hazardous materials into the restricted airport area,[1] extremely difficult. The airport security system should prevent such cases. It needs to be remembered, however, that humans are the inherent component of this system - security guard personnel who can commit an error.

Human error is an integral part of human nature, and it cannot be "eradicated." Professor James Reason stated that an error occurs in a situation, in which an undertaken action or an accepted way of thinking have not led to the intended result.

The most common types of errors committed by people arise from:

[1] The security restricted area refers to the operational airport zone, in which, apart from a restricted access, other aviation security norms are also applied.

- an undetected stimulus and lack of response;
- no reaction despite a detection of a stimulus;
- improper identification of a stimulus;
- abnormal response to a stimulus;
- making a wrong decision;
- delayed decision (with a deficit of time) about an action.

The fight against human errors is possible due to an optimal protection strategy, which should be based on a specific sequence of barriers which constitute: an effective system of training and quality, trained staff, information about threats and execution of tasks in accordance with procedures and quality control in the field of civil aviation security.

If humans, in the airport security system, commit an error, they will act inappropriately in such a situation. His action will cause a situation of unlawful interference, although avoiding such a situation was possible. As a rule, in such a situation one usually wonders about the reason for the failure: lack of information about a threat, training, equipment, inadequate control, etc. There may be a range of hypothetical reasons, however it is necessary to indicate one of them - the lack of proper security awareness. “Awareness” is an integral part of a human being. Awareness is a concept which is difficult to define, referring to the sense of experiencing specific mental states (mental phenomena). Owing to perception, the human being is aware of the surrounding environment. He adapts his activities to the relevance of events. Also, he is aware of the contents of own mental experiences (experiencing one’s own “Self”) and the very fact of their cognition (PWN, 2020).

The personnel of airport security should have a high level of "security awareness". This means that they should possess the ability to perceive hazards, maintaining awareness of things which pose the greatest threat in the near and further environment, and at the same time, they need to be able to take action to minimize these threats. At the same time, they should be able to anticipate the consequences of their own actions.

7. Direct aviation security systems

There are a number of measures and aircraft protection systems against the most common MANPADS attacks. They differ in the mode of operation, the possibility of using them, degree of complexity and obviously the price, which undoubtedly is one of the key issues when making a decision on the purchase and the application of a given asset by an air carrier.

MANPADS – Man Portable Air Defense System is a portable anti-aircraft missile intended to fight visually observable air targets, including planes, helicopters and other objects emitting radiation in the infrared spectral range. Due to the risks involved with this type of a weapon, its possession as well as international sales are tightly controlled. In addition, too much attention is placed on terrorist attacks and an international trade, also in view of the threat of terrorist attacks using anti-aircraft rocket sets. The advances of techniques and technology had made it possible to construct portable anti-aircraft missile sets, operated on the battlefield by one soldier. They are now used at all levels of air defense. They are capable of fighting objects at distances ranging from several hundred meters to several kilometers and altitudes between several meters to tens of kilometers. Thus, there is no doubt that anti-aircraft sets which remain in the hands of terrorists and accidental persons, pose a threat to civil aircraft.

MANPADS systems are mostly intended to be used by a single soldier. They have been frequently used in various armed conflicts since 1969, i.e. since the Egyptian-Israeli border clashes. The main element of MANPADS is an anti-aircraft missile, placed in a tabular launcher, which guides itself to the most intense source of thermal

radiation, which is the aircraft engine. By assumption, it is designed to be an inexpensive system, which is why its construction is simplified. For example, the same rocket does not have a proximity fuse, but an impact one, hence the eruption occurs at a time when it directly hits the warmest place of the aircraft. In addition, generally external detection systems are not used, and the detection itself is made by using a rocket homing warhead, in-built in the launcher tube. Additionally, the launch device is switched off and can be reused after replacing the used launcher.

The simplicity of design of MANPADS translates into an easiness of its use. It does not have any special calibration, testing and aiming systems. Everything is quite tough and rough as well as 'idiot-proof". The shooting procedure in the case of terrorist activities only consists in mounting the trigger mechanism and the coolant tank on the launch pad, removing covers, placing it on the shoulder and aiming into the direction of an aircraft. The engagement of a target is signaled to the operator by a light signal or a sound signal. Firing is done only by pressing the trigger. Next, an empty launch tube is disposed of, obviously after removing the trigger mechanism, which can be later reused. It is clear that firing from MANPADS does not need a well-trained specialist, which was proved by Russians in Afghanistan. Often illiterate Taliban launched attacks on them. Currently government aviation in Syria is frequently attacked by rebels.

The simplicity of the system does not mean that it is ineffective. Initially, the most effective were easily accessible Russian rockets. Terrorists act primarily using the surprise element, i.e. in an environment where no one is expecting an attack and where prevention is absent. Moreover, a terrorist does not act under the pressure that he will die if he does not shoot. He is the one to select the time and place of an attack.

The availability, mobility and possibility to hide MANPADS make this weapon one of the most frequent tools to carry out terrorist attacks. The attacks which occurred several years ago by means of short range infrared homing missiles led to a situation that aircraft developers and supervisory bodies began to consider equipping commercial aircraft with anti-missile defense systems. The idea was considered to be too expensive, unreliable and ultimately too dangerous for airlines. Various surface-to-air missiles require different defense systems, which creates a number of opportunities for their producers and also would fundamentally change the role of commercial pilots. Equipping aircraft in anti-missile systems would cost enormous amounts of money and would turn the pilot's work into a real nightmare. Additionally, new safety issues would arise because of the equipment itself: lasers are harmful to eyesight, other means of defense may be poisonous (Radomyski, and Bernat, 2018; Radomyski, 2019).

The technical measures for the individual protection of military aircraft include: devices warning about radar or laser radiation, warning devices about incoming missiles, jamming and deception devices, devices of active infrared interference, stations of active radio interference and electronic devices, anti-radiation missiles and passive infrared interference systems, as well as radio electric dipoles.

Undoubtedly, these days it is necessary to undertake actions with regard to the protection of passenger aircraft as terrorist attacks and hijacks are becoming more common. The incident of 28 November 2002 in Mombasa, when there was an unsuccessful attack on a Boeing 757, forced the Israeli government to develop an innovative project. In accordance with the governmental Sky Shield programmed, jet aircraft belonging to the national carrier El Al Israel Airlines, Arkia Israel Airlines and Israir Airlines are equipped with such equipment, which is manufactured by the local company Elbit Systems. The position of Israel was that the benefits outweigh costs and insecurity. The lowest level of security against terrorist attacks pertains to Israeli airlines and therefore they are considered

to be the most dangerous ones. Therefore, Elbit company decided to develop a system named Commercial Multi-Spectral Infrared Countermeasures (C-MUSIC), which introduces a revolutionary concept in fighting ballistic missiles and rockets. A pod, which is installed under an aircraft fuselage, has got a strong laser (jamming the operation of a missile head) and a guidance system. In this way, in a matter of seconds, the system is capable of destroying a dangerous incoming threat. What is more, it can engage a missile using a thermal camera (it detects a threat by heat seeking). Next, it "fires" into its navigation system to change its trajectory and avoid a crash. This system largely reflects military anti-missile systems designed to counter ballistic missiles, yet on a smaller scale. C-MUSIC is already mounted under the fuselage of the Boeing 737-800 belonging to the El Al Israeli airline. The system is fixed in the lower rear part of the fuselage of a passenger aircraft (Fig. 1).

Figure 1. El Al's Boeing 757-800 equipped with C-MUSIC system. Adopted from: (Altair, 2014).

This system is one of the most desirable security systems in the world since the current level of threat from missiles and ballistic missiles is very high. It gives hope for both civil aviation and military aviation due to a breakthrough in the field of security. In the foreseeable future, all passenger aircraft in Israel are to be equipped with C-MUSIC systems in order to improve their level of security (Ogonowski, and Bogusz, 2018).

In 2016, the Elbit Systems company completed testing the system, consisting of three main subsystems that facilitate a reduction of the danger that exists mainly from Man Portable Air Defense Systems (MANPADS). The subsystem of detectors is designed to detect and locate an incoming missile. After a positive identification of the autonomous control system, an optical system, placed in a special copula, guides the head of the anti-aircraft rocket, using a laser beam. In this way, the thermal matrix of a projectile is blinded, and finally the projectile goes astray, exploding at a safe distance from an aircraft (Fig. 2).

Figure 2. Components of the C-MUSIC system and their distribution in the pod. Adopted from: (Opli, 2012).

The aircraft used by the President and Prime Minister of the French Republic has been equipped with the Israeli defense anti-aircraft infrared guided missile system - "surface-to-air." The French decided to assemble this system of self-defense, due to more frequent visits of the president and prime minister in the countries of central Africa, where there is a very high risk of terrorist attacks using MANPADS. The Israeli solution was chosen since the country has vast experience in the fight against this type of threats, gaining it for decades.

The majority of anti-missile systems, designed for aircraft and helicopters, are to counter short-range and shoulder-launched missiles. The USA has equipped most of its military transport units with such protective devices, similarly to the

United Kingdom and Australia. The systems manufactured by Northrop Grumman are in service with the heads of states, for example, the Air Force One carrying the President of the United States as well as the German aircraft transporting the Chancellor.

The most important effect of mounting the system of self-protection on board an aircraft is to enhance the situational awareness for pilots, who are being informed about possible risks from anti-aircraft infrared guided missiles. The main aim of the kit is to defend against terrorists', militants' or various rebels' weapons, i.e. against portable anti-aircraft short range missile systems, MANPADS-type.

The aircraft protection against IR guided missiles is one of the priorities in the present time. The reason is very high effectiveness of such missiles. Recent war experiences show that approximately 90% of all aircrafts shot down in armed conflicts are destroyed by infrared guided missiles.

The protection of aircraft against MANPADS-type missiles is usually ensured by creating false thermal targets by means of thermal or optical active electronic jamming systems. The operation of the electronic-optical active jamming systems is based on the principle of modular jamming of infrared radiation.

8. Conclusions

This article deals with the protection of air transport against acts of unlawful interference with an indication of trends that are likely to occur in the future. The aim of this article is to focus on the problems of air transport security at airports, associated with the evolution of threats and the functioning of an airport security system.

The problem that the authors wished to signal was expressed by a question - what are the directions of improving the current solutions in the field of air transport security in order to effectively prevent future acts of unlawful interference? This is a difficult question, since the challenges and threats are variable in their nature, and in practice it is difficult to follow them.

The authors are of the opinion that, in the first place, it is essential to change the perception of airport security. A modern airport might be compared to a fortress guarded by various services and various types of technical systems. Using military terminology, the defense is fairly static, important, however it is only one of its elements. Areas, objects and devices which are important for the defense, economic interest, public safety and other important state interests must be protected. An airport combines all of these attributes. One should realize that airports will not only be the scope of interest of criminal organizations, but also of countries which do not exclude conducting the so-called hybrid warfare. Therefore, it can be argued that airports, as communications centers, are exposed not only to criminal organizations, but also reconnaissance or saboteur groups, detached from armed forces of other countries. The forces will be well-equipped and mentally prepared for such an operation. The question remains whether the threat, however real, is included in various scenarios of services that are responsible for airport security?

The presented modern technologies are essential to significantly strengthen the protection of airports and other critical infrastructure installations. They facilitate an instant detection of threats and often shorten the response time of airport security and emergency services. New technology significantly supports the protection within the airport perimeter area and in the very buildings. The awareness of using these devices is a "psychological barrier", which, in a preventive manner, often deters potential perpetrators. The latest trends in the development of technical measures used in protection are closely related to biometrics. The biometric systems are already used in practice and will be further developed.

The law and technology applied in protecting airports prove insufficient. The actual level of airport security rests with those working in the services. If someone in the airport security system, commits an error, he/she will act inappropriately in such a situation. Actions taken will cause an unlawful interference, even though avoiding such a situation was possible. As a rule, in such a situation one usually wonders about the reason for the failure: lack of information about a threat, training, equipment, inadequate control, etc. There may be a range of hypothetical reasons, however it is necessary to indicate one of them - the lack of proper security awareness. “Awareness” is an integral part of a human being. Awareness is a concept which is difficult to define, referring to the sense of experiencing specific mental states (mental phenomena). Owing human perception, one has a sense of orientation in the environment that adapts operation to the relevance of events. One is also aware of the content of own psychic experiences (by experiences own "Self") and the very fact of experiencing them.

Airport security personnel should have a high level of "security awareness". This means that they should possess the ability to perceive hazards, maintaining awareness of things which pose the greatest threat in the near and further environment, and at the same time, they need to be able to undertake action to minimize these threats. At the same time, they should be able to anticipate the consequences of their own actions.

One final conclusion - the security of a facility should be approached in a systematic manner. This means that authorities, departments, state services, which can provide information about a potential threat and can be used for its naturalization, should act in one coherent system of civil aviation security, in compliance with predetermined rules. In practice, the protection of airports should be given a dynamic, maneuverable character, associated with the protection of its operational zone.

In the opinion of the authors of this article, the working hypothesis adopted in the introduction has been positively verified.

References

1. Altair. (2014). Zakończenie prób C-MUSIC, Altair Agencja Lotnicza. 28.02.2014. Retrieved from https://www.al-tair.com.pl/news/view?news_id=12839&q=C-MUSIC, 12.10.2020.
2. Annex 14 to the Convention on International Civil Aviation of 7 December 1944 (1974). Retrieved from https://www.icao.int/safety/airnavigation/nationalitymarks/annexes_booklet_en.pdf, 16.10.2020.
3. Annex 17 to the Convention on International Civil Aviation of 7 December 1944 (1974). Retrieved from https://www.icao.int/safety/airnavigation/nationalitymarks/annexes_booklet_en.pdf, 16.10.2020.
4. Biernacki, R. (2018). Służba ochrony lotniska – stan szkolenia podstawowego po deregulacji zawodu pracownika ochrony. *Zeszyty Naukowe WSOSP*, *1(2)*, pp. 31-45.
5. Chicago Convention - Convention on International Civil Aviation of 7 December 1944 (1944). Retrieved from https://www.icao.int/publications/Documents/7300_orig.pdf, 16.10.2020.
6. Compa, T. (2013). *Bezpieczeństwo operacji w portach lotniczych: Obsługa handlingowa*, Dęblin: WSOSP.
7. Evans, A. E. (1969). Aircraft Hijacking: Its Causes and Cure. *American Journal of International Law*, *63*, 695-710.
8. Kubisa, E. (2017). Największe lotniska na świecie. Retrieved from https://biurorekordow.pl/najwieksze-lotniska-na-swiecie, 20.03.2019.
9. Ogonowski, K., and Bogusz, D. (2018). Conception of protecting civil aircrafts

from man-portable air-defence system. *Transport Means* 2018 – *Proceedings of the 22th International Scientific Conference. Part III. Juodkrante*, Lithuania 2018, pp. 1124-1132.
10. Opli. (2012). Elbit Systems Introduces J-MUSIC™, the Newest Member of its DIRCM Systems Family. Opli, 09.07.2012. Retrieved from https://www.opli.net/Opli-old/magazine/eo/2012/news/elbit_systems_j_music.aspx, 12.10.2020.
11. PWN. (2020). Świadomość. *Encyklopedia PWN*. Retrieved from https://encyklopedia.pwn.pl/haslo/swiadomosc;3984376.html, 12.10.2020.
12. Radomyski, A. (2019). Contemporary aspects of civil aviation security against aviation terrorism, *Transport Means 2019 – Proceedings of the 23th International Scientific Conference. Part III*. Juodkrante, Lithuania 2019. pp. 1121-1127.
13. Radomyski, A., and Bernat, P. (2018). Contemporary Determinants of Organising Effective Protection of Civil Aviation Against Terrorism, *Transportation Research Procedia*, 35. pp. 259-270. DOI: 10.1016/j.trpro.2018.12.021.
14. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 with all implementing regulations (2008). Retrieved from https://op.europa.eu/en/publication-detail/-/publication/da45f838-cc98-4788-be3b-2ac0a9768ae1/language-en, 12.10.2020.
15. Sillitto, H. et al. (2017). Defining "System": A Comprehensive Approach. *27th Annual INCOSE International Symposium (IS 2017)*, Adelaide, Australia, July 15-20, 2017. DOI: 10.1002/j.2334-5837.2017.00352.x.
16. Ustawa o ochronie osób i mienia, Dziennik Ustaw (1997). Retrieved from http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19971140740/U/D19970740Lj.pdf, 20.10.2020.

