

WŁADYSŁAW LEŚNIKOWSKI *

Akademia Sztuki Wojennej, Warszawa, Polska

THREATS FROM CYBERSPACE FOR CIVIL AVIATION



ABSTRACT: Digital transformation and mobility, which is what drives the revolution in aviation, they are also a challenge to ensure safety. Increasing automation means a greater risk of cyberattack. The author in the article below touches on the issues related to Cyberspace, characterizes it and shows the issues related to violation of civil aviation security by performing cyberattacks, drone attacks, and thus violating civil aviation security. Civil aviation is a specific user of highly advanced information technology and therefore requires special protection against unauthorized access (cyberattacks). This protection covers the entire aviation ecosystem, and in it; Air Traffic Control, aircraft (aviation industry), airports. In the whole process of civil aviation security, and in particular the prevention of cyberattacks and air terrorism, legislation plays a very important role. In recent decades we have witnessed various events that were a serious threat to the safety of air navigation. These situations gave impetus to search and creating new preventive systems ensuring a high level of security in international civil aviation transport.

KEYWORDS: Cyberspace, cyberattacks, air terrorism, aviation security, prevention.

INTRODUCTION

The modern world is the world of the Internet, the world of global network, the world of "global village", global interpersonal communication, the world of mass social communication using the latest technological achievements. When we use this global network, we exist in it, and if we exist, we leave a trace after this presence, which may be a "trail" for the criminal. The Internet together with applications such as "Windows", a word meaning window, window to the world, which can invite

* dr Władysław Leśnikowski, War Studies University, Warsaw, Poland

 <https://orcid.org/0000-0001-9592-6145>  lesnikowski10@wp.pl

not only the desired guests, but also can invite people with not necessarily pure intentions. The globalization of the modern world brings with it the possibility of rapid communication of people from different parts of the world, allows to carry out multi-million transactions in several seconds. This situation changed our social life, way of spending free time, conducting financial operations. Public access to computers and the Internet, as well as the rapid development of technology in the field of social communication has dramatically changed our lives and state of social sense and international security. Cyber security experts warn us that criminals, people with different priorities than the rest of society, have followed the latest social technical advances and new methods of action.

Certain specific social groups and typical criminals along with the changing world have also changed their ways of criminal activity, rapidly adapting to the new requirements and conditions of modern society. Social networks have an open structure and are used to communicate, which creates favorable conditions for people who are deprived of any moral brakes and have no qualms about taking advantage of the opportunities that arise. As a result of such "specialists", consumers and companies, including air carriers, lose millions of dollars and euros and pose a threat to the security of society. This state of affairs speaks of a structural, regional, and global threat of a new form of terrorism - cyber terrorism.

In the first part of the article, the author describes cyberspace as a new domain of human activity and the influence of cyberspace on the functioning of private institutions, such as and state. The effects of the impact from cyberspace on Estonia in 2007 and elsewhere in the world are presented. It also characterizes global commons areas and the dependence of nations and organizations on complex networks of physical and virtual infrastructure for their resources, trade, capital and intellectual property. Our age is characterized as a world of crises and security deficiencies, a world dominated by cyberattacks across the spectrum of social life, critical infrastructure, including civil aviation. Threats from cyberspace and cyberterrorism are characterized. Then, the unauthorized access to passenger planes is presented, as well as cyberattacks, which in this industry have important economic and social consequences. By analyzing the available materials, the author states that the aviation sector is not immune to cyber threats, which are critical problems for this sector.

The author is of the opinion that the aviation industry and civil aviation are important elements of cybersecurity in air transport, which is an important link in the Critical Infrastructure of every country and the world economy. Along with the dynamic development of new technologies, e.g. the Internet, global aviation, and the aviation industry, they are subject to a new and dynamically growing

type of threat which are cyberattacks. The purpose of these cyberattacks may be, for example, the capture of information, specific political action, achieving specific financial profits, weakening competition or an attack on individual cells of civil aviation.

The author goes on to ask why cyber threats are so important in the field of aviation security and the entire aviation ecosystem. And shows how important cybersecurity is in air traffic. It concludes that the entire aviation sector is not sufficiently resilient to cyber threats. It is a well-known truth that passenger planes such as the Boeing 777 are very complex IT systems that rely on many systems, including multiple transponders to visualize the position of planes for air traffic control and are easy targets for cyberattacks.

In the final part of the article, the author focuses on the protection of airports and passenger airplanes against unauthorized intrusions of drones into the airport area and the use of drones to defend themselves against the attack of unauthorized drones. Unmanned aerial vehicles are used as tools supporting the protection of airport infrastructure.

CYBERSPACE AS A NEW DOMAIN OF HUMAN ACTIVITY

"The light goes out, the Internet is down. Banks are closed, you cannot use from an ATM. Radio and television are silent. Airports and railway stations empty. But the streets are completely congested. Looters appear after a long night - the police are not able to restore order. No one has access to money, the only thing that matters now is fuel, food and water. Panic begins ... ²" This is not a movie script from the genre of horror or science-fiction, and a quote from the speech of Sami Saydjari, head of the organization Professionals for Cyber Defense, before the Internal Security Commission of the US House of Representatives, which took place in April 2007. Saydjari's speech took place on the eve of events that again drew the world's attention to the threat of from Cyberspace. From April 27 to May 11, 2007, Estonia became a victim of cyberattacks. Devices such as a mobile phone, satellite TV, computers, fax machines and other IT³ groups have resulted in the concentration of communications networks. The growing convergence of computer and communication techniques, which use digital means to process, send and store information, has

² <http://www.angelfire.com/az/sthurston/Cyberwar.html> access. on 21.08.2021.

³ IT - Information Technology, information technology - all issues, methods, measures and activities related to information processing, is a combination of information applications and telecommunications, and also includes computer hardware and software, as well as tools and other technologies related to the collection, processing, transmission, storage, protection and presentation of information. It provides the user with tools with which he can obtain information, select it, analyze, process, accumulate, manage and transfer it to other people. https://pl.wikipedia.org/wiki/Technology_informative access on 21/08/2021.

revolutionized the functioning of our societies⁴. We live and work in the world of global communication⁵, the modern world of social communication using modern technical means, enabling global communication and multi-million financial transactions in a matter of seconds⁶.

Subject experts believe that the modern world exists in global common areas, where nations and organizations are dependent on complex physical and virtual infrastructure networks in terms of their resources, trade, capital and intellectual property⁷. The main element linking the current dynamic development of technology is the Internet, which was invented and created in the sixties of the last century by scientists working for the American army. Currently, over 200 million Internet users use its services in less than a minute via Google entries. Modern technology and new methods of operation are not always used for useful purposes. Criminals and other criminals also use them. A new global threat of cyber terrorism has emerged, and ultimately cyber warfare⁸.

Our society in which we live is called a global information society that operates in a certain climate of uncertainty and risk. This situation is seen not only on a regional scale, but also on a global or individual scale, and is also recognized as the existence of modern man. Experts define our age as a world of crises and security shortages, as a world dominated by cyberattacks on all areas of life, including Critical Infrastructure⁹ and civil aviation.

Our country, together with connection to the Internet in 1991, also became the object of possible cyberattacks by means of IT. In the initial phase of Internet use, there were typical hacker attacks aimed at obtaining financial benefits, but with the passage of time these cyberattacks evolved not only to obtain funds, but also aimed at obtaining economic and military information, obtaining so-called identity or unauthorized access to civil aviation cells. The highest level in this evolution is the

⁴ Gregory J. Rattray *Strategic war in cyberspace. Secret - Attack - Defense*. "Scientific and Technical Publishing House", Warsaw 2004. p.13

⁵ Scoott Jasper, *Conflict and Cooperation in the Global Commons. A Comprehensive Approach for International Security*, "Georgetown University Press" Washington, DC, 2012r. s.1

⁶ W. Leśnikowski, *Welcome to the cyberwar world*, "Air Force Review", 2011, No. 4 (046) p. 2

⁷ W. Leśnikowski, *Military use of cyberspace and conventional combat operations*, Monograph, Contemporary bioterrorist and cyberterrorist threats and Polish national security, Warsaw, December 2013, p. 374.

⁸ W. Leśnikowski, *Welcome to the cyberwar world*, "Air Force Review", 2011, No. 4 (046) p. 7

⁹ Critical Infrastructure - a term used to refer to resources that are fundamental to the functioning of society and the economy. Usually associated with this term are means: for the production, transmission and distribution of electricity (energy); for production, transport and distribution of gas fuels; for the production, transport and distribution of crude oil and petroleum products; telecommunications (electronic communications); water management (drinking water, sewage, surface water); for food production and distribution; for heating (fuel, heating plants); health care (hospitals); transport (roads, railways, airports, civil aviation, ports); financial institutions (banks); security services (police, army, rescue). <https://rcb.gov.pl/infrastruktura-krytyczna/> access. on 21/08/2021

attempt to paralyze the state economy by comprehensive cyberattacks by Critical Infrastructure, as exemplified by the case of Estonia in 2007.