SAFETY&DEFENSE
Scientific and Technical Journal ISSN 2450-551X

Hypersonic Weapon as a New Challenge for the Anti-Aircraft Defense Command and Control System

Piotr MALINOWSKI

Military University of Aviation, Dęblin, Poland; p.malinowski@law.mil.pl,
ORCID: 0000-0002-4240-982X

DOI: https://doi.org/10.37105/sd.87

Abstract

The intensification of the air threat resulting from the emergence of hypersonic weapons in the immediate vicinity of Poland has become a significant challenge for the Polish armed forces, including anti-aircraft defense. The capabilities of the new type of weapon determine not only the need to modernize and acquire systems designed to engage aerial targets, but also the command and control systems that control them. Due to the nature and the limited scope of the article, the deliberations presented in it are generalized results of a research on the scale of the threat posed by hypersonic weapons in the airspace and the need to modernize anti-aircraft defense command and control subsystems, which may be involved in combating them as part of the national air defense system. The presented conclusions also concern the problems of multiplying the current level of automation of the command and control subsystem. This is related to the need for the effectiveness of the military decision-making process as well as uninterrupted and efficient cooperation with the national and allied elements of the air reconnaissance and air defense assets subsystems, including the components of missile defense, which is predestined to engage hypersonic weapons.

Keywords: military security, hypersonic weapons, anti-aircraft defense, C2 system

1. Introduction

The advent of the era of hypersonic air threats in tactical operations is redefining the requirements for the entire anti-aircraft defense system, including its command and control subsystem. Although the idea of creating a weapon capable of immediate reaction, of large range, is not new, still its embodiment in the form of a Russian hypersonic weapon is a significant transformation

of the threats that determine the necessary transformation of the domestic anti-aircraft defense potential.

The desire to intensify the automation of anti-aircraft defense command and control processes results from the complexity of effective combat against aerial targets that are so difficult to engage. It is also a requirement for the dynamization of operations on the contemporary battlefield where not only hypersonic weapons pose significant air threats. However, its current introduction into the strike assets arsenal of several armies around the world reveals not only the scale of the new threat. It also determines, as shown by the conducted research, an urgent need to achieve an appropriate level of defense against this type of air threats, which will be also influenced by the efficient functioning of the command and control subsystems.

This article contains considerations and conclusions, the purpose of which is to present the characteristics and capabilities of hypersonic weapons, particularly emphasizing the armament of the Russian Federation, as well as the impact of these weapons on the modernization and automation of the anti-aircraft defense command and control subsystem. Therefore, the author focused on solving the following research problem: How do the capabilities of hypersonic weapons affect the needs of modernization and automation of the anti-aircraft defense command and control subsystem? A mixed research method, based on the elements of text and literature exploratory research (analysis), simulation of anti-aircraft defense combat capabilities, experiment during military exercises was used to solve the indicated problem during the research, the generalized results of which are included in the article.

2. Hypersonic weapons as an air threat

For around two decades, several countries around the world (GMTFF, 2019) including Russia, were working towards primarily using hypersonic technology in the ballistic missiles weapon segment, boost-glide vehicles, and cruise missiles. The emergence of military strike systems in the airspace that are capable of delivering precise strikes at speeds several times the speed of sound is a significant challenge for the entire air defense system, including anti-aircraft defense. Currently, such weapons are classified as supersonic or hypersonic. The first group includes missiles which fly above Mach 1. They are generally regarded as flying between Mach 1 and Mach 5, about 1,000 to 5,000 km/h (Speier, 2017, p. 2). Whereas the term hypersonic weapon is generally understood to refer to the ones that fly within the atmosphere at speeds above Mach 5 (five times the speed of sound), or above 6,100 km per hour. One focus of military interest is hypersonic missiles that can travel at approximately 5,000 to 25,000 km per hour (or between 1.4 and 7 meters per second) (Speier, 2017, p. 2) – up to 25 times faster than a standard airliner. Additionally hypersonic weapons refer to weapons that not only travel faster than Mach 5 but also have the capability to maneuver during the entire flight.

New hypersonic systems currently have two primary sub-varieties: hypersonic glide vehicles (HGVs), and hypersonic cruise missiles. The first sub-variety, hypersonic glide vehicles are typically launched by rockets into the upper atmosphere. After disengaging from the carrier missile, the hypersonic vehicle lowers its altitude and continues to fly to its target by itself. They are released at altitudes that can vary from around 50 km to higher than 100 km and glide to their targets by skipping along the upper atmosphere. HGVs have a range comparable to ballistic missiles but they fly at a lower altitude, and a negligible portion of their flight path follows a ballistic trajectory. This results in the time between detection by ground-based sensors and impact being shorter compared to a ballistic missile's re-entry vehicle (Brehm, Weeler, 2019, p. 2). The HGVs are carried to the upper layers of the atmosphere

by rocket missiles, which give them an appropriate initial velocity.

The second sub-variety are hypersonic cruise missiles (HCMs). Hypersonic missiles typically operate using air-breathing supersonic combustion ramjet (scramjet) engines to accelerate and maintain missile velocity. A scramjet usually begins operating at Mach 4 or Mach 5. Therefore, a hypersonic cruise missile must first be accelerated to Mach 4 or Mach 5 by other means, such as rocket engines (Hruby, 2019, p. 18).

HCMs could be ground-, air- or ship-launched and would likely fly at an altitude of 20 to 30 km, beyond the reach of most current air-to-surface missile defence systems (Brehm, Weeler, 2019, p.2). The principal advantages of an HCM would be its speed and maneuverability. These cruise missiles are difficult to defend against because of their unpredictable trajectories. Both hypersonic types of weapons can carry a nuclear warhead, a conventional explosive warhead, or no warhead at all, instead relying on sheer kinetic force to destroy its target. There are many other potential types of hypersonic weapon being developed. These include more complex missile systems, manned and unmanned reusable air vehicles, and space launch systems (Speier, 2017, p. 4).

The threat of using hypersonic weapons in an armed conflict, resulting from one party's possession of these is a factor that creates a completely new dimension of air threat. This is because hypersonic weapons combine the speed of a ballistic missile with the maneuvering capabilities of a cruise missile. In the opinion of the US military analysts "while the designed speed of the hypersonic missile is faster than that of sound, its advantage lies in its enhanced maneuverability and smooth flight path, which is much harder to track than that of traditional missiles" (Osborn, 2017). It is also a weapon which is specifically designed for increased survivability against modern ballistic missile defense systems. Additionally, for users, hypersonic weapons have the advantage of being the type of weapon whose "accuracy minimizes the risk of collateral damage, that pose no risk to aircrews, are unstoppable and phenomenally accurate, can yield an impact equal to five to ten tons of high explosive with no warhead at all yet be capable of delivering a nuclear bomb, and can reach nearly every coordinate on the surface of the earth within 30 minutes" (Simon, 2020). For this reason, it is recognized as a threat that can change the perception of the implementation of air strikes and the way of achieving strategic goals of military operations. This is influenced by the possibilities of the hypersonic weapons due to which "they are able to evade and conceal their precise targets from defenses until just seconds before impact. This leaves targeted states with almost no time to respond" (Speier, 2018).

Taking into account the geostrategic location of Poland, after analyzing the development trends of hypersonic weapons, it can be concluded that the most serious air threat related to the use of this type of weapon is likely from the Russian systems of this weapon. It may result from the use of both hypersonic glide vehicles (HGVs) and hypersonic cruise missiles (HCMs) owned by the Russian Federation.

The first strategic type of Russian hypersonic weapon is the Avangard (Vanguard) hypersonic boost-glide vehicle, which is part of an intercontinental ballistic missile (ICBM) missile complex equipped with a hypersonic glide warhead (Trimble, 2019, p. 20). Each ICBM is armed with one hypersonic boost-glide warhead. Avangard is carried to its suborbital apogee of around 100 km by a ballistic missile. Once boosted to its suborbital apogee, the glide vehicle separates from its rocket. It then cruises down towards its target through the atmosphere and can reach speeds of up to Mach 20 (6.28 km/s) and can maneuver (MDPA, 2019). Therefore, Avangard's trajectory is unpredictable and makes intercept attempts difficult after its boost phase.

Avangard, a hypersonic glider previously known as 'Project 4202' or 'Yu-71', or the Aerobalistic Hypersonic Warhead has been tested multiple times since February 2015 (Sputnik, 2016). Currently, warheads of this type are mounted on intercontinental

ballistic missiles UR-100NUTTH (SS-19 Stiletto). The first regiment of ICBMs, armed with the newest, hypersonic Avangard system, achieved combat readiness in December 2019 (TVN24 BIS, 2019). By the end of 2027, that regiment and one other are to have six Avangard systems each, for a total of 12 systems (GMTFF, 2019). Ultimately , the hypersonic boost-glide vehicles (HGVs) Avangard are intended to be mounted as an element of the Russia's RS-28 Sarmat (SS-X-30) – the state-of-the-art heavy liquid-propelled ICBM which are currently being developed for the Russian army.

Another type of Russian hypersonic weapon is The Kinzhal (Dagger) system, which is essentially a combination of a KH-47M2 heavy hypersonic rocket and a MiG-31K fighter jet or Tu-22M3 carrier bomber (Global Security, n.d.). It is planned that it will be also carried by a new Su-57 stealthy multi-role fighters (Military Today 2020a, n.d.). The aeroballistics hypersonic missile Kinzhal (Dagger) has a "quasi-ballistic" flight path at altitudes from 35 to 50-80 or more kilometers. The Kinzhal (Dagger) is a hypersonic missile, which, according to Russian data, has a range of about 1,500 to 2,000 km (Palowski, 2020b). It is an air-launched ballistic missile (ALBM) (MDP, 2019) carried by a combat aircraft with speeds above 5 Ma (according to some sources, even 10 Ma) at certain stages of flight, on a similar basis as ballistic missiles launched from the ground. During the flight, the missile maintains the ability to maneuver and correct its trajectory. According to Russian doctrine, it is capable of carrying both conventional warheads (weighing around 480 kg) and nuclear charges as well.

The Kinzhal (Dagger) missile has a similar design to the Iskander-M missiles. However, its launch not from the ground, but from an aircraft flying at more than twice the speed of sound, in addition to high altitude, makes it a much greater air threat than the Iskander missile. Such a missile launched from an airplane does not have to use energy to take off from the ground, thus it has greater spatial possibilities in terms of velocity and range.

The KH-47M2 Kinzhal (Dagger) missile introduced in 2018 may therefore be a very dangerous strike system, used to blackmail and "cut off" support for NATO's eastern flank far ahead of the potential conflict area, or to perform quick, hard-to-repel strikes on Poland or the Baltic countries (Palowski, 2020a). It results from the possibilities of this armament, presented in Figure 1.

Figure 1. The potential operational range of The Kh-47M2 Kinzhal (Dagger). Adopted from: "Hipersoniczny wyścig potęg [ANALIZA]" by M. Dąbrowski. Copyright 2020 by Defence24 (Dąbrowski, 2020).

An air-launched KH-47M2 Kinzhal hypersonic missile traveling at Mach 10 could hit Sofia, Bulgaria, about 2000 km to the south, in 11 minutes from the Gulf of Finland. Re-orienting the firing line to Russia's western borders, a Kinzhal could reach London, Paris, or Rome equally quickly. To put it another way, hypersonic weapons mean that a hypothetical target 2000 km away has the same potential of being threatened as those within roughly 150 km of a subsonic cruise missile. On the other hand, the Mach 20 Avangard expands the threat umbrella to cover ranges reportedly in excess of 6000 km with a flight time of around 20 minutes (Cummings, 2019). Therefore, only those systems that are capable of destroying maneuvering ballistic missiles may be able to combat such threats as the KH-47M2 Kinzhal (Dagger), provided that the threat is detected and classified early and can be tracked by fire control systems.

The multi-purpose operational/tactical hypersonic cruise missile 3M22 Tsirkon (Global Security, 2019) has also been

developed in Russia. HCM Zircon is mostly an antiship missile, but can also hit ground targets (Vavasseur, 2020). It will be used for arming, among others, Kirov cruisers, missile frigates, Husky ANNs and modified Tu-160M bombers. During test shooting, this HCM achieved a range of over 400 km and a speed corresponding to 5÷6 Ma (Dąbrowski, 2020), although the Russians indicate that that it can reach speeds of approximately Mach 9 and strike a target of more than 1,000 km away (SS-N- 33, 2019). This speed is achieved by a solid-fueled first phase, followed by a scramjet second phase. At the end of 2019, HCM Zircon was launched for the first time from a warship (Defense World, 2019). Although it has not yet been officially confirmed, this missile, in addition to the conventional variants, can be equipped with a nuclear warhead, similar to the American Tomahawk sea launched cruise missile.

Another Russian weapon that only partially uses hypersonic speeds is the Iskander system. Its missiles at the initial stretch of the trajectory, the curve of which is not ballistic and difficult to predict, develop a speed of 2,100 m/s (OAS, 2016). Additionally, these missiles are controlled along the entire flight path. One of the versions of these missiles, designated as 9M723-1, was used to develop the high-precision hypersonic missile KH-47M2 Kinzhal (Dagger) (Global Security, 2020). On the other hand, newer versions of the Iskander system weapons, which are cruise missiles, have lower speeds, but can maneuver around the entire flight path. Currently, a new type of cruise missile 9M729 (MDF, 2020; Military Today, 2020b) has been introduced into combat use in 2017, the range of which can be up to 2,500 km (Military Today, 2020b). According to Russian sources, the Iskander system is capable of eliminating such targets as multiple rocket launchers, long-range artillery, command and communication centers and planes and helicopters on the ground (TASS, 2017). The equipment of this system will be further modernized, as reported by the Russians, who indicate: "We are going ahead with further research and development to create new missiles for the Iskander system. (...) Now we have seven types of missiles, or possibly more" (TASS, 2017).

Russia, however, does not stop at increasing the potential of the three indicated models, but having extensive experience in the field of missile technology, it is preparing further improved solutions for hypersonic weapons launched from the air, water and ground for various purposes. At the same time, it implements and constructs defensive weapon systems prepared to combat the enemy's hypersonic weapons.

3. Determinants of the operation of the anti-aircraft defense command and control subsystem

The operation of the command and control subsystem is crucial for achieving the goal of anti-aircraft combat and performing the tasks of the anti-aircraft defense system. Its effect, ensuring optimal information support and the reactions of other elements of the system, especially the reconnaissance subsystem and the fire subsystem, determines the speed of reaction to changes in the air situation and emerging air threats. The functioning of this subsystem also determines the efficiency of cooperation with other elements of air defense. It also influences the outcome of the fight against the means of air attack that threaten protected military facilities and groups of troops during tactical operations, as well as self-defense (self-protection).

A command and control subsystem, integrating C2 organization, C2 process and C2 facilities within itself, should meet three basic requirements, i.e. ensure the implementation of goals, be structurally stable, facilitate adaptation to changes in external conditions (Kręcikij, and Wołejszo, 2007, p. 64). Its functionality, in all conditions of anti-aircraft defense system operation, ensures compliance with several basic criteria, including:

- Adaptability to the high dynamics of activities in the airspace.
- Mobility combined with the ability to direct the actions of subordinate forces.
- Multifunctionality related to the needs of cooperation with other subsystems and contractors of tasks as well as elements supplying information.
- Operational selectivity aimed at the coordination of various activities necessary for the combat effectiveness and security of the air defense system.
- Centralization of planning and decentralization of task execution.
- Modularity that guarantees reconfiguration necessary to perform new tasks.
- Resistance to various disturbances in functioning (Rajchel, and Załęski, 2011, p. 235).

At the same time, the operation of the command and control system is to ensure flexibility that allows the commander to operate freely and to react in various unforeseen situations. It is also to guarantee efficiency, i.e. such a method of operation that allows to achieve better results with the same resources and efficiency expressed in the possibility of quick decision-making and bringing them to contractors while maintaining the requirement of secrecy (PP, 2009, p. 318-319). On the other hand, the requirements to achieve an appropriate level of compatibility and interoperability in the course of cooperation in the Alliance structures mean that the anti-aircraft defense command and control system must have the ability to cooperate with other allied or coalition air defense command systems.