Experts of the topic are convinced that actions in the virtual world have a real impact on the effects in our world, and that they cover extensive areas of science, culture, relate to social and technical matters, and in this may affect the safety of civil aviation.

In conclusion, it can be said that modern security threats, and including the safe functioning of civil air carriers can have a variety of substrates; political, economic, social, military or religious, as well as the syndrome of the injured employee, may be external or internal. Cyber security experts use a variety of classifications for threats from Cyberspace, which can generally be classified as;

- regional nationalisms;
- nationality problems;
- religious fundamentalism;
- cultural differences;
- territorial disputes;
- independence movements;
- uneven economic development;
- political instability;
- competition for domination in the region;
- organized crime;
- proliferation of weapons of mass destruction;
- międzynarodowy terroryzm¹⁰.

To sum up, it should be stated that the main categories responsible for describing the concept of security are¹¹;

- interests of the national entity,
- operational and strategic goals of security,
- security environment,
- long-term and current goals of state action,
- security system.

¹⁰ Ibidem p. 10

¹¹ S. Koziej, *Security: Essence, basic categories and historical evolution*, "National Security", 2011, No. 18, p. 26.

GENESIS AND CHARACTERISTICS OF CYBERSPACE

The modern world and the world of the turn of the century were the arena of two phenomena that dominated our thinking about the future, one of them was globalization, which in the first place covered such spheres as; economics, politics and culture, while the second was and is currently the acceleration of the development of information and IT technologies, whose most prominent product is the Internet and its uncontrolled development. It is very dynamic development has created a phenomenon that is called "shrinking time and space" on a global scale¹².

The term "Cyberspace" was first used by William Gibson, a cyberpunk classic who in his novel *Neuromancer* published in 1984. He described cyberspace as "Consensual hallucination, experienced every day by billions of authorized users in all countries. Graphic representation of data downloaded from the banks of all computers in the world. Unbelievable complexity. ¹³" This space has also been described as "a graphic, multifunctional environment, creating an extremely reliable world, experienced primarily visually." (K. Aoki). In 2010, in our country, it was defined as "a digital space for processing and exchange of information, created by ICT (Information and Communications Technology) systems and networks with connections between them and relationships with users".

The term, the concept of Cyberspace, also brings with it new threats such as cybercrime, which arose with the emergence of the new concept of "IT highways" announced by Bill Clinton in 1992 during his presidential campaign. The main idea of this concept was the idea that all kinds of information containing text, sound and image could be transmitted over a long distance quickly and without obstacles.¹⁴

Subject experts say that the global network is subject to a continuous process of expansion, as a result of this process becomes more and more similar to our real world, and therefore some phenomena from the real world such as crime and terrorism automatically begin to exist in a new reality - in Cyberspace. In the modern world, information (IT) exists as a commodity, and therefore it can be stolen, destroyed or sold or used for material, ideological or other benefits. Due to this state of affairs, it must be protected against unauthorized access¹⁵.

Our world has changed its direction, giving up mass, a large number for the benefit of several people and several specialized programs that allow to achieve the assumed goal, i.e. paralysis of the

¹² P. Sienkiewicz, *25 lectures, „AON”*, 2013, p. 1988

¹³ W. Gibson, *Neuromancer*, ed. II, Poznan 1999, p. 53

¹⁴ W. Leśnikowski, *Welcome to the cyberwar world; "Air Force Review"*, 2011 No. 4 (046) p. 10.

¹⁵ W. Leśnikowski, *Cyberattacks against critical infrastructure as cheap and effective means to paralyze developed countries, "Air Force Review"*, September 2012 No. 02 (059), p. 1 (electronic version)

state. So this situation shows that we are living in a world where the main sources of all kinds of threats to our society will generate Cyberspace. World experts in the field of Cyberspace claim that it has become another area of competition, an area of regular combat. The arsenal in this fight are computer viruses, worms, electromagnetic impulses to destroy the enemy's networks and computers, Trojan horses, as well as high-intensity data streams that cause short-term or long-term blocking. Further, experts say that the response to a cyberattack may involve a completely different area, and the impact on a computer network or other object, e.g. an air carrier, will be unilateral, and the fight may be very uneven¹⁶.