Significant requirements for the anti-aircraft defense command and control system are also related to its operational efficiency during the implementation of tasks, expressed in the speed of the information-decision cycle. This efficiency, defined by the time dependence (OP, 1996, p. 60), presented below, is a set of indicators of the time capabilities of the command and control and fire systems and a *sine qua non* condition for engaging aerial targets.

$$Tdc \geq To + Td + Tz \quad (1)$$

where:

- Tdc - target arrival time (from the moment of detecting the source of the air attack to its arrival to the border of the aerial target engage);
- To - delay of information on the basis of which the decision is made to engage an aerial target);
- Td - decision making time and handing it over to executors;
- Tz - the time from the moment of receiving the task by the anti-aircraft defense fire assets until the destruction of the aerial target on the assigned task execution area).

The time indicators related to the operation of the command and control system are the components of the fire mission completion time, which can be significantly reduced by the proper organization of the system and its equipment.

The anti-aircraft defense command and control system is to meet the presented criteria and requirements both in tactical command (combat control) and during fire command (fire control), regardless of the type of air threat that appears in the airspace. This is especially important in fire control, during which, thanks to the efficient cooperation of the anti-aircraft defense subsystems, as well as the cooperation with the air defense system, an effective combat against the assets of air attack of the potential enemy is ensured.

4. The influence of hypersonic weapons on the modernization of the command system

In terms of effectiveness of the hypersonic weapons, the speed and altitude at which these vehicles fly significantly challenge an adversary's ability to detect, track, target and engage (Raytheon Missiles & Defense, 2020). Interception of a hypersonic missile or a warhead requires detection,

tracking with high precision, calculating the flight trajectory, accurate forecasts of its further heading and programming of anti-missiles. The later the target of an enemy's hypersonic weapon is detected, the less time is left for an effective response. For example, if the opponent plans to strike the target within a 1,000-km range, a hypersonic missile traveling at 10 Ma can cover that distance and reduce the response time to about six minutes. In addition, in the case of hypersonic missiles, apart from high speed, we also deal with maneuverability, which makes it very difficult or virtually impossible to predict the exact direction of the flight. At the same time, the closer to the potential target of the attack, i.e. the protected object, the predictability of the projectile's flight path increases, but the time to react significantly decreases.

Due to the fact that the scope of anti-aircraft defense, depending on the scale and type of aerial threat, may be different, it cannot be ruled out that in the near future it may be extended to combat this type of weapon due to a significant increase in the potential enemy's arsenal of hypersonic weapons. All the more so because, according to some experts, hypersonic weapons function more effectively against threats from strategic anti-missile systems than from operational-tactical ones (Dąbrowski, 2020). This approach is also confirmed by theoretical assumptions and modern hardware solutions indicating that the anti-aircraft defense goes beyond the fight against enemy aviation and extends the scope of tasks to engage ballistic and winged missiles, and even "ground-to-ground" missiles (PP, 2009, p. 172). However, in the opinion of Simon Steven, analyst at the Quincy Institute, "No existing defenses can stop such weapons" (Simon, 2020), which means that the currently functioning anti-aircraft defense systems must undergo deep modernization and reorganization to meet the challenge of the emergence of hypersonic weapons as an air threat to sheltered objects.

Although, as indicated by a number of studies (Radomyski, 2015, p. 117), the quantitative and qualitative potential of anti-aircraft missile systems and reconnaissance measures as well as the importance of the command subsystem should not be overlooked, in the first place. Its development, focused on the modernization or acquisition of new automated elements, in general is to ensure the reception, selection, analysis and extrapolation of information from superior command and control systems and autonomous and cooperating sources of reconnaissance. The need to improve the command and control system in terms of the speed of these actions is significantly determined by the multiplied possibilities of hypersonic weapons. Meeting the time requirements for the operation of the command system requires a significant shortening of automated analyzes and forecasts as well as the visualization of results and the selective acquisition of reliable and timely information enabling making optimal decisions about opening fire. A similar increase in efficiency should take place in the way of delegating tasks to their contractors, which is supposed to significantly minimize the time needed to make a decision and transfer it to executors (*Td*). At the same time, one should be aware that the last variable, which is the time of mission execution by anti-aircraft fire assets (*Tz*), has a constant value which cannot be reduced without replacement with more efficient anti-aircraft defense assets. The functioning of command and systems in the era of hypersonic weapons should additionally, based on increased automation, reduce the basic advantages of this weapon, resulting from its speed and difficulties in predicting the flight trajectory, i.e. minimizing the information delay time (*To*) also thanks to cooperation with various allied, including space, sources of reconnaissance.

The transformations of the anti-aircraft defense command and control system in the perspective of several years are unlikely to eliminate the human factor from the process of making decisions to fire. However, they are to optimize solutions and accelerate their creation based on a number of available data and incoming information, so as to significantly support the action of the decision maker. In perspective, however, it should be

assumed that due to the significant increase in the speed of some hypersonic strike systems, it is likely in the next generations of anti-aircraft defense command and control systems that the decision-maker will be replaced by artificial intelligence in the process of making decisions to fire.

The increased risk of using hypersonic weapons by a potential aggressor due to the significantly limited reaction time also forces, in addition to the applied decentralization of command and control, a change in the way of making decisions about the use of anti-aircraft defense assets. The transformation of the anti-aircraft defense command and control system related to the decisions made is to guarantee the performance of all the most labor-consuming and complex analytical activities related to the features of the facilities being the subject of the decision-making process. Then, supporting the decision maker is to guarantee the generation of acceptable course of action and indication of optimal course of action among them, which will enable a rational decision. This applies in particular to analyzes related to the possible directions of a potential enemy's attacks, anti-aircraft fire assets formation planning and the distribution of tasks to sub-units.

The anti-aircraft defense command and control system in the face of the threat of combat troops and military facilities, such as hypersonic weapons, should under all conditions play the role of an efficient and resistant to interference integrator of complex radiolocation and reconnaissance systems as well as anti-aircraft fire assets. Its operation is to ensure the effective creation of a multilayer system of protection against air attacks. At the same time, it is to guarantee efficient cooperation with anti-missile defense systems, which are and will continue to be the main executors of the missions of engaging hypersonic weapons of a potential enemy.

5. Conclusion

Highly maneuverable (in terms of heading and altitude) and non-ballistic hypersonic systems can be a difficult target for the currently used anti-missile defense systems and anti-aircraft defense systems cooperating with them. Although future strategic and operational anti-missile systems are indicated as defensive systems against hypersonic weapons, the participation of the anti-aircraft defense system in this project may increase in the future. Therefore, the main direction of the development of the anti-aircraft defense command and control subsystem, which was initiated by the LOWCZA and REGA systems, is the further development of cooperation with other command and control and reconnaissance systems and reducing to a minimum the time needed for detailed analyzes and assessment of information necessary to optimize the planning of activities, as well as accelerate the decision-action cycle and ensuring higher-quality decisions to effectively engage aerial targets.

The facts collected in the course of the research show that the anti-aircraft defense command and control system is facing another challenge which is also its integration with the IBCS (Integrated Air and Missile Defense Battle Command System) providing reciprocal exchange of information with an accuracy sufficient to direct the anti-aircraft fire assets of both systems. The requirement for modernization or a new generation of the anti-aircraft defense command and control subsystem is also the integration and backward compatibility with all elements of the national anti-aircraft defense system (identification and control of anti-aircraft fire assets of all types of armed forces), as well as a multichannel function of higher level than before enabling simultaneous engaging of a larger number of aerial targets. Finally, one should not forget about the issue of mobility, which allows for accompanying combat forces, and modularity ensuring the substitutability of the elements of the anti-aircraft defense command and control system.

While summarizing the presented considerations, however, it should be kept in mind that in the short term, mainly for economic reasons, it will be necessary to make an inevitable choice what kind of anti-aircraft defense command and control system capability to introduce or modernize in the first place. On the other hand, in the next few years, it seems necessary to start work on the successors of the anti-aircraft defense command and control systems used so far, i.e. a new generation of them capable of comprehensive cooperation with other air defense command systems and various reconnaissance sensors, as well as conducting autonomous or dispersed actions against advanced air threats.

Acknowledgement

This article is an outcome of the research project "Automation of air defense's information and decision making processes in the modelled environment of air threat to armed forces and critical infrastructure objects" project, No GB/5/2018/209/2018/DA funded by the Polish Ministry of National Defense in 2018 – 2022.

References

1. Brehm, M., and de Courcy Wheeler, A. (2019). Hypersonic Weapons. *Article36*. Retrieved from https://www.researchgate.net/publication/334050433_Hypersonic_Weapons, 15.06.2020.
2. Cummings, A. (2019). Hypersonic weapons: Tactical uses and strategic goals. *War on the Rocks*. Retrieved from https://warontherocks.com/2019/11/hypersonic-weapons-tactical-uses-and-strategic-goals/, 15.06.2020.
3. Dąbrowski, M. (2020). Hipersoniczny wyścig potęg [ANALIZA]. *Defence24.pl, April 20, 2019*. Retrieved from https://www.defence24.pl/hipersoniczny-wyscig-poteg-analiza, 08.06.2020.
4. Defense World (2019). Russia Likely to Launch Zircon Hypersonic Rocket from a Warship by Yearend. *DefenseWorld.net, March 14, 2019*. Retrieved from https://www.defenseworld.net/news/24458/Russia_Likely_to_Launch_Zircon_Hypersonic_Rocket_from_a_Warship_by_Yearend#.X3MiZzbVI2w, 18.06.2020.
5. Global Security (2019). SS-N-33: T3K22 Zircon/Tsircon/3M22 rocket. *GlobalSecurity.org*. Available online https://www.globalsecurity.org/military/world/russia/zircon.htm, 15.06.2020.
6. Global Security (2020). *9M730 Knizhal - Dagger / Product 75 / Product 715*. Available online https://www.globalsecurity.org/wmd/world/russia/9m730.htm, 15.06.2020.
7. Hruby, J. (2019). Russia's New Nuclear Weapon Delivery Systems: An Open-Source Technical Review. *Nuclear Threat Initiative*. Retrieved from https://media.nti.org/pdfs/NTI-Hruby_FINAL.PDF, 18.06.2020.
8. Kręcikij, J., and Wołejszo, J. (Eds.) (2007). *Podstawy dowodzenia*. Warszawa: Wyd. AON.
9. MDF [Missile Defense Project] (2018). Kinzhal. *Missile Threat*. Center for Strategic and International Studies, March 27, last modified June 23, 2020. Retrieved from https://missilethreat.csis.org/missile/kinzhal/, 24.06.2020.
10. MDF [Missile Defense Project] (2019). Avangard. *Missile Threat*. Center for Strategic and International Studies, January 3, last modified June 23, 2020. Retrieved from https://missilethreat.csis.org/missile/avangard/, 24.06.2020.

11. MDF [Missile Defense Project] *(2020)*. SSC-8 (9M729). *Missile Threat*. Center for Strategic and International Studies, October 23, 2018, last modified June 30, 2020. Retrieved from https://missilethreat.csis.org/missile/ssc-8-novator-9m729/, 08.06.2020.
12. Military Today (2020a). *Kh-47M2 Kinzhal: Air-launched ballistic missile*. Available online http://www.military-today.com/missiles/kh_47m2_kinzhal.htm, 08.06.2020.
13. Military Today (2020b). *SSC-8: Long-range cruise missile system*. Available online http://www.military-today.com/missiles/ssc_x_8.htm, 08.06.2020.
14. OAS [Ośrodek Analiz Strategicznych] (2016). Rosyjskie rakiety balistyczne zagrożeniem dla NATO [Raport]. *Defence24.pl, August 24, 2016*. Retrieved from https://www.defence24.pl/rosyjskie-rakiety-balistyczne-zagrozeniem-dla-nato-raport, 23.12.2020.
15. *OP* [*Obrona powietrzna*] (1996). Warszawa: Wyd. AON.
16. Osborn, K. (2017). Hypersonic Weapons: Everything You Need to Know About the Ultimate Weapon. *The National Interest, July 22, 2017*. Retrieved from online https://nationalinterest.org/blog/the-buzz/hypersonic-weapons-everything-you-need-know-about-the-21637, 08.06.2020.
17. Palowski, J. (20201). *„Hipersoniczny" Kindżał zagrożeniem dla Europy [OPINIA] (2020a). Defence24.pl, May 10, 2018*. Retrieved from https://www.defence24.pl/hipersoniczny-kindzal-zagrozeniem-dla-europy-opinia, 08.06.2020.
18. Palowski, J. (202b). Rakiety Kindżał i Kalibr strzelają nad Morzem Czarnym. *Defence24.pl, January 10, 2020*. Retrieved from https://www.defence24.pl/rakiety-kindzal-i-kalibr-strzelaja-nad-morzem-czarnym, 08.06.2020.
19. *PP* [*Podręcznik przeciwlotnika*] (2009). Warszawa: Wyd. AON.
20. Radomyski, A. (Ed.) (2015). *Podstawy obrony powietrznej*. Warszawa: Wyd. AON.
21. Rajchel, J., Załęski, K. (2011). Dowodzenie siłami powietrznymi, aspekt narodowy i sojuszniczy: Uwarunkowania, Tendencje i kierunki zmian. *Zeszyty Naukowe AMW*, *3(186)*, 229-250.
22. Raytheon Missiles & Defense (2020). *Hypersonics*. Available online https://www.raytheonmissilesanddefense.com/capabilities/hypersonics, 15.06.2020.
23. Simon, S. (2020). Hypersonic Missiles Are a Game Changer. *The New York Times, January 2, 2020*. Retrieved from https://www.nytimes.com/2020/01/02/opinion/hypersonic-missiles.html, 15.06.2020.
24. Speier, R.H. (2018). Hypersonic Missiles: A New Proliferation Challenge. *Georgetown Journal of International Affairs, March 26, 2018*. Retrieved from https://www.georgetownjournalofinternationalaffairs.org/online-edition/2018/3/26/hypersonic-missiles-a-new-proliferation-challenge, 15.06.2020.
25. Speier, R.H., et al. (2017). Hypersonic Missile Nonproliferation: Hindering the Spread of a New Class of Weapons. *Rand Corporation*. Retrieved from https://www.rand.org/pubs/research_reports/RR2137.html, 08.06.2020.
26. Sputnik (2016). Russian Top Secret Hypersonic Glider Can Penetrate Any Missile Defense. *Sputnik, June 11, 2016*. Retrieved from https://sputniknews.com/politics/201606111041185729-russia-hypersonic-glider/, 18.06.2020.
27. TASS (2017). Iskander-M system gets new types of missiles — manufacturer. *TASS, September, 14, 2017*. Available online https://tass.com/defense/965611, 15.06.2020.
28. Trimble, S.A. (2019). Hypersonic Sputnik? *Aviation Week*, *January 14-27*, pp. 20-21. Retrieved from

https://archive.aviationweek.com/issue/20190114, 15.06.2020.
29. TVN24 BIS (2019). Odpowiednia i symetryczna odpowiedź: Rosyjskie awangardy w gotowości bojowej. *TVN24 BIS, December 27, 2019*. Available online https://tvn24.pl/swiat/rosja-system-pociskow-hipersonicznych-awangard-osiagnal-gotowosc-bojowa-ra996031-2857102, 08.06.2020.
30. Vavasseur, X. (2020). Analysis: Russia's Tsirkon Hypersonic Missile Trials Enter Final Stage – Part 2. Naval News, March 3, 2020. Retrieved from https://www.navalnews.com/naval-news/2020/03/analysis-russias-tsirkon-hypersonic-missile-trials-enter-final-stage-part-2/, 08.06.2020.

SAFETY&DEFENSE
ISSN 2450-551X

Counting the Uncountable: Introduction to the New Method of Evaluation of the Efficiency of Air Defense

Daniel MICHALSKI[1]*, Adam RADOMYSKI[2]

[1] Military University of Aviation, Dęblin, Poland; d.michalski@law.mil.pl,
ORCID: 0000-0001-8202-6738
[2] Military University of Aviation Dęblin, Poland; a.radomyski@law.mil.pl,
ORCID: 0000-0001-7522-308X
* Corresponding author

DOI: https://doi.org/10.37105/sd.91

Abstract

The aim of the research was to create such a calculation model for air defense efficiency that will enable us to determine the level of capabilities to complete tasks by air defense in combat conditions. The innovative approach to the efficiency of air defense presented in the article focuses on the methods and algorithms enabling the assessment of the feasibility of the air defense task. In its general form, it is based on the determination of the probable number of aerial threats intended for the implementation of an air task (destruction, disablement, disruption of the protection unit) and the possibility of air defense systems to repel an air attack. The research was conducted with the use of qualitative methods – when determining the elements of protection or tactical and technical data. The results of the presented research can be implemented in the military decision making process in air defense in tactical level of command.

Keywords: defense, efficiency, air defense, air threats, combat capabilities.

1. Introduction

The changing air safety environment (Radomyski et al., 2018), the growing importance of aviation in armed conflicts and the development of aerial threats (Kulik, 2020) necessitate the search for solutions aimed at increasing the ability to counteract air attacks. A. J. Wilson noticed that "studies such as these (on the development and enhancement of air defense capabilities – the author's explanation) must address all the systems needed to collect information, facilitate its interpretation, aid subsequent decision making and take the necessary action" (Wilson, 1994). Current research focuses primarily on technological development such as radar systems, missile guidance (Wen, and Orlando 2020; Wand, Dong, 2013) and real-time decision support, also using artificial intelligence (Hocaoğlu, 2019; Baldwin, and Felder, 2019; Goztepe et al., 2015). In other words, the emphasis is given to the conduct of the air defense operations, while the entire decision-making process carried out by the armed forces along with the assessment (evaluation) of the adopted course of action (CoA) is marginalized.

For modern war in which an environment is uncertain and things are too complex to understand from only one aspect, the military decision making process (MDMP) eases the commander's decision making (Snyder, 1989). According to FM-6-0, the MDMP is an iterative planning methodology for understanding the situation and mission, develop a course of action, and produce an operation plan or order (FM 6-0, 2014). Regardless of the differences in MDMP in various states one of the most common assumptions about decision making is that decisions should be as rational as possible "people make decisions by identifying and comparing options to determine which one produces the optimal outcome for a given set of circumstances" (Vasilescu, 2011). The assessment of the adopted CoA plays a special role in this respect, i.e. in the case of air defense, and the assessment of the efficiency of air defense.

The evaluation of the efficiency of air defense allows determining (within the limits of probability) whether the variant of action developed by the staff will accomplishment of the air defense mission (operation) – to protect the force and selected geopolitical assets from aerial attack, missile attack, and surveillance (FM 3-01-11, 2000). This is especially important in the case of a limited number of air defense systems, both locally and globally.

So far, the conclusions from the research conducted on the implementation of decision support systems such as AI in air defense clearly indicate that "data scientists might use not only AI techniques and technologies, but also other sciences to apply expertise in data preparation, statistics, and analysis to investigate complex problems" (Goztepe et al., 2015). Undoubtedly, determining the effectiveness of air defense is a complex problem, which is why we believe that conducting the evaluation of efficiency in a systematic and scientifically justified manner will allow for a more accurate formation of predictions with regard to the activities carried out and the development of the best possible decision during the implementation of the MDMP at the tactical level of operation. Therefore, the purpose of the research on the effectiveness of the air defense described in this article was to create a calculation model (algorithm) that would enable the determination of the level of task completion by units and sub-units of air defense in combat conditions.

When developing a new method of calculating effectiveness, the authors used the so-called "effective theory", designed to model a certain observed phenomenon (in this case, the efficiency of air defense) without describing the underlying processes in detail. Such a theory predicts behavior with moderate success because decisions are often irrational and based on a wrong analysis of the consequences of a choice. In particular, considering the possibility of modeling or predicting decisions from the perspective of an

armed conflict, where "surprise" is one of the basic principles of warfare. Moreover, due to cognitive, time and technical limitations, the observer is frequently not able to describe the observed phenomenon precisely or the information obtained is incomplete. The most famous astrophysicist of our time, Stephen Hawking, explained the use of effective theory in physics, "...we are not able, for example, to strictly solve the equations describing the gravitational interaction of every atom of the human body with every atom of the globe. But for practical purposes, a few numbers are enough to describe the force of gravity (...). " Therefore, it should be kept in mind that the proposed solution for calculating the efficiency of air defense is to some extent a generalization. It is impossible to describe all the dependencies related to the concept of air defense efficiency with a mathematical formula. During the research process, over 100 variables influencing the effectiveness of air defense were distinguished. However, in order to simplify the process, it was decided to include the most important of them based primarily on the opinion of experts.

2. Literature and methods

Despite the fact that the efficiency of air defense is a very important factor helping to assess the feasibility of a task, the vast majority of research in the early twenty-first century was fragmentary. As a result of the analysis of their content, it can be concluded that they propose various qualitative and quantitative methods of determining efficiency. Most often, however, they are detached from the command process carried out at command posts at the tactical and operational level. One of the few publications in which the procedure algorithm determining the effectiveness was presented is the use of "techniques to assess the modernization needs of the military". The solution (method) presented in it allows us to calculate the efficiency of the particular air defense measures performing the task of covering. Its drawback, however, is that it lacks detailed information on the values (indicators) adopted for the calculations (Kacer, and Májek, 2006). In the case of other publications, it can be seen that the efficiency of air defense is defined as the ratio between the reduced potential of the aerial threats obtained thanks to the activity of the anti-aircraft defense forces and the total of this potential (Kazakhov, 2010). These studies also lack the basic information relating to the method of determining the potential, which makes the entire methodology of determining the efficiency difficult to verify from the point of view of the correctness of the assumptions adopted and the possibility of their implementation (Tsyrndorzhiyev, 2012).

Yet another publication proposes the adoption and use of a SWOT analysis for evaluating efficiency, especially at command level (Şandru, 2016). It should be noted that this method is one of the most popular in strategic management of an organization. However, despite the many advantages of SWOT, it also has certain disadvantages. This applies to subjectivism in assessing the efficiency of air defense without taking into account the detailed data on the aerial threats. In this situation, the assessment of air defense may vary despite the same input data and tactical situation and its results will be heavily dependent on the knowledge and experience of the assessor, which may be quite varied.

Another option adopted in evaluating the efficiency of air defense is the use of computer simulation techniques (Zdrodowski, 2003). In this regard, it should be noted that when acting in the conditions of combat operations with limited planning time, during which variants of the operation of the enemy and his own troops are being developed, the commander of the air defense unit (subunit) may not be able to conduct a computer simulation. In addition, it should also be emphasized that the simulation result is largely dependent on the prepared input databases and also the mathematical formulas used to

determine the probability of target destruction.

For many years, the Polish Armed Forces used programs supporting the process of calculating the effectiveness of air defense. They were based on the number of areal threats in the operation, the number simultaneous engagement capability and the so-called fire units used by the air defense unit (sub-unit). The following formula was used to calculate the efficiency of the air defense:

$$E_{AD} = \frac{\sum_{i=1}^{n} K_i * N_{ADSi} * J_i * R_i}{N_s} * 100\% \qquad (1)$$

Where:

E_{AD} – efficiency of air defense;
K_i – general coefficient for particular types of air defense (anti-aircraft) means;
N_{ADSi} – the number of capabilities to simultaneous engagement of multiple targets of AD systems (sub-units), capable of destroying a target on its own with a certain probability, in one firing cycle;
Ji – number of missiles (ammunition) available for i-th type of equipment;
Ri – the coefficient taking into account the number of interactions of the i-th type of equipment, in one firing cycle.

In another variant, the efficiency was calculated on the basis of the number of aircrafts involved in the raid (attack), the raid duration, the number of simultaneous engagement capability and the fire unit provided for a given anti-aircraft system. The following formula was used for this purpose:

$$E_{AD} = \frac{\sum_{i=1}^{n} K_i * N_{ADSi} * \left(\frac{C}{Y} \cdot \frac{T_n}{T_C}\right) * P_i}{N_s} * 100\% \qquad (2)$$

Where:

E_{AD} – efficiency of air defense;
Ki – general coefficient for particular types of air defense (anti-aircraft) system;
N_{ADSi} – the number of capabilities to simultaneous engagement of multiple targets of AD systems (sub-units), capable of destroying a target on its own with a certain probability, in one firing cycle;
Pi – the probability of hitting an air target with a certain number of missiles (ammunition) without taking into account the impact of interference'
C – the number of missiles (ammunition) for a given type of firearms of the air (anti-aircraft) defense;
Y – the estimated average number of missiles (ammunition) used to destroy;
Tn – duration of the raid;
Tc – duration of a firing cycle for the given type of AD system.

In the next variant, it was possible to calculate the air defense efficiency on the basis of the number of air threats in the raid, the duration of the raid, the spatial impact conditions, the number of firing channels and the firing units. The following formula was used for this purpose

$$E_{AD} = \frac{\sum_{i=1}^{n} K_{PUi} * K_i * N_{ADSi} \left(\frac{C}{Y} \cdot \frac{T_n}{T_C}\right) * P_i}{N_s} * 100\% \qquad (3)$$

Where:

E_{AD} – efficiency of air defense;
K_{PUi} – the spatial contribution coefficient for particular types of air defense system;
Ki – general coefficient for particular types of air defense (anti-aircraft) system;
N_{ADSi} – the number of capabilities to simultaneous engagement of multiple targets of AD systems (sub-units), capable of destroying a target on its own with a certain probability, in one firing cycle;
Pi – the probability of hitting an air target with a certain number of missiles (ammunition);
C – the number of missiles (ammunition) for a given type of firearms of the air (anti-aircraft) defense;
Y – the estimated average number of missiles (ammunition) used to destroy the target;
Tn – duration of the raid;
Tc – duration of a firing cycle for the given type of AD system.

Based on the presented examples (variants) of the calculation of the air defense efficiency, it can be noticed that it depends to a large extent on the coefficients adopted when calculating the value of the expected number of destroyed aerial threats. On this basis, it can be concluded that the model for calculating the air defense efficiency will be the more precise, the more precisely the coefficients used in it are selected. Therefore, an attempt was made to define a new methodology where the selection of coefficients will be firstly optimal, and secondly will correspond to the actual, real parameters of individual components on the modern battlefield.

The presented research is the result of a two-year research work carried out under a

research grant financed by the MoD. The research team consisted of four pilots, four specialists in the field of air defense and representatives of air defense support units such as radio engineering troops. Moreover, representatives of the commands and staffs of the Air Defense units and the Air Force of the Polish Armed Forces were invited to participate in the qualitative research.

3. Efficiency of air defense

For the purpose of quantifying the efficiency of aid defense, it is reasonable to use efficiency coefficients that should be: representative, sensitive, simple, systemic and stochastic (Zdrodowski, 2003). The representativeness of the indicator means that it should quantify the degree of performance of the task (achievement of the goal) by the air defense.

1. The sensitivity of the coefficient should be understood as its sensitivity to changes in parameters relevant to the implemented air defense task.
2. Simplicity means that it only includes parameters relevant to the purpose of the air defense. Secondary parameters are omitted here, as they can only complicate the evaluation without increasing the precision of the results.
3. The systemic character consists in selecting the coefficient in such a way that it takes into account the influence of all important factors determining the combat operations of the air defense.

The occurrence of random factors, which is characteristic of the air defense system, is reflected in random variables and determines that the combat efficiency indicator itself - as a function of random variables - is also a random variable, too. For this reason, the value of the efficiency index is most often directly related to the average (expected) value of the aerial threats destroyed by the air defense.

The general formula for calculating the efficiency of air defense systems was thus defined as the quotient of the air defense capabilities, expressed as the expected number of enemy aerial threats destroyed to the expected number of enemy aircrafts operating on the area of operation.

$$E_{AD} = \frac{M_{AD}}{N_{EA}} * 100\% \qquad (4)$$

Where:

EAD – efficiency index (in %);

MAD – air defense capabilities, demonstrated by the average (expected) number of the enemy's destroyed aerial threats;

NEA – the number of enemy aircraft affecting the covered troops (facilities).

The above formula shows that the air defense combat efficiency index is such a numerical characteristic that determines the degree of adaptation of the air defense system to the implementation of the tasks assigned to it. For this reason, the value of the efficiency index is most often directly related to the average (expected) number of the enemy's destroyed aerial threats.

Formula (4) shows that EAD = f (MAD) should be proportional and linear, i.e. each increase in the combat potential of the air defense should be accompanied by a steady increase in the air defense combat efficiency index, as shown in the figure below.

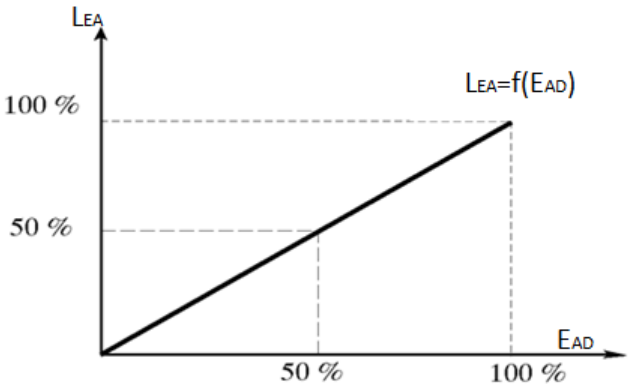


Figure 1. The ratio of aerial threats not performing any tasks (LEA) to the efficiency of air defense (EAD), Adopted from: "Obrona powietrzna" by Zdrodowski et al. p. 29. Copyright 1996, by AON.

The adoption of such assumptions, however, leads to the erroneous conclusion that in order to fully achieve the goal of the air defense in opposing one strike, it is necessary to destroy 100% of the aerial threats affecting the covered troops (facilities). In this regard, it should be noted that this conclusion will be appropriate in a situation where the attack will be carried out only by unmanned aerial systems (UAVs, cruise missiles), which will be characterized by complete remotely or automation of navigation and pilotage. The figure below this situation is represented by the ratio for UAVs.

At this point, it should be noted that assuming that the enemy is conducting an air attack against protected assets only with the use of unmanned aerial and missile threats (ballistic missiles, cruise missiles or unmanned aerial vehicles), there will be no impact on the so-called human factor (pilots and crew).

However, in other situations where there is at least a partial human participation this relationship will change Lea = f (EAD) according to the trajectories shown in the figure for attacks carried out by manned aircrafts and in the mixed formula (manned and unmanned).

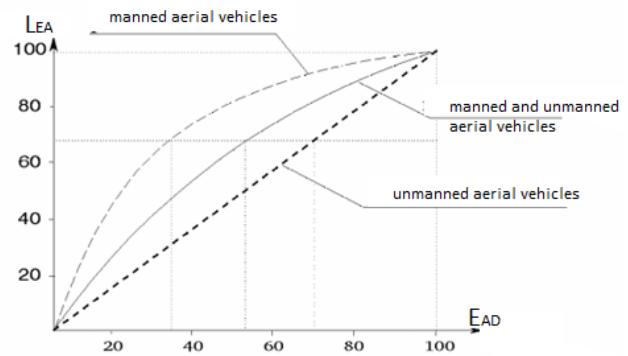


Figure 2. Ratio of LEA = f (EAD) in the contemporary circumstances; Adopted from: "Obrona powietrzna" by B. Zdrodowski et al., p. 29. Copyright 1996, by AON.

In these cases, we are dealing with the psychological impact of aerial threats on aircraft crews. Therefore, it can be assumed that under heavy ground-based fire some of the pilots will perform their tasks in great haste or will abort the mission in fear of losing their own lives.

Following this line of reasoning, it can be concluded that in the case of determining the efficiency of air defense, it will not be only the resultant of the physical destruction of a certain number of the enemy's aerial threats. By adopting this philosophy, it can be assumed that the air defense will be effective when the fire of missiles and artillery will leave the enemy unable to destroy the troops (objects) covered by the air defense forces and, as a result, will not fulfil the combat task.

Therefore, the characteristics of the air defense were determined depending on the efficiency value expressed as a percentage (Table 1).

Table 1.
Characteristics of air defense depending on the value of its efficiency EOP

Air defense efficiency coefficient value	Characteristics of air defense	Expected results
30 % and more	Very strong	Destruction of the enemy air force on day 1 of air operation
20 - 29 %	Strong	Ceasing the air operation within 2-3 days
10-19 %	Average (sufficient)	Maintaining status quo in the air space
Below 10 %	Poor (insufficient)	Winning the control over the airspace by the aerial threats

Adopted from: "Obrona powietrzna" by B. Zdrodowski et al., p. 32. Copyright 1996, by AON.