The origin of the name Cyberspace and cyberattacks¹⁷ also has Polish roots, it should be mentioned here that in the 1960s Stanisław Lem in his *Cyberiada* publications and in *Robot fairy tales* announces events that are taking place today¹⁸.

Our contemporary, dynamically developing world and all its fields require us to quickly adapt to new conditions and new challenges. In order to achieve these assumptions, it is necessary to specify the causes of these phenomena with particular precision and determine the effects that these threats may cause, and then to set tasks for elements of the security system capable of reacting immediately and effectively to these emerging threats in a timely manner.

CYBERSPACE ITS ATERRITORIALITY AND ANONYMITY

"Cyberspace is a metaphor that allows us to embrace a place where, more or less since World War II, we have been gradually creating more and more things that we define as civilization."

William Gibson

Cyberspace experts define it in various ways in their publications, often "as a space having a virtual, non-spatial character in physical, aterritorial and ageographic terms, and this applies to all connections created and implemented by information technologies and their physical manifestations, or on their basis ¹⁹". In contrast, another cyberspace theorist Pierre Levy believes that

¹⁶ W. Leśnikowski, *Military use of cyberspace and conventional combat operations*, Monograph, *Contemporary bioterrorist and cyberterrorist threats versus Poland's national security*, Warsaw, December 2013, p. 383.

¹⁷ Cyber war - potential use of computers, the Internet and other means of storing or spreading information in order to carry out attacks on enemy information systems. Since the classic wars, the cyber war (it should not be confused with the information war) distinguishes the battlefield environment - IT systems and networks. https://pl.wikipedia.org/wiki/War_netic access. on 11.05.2018

¹⁸ W. Leśnikowski, *Welcome to the cyberwar world*. Part I, "Air Force Review", 2011, No. 4 (046) p. 8

¹⁹ A. Bogadał-Brzezińska, M. F. Gawrycki, *Cyber terrorism and the problem of IT security in the modern world*, "ASPRA-JR", Warsaw 2003, pp. 37-39.

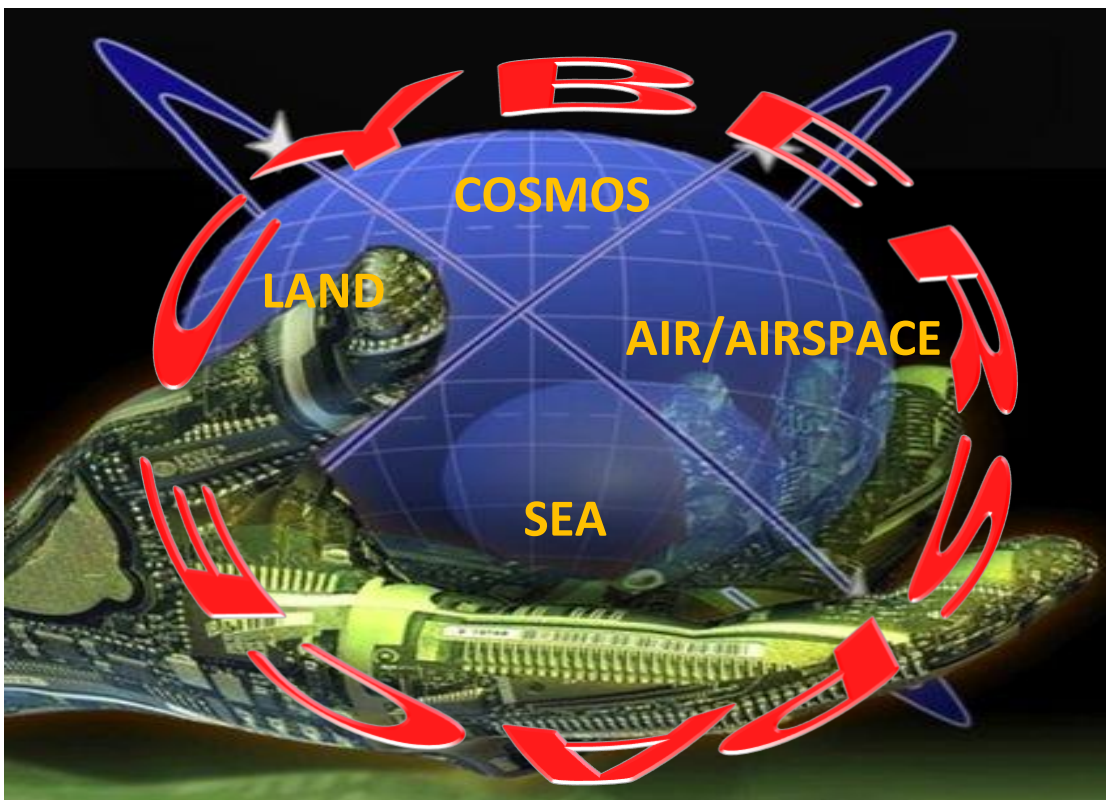
cyberspace is "plastic, fluid, computable with high accuracy and processable in real time, interactive and finally virtual²⁰".