On the basis of the conducted research, it was established that, in order to prevent the performance of tasks by the aerial threats, they should be contrasted with the air defense potential. It will be characterized by an efficiency index of 30% to 50%, depending on the share of unmanned aerial threats in the total number of aerial threats affecting

the covered troops (facilities). Then, such an air defense can be considered very strong and sufficient, because it promises that on the first day of the operation (combat) the enemy's air operation will be ceased (the enemy's air force will be broken) and thus an absolute superiority in the air (air control) will be achieved. With the efficiency coefficient = 20-30%, conditions are created to break the enemy air operation within 2-3 days, and such an air defense should be described as strong. The efficiency around 10-20% ensures maintaining the status quo of the initial state in the aerial battlefield, i.e. the aerial threats will operate in a limited way, but neither side creates conditions for gaining an advantage in this dimension of the armed struggle. The air defense characterized by such a combat efficiency coefficient should be considered average (sufficient in the range of 10-19%). On the other hand, the efficiency below 10% is insufficient to effectively protect troops (facilities). Moreover, with such an air defense, there is a high probability that the aerial threats will achieve local or operational air control, which in turn may lead to a defeat in all aspects.

4. Determining the amount of aerial threats

The next step in determining the efficiency of air defense is the diagnosis of the capabilities of own forces and assets, expressed in the expected number of aircraft destroyed. In this case, the ability of these troops (including their individual components) to perform combat tasks resulting from the assumed intent, purpose and function of air defense. This ability in operational and tactical evaluation (calculations) is mapped using appropriate numerical indicators characterizing the space, time and effectiveness of air defense forces and its individual components (Halama, and Radomyski, 2003).

It follows that the anti-aircraft defense capabilities result primarily from the qualitative indicators of a particular combat asset and the number of missiles (ammunition) possessed by the given air defense system. In addition, the proposed solution was also extended with the environmental impact (terrain, weather) of the air defense systems. However, this time it was assumed that it may have a negative effect on the capabilities of the air defense. This is due to the fact that the capabilities of the air defense are calculated primarily on the basis of the tactical and technical data of the equipment, i.e. in ideal conditions. Therefore, it was assumed that along with the deterioration of environmental conditions, effectiveness will decrease of the air defense systems would degrade.

The general formula for the air defense capabilities therefore adopted the following form:

$$M_{AD} = \sum_{k=1}^{n} L_k * K_k * J_k - [(1 - W_E) * 100\%] \quad (5)$$

Where:

L_K – the amount of equipment of the k type air defense systems;

K_K – the k type AD system quality coefficient;

J_K – the number of missiles of the k type AD system;

W_E – environmental impact coefficient.

It follows that the capabilities of the air defense are directly proportional to the number of air defense equipment (sets, simultaneous engagement capability), their quality and the number of missiles and/or ammunition available

5. Determining the qualitative coefficients

The greatest challenge of the research was to determine the coefficients used in the algorithms presented. This was due to their

qualitative nature and the confidential nature of some data (e.g. some tactical and technical data of aerial threats and air defense, and the probability coefficients of destroying the target of the missiles).

5.1. Aerial threats impact coefficient

Firstly, an assumption was made regarding the impact coefficient, which determines the percentage of the total combat potential that should be destroyed in order to achieve the goal of the operation. It was also specified that the goal of the action of the aerial threats may be:

Disruption - means that the operation of the object is disturbed, but still possible - 10% of the combat potential destroyed.

Disablement - means that the operation of the object is limited, and recovery to full operability is possible after repairing or replenishing losses - 30% of the combat potential destroyed.

Destruction - means that the object is out of service and cannot be repaired or refurbished - 60% of the combat potential destroyed.

5.2. Defended assets survivability

Generalizing the combat life of the elements of the formation on the battlefield, it was assumed that from a technical point of view (not taking into account the battlefield environment), the following factors will affect the combat life: the ability to recognize the object - i.e. its length and width, speed of movement and armor. The greatest importance is given to length (Wd) and width (Ws) and armor (Wo) - 0.3 each, and the march speed 0.1 (Wpm). From the obtained calculations for individual types of combat equipment, the average value adopted was 3.3, therefore this value was adopted as the unit of the quality coefficient of combat life. Ultimately, the calculation of the combat life took the following form:

Table 2.
Combat life coefficient of the selected military equipment

Coefficient multiplication index	Width [m]	Ws 0.3	Length [m]	Wd 0.3	March speed [km/h]	Wp 0.1	Armor	Wo 0.3	Wż 3.30
Leopard tank	2.7	0.81	3.7	1.11	70	7	2.5	0.75	**1.43**
PT-91 tank	3.5	1.05	9.6	2.88	60	6	2.5	0.75	**4.12**
Infantry Fighting Vehicle	2.3	0.69	5.7	1.71	100	10	1.5	0.45	**1.61**
Reconnaissance Fighting Vehicle	2.9	0.87	6.7	2.01	100	10	1.5	0.45	**2.38**
23 mm ZUR-23-2	1.8	0.54	4.5	1.35	50	5	1	0.3	**0.33**
Automated command and staff vehicle	2.3	0.69	5.7	1.71	100	10	1	0.3	**1.07**
Engineering reconnaissance transporter	2.9	0.87	6.7	2.01	100	10	1	0.3	**1.59**
Engineering vehicle	2.8	0.84	6.4	1.92	60	6	1.5	0.45	**1.32**
Armored vehicle-launched bridge BLG-67M	3.2	0.96	10.4	3.12	50	5	1.5	0.45	**2.04**

5.3. SAM missile combat effectiveness coefficient

It is a factor that generalizes the probability of hitting a target with a rocket. The need to use this coefficient results from the classified nature of these data. Therefore, it was assumed that the guided missile has a 90% probability of hitting the target, and the unguided missile 70%.

5.4. Quality of the aircraft

Another variable related to the calculation of the aerial threats quantity is the aerial threats quality factor (or in other words - the combat value of the aircraft). Since efficiency is closely related to tactics, i.e. with the methods of performing combat tasks in a specific type of aircraft. The combat efficiency of a fighter will be considered in relation to tasks in the scenarios typical for attack aircraft (bombers, fighter-bombers, assault aircraft) will be evaluated in terms of effectiveness in operations against ground or surface targets.

The adopted procedure for assessing the combat value of airplanes included the following elements:

- determining the model parameters of airplanes performing various tactical tasks defined as fighting ground/surface targets;
- determining the values of coefficients that define the degree of compliance of parameters with the standard;
- calculating the partial components for determining the combat value of aircraft;
- determining the overall combat value of the tested aircraft.

The following physical parameters were included in the criteria for evaluating the combat value of airplanes:

- Maximum range
- Radar cross section
- Radar range
- Maximum speed at cruising altitude
- Cruising speed
- Maximum ceiling
- Weapon load capacity

It should be emphasized that during the research, other parameters characterizing the aerial threats were also distinguished, such as:

- maximum speed at low altitude,
- maximum climb speed,
- minimum flight speed,
- number of simultaneously tracked targets,
- number of simultaneous engagement capability (missile),
- maneuverability and thrust vectoring ability,
- spatial parameters of the on-board air and ground target detection and destruction system,
- supercruise flight capability,
- advanced stealth systems,
- rescue, warning and survival systems,
- the scope of using external C4I systems,
- ability to steer unmanned platforms.

However, due to the degree of repetitiveness of the respondents' answers and in order to simplify the calculation, the scope was limited to the seven previously mentioned parameters.

The reference model, adopted to determine the basic combat value indicators and measurements of the analyzed potential enemy aircraft, was based on the Su-25 aircraft data. After calculating the comparative indicators for the detailed parameters of the aircraft, the partial indicators of the combat value were calculated. The obtained results are presented in Appendix 1.

5.5. Type *k* air defense system quality coefficient

For the purposes of the research, it was necessary to compare the combat potentials of anti-aircraft units and sub-units equipped with various anti-aircraft equipment. Therefore, in order to use formula 2, it was necessary to create two databases. The first was a database of anti-aircraft units and sub-units, containing data on the structure, equipment and quantities of anti-aircraft equipment. The second was the anti-aircraft equipment database, containing basic tactical and technical data of the equipment and the calculated quality coefficient of the given type of anti-aircraft equipment.

Determining the quality coefficients for the given type of combat equipment began with the selection of a list of factors characterizing the combat capabilities of anti-aircraft equipment.

From among these factors, those which significantly affect the combat potential of anti-aircraft units and sub-units were selected. They include:

- probability of hitting the target;

- slant range border of the SAM engagement envelope;
- altitude border of the SAM engagement envelope;
- multiple target engagement capability;
- firing cycle;
- time to be ready to open fire from the march position;
- marching speed on dirt roads;
- the ability to cross fords, bridges, ferries and ditches.

The remaining factors were rejected because they are secondary indicators or they have little or no impact on the final result of the study. Secondary indicators include the probability of hitting a target with n number of missiles, which are derivatives of the probability of hitting a target.

The next research step was to define the reference coefficient and the rules for calculating the coefficients for individual pieces of equipment.

The coefficient was calculated with the following formula:

$$JWJ_{AD} = \frac{W_i}{W_w} \qquad (6)$$

Where:

W_i - the conversion factor of the i-th type of anti-aircraft equipment

W_w - the conversion factor of the reference type of anti-aircraft equipment

As a model factor, or a reference factor, the factor calculated for a single OSA anti-aircraft combat vehicle (SA-8) anti-aircraft combat vehicle firing a series of two missiles (in the normal mode of fire). Therefore, for OSA anti-aircraft combat vehicle, the value of the JWJ qualitative index is one.

$$JWJ_{AD} = \frac{W_i}{W_w} = 1 \qquad (7)$$

The value of the conversion factor was calculated as follows:

$$C_K = C_P + C_{DG} + C_{GG} + C_{CS} + C_{TG} + C_{VM} + C_M \qquad (8)$$

Where:

C_P - coefficient taking into account the probability of hitting the target;

C_{DG} - coefficient taking into account the further border of the SAM engagement envelope;

C_{GG} - coefficient taking into account the upper border of the SAM engagement envelope;

C_{KC} - coefficient taking into account the number of simultaneous engagement capability;

C_{CS} - coefficient taking into account the firing cycle;

C_{TG} - coefficient taking into account the time to be ready to open fire from the march position;

C_{VM} - coefficient taking into account the marching speed on dirt roads;

C_M - coefficient taking into account the ability to cross fords, bridges, ferries and ditches.

From the defined dependencies, the Ck coefficient was calculated for a given type of set (measure) of air defense. The values of this coefficient for the selected sets are presented in Table 3.

Table 3.
Value of the Ck coefficient for the selected SAM system

Item	Name of equipment	Kk coefficient
1	AVANGER	1.77
2	BUK (SA-11 Gadfly)	10.59
3	CAROL	1.48
4	HAWK	5.80
5	KUB (SA-6 Gainful)	0.72
6	MANPADS	0.47
7	MISTRAL	0.25
8	S-125 NEWA (SA-3 Goa)	1.16
9	9K33 OSA-AK (SA-8 Gecko)	1.00
10	PATRIOT	2.59
11	RAPIER FSB2	0.72
12	RAPIER FSC	0.83
13	REDEYE	0.16
14	S-300W (SA-12A Gladiator)	3.92

5.6. Environmental impact coefficient

As part of the calculation function, it is calculated how the user-determined atmospheric (weather) and terrain conditions affect own and enemy troops. In order to determine the degree of impact, the program uses the sum of the individual components of the coefficient. This means that the impact of the environment (Wen) is the sum of the impact of weather conditions (Wwth) and terrain conditions (Wt).

$$Wen=Wwth+Wt \quad (9)$$

The weather impact indicator is the sum of the influence of wind, rainfall, fog, cloudiness and temperature, while the field impact indicator is the sum of the influence of the terrain in terms of observation, masking, obstacles, key terrain and approach and maneuver paths. The values assigned to particular parameters oscillate between 1-2% depending on the degree of their impact on the operation (1% - medium impact; 2% - high impact).

6. Conclusion

In conclusion, it should be stated that the air defense efficiency is a numerical value that determines the degree of adaptation of the air defense system to the implementation of the given task. This indicator can be used in both ex ante[1] and ex post[2] evaluations. It is also undoubtedly an important element, inseparable in the decision-making process and in the assessment of the possibility of completing the task by air defense units and sub-units.

The proposed methodology for determining the efficiency of air defense in the tactical level of command, along with algorithms and mathematical formulas, should be treated as the subject of further scientific considerations and at the same time constitutes a kind of invitation to a scientific discussion, which will allow for its improvement. We are also deeply convinced that despite the qualitative nature of the research and many limitations resulting from the extensive nature of the problem under consideration, our study generated the interest of the reader.

For the future study, we are planning to compare real life experiences with the method and equations proposed in this article.

Acknowledgements

The article is an outcome of the research project "Automation of air defense's information and decision making processes in the modelled environment of air threat to armed forces and critical infrastructure objects" project, No GB/5/2018/209/2018/DA funded by Ministry of National Defense during 2018-2022.

References

1. Baldwin, W.C., and Felder, W.N. (2019). Use of the Belonging Metric to Inform Architectural Decisions in an Air Defense Scenario. *Procedia Computer Science*, *153*, 166–176. https://doi.org/10.1016/j.procs.2019.05.067.
2. Fatih Hocaoğlu, M. (2019). Weapon Target Assignment Optimization for Land based Multi-Air Defense Systems: A Goal Programming Approach. *Computers & Industrial Engineering*, *128*, 681-

[1] Ex ante evaluation – a term for an analysis aimed at identifying (assessing) the need for a specific activity carried out before its implementation. Ex ante in Latin means in advance, before something happens.

[2] Ex post evaluation – assessment (evaluation) of the project or undertaking after its completion.

689. https://doi.org/10.1016/j.cie.2019.01.015.
3. FM 3-01-11 (2000). *Air defense artillery refence handbook*. Army HQ, October 2000.
4. FM 6-0 (2014). *Commander and staff organization and operations*. Army HQ, May 2014.
5. Goztepe K., Dizdaroğlu V., and Sağıroğlu Ş. (2015). New directions in military and security studies: artificial intelligence and military decision making process. *International Journal of Information Security Science*, *4(2)*, 75-80. Retrieved from https://www.academia.edu/13666615/New_Directions_in_Military_and_Security_Studies_Artificial_Intelligence_and_Military_Decision_Making_Process, 12.10.2020.
6. Halama A., and Radomyski A. (2003). *Taktyka wojsk obrony przeciwlotniczej*. Warszawa: AON.
7. Klukowski Z., (1999). *Środki napadu powietrznego*, Koszalin: Centrum szkolenia obrony przeciwlotniczej.
8. Kulik, T. (2020). The Selected Aspects of Contemporary Air Threats. *Safety & Defense*, *6*(1), 11-21. https://doi.org/10.37105/sd.47.
9. Li, W., Yi, W., Wen, M., and Orlando, D. (2020). Multi-PRF and multi-frame track-before-detect algorithm in multiple PRF radar system. *Signal Processing*, *174*, https://doi.org/10.1016/j.sigpro.2020.107648.
10. Kazakhov, B.D. (2010). Estimating the Efficiency of Combat Employment for Air Defense Troops in Interservice Formations, *Voyennaya mysl*, *1*. 91-98.
11. Tsyrndorzhiyev, S.R. (2012). On Attempts to further the theory of air defense efficiency. *Military Thought*, 1(21).
12. Radomyski, A., Malinowski, P., and Michalski D. (2018). *Air safety environment of the state*. Wrocław: Grafpol. Retrieved from https://depot.ceon.pl/handle/123456789/16671 12.10.2020.
13. Snyder, J. (1989). *The Ideology Of The Offensive: Military Decision Making and The Disasters of 1914*. New York: Cornell University Press.
14. Şandru, V. (2016). Performances of air defence systems measured with AHP-SWOT analysis. *Forum Scientiae Oeconomia*, *4(1)*, 43-55. Retrieved from https://wsb.edu.pl/container/Wydawnictwo/Forum%204%202016%20Special%20Issue%20no1/forum-004.pdf 12.09.2020
15. Vasilescu, C. (2011). Effective Strategic Decision Making, *Journal of Defense Resources Management*, *2(1)*, 101-106. Retrieved from http://www.jodrm.eu/issues/volume2_issue1/12_vasilescu.pdf, 02.10.2020.
16. Kacer. J., and Májek. V. (2006). Air Defence efficiency according NATO. *Cybernetic Letters*, *1*, 1-9. Retrieved from http://www.cybletter.com/index.php?id=39, 12.09.2020.
17. Wang, F.B., and Dong, C. H. (2013). Fast Intercept Trajectory Optimization for Multi-stage Air Defense Missile Using Hybrid Algorithm. *Procedia Engineering*, *67*, 447-456. https://doi.org/10.1016/j.proeng.2013.12.045.
18. Wilson, A.J. (1994). Technical challenges and opportunities for future air defence. *The RUSI Journal*, 139(5), 64-71. https://doi.org10.1080/03071849408445859.
19. Zdrodowski B., and Zych J. (2003) *Założenia funkcjonalno-techniczne symulatora operacyjno-taktycznego działań sił powietrznych*. Warszawa: AON.
20. Zdrodowski, B., et al. (1996). *Obrona powietrzna,*. Warszawa: AON.