Experts in Cyberspace take the position that it has become a new domain (see Fig. 1) of human activity along with its specific features that are so different from those that we can meet in our everyday reality. This means that certain phenomena, and thus many entities or factors that exist in the real world and have the status of strength, in the virtual world may lose their significance or may be deprived of such status.

Cyberspace can also present itself as a domain of potential conflicts, it can also present itself as a kind of "power equalizer", as it provides opportunities to equalize opportunities for both strong states or weak as well as and for non-state actors and also reduces the differences between them.

This state of affairs is the result of the aterritorial nature of Cyberspace, although it has physical anchoring in reality, which may reduce the importance of certain important factors that may provide advantage in the real world, e.g. natural resources or armed forces.

Fig.1. The 'five dimensions' model, domains. Cyberspace as the fifth dimension



Source: own study

²⁰ B. Gagnon, *Are We Headed for a "Cyber-9/11?"*: The American Failure in Cyberstrategy, "Center for United States Studies of the Raoul Dandurand Chair of Strategic and Diplomatic Studies", Occasional Paper no 5, Quebec, 2004, p. 3.

The exact definition of Cyberspace poses a lot of problems for scientists researching it. Despite numerous analytical works and studies, it was not possible to establish an unambiguous definition, but it was possible to find a number of terms related to the nature of activities within its area-related framework, and the most important were included; global reach, very fast pace of development, no scale problem, relative amines, scarcely controllable, boundless reach, aterritoriality and immateriality, and regularity.

ATERRITORIALITY

Cyberspace is blurring the concepts of geography and geopolitics, which means that, for example, geographical distance does not matter²¹. Aterritoriality also means the absence of any spatial restrictions, e.g. geographical, political borders, etc., which indicates that all activities in Cyberspace can be directed either directly or indirectly to the security of e.g. the state, passenger aviation, or even to a single person. It should be noted that a cyberattack can be initiated from anywhere on the globe. This situation means that factors such as distance and time in Cyberspace are a relative concept.

Subject experts state that the Internet, and in this case Cyberspace, has been a domain without control mechanisms, any barriers or "real" comprehensive protection methods from the very beginning. The only limitation can be the bandwidth of the internet connection or individual human capabilities.

As mentioned earlier, the freedom and freedom of Cyberspace users is its greatest asset, but it also brings with it a significant level of threat. The relative ease of achieving a significant level of anonymity together with easy access make Cyberspace a very attractive and profitable domain in which a very large part of our population already operates, of course, both good and bad. The globalization of our lives, a global network, have overcome the existing obstacles to interpersonal communication. Experts say that some of the current difficulties that may have prevented the free exchange of thoughts among communities, e.g. state borders, censorship, are now only a former relic of the past.

The concept of "global village" and referring to our modern life has been permanently introduced by M. McLuhan, which is a very apt term, and which takes into account in its name the external

²¹ W. Leśnikowski, *Military use of cyberspace and conventional combat operations*, Monograph, *Contemporary bioterrorist and cyberterrorist threats and Polish national security*, Warsaw, December 2013, p. 382.

conditions of mutual communication that modern technology enables, concentrating a huge number of interlocutors in the network and thus reducing the distance expressed in a geographical dimension²².

The aterritoriality of Cyberspace causes related costs carrying out activities in it practically boils down to expenditure related to the purchase of appropriate computer equipment, its software, appropriate knowledge and skills, and access to the Internet.

To sum up, it should be stated that with minimal investment the assumed results can be achieved, e.g. huge financial losses as a result of a cyberattack on a given object, e.g. an air carrier.

ANONYMITY

The globalization of our lives in connection with the dynamics of global communication development has resulted in very easy access to information for all its users. In this situation, physical dispersion is no longer an obstacle in the process of exchanging views, beliefs or interests for governments, organizations, associations or individuals.

Cyberspace is becoming a very attractive domain because it offers cyber planners a specific type of amino acid because it is very difficult to determine the source of a cyberattack. Anonymity in Cyberspace de facto results not from the weakness of the domain, but from the weakness of the Internet structure itself. Another ally of anonymity in Cyberspace is the rapid increase in the transfer of all kinds of data, which makes it unprofitable and technically almost impossible to record and store information that could allow the identification and tracking of any amount of data transmitted via the Internet. In such a situation, it becomes clear that the architecture of Cyberspace is dependent on material devices that are used to collect, send and process information that is susceptible to forming, modifying, reconfiguring, e.g. technologically²³.

In conclusion, it can be argued that the property of Cyberspace, known as aterritoriality, causes difficulties in determining the local and material property that could violate the laws of a given country, and the anonymity of the information sent results in a lack of entity that could be accused of violating the rights of another entity and made using the Internet, e.g. commercial transactions, and thus the interests of the parties to the contract are not properly secured.

²² B. Borowik, R. Borowik, *Changes in cultural awareness in the era of the information society*, <http://www.uci.agh.edu.pl/agh/dep/wsss/konferencja/doc> access. on 21/08/2021

²³ K. Dobrzeniecki, *Law and ethos of cyberspace*, "Adam Marszałek", Torun 202, p. 11

Analysis of global and national reports on cyber security as well as monitoring and counteracting threats in Cyberspace provides us with the knowledge that the largest number of threats in this domain is produced by the human factor. Subject experts state the motivation for negative activity in Cyberspace is very diverse.

The Cyberspace domain is an arena of various factors, the so-called. villains with very different motivations for their activities. These include; *cracker, businessman, accountant, spy, terrorist, former employee* and others. *Cracker*, the main goal of his activity will be information theft and his method of work will certainly be testing the security system and then breaking the security programs. *The businessman* will be looking for strategic information related to the plans and intentions of the competition. However, the motive of the accountant will be to raise the money of the company they usually work for. *The spy* will seek to obtain bank account numbers as well as credit cards with logins and passwords. Another can be *a Terrorist*, and his main goal will be to destabilize the attacked target and to make the highest possible level of losses that would entail huge financial losses. The next will be *a former employee* who will try to take revenge on his dismissal²⁴.

To sum up, one may be tempted to say that the Internet and thus Cyberspace has been an area without control mechanisms, barriers or "real" comprehensive protection methods from the very beginning. Subject experts say that human perception is the only limit²⁵.

AN ATTEMPT TO DEFINE CYBERSPACE AND ATTACKS ON IT

Attempts to define Cyberspace are a very difficult process and constantly lead to the discussion of various scientific centers and celebrities in order to create a uniform definition of this phenomenon that is accepted by international opinion. As it was mentioned before, in the 1960s Stanisław Lem foresaw activities related to cyberattacks and cyberwar, publishing his own stances in works; "*Cyberiada*" and "*Robot fairy tales*." These publications are a kind of Bible of what can happen in the modern world. There is such a belief that if something can happen it will probably happen, it is only a matter of time. To confirm such a position, there are very frequent publications in the press about frequent cyberattacks on various government and company agencies, devices and systems as well as air transport.

²⁴ Own study based on R. Tadeusiewicz, *Threats in cyberspace*, "Science", 2001, No. 4, p. 39.