Appendix

Basic tactical and technical parameters of aircraft used by the Air Force of the Russian Federation

	Range max [km]	Wz max	SOP [m2]	Wsop	Radar range [km]	Wzr	Max speed [km/h]	Wpmax	Cruising speed [km/h]	Wpprzel	Max ceiling [km]	Wpumax	Load [T]	Wumax	JWJ * 100
Coefficient multiplication index	0.1		0.1		0.1		0.1		0.3		0.1		0.3		
MIG-25	1865	186.5	4	0.025	100	10	3390	339	2500	750	23	2.3	5	1.5	1.2
MIG-29	1500	150	3	0.03333	70	7	2400	240	1500	450	18	1.8	5.5	1.65	0.32
MIG-31	3300	330	3	0.03333	160	16	2500	250	1500	450	24.4	2.44	6	1.8	2.55
MIG-35	2000	200	2	0.05	160	16	2560	256	1500	450	17.5	1.75	6.5	1.95	1.84
Su-24	940	94	3	0.03333	150	15	2320	232	1530	459	17.5	1.75	9	2.7	0.69
Su-25	500	50	3	0.03333	100	10	880	88	600	180	10	1	4.3	1.29	1
Su-27	3790	379	4	0.025	240	24	2450	245	1350	405	18	1.8	8	2.4	2.86
Su-30	3000	300	4	0.025	240	24	2600	260	1650	495	23	2.3	8	2.4	3.75
Su-34	4000	400	2	0.05	240	24	2200	220	1300	390	14	1.4	8	2.4	4.06
Su-35	3600	360	1	0.1	398	39.8	2750	275	1300	390	18.8	1.88	8	2.4	20.35

SAFETY&DEFENSE
ISSN 2450-551X

Directions of Artillery Development on the Example of the US Military and Artillery Use in the Baltic Sea Region

Adrian GOLONKA
Military University of Land Forces, Wroclaw, Poland;
adrian.golonka@awl.edu.pl, ORCID: 0000-0003-3624-5029

DOI: https://doi.org/10.37105/sd.88

Abstract

This article discusses role of field artillery on battlefield and the current state of field artillery. The purpose of this article is to outline development directions of artillery capability. Army surface-to-surface indirect fires will have a crucial part on the future battlefield. Essential trends in field artillery include: increase in range of fires systems; develop and disseminate of multi-sensor active-seeker munitions; advancement automated command and control; develop and implementation systems order to protect ground forces and forward operating bases from the threat of rockets, artillery, and mortars (C-RAM).

Keywords: fires, field artillery, defense, technology development

1. Introduction

Modern artillery is one of the components of fire support (FS) and it is found in every modern army. The Field Artillery (FA) is one of the basic types of land forces designed to perform fire support tasks. FA is consisted of headquarters and units, as well as fire, reconnaissance and logistic units. Since very beginning of this military brand it was a subject of science discussion concerning modern solution (Walter, 1880) and future development (Walford, 1891) (Sawhney, 1984). Currently, the process of

replacing and modernizing equipment in artillery units is underway. The components introduced into service are equipped with fire platforms, command vehicles, reconnaissance systems, logistic facilities and special-purpose ammunition.

The large differentiation in the intensity of the number of fire platforms is illustrated by the conflict in Ukraine. For example, on the morning of July 11, 2014, the Ukrainian 24th Mechanized Brigade was moving near Zelenopillya (Luhansk Oblast, eastern Ukraine), approx. 10 km from the border with Russia. After occupying the designated area, the Ukrainian forces found interference with their communication and navigation systems. Around 4.20am, unmanned aerial vehicles were spotted watching the columns. Then there was a rocket attack. Around 40 salvos of Russian rockets hit the Ukrainian position. During the five-minute fire attack, the equipment of two battalions was destroyed. This incident was not the only one and caused alarm among western officials (Watling, 2019, p. 8). The great fire possibilities and short reaction time of modern artillery systems are shown by rocket attack. It should be emphasized that the Russian motorized brigade has 81 organic units of artillery equipment (Sutyagin, and Bronk, 2017, p. 30). The organic artillery includes self-propelled howitzers (152 mm and 203 mm) and 300 mm MLRS systems (Multiple Launch Rocket System). In addition, the brigade includes an electronic warfare battalion (Watling, 2019, p. 2). The battalion tactical group has about 18 self-propelled guns (Fox, and Rossow, 2017, p. 6) and can receive support from the MLRS at the brigade level. This illustrates the high saturation with artillery and electronic warfare systems in branches and subunits of the Russian army. In order to reduce the divergence of fire possibilities it is necessary to develop modern artillery systems.

The aim of this work is to present the role of field artillery and to describe the directions of development. Due to the nature and limited scope of this article, the discussion is limited to the most crucial ideas and problems. The article was mainly based on an analysis of the artillery of USA and Russian Federation (RF). Theoretical research methods such as: analysis and synthesis of information comprised in literature and source materials, as well as the inference method were used to develop this article.

2. Role of field artillery

Army surface-to-surface indirect fires includes cannon, rocket, and missile systems as well as mortars organic to maneuver elements. It is necessary to identify the rules of use and tasks of artillery to indicate the future of artillery. The rules for the use of artillery follow the rules of the art of war and include:

- Purposefulness of actions - in relation to artillery, it indicates the need to formulate its tasks aimed at achieving the combat goal. The tasks are assigned to the artillery subunits by the general military commander, in accordance with the purpose and intention of fighting and in accordance with their combat capabilities.
- Activity - is expressed by the constant fire attack on the opponent. Being active also means showing initiative in the way of performing tactical tasks by using various types of fire adequately to the reconnaissance information and types of ammunition.
- Economy of forces - requires commanders at all levels to rationally dispose of the artillery potential. It boils down to observing the rule of designating a sufficient number of fire

platforms to perform the assigned tasks. Higher effectiveness of FS can be achieved by focusing fire on high-value targets (HVT) located in key directions (regions). The concentration of fire is achieved by decentralized operation of artillery subunits with the possibility of its centralization. This is based on the operation of artillery subunits that would provide support to the fighting units and would also enable them to independently perform the tactical tasks they receive. In critical moments of combat, however, it must be possible to centralize the artillery command in order to concentrate the FS effort. This requires the constant selection of HVT and hitting them with separate platforms.

- Maneuverability - performs two basic functions in artillery. It enables the efficient reception of an appropriate formation and a systematic maneuver between regions in order to occupy a convenient formation to perform tactical tasks. Maneuver enables focusing and shifting the fire effort on the most important directions of activities. It is subordinated to the principle of the economy of power and the need to ensure the continuity of FS for troops. Maneuverability is also a method of maintaining combat vitality. The implementation of this principle is ensured by the maneuverability of artillery units (the ability to cross a variety of terrain) and their armor.
- Surprise with artillery fire - is expressed by unexpected fire for the opponent with high intensity. Combat capabilities of artillery guarantee achieving this effect. Compliance with the principle of surprise is essential for the effectiveness of artillery fire. Fire made by surprise is highly effective, measured by the amount of material and psychological losses of the opponent. The greatest effects of a fire resulting from a surprise are achieved in the initial moment of its conduct. Fire for effect should be precise, intense and conducted in a short period of time. It should be performed when the opponent is out of cover (trenches, armored vehicles), then his orientation is difficult and the routine counteracting the effects of fire is disturbed. The surprise is also obtained by precisely recognizing the enemy and keeping the artillery's maneuver preparing to open fire in secret.
- Maintaining combat capability - compliance with this principle consists in using artillery in such a way that will ensure its constant readiness to perform FS throughout combat. This means the necessity of rational management of human and material potential. In order to maintain combat capability, an appropriate formation of artillery units should be received. Moreover timely relocations to the next, more convenient areas, including the change of gun fire positions immediately after each fire task should be completed (Działania, 2016, p. 11-14).

In line with US doctrines, the role of the field artillery (FA) is **to destroy, neutralize, or suppress** the enemy by cannon, rocket, and missile fire and to integrate and synchronize all fire support assets into operations. Fire support is fires that directly support land, maritime, amphibious, and special operations forces to engage enemy forces, combat formations, and facilities in pursuit of tactical and operational objectives (ADP 3-19, 2019, p. 21).

The basic tasks of artillery in accordance with the Polish nomenclature include:

- Close Supporting Fire;
- Deep Supporting Fire;
- Counter Battery Fire;
- Command and Control Warfare;

- Suppression of Enemy Air Defense (*Działania*, 2016, p. 15).

Close support fire is artillery fire placed on enemy troops, weapons, or positions which, because of their proximity, present the most immediate and serious threat to the supported unit. **Deep Supporting Fire** is artillery fire directed at objectives not in the immediate vicinity of our forces, for neutralizing and destroying enemy reserves and weapons, and interfering with enemy command, supply, communications, and observations. It is carried out to prevent and disorganize the approach and deployment for action, reduce the enemy's combat potential and disrupt the supply system. **Counter Battery Fire** is the primary task of a division's artillery. Counter Fire is a battlefield military activity to defeat the enemy's indirect fire elements (guns, rocket launchers, artillery and mortars), including their target acquisition, command and control components. This task is carried out artillery units independently or in cooperation with aviation and electronic warfare. **Command and Control Warfare** consists in hitting and disrupting the work of selected elements of command post (brigade and division levels)(CP), command points (tracking, interfering, etc.) of reconnaissance and electronic warfare units. This task should be carried out continuously at all stages of the fight. For effective use, artillery fire should be coordinated with electronic interaction. **Suppression of Enemy Air Defense-** activity that neutralizes, destroys, or temporarily degrades surface-based enemy air defenses by destructive and/or disruptive means.

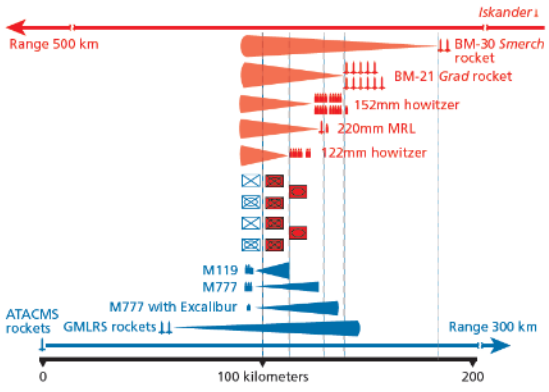
In summary, the four main roles of artillery on the modern battlefield can be identified:

- suppression of enemy fires;
- striking high-value targets (HVTs);
- breaking up enemy force concentrations;
- providing fire support to enable maneuver (Watling, 2019, p. 5).

Completing each task will facilitate the execution of consecutive tasks.

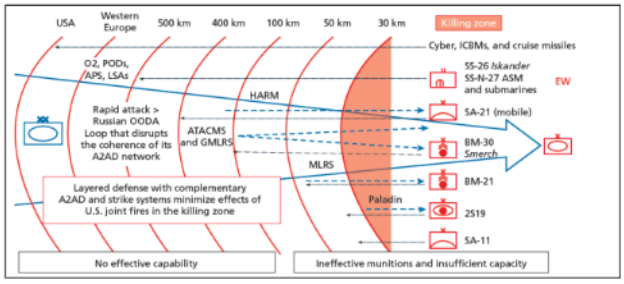
3. Modern artillery

The artillery of the U.S. and RF were compared in this article to present modern artillery capabilities. The U.S. Army field artillery has been recognized as one of the most powerful and relevant branches of the service since at least World War II. Field artillery played a major role during: the “hybrid” warfare period of Vietnam (1964–1972) and Operation Desert Storm of 1991. There was a very large amount of field artillery to support the armored units. By 2013, there was renewed interest in preparation for conventional combat. Offensive moves by Russia against Crimea and Ukraine, fear of Russian coercion against the Baltic states, an expanding Iranian military, and expeditiously growing Chinese military capabilities all contributed to the revived U.S. interest in conventional operations. Since 2017, the Russian Army has made significant advances in its artillery. Key Russian artillery capabilities include long-range multiple rocket launchers, such as the BM-30 Smerch, which can fire a wide variety of warheads up to 90 km. The SS-26 Iskander short-range ballistic missile also fires various warheads (including nuclear weapons) against targets at ranges of over 400 km. The Russian Army has deployed large numbers of cannons and rocket launchers at the brigade and battalion tactical group levels. When combined with a growing, multifaceted targeting and reconnaissance capability, Russian artillery is a tremendous potential opponent. Target acquisition systems are also improving. For example, the U.S. military has greatly expanded its use of unmanned aerial systems (UASs) since the start of Operation Enduring Freedom in 2001. Other countries have followed a similar course of action (Gordon IV, 2019, p. 14-15).



NOTES: MRL = multiple rocket launcher; ATACMS = Army Tactical Missile System; GMLRS = Guided Multiple Rocket Launch System.

Figure 1. U.S. Army Fires Compared with Russian Fires in a Baltics Scenario (Gordon IV, 2019, p. 15).



NOTES: ICBM = intercontinental ballistic missile; HARM = High-Speed Anti-Radar Missile; OODA = observe, orient, decide, and act; MLRS = Multiple Launch Rocket System; TACMS = Army Tactical Missile System.

Figure 2. Imbalance Between NATO and Russian Long-Range Fires Capabilities (Gordon IV, 2019, p. 42).

A simple comparison of the U.S. Army field artillery its counterpart systems in the Russian Army is shown in Figure 1. Russian artillery platforms (Iskander) have a greater range than that of the U.S.

Figure 2 shows that U.S. and NATO forces and assets can come under fire throughout the theater from Russian systems, such as the Iskander and the SS-N-27, with no system capable of responding beyond fixed-wing aircraft. This problem is compounded by Russian longrange IADS, built around the SA-21 (along with Russian airpower), that can block NATO from using its airpower in a decisive way early in the conflict. Russian rockets and artillery also outrange their NATO counterparts and thus can threaten NATO ground forces while protecting Russian forces from what could be decisive NATO close combat capabilities (Gordon IV, 2019, p. 41).

The following recommendations are presented to reduce disparities:

- increase the number of field artillery units that can deploy quickly to a crisis or that are located forward, where the fast arrival of allied forces is essential;
- improve the Army's ability to quickly get and utilize intelligence, surveillance, and reconnaissance (ISR) data from the other services;
- modernize the Army's cannon systems, particularly in terms of range and rate of fire;
- ensure that there is a timely and adequate replacement for the Army Tactical Cruise Missile System (ATACMS);
- improve Army ground forces target acquisition capabilities;
- improve the artillery's ability to provide fire support to allied and coalition partners;
- enhance the field artillery's electronic warfare (EW) and cyber resilience;
- reduce the artillery's vulnerability to enemy fires through reduced exposure to EW targeting, improved mobility, and use of camouflage and decoys;
- improve the survivability of artillery units against enemy indirect fire, airborne, and ground threats;
- emphasize major conventional opponents in field artillery, combined arms, and joint training exercises;
- continually assess technology trends that could improve the effectiveness of field artillery units (Gordon IV, 2019, p. 16-17).

4. Trends in increase artillery capability

Presently technological developments in artillery are incremental and slow. Nevertheless, some technological trends that are likely to have a transformative effect on the delivery of fire against ground targets can be mentioned. Based on analysis of the U.S. and RF artillery, four crucial trends can be indicated while acknowledging that the capabilities outlined in this article do not remove the value of unguided high explosives, and are transformative only when employed as part of a coherent concept of operations. The following trends should be considered:

- the increasing range of artillery systems;
- the maturation of active seeker munitions with sufficient fidelity to reliably strike ground targets;
- automated command and control (C2) systems able to decrease the complexity of kill chains;
- increasingly sophisticated Counter-Rocket, Artillery, Mortar (C-RAM) systems.

These capability trends induce fires capabilities in three critical ways:

- the probability of kill (PK) of fire missions is increasing, reducing the number of platforms needed to deliver significant effects;
- there is a growing tension between the need to manage munitions, and the speed of engagement, which is pulling C2 both down and up echelons;
- the battlefield is increasingly divided not so much by range, but by zones where fires outweigh protection, and vice versa (Watling, 2019, p. 17).

Increasing range. Modernly, 155-mm and 152-mm howitzers have reached ranges between 32km and 48km using base bleed, while MLRS systems have achieved 70–120-km ranges. Under test conditions, the artillery achieved even greater range (155-mm howitzers able to deliver rounds up to 70km (Keller, 2019)). By using gliding bombs (stand-off bombs), 120-mm mortars have extended their ranges from 5km to up to 16km (Watling, 2019, p. 17). In 2021, the U.S. Army will test the Precision Strike Missile (PrSM) at its maximum range of over 480 km (Freedberg, 2020). Across the world, the ranges of standard artillery systems are being pushed further and further. It should not be assumed that this trend will continue infinitely. With the use of conventional projectiles accuracy decrease as the range increases (especially at maximum ranges). It is estimated that ranges of artillery systems are likely to increase by 50–100%. The general increase in range will have a complex impact on the modern battlefield. Improvement will effect C2 and how maneuver elements will need to operate, and coordinate with their fires. The range of artillery is increasing while the speed of advance of maneuver formations does not. In effect the correlation between the range of fire systems and the reach of maneuver elements is being changed. A greater range means that batteries are less tied to brigade displacements during combat. It therefore becomes possible to provide support by artillery batteries to a greater number of independently maneuvering elements. This means that a gun line may be dispersed further to the rear, and operate as a centrally managed divisional fires group, but still provide support to each maneuver brigade. Thus, the command of the emplacement and fires plans of guns may be held for longer at a higher level. A further consequence of the increase in range is that whereas traditionally a brigade would receive fire support from the batteries assigned to support its operations, the increase in range enables a smaller number of guns in a divisional fires group to nevertheless bring a higher proportion of the group's fire to bear in support of a specific maneuver brigade. A further significant effect of the increasing range of fires systems is its impact on sustainment operations (Watling, 2019, p. 18-19).

Multi-Sensor Active-Seeker Munitions. Most early precision weaponry con-

tained guided munitions, brought on to target by a laser designator, or with the course corrected by an operator. The need for constant communication between the operator and projectile reduces the effective range or provides a single dependency that could be disrupted by opponent EW capabilities. These challenges are now being overcome with the miniaturization of computing and the integration of multi-sensor munitions, with the ability to autonomously seek targets. Inertial guidance is consistently able to bring munitions close enough for onboard sensors to begin course correction during the last phase. All single sensors have curtailments. Electro-optical sensors, for instance – presumably to offer the most accurate strikes – tend to struggle if visibility is limited below 700m. Millimetric radar seekers are able to pick out armored vehicles in dense terrain or poor visibility, but struggle to distinguish between a priority target, a not-priority target and the decoy beside it. In the meanwhile, camouflage materials are able to counter infrared seekers. The ability to integrate multiple targeting systems into a single munition has greatly increased the reliability, fidelity and accuracy of precision munitions, while computer processing has enabled munitions to autonomously course correct to deliver precision strikes. The develop and application of multi-sensor active-seeker munitions is increasing the lethality of a range of fires systems against dynamic targets. Munitions with multi-sensors reduce the number of rounds required to break up enemy force concentrations of vehicles or conduct counterbattery fire (Watling, 2019, p. 21-22). Another crucial path of development for multi-sensor active-seeker capabilities is small-target unmanned aerial vehicles (UAVs). There has been a great deal of hype regarding autonomous swarms of UAVs, and while such technologies may have some utility in spoofing radar systems, swarming technology is unlikely to be transformative in the delivery of fires (Davis, 2014, p.4). An additionally critical element of these systems is their capacity to act as loitering munitions to deny ground. The emplacement of such active-seeker munitions into identified corridors of adversary advance enables tactical units to canalize enemy forces and shape their movement, diverting them into kill zones for conventional artillery. The capabilities of Multi-Sensor Active-Seeker Munitions causes complications in the management of fires. If the range of conventional fires is enabling their management at higher echelons, the speed of engagement required to maximize the effects of active-seeker munitions forces the decision to employ fires as low as possible. The point is that an active-seeker only functions if there is a target within the area that it can scan. Either the friendly maneuver element calling for fire must fix the target, potentially exposing themselves to comparable effects, or the time between the call for effect and its delivery must be reduced as much as possible. Units in contact with enemy which will be calling for fire will tend to calling for the effect with the highest PK to engage any and all available targets. As a result of a limited amount of active-seeker munitions available this will deplete ammunition supplies. Ensuring a quick enough kill chain therefore demands the development of appropriate supportive C2 processes (Watling, 2019, p. 23-24).

Automated command and control (C2). The concept of a unified and complete battlespace management system enabling the three-dimensional visualization of the battlespace in real time is important in military nowadays. It is questionable that such a system becoming feasible. However, the drive towards advanced battlespace management is creating an increasingly diverse range of methods for fusing disparate sensor feeds. The most important developments are systems designated to translate separate and distinct data sets into a single language, enabling different types of data to be compared. These capabilities have important implications for artillery systems by reshaping

kill chains, and the decision point for the application of fires. The quantity of sensor data is still to expand, but in a high-intensity conflict the capacity to process it will be limited, and the viability of having a large targeting cell supporting the high number of synchronic operations involved is doubtful. Moreover, the need to transfer large quantities of data to centralized headquarters for it to be processed produces a slow kill chain. The time lag created by the transmission and processing of data also makes keeping track of dynamic targets difficult without a constant exchange between sensor and shooter, which must be vulnerable to interference. The link also creates a durable signature, enabling foes to locate and fire upon command infrastructure. System operation can be presented as follows: a sensor has located an enemy truck-mounted command vehicle. Rather than passing its coordinates, the observer takes a picture, marking one of the pixels from the target, and transmits this image in a single explosion to the fires CP. At the CP, the image is received and fused with other images from other planes, most importantly a satellite or aerial image, which allows the target pixel in the vertical plane to be translated into a point on a map. The fusion system – using computer vision – also notes that the target is specific type of equipment and attaches the electro-optical, infrared and radar signature of this target to the data packet containing the target's coordinates. This is transferred to a fire platform, and the data is ingested by the munition, which is launched to the area containing the vehicle. Having reached the area, the sensors in the missile warhead first identify the pixel from the original photograph, and then scan to see whether the target still resembles the command vehicle. If the signature has changed, the missile could then scan the area to see where the target had moved to, and course correct (Watling, 2019, p. 25).

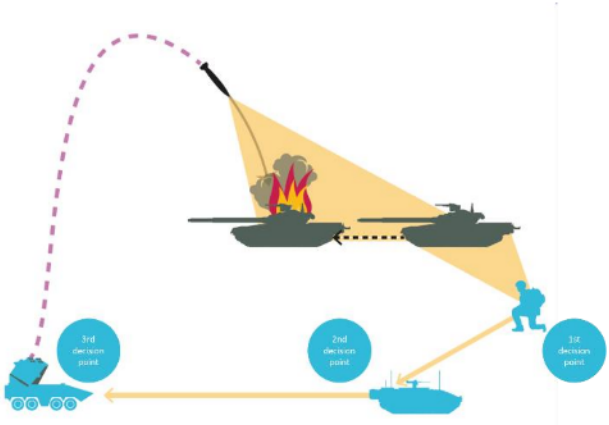


Figure 3. Kill Chain with decision points. Own work basis on Watling, 2019, p. 26.

The system described above is indicative of a C2 architecture for fires that is probably to become increasingly viable and widespread. Its application has the effect of increasing speed of the targeting cycle, while reducing the amount of calculations required by fire controllers. Such a system has three decision points: the sensor operator deciding to call for fires; the fires CP which must assess whether the target selected is worth the ammunition necessary to destroy it; and the fire platform commander, who must assess whether launching would expose their platform to risk. In general, as the supply of ammunition is an operational affair, command would rest with the CP, but the need to ensure the fastest possible speed of engagement would encourage pushing control to the sensor operator (Watling, 2019, p. 26).

C-RAM. Counter-Rocket, Artillery, Mortar system was developed early during Operation Iraqi Freedom/Enduring Freedom in order to protect ground forces and forward operating bases from the threat of rockets, artillery, and mortars. C-RAM systems must be coordinated through airspace control means and be integrated in the NATO Integrated Air Defense System (NATINAMDS) architecture. The C-RAM serves as defense against artillery, and in this context, its development sets new directions for field artillery. C-RAM is made up of a variety

of systems which provide the ability to sense, warn, respond, intercept, command and control, shape, and protect deployed forces. C-RAM components include the Forward Area Air Defense Command and Control (FAAD C2), Land-based Phalanx Weapon Systems (LPWS), Lightweight Counter Mortar Radars (LCMR), Firefinder radars, Kaband Multi-Function Radio Frequency Systems (MFRFS), Air and Missile Defense Workstation (AMDWS), and several other components that contribute to system intercept and communications (*Counter-Rocket,* 2018). The development of high-accuracy search-and-track radar has reached the point that it can direct rotary cannon to accurately and consistently engage mortars and artillery rounds, causing them to detonate in flight. The capacity to hard-kill incoming artillery, providing area defense against indirect fires, is meaningful. The location of such systems can provide a final and strong layer of point defense for critical areas. However, these systems speedily deplete their ammunition, can be saturated and are expensive. Moreover, they are easily to trace due to their radar emission. It should be noted that as munitions are increasingly dependent on sophisticated sensors to locate their targets, so too do they become potential victims of decoys. The ability to absorb precision strikes by setting up dummy systems has the potential to notably increase the amount of munitions needed to destroy a set of targets. Decoys, however, are large, heavy, and generally take time to assemble, so while they may be used to protect HVTs, they are less likely to provide protection to maneuvering tactical platforms. The one exception is against EW directed fires, as it is now possible for very small emitters to imitate the signature of battlegroup headquarters and other HVTs (Watling, 2019, p. 29-31). Further work on the development of this technology is necessary.

5. Summary

This work has tried to outline the critical trends in the development of the next generation artillery systems. They include:

- the increase in range of fires systems, potentially doubling the range of most precision ammunition;
- the development and dissemination of multi-sensor active-seeker munitions;
- the capacity to link various information to advance the targeting process and centralize control of fires;
- the development C-RAM capable of creating protected nodes from artillery.

Despite this technological progression, however, it is understandable that conventional ammunition have a crucial role on the future battlefield in view of the cost and limited stockpiles of precision-guided munitions that forces can maintain. The future battlefield created by new trends will be packed with the growing number of sensors. They will give the ability to aggregate and fuse their data rapidly. As a result of the enlargement in the range of systems with a high PK, enabling the delivery of a high amount of projectiles onto maneuvering force concentrations on the future battlefield will be a much smaller force density. Field artillery will be a crucial component of the future battlefield. The next phase of development will be the implementation of an automatic C2 system for autonomous unmanned fire platforms with using UAVs.

References

1. *ADP 3-19*. (2019). Headquarters Department of the Army.
2. Walter H. James R.E. (1880). *Modern Field Artillery*, Royal United Services Institution. Journal, 24(107), pp. 737-759, DOI: https://doi.org/10.1080/03071848009417168
3. *Counter-Rocket, Artillery, Mortar (C-RAM)*. (2018). U.S. Air Defense, intercept, missile defense https://missiledefenseadvocacy.org/defense-systems/counter-rocket-artillery-mortar-c-ram, access: 30.10.2020
4. Davis L.E. et al. (2014) *Armed and Dangerous? UAVs and U.S. Security* (Santa Monica, CA: RAND Corporation.
5. *Działania Taktyczne Pododdziałów Artylerii– Poradnik (155 mm Krab)* (2016). DGRSZ, ZWRiA
6. Fox, A.C., Rossow, A.J. (2017). *Making Sense of Russian Hybrid Warfare: A Brief Assessment of the Russo–Ukrainian War*. The Land Warfare Papers, No. 112.
7. Freedberg Jr., S.J. (2020) https://breakingdefense.com/2020/04/army-lockheed-prsm-missile-aces-third-flight-test/ (access: 30.10.2020).
8. Gordon IV, J. (2019). *Army Fires Capabilities for 2025 and Beyond*. RAND Corporation.
9. Keller, J. (2019). *Meet the M1299, the new Army howitzer with twice the range of the Paladin*. Available online https://taskandpurpose.com/military-tech/army-m1299-howitzer-designation, access: 30.10.2020
10. Sutyagin, I., Bronk, J. (2017). *Russia's New Ground Forces: Capabilities, Limitations and Implications for International Security*. RUSI Whitehall Paper 89, London, 2017.
11. Sawhney R. G. (1984) Field Artillery Today and Tomorrow, Strategic Analysis, 7(11), pp. 928-941, DOI: https://doi.org/10.1080/09700168409428662
12. Watling, J. (2019). *The Future of Fires Maximising the UK's Tactical and Operational Firepower*. RUSI Occasional Paper.
13. Walford R.A. (1891) *The Development of Field Artillery Material*, Royal United Services Institution. Journal, 35 (158), pp. 321-344, DOI: https://doi.org/10.1080/03071849109417294

SAFETY&DEFENSE
ISSN 2450-551X

Air Terrorism as a Threat to the Safety of Air Transport

Jacek PAJĄK

General Tadeusz Kościuszko Military University of Land Forces, Wrocław, Poland;
jacek.pajak@awl.edu.pl, ORCID: 0000-0003-0770-1881

DOI: https://doi.org/10.37105/sd.90

Abstract

The author of this article addresses the issue of the threat posed to air transport security by air terrorism. The main goal of this article is to identify the specific threats arising from air terrorism and examine their implications for the functioning of air transport as a whole. The dangers posed by attacks using hijacked light aircraft as well as large passenger airliners are highlighted. The article is based on the literature study and the author's own analyses of the issue.

Keywords: air security, air terrorism, safety of air transport, safety.

1. Introduction

The turn of the 20th and 21st centuries has been a period in human history characterized by dynamic changes in the living conditions of the inhabitants of the Earth. Despite being largely positive, these changes have not been without their negative effects. Globalization is one of many processes that is developing dynamically. It fosters a situation in which state borders do not pose an obstacle to the movement of people or goods of all kinds, whether by sea, air or land. A crucial factor serving to accelerate this process is the communications revolution that is taking place in physical as well as virtual reality. Individual areas of social and economic life are becoming elements of a new, more interdependent system. The globalization of markets is resulting in changes to the scale and nature of activity occurring in international airspace. Air transport, which includes both air travel and air freight, may be defined as the displacement of people or goods via the air by means of aircraft, which is to say airplanes or helicopters. The principal aim of this article is to identify and analyze the spectrum of air terrorism threats

and their impact on the safety of air transport. The author pays special attention to such counter-measures that may prove effective against the threats posed to air transport safety by air terrorist activity.

The thesis assumes that the phenomenon of air terrorism over the last several decades has become the greatest threat to air transport safety by posing a direct threat to lives of both travelers and ordinary residents who may die as a result of an act of air terror. In addition, there is a noticeable increase in the psychological impact on society and economic impact on the aviation industry.

2. Identification of threats to air transport safety

Air transport may be classified as either civil or military. Civil aviation is a widely available means of air transport, comprising Sport Aviation (e.g. gliders), General Aviation (private planes, VIP planes) and Transport Aviation (passengers and freight transport). Military aviation is conducted by individual countries. This type of aviation is commonly used to deliver humanitarian aid, transport political VIPs and escort civil planes with technical problems.

Security threats in airspace can be of various natures and sources. Among them we distinguish, natural threats, the occurrence of which humanity has no control over and which it cannot actually counteract. These are passing meteorites, volcanic eruptions and other cataclysms. Safety may also be adversely affected by inadequately operating and obsolete airborne radio, navigation or meteorological maintenance systems and factors such as faulty traffic control and poor training, fatigue or fatigue of pilots. There were also cases of shooting down aircrafts, including civilian ones, and violating the airspace of other countries. Another important factor determining safety in the airspace is the constantly growing number of aircraft and systematically increasing air traffic. Concomitantly it can be asserted that air transport is state-of-the-art and is the most dynamically developing branch of transport. It is based on sophisticated means of transport, navigation and ground maintenance and it involves enormous financial outlays and highly qualified personnel. Air transport allows one to reach a given destination quickly. As mentioned above, despite its many positive social aspects, air transport is connected with one negative phenomenon, namely air terrorism. That phenomenon poses a threat to the lives of passengers and to the lives of others, who are the potential victims of terrorist attacks by virtue of being in an affected air-space or airport zone.