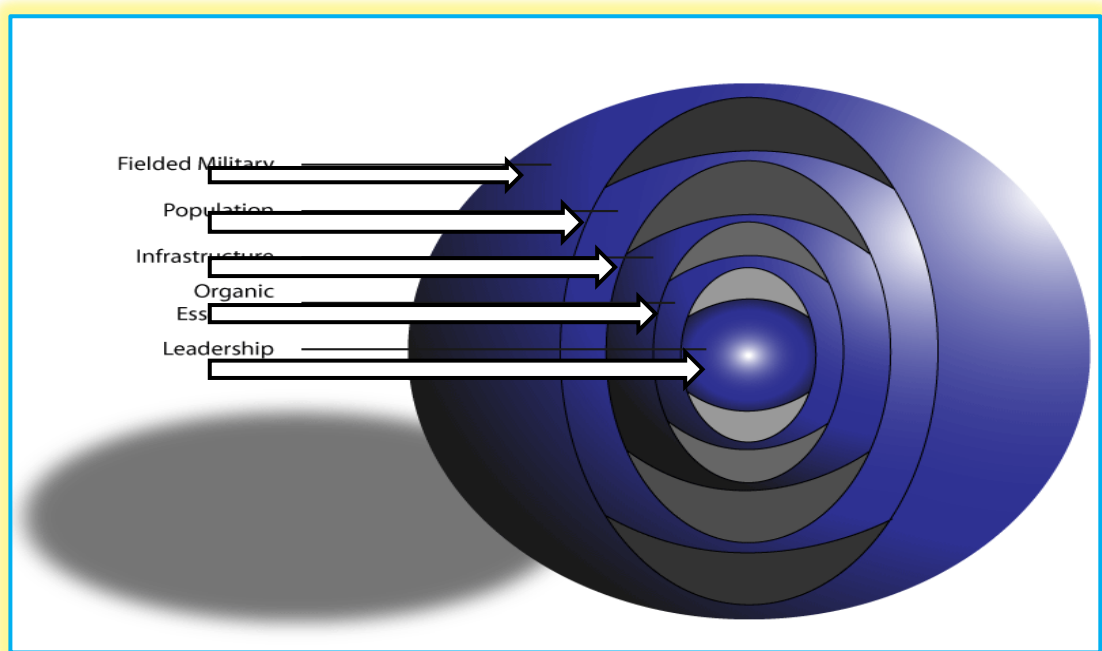
²⁵ J. Horoszkiewicz, *Internet - an uncontrolled zone in cyberspace*, "Police Review", 2001. No. 2 (62), p. 100 et seq.

WHAT IS CYBERTERRORISM?

What is cyber terrorism? Experts say that this phenomenon is not entirely new, and the first mentions and the name of "cyberterrorism" appeared already in 1972 in the Swedish Ministry of Defense, when this term was included in the report on computer threats and was placed in recommendations to the government to monitor public and private computer networks. Modern analysts of the phenomenon of cyberterrorism state that the modern world has already become a regular battlefield and placed in Cyberspace. They further claim that the attack on the computer network of a hostile state will be one-sided, but all, if any, warfare can be extremely uneven.

The conventional image of warfare was based on the idea that wars were won by the side that had a larger army. The modern world and the IT world have made it more important to have full access to modern technology, which can give you an advantage and, ultimately, victory. Subject experts say that even cyberattacks carried out by individuals, entities and non-state actors can achieve the desired positive results. A minority can decide about the success of the mission. Strategists and experts in military operations in cyberspace have added to the "Warden model" as a new element of the war model - cyber terrorism.

Fig. 2. The Five Rings of Warden presents the theory of military strategic attack based on five levels of system attributes.



Source: Own study based on - <https://warontherocks.com/2020/09/the-five-ring-circus-how-airpower-enthusiasts-forgot-about-interdiction/>

What was typical means of struggle in the real world, in the virtual world has been enriched by, among others computer viruses, Trojan horses, worms, magnetic impulses, which are designed to destroy the computer networks of the other side, and data streams of very high intensity cause their short-term or long-term blocking. What was typical means of struggle in the real world, in the virtual world has been enriched by, among others computer viruses, Trojan horses, worms, magnetic impulses, which are designed to destroy the computer networks of the other side, and data streams of very large In such an environment it is difficult to create the only definition that would be quoted in the context of considering the IT security of international society. Such a definition, close to ideal, is the definition created by Mark Pollit, an FBI agent, who said that cyberterrorism is "intentional, politically motivated attack against information, computer systems, computer programs and data, which is directed against civil and military targets by state and non-state actors". Subject experts say it should be distinguished from other cyberattacks such as computer crime, economic espionage and information warfare. An attack in the area of cyberterrorism is a deliberate cyberattack and is a very well organized phenomenon. Usually, the reasons for this type of cyberattack are political reasons²⁶, while the result is the negative impact, violence of groups or secret services against outsiders. However, the essence of this phenomenon cannot be enclosed in one common definition, because it is so unpredictable in its form that each attempt turns out to be incomplete.

Professor Dorothy Dennig of Georgetown University, an IT and security expert, states that a cyberattack can be classified as cyber terrorism when it "results in violence against people or property, or at least causes fear." Next, the professor states that this is a cyberattack carried out by means of an ICT network and which leads to "death, mutilation, explosion, aircraft crashing, water pollution or drastic economic losses²⁷." Subject experts say that cyber terrorism is terrorism directed against teleinformatic systems, networks and services that are sensitive to the state, transport, and including air transport.

²⁶ A. Janowska, *Cyberterrorism - reality or fiction?*, [In:] *Information society - vision or reality?*, Krakow 2003, pp. 448-449, <http://www.angelfire.com/az/sthurston/Cyberwar.html>

²⁶ AIAA - The American Institute of Aeronautics and Astronautics, <https://www.aiaa.org/> access. on 21/08/2021.