3. Terrorists attacks

The very term “terrorism” is derived from the Latin word terror, which means terror, fear, fear as well as various aspects of violence and rape that cause a feeling of fear. Terrorism is the use of violence, rape, cruelty to intimidate someone (Witkowski, 2000). There are two meanings of this word in Polish. Terror means the use of the violence including rape, cruelty to intimidate the opponent and the very effect of such behavior in the form of terror, fear, dread or intimidation (Terror, 1989). Air terrorism, as one of the phenomena of terrorism, belongs today to the most dangerous social phenomena. It is a deliberate and systematic method used to achieve goals by terrorist groups, and one that is constantly evolving. With a high degree of probability it can be repeated after some of the greatest experts in aviation terrorism in the world: B. Jenkins and P. Wilkinson, that we are currently preparing legally and organizationally only for past terrorist attacks - and not those that will follow.

This type of crime is an excellent and extremely cheap tool of intimidation, and perhaps above all, international publicity. Suffice it to quote the statement made in 1970 by Dr. George Habasch, the former leader of the People's Front for the Liberation of Palestine.

Hijacking large plane has a greater effect in propaganda and the media than killing one hundred Israelis in a battle (Gotowała, 2006). Therefore, it is almost certain that this phenomenon will continue to be one of the basic instruments for achieving goals by existing or aspiring to such a name international terrorist organizations. In today's world we are dealing with an increase in the field of:

- information exchange;
- moving around;
- transport of goods;
- development of incentives influencing the environment in which we operate.

The main factor influencing the speed of changes is of course, time in these areas of human activity. The speed of movement, the flow of information, or the timely delivery of raw materials for pro-duction, etc., undoubtedly affects the pace of development in almost all spheres of human existence.

Due to this, air transport, and above all civil aviation, is such a very important element defining the way the reality around us functions. It was civil aviation that was and will continue to be the target of terrorist attacks. Therefore, a key element of the state's anti-terrorist security system is the protection of civil aviation - not only and only aircraft, but also airports. The figure below shows the possibilities of carrying out attacks related to the phenomenon of air terrorism.

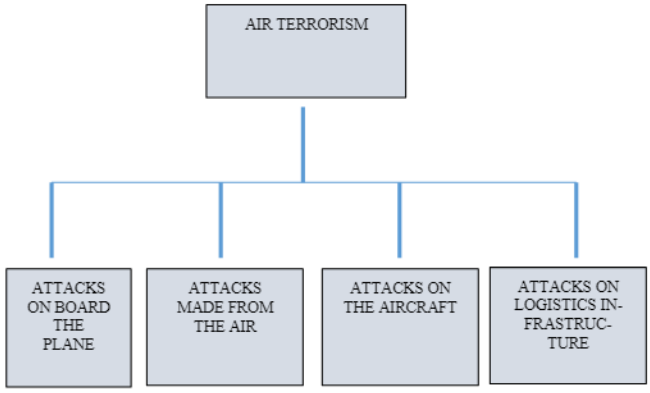


Figure 1. Possibility of attacks – air terrorism

Some researchers describe the phenomenon of terrorism as the new paradigm of war and it is becoming a primary threat for many countries (Marks, 2006; Kingshott, 2003). Counteracting this threat requires not only preventing direct losses to people or damages of an economic nature. The fight against terrorism is also an element of efforts to:

- social and political stability of the state;
- safe development;
- undisturbed course of processes that determine the normal functioning of the community.

It can be seen that over time, various social groups are targets of terrorist attacks. These attacks take more and more massive forms, and terrorism itself is becoming more and more brutal and less and less precise.

Historically, the first recorded hijacking case was the hijacking of a Peruvian airline in 1930. However, based on the data provided by the International Civil Aviation Organization, the first post-war case of "hijacking" involving the unlawful seizure of an aircraft by force or threat was hijacking a plane flying from Macao in 1948. In the following years, we can already observe a jump in the phenomenon, the peak of which took place in 1969, when 80 cases of hijacking were recorded.

Based on an analysis of the motives of air terrorism, it appears that the initially hijacked aircraft were used as a means of transport. They consisted in taking control of the plane by forcing the pilot to change

course and forcing him to land in another country in order to escape. The planes were then hijacked to take hostages or to destroy an aircraft in order to obtain adequate benefits from the government of the country concerned.

A completely new page in the history of air terrorism was turned by the aforementioned events of September 11, 2001. Then we not only faced a change in the way the attacks were carried out, but also a completely different personal format of the attackers. Not a single plane was hijacked, but four ships. These planes were used as means of destruction for military, public and civil administration purposes. The kidnappers turned out to be educated people at the same time ready to sacrifice their own lives. The world has faced an enormous challenge to define the perpetrator, without which it is impossible to effectively counteract.

Nowadays, terrorism is one of the most dangerous social phenomena in the world and poses a worldwide threat to security. The most developed, wealthy and democratic countries are especially exposed to terrorist attacks of all kinds.

From ancient times, the methods and forms of terrorist activity have developed alongside and keeping pace with those of civilization itself. This kind of activity has, however, always been dominated by brutality and the urge to gain publicity for a cause. Terrorists very often place the issues that they fight for above their own lives and they do not bother about the lives of others. The development of civilization is responsible for the delivery of novel tools and also targets: urban communications systems such as the metro; shopping centers, hotels, passenger ships. Planes have been of great interest to terrorists as potential targets since the 1930s. The incident that took place on the night between 22 and 23 July 1968, when three terrorists from the Popular Front for the Liberation of Palestine took over an Israeli airliner, El Al Flight. El Al Flight 426 was route from Rome to Tel Aviv when the Boeing 707 was hijacked by three terrorists from the PFLP (Popular Front for the Liberation of Palestine), who ordered the pilot to land in Algeria. They had assumed that Yitzhak Rabin, the Israeli ambassador in the USA, would be taking this flight. There were 38 passengers and 10 crew members on board. Negotiations with the hijackers took four days and eventually ended with the release of the hostages (O2, 2016). This fact marked the beginning of a period in which passenger airplanes became the principal target of terrorist attacks. Over the years, terrorists have extended the range of their attacks upon aviation-related targets. They have turned their attention to airports, aviation infrastructure and the offices of airlines (Wilkinson, and Jenkins, 1999). Rationales for the planning and execution of air terrorist attacks have multiplied. The methods and forms of the attacks themselves have evolved, as has the scale of their impact.

Air terrorism is either directed against aviation-related targets or uses aviation personnel or aircraft equipment instrumentally against targets unrelated to aviation. It can also do both, i.e., use air devices and operational personnel to target other aviation-related targets. Terrorist attacks against civil transport aircraft or air transport systems can use:

- light aircraft;
- transport aircraft;
- civil transport aircraft;
- man-portable air defense;
- man-portable anti-tank systems;
- grenade launchers and firearms;
- explosives;
- anti-personnel mines;
- chemical, biological agents;
- cyberterrorism.

Considering the first item on this list, namely light aircraft. During periods of elevated terrorist threat, the risk of light aircraft or helicopters being used to carry out an attack against civil transport aircraft and/or air transport should be taken extremely seriously as such an attack can be devastating. The events of 11 September 2001 in New York and Washington show just how significant a threat this is. Nowadays terrorist attacks using hijacked light aircraft are facili-

tated by easy access to unprotected small airdromes and landing strips. For as long as the special protection of such places is not prioritized, the probability of a terrorist attack using light aircraft during periods of elevated threat is going to be high.

The next category to consider is that of civil transport aircraft, such as airliners or other transport aircraft that carry cargo or mail. Nowadays, it is estimated that passenger aircraft in associated airlines number 13 300, a passenger airline is an airline dedicated to the transport of passengers. There are several types of passenger airlines, mainly: transcontinental, medium and short-range (Domański, 1974), although it is anticipated that the need for such aircraft will decrease and that the number will drop to 28 500 in 2026 (Augustyniak, 2008). In the aviation sector, 750 carriers are in operation, carrying 4.5 billion passengers every year. According to estimated data from the Airport International Council (AIC), headquartered in Geneva, the number of travelers using aviation transport will have doubled by 2025 so as to exceed 9 billion passengers (Puls Biznesu, 2007). It should be noticed that these numbers do not involve private carriers and their aircraft.

Such rapid expansion of passenger air transport is a consequence of the corresponding growth in the clientele of low-fare airlines which have come to control one quarter of the market. The prevalence of air transport, with its ever-expanding passenger numbers and air carrier fleets, creates an opportunity which is highly likely to be exploited by terrorists. After 11 September 2001 the strictest security regimes were introduced by aviation authorities all over the world. However, a series of thwarted attempts to hijack civil transport aircraft since then have shown that terrorists are perpetually on the look-out for new methods, forms and ways to take over such aircraft. In Great Britain in August 2006, terrorists tried to take over seven scheduled flights. British intelligence services foiled the attempt of several dozen terrorists to hijack commercial air-liners taking off from Heathrow airport. Terrorists intended to use those aircraft to attack public places located in one of the biggest cities in the USA. Their plans involved using chemical liquid substances trafficked in carry-on luggage to create explosives on the planes (RMF.FM, 2006)

The next attempt to use an airliner, in this instance one belonging to the USA's Northwest Airlines, for a terrorist attack occurred on 23 December 2009. As this plane was landing at the Detroit Airport with 278 passengers and 11 crew members on board, Nigerian bomber Umar Faruk Abdulmutallab, associated with Al-Qaeda, tried to detonate an explosive charge called PETN which was sewn into his clothes. The detonation was supposed to be carried out by means of a syringe containing an incendiary chemical. The attack did not succeed, because instead of exploding, the explosive charge started burning, the terrorist was exposed and in the aftermath, disarmed by passengers. It is noteworthy that the timing of the detonation was designed to maximize casualties by including people on the ground who would have been hit by wreckage from the plane (Wyborcza.pl, 2012).

Over the last several decades, it can be clearly stated that the phenomenon of air terrorism has significantly evolved towards increasing the possibilities of obtaining effects by terrorist organizations, and thus increased the degree of danger for air transport. As it was noted in this part of the article, the evaluation of the phenomenon of air terrorism went towards simultaneous attacks, superterrorism and cyberterrorism.

The threats posed by air terrorism today have consequences such as: a large number of human casualties and direct losses after the attack, long-term economic losses resulting from a decrease in the number of passengers and contractors for the airlines concerned, psychological effects on society, long-term political and social consequences. Of the above-mentioned effects of the threat of air terrorism, only in the case of the first, can clear assumptions in the area of counteraction be defined. (Glen, 2010)

4. Counteracting threats in the field of air terrorism

Currently, in order to improve the safety of air transport, organizational and technical solutions are designed and implemented for air transport in both airplanes and airports. The level of detail of checks at airports from passengers and their luggage to checks around airports and inside airports has generally been increased. It develops and introduces more and more modern and technologically advanced technical control measures. In order to improve the security situation, organizational and technical solutions for air transport, and more specifically for aircraft and airports, are currently being designed and implemented. New security standards involve mounting bulletproof doors and electronic access control into the cockpit. Additionally TV cameras placed in cockpits provide video feeds to Air Traffic Control, and armed agents - the so-called Air Marshals - can be found on board during the flight. Effective technical solutions aimed at increasing the resilience of aircraft in the case of a bomb attack include the widespread deployment of reinforced bulkheads designed to effectively contain an explosion, should a bomb go off in the luggage compartment.

Airport security is similarly being improved through the restriction of parking in areas adjacent to airports and run-ways, the restriction of movement in areas where people wait for the arrival of an aircraft, and the installation of gates that can monitor the temperature of passengers' bodies to detect overexcited persons. An apparatus analyzing the composition of the air is installed to make possible the detection of explosive materials and more detailed control concerning passengers' identity and their luggage.

5. Summary

It is undoubtedly noticeable that the threat of air terrorism is multi-faceted and multi-dimensional. Above all, it is international. The process of combating this threat entails significant financial, logistic and organizational consequences, and at the same time, it forces the introduction of new legal regulations. In addition, it is a threat that affects all who travel by air, which translates into disrupting the special and priority role of air transport as the fastest and safest means of movement of people, which in today's dynamic times is undeniably an important factor in the functioning of humanity. In summing up this article, it can be asserted that even the best solutions are not able to provide total security for the aircraft. The implementation of security systems is unfortunately a long-term project and security systems that are being used in individual countries to secure airports and passenger aircraft are characterized by considerable diversity. A key consideration is the level of funding assigned to the creation and maintenance of air security systems. It is still all too likely that an aircraft from a poorly developed country, where the level of security systems for airports and aviation is very low, will be hijacked. Such a flight can then proceed from that poor country to a wealthy country with the aim of staging a terrorist attack against that country's public buildings and/or national monuments.

Undoubtedly the situation mentioned above can happen and must be taken into account by special services responsible for air transport security.

The threat of terrorist attacks is in a constant process of evolution. One should take into account that anyone who travels by air today may be a victim of an attack. Therefore, it is indispensable for the inter-national community and individual countries had effective countermeasures.

A properly functioning state must have an organized system to respond to such dangers. The growing threat of air terrorism is

leading the international community and individual countries to take political, strategic and tactical actions aimed at neutralizing its effects. Scientists have a significant role to play in building organizational efficiency where such actions are concerned and the results of their research should most certainly be taken into account by decision-makers responsible for implementing new solutions in transportation security systems.

The thesis of this article adopted in the introductory part that the phenomenon of air terrorism over the last few decades has become the greatest threat to air transport safety by direct threat to human life of both travelers and ordinary residents who may die as a result of an act of air terror. Air terrorism has a huge impact on the functioning of the entire human community, by influencing the modification of life on our planet, the processes regulating the social life and mental state of people, which was experienced by the whole world, especially after the 9/11 attacks. It should be emphasized that air terrorism is constantly changing, using both highly qualified and expertly prepared human resources as well as the most modern technical achievements for the purpose of attacks, which significantly hinders counteracting these threats. Only the effort of all the decision-makers responsible for maintaining the safety of air transport and the application of maximum measures for the protection and defense of air traffic will effectively reduce the degree of threat of terrorist attacks directed at air transport.

References

1. Augustyniak, S. (2008). *Prognozy lotnicze w górę*. Retrieved from: https://www.pcworld.pl/news/Prognozy-lotnicze-wgore,140624.html/, 15.05.2020.
2. Puls Biznesu (2007). *Do 2025 roku podwoi się liczba latających samo-lotami*. Retrieved from: https://www.pb.pl/do-2025-roku-podwoi-sie-liczba-latajacych-samolotami-354104/, 25.05.2020.
3. Domański, J. (1974). *1000 słów o samolocie i lotnictwie*. Warszawa: Wydawnictwo MON.
4. O2 (2016). *Najgłośniesze porwania samolotów*. Retrieved from: https://www.o2.pl/galeria/najglosniesze-porwania-samolotow-5977047098122881g/2/, 15.05.2020.
5. Gotowała, J. (2006). Niepokój w powietrzu – nowe oblicze terroryzmu. In K. Kowalczyk, and W. Wróblewski (Eds.), Terroryzm: Globalne wyzwanie (115-126). Toruń: Wydawnictwo Adam Marszałek.
6. Kingshott, B. (2003). Terrorism: The "New" Religious War. *Criminal Justice Studies*, 16(1), 15-27. DOI: 10.1080/08884310309603
7. Terror (1989). Terror. In M. Szymczak (Ed.), *Słownik języka polskiego*, vol. III (p. 498). Warszawa: PWN.
8. Marks, S.P. (2006). Branding the War on Terrorism: Is There New Paradigm of International Law? *Michigan State University Journal of International Law, 14(1)*, 71-119.
9. Wyborcza.pl (2012). *Nigeryjski zamachowiec z lotu Delta Airlines dostał dożywocie*. Retrieved from https://wyborcza.pl/1,75399,11164004,Nigeryjski_zamachowiec_z_lotu_Delta_Airlines_dostal.html?disableRedirects=true/, 25.05.2020.
10. RMF.FM (2006). *Udaremniono zamach na ogromną skalę*. Retrieved from https://www.rmf24.pl/fakty/swiat/news-udaremniono-zamach-na-ogromna-skale,nId,218653/, 25.05.2020.
11. Wilkinson, P., and Jenkins B.M. (1999). *Aviation terrorism and security*. London: Frank Cass Publisher.
12. Witkowski, P. (2000). Pojęcie terroryzmu. Cele i metody działań terrorystycznych. In D. Kowalski, and M. Wróblewska (Eds.), *Ochrona osób i mienia: Vademecum*. Lublin: Wydawnictwo Policealnej Szkoły Detektywów i Pracowników Ochrony O'CHIKARA.

13. Glen, A. (2010). Reagowanie państwa na zagrożenia terroryzmem lotniczym, Warszawa: AON.