UNAUTHORIZED ACCESS TO PASSENGER AIRCRAFT - CYBER ATTACK

Experts and experts on the subject believe that the aviation industry is one cybersecurity elements in air transport (see Figure 3) is an important link in the Critical Infrastructure of every country and global economy. According to data in 2013, civil transport aviation carried more than 48 million tons of cargo and more than 2.6 million passengers, and its global economic value reached \$ 2.2 trillion (AIAA²⁸). Cyber security analysts are of the opinion that any cyberattacks in this industry will have important economic and social consequences.

Along with the dynamic development of new technologies, e.g. the Internet, global aviation, the aviation industry, they are subject to a new and dynamically growing type of threat such as attacks from Cyberspace. The purpose of these cyberattacks may be, for example, the collection of information, specific political action, achieving specific financial profits, weakening competition or attack on individual civil aviation cells. As part of such activities, actions may be wreaked havoc among computers responsible, e.g. for airport power networks, air traffic control and telecommunications.

Cyber security experts state that the aviation sector is not immune to cyber threats, which are also critical issues for other industries. It should be emphasized that aircraft such as the Boeing 777 have very complex systems that are based on many transponders and are used to transfer their position for air traffic control. These systems are quite difficult to hack together with onboard systems such as two-way radios, ACARS²⁹ air addressing and reporting systems, which is used to send messages or information about aircraft instead of voice transmission.

Strategies for the development of large air carriers are developing possible cyber threats in relation to technologies: computer viruses, malicious attacks, etc. Such activities are aimed at the security of the growing number of travelers, along with the creation of new and the development of existing airports, along with the introduction of more complex modern aircraft, and thus the use of modern information technology and advanced computer systems. With the passage of time, the risk of cyberattacks also increases, in addition, the digitization of the sector using electronics, e.g. a ticket sales system, should be taken into account. There are two types of cyber security breaches in the aviation industry:

²⁹ ACARS - Aircraft Communicatio Addressing and Reporting System, a digital transmission system that allows the exchange of short text messages between aircraft and ground stations, operating via radio waves. <https://pl.wikipedia.org/wiki/ACARS> access. on 21.08.2021.

1. "Opportunistic", which aims to use errors made by internal users, such as employees using information systems to cause difficulties, inconveniences and nuisance to all users of the aviation ecosystem.

2. "Calculated and pre-planned", these will be all malicious attacks aimed at disrupting operations or may be life-threatening. This type of violation is critical, as is terrorism that is fully aware of the potential of technology and cyberattacks.

The next step will be to list the various factors that are able to do so and can definitely influence the cyber security strategy;

- increased interpersonal interaction as well as devices and services. Said increase and diversity of interactions create a kind of path, and thus attacks become unpredictable.
- innovation and cost reduction as a result of the transformation of the aviation ecosystem³⁰ create common goods, and moreover, software is increasingly used to provide effective digital solutions for experienced employees of the aviation industry and passengers.

The end result of such evolution may be the increasing exposure of internal and external systems of the aviation ecosystem to potential threats of cyberattacks.

Until recently, cyberattacks used by hackers were mainly directed at home computer users or company equipment. What if cybercriminals direct their actions to passenger planes? Expert reports from the DHS group (Department of Homeland Security) show that unauthorized access to outside passenger aircraft systems is becoming a reality. Experts stated that the testing group used only tools that did not create suspicion during routine airport security screening. The report shows that the whole problem boils down to financial issues.

During the simulated cyberattack, an extremely popular model of the Boeing 757 aircraft was used, and physical access to the passenger aircraft systems was not required, and access to radio communication was provided on every passenger aircraft, which gives a lot of scope for hackers. Modern passenger aircraft can be described as flying IT systems. A large number of passenger aircraft computers are subjected to very strict safety requirements and checks before being installed on the aircraft, followed by regular maintenance, which requires a certain number of man-hours. The problem is the fact that the software controls the main components of the passenger aircraft in standard reviews it is not subject to control or reviews, because it is a relatively costly procedure generating costs of several hundred thousand euros. The software installed on passenger planes is

³⁰ Aviation 'ecosystem' - www.rynekinfrastruktury.pl/.../nowanistrategia-roz-Rozwoju-Europejska-Lotnictwa-52198 ... access. on 21.08.2021.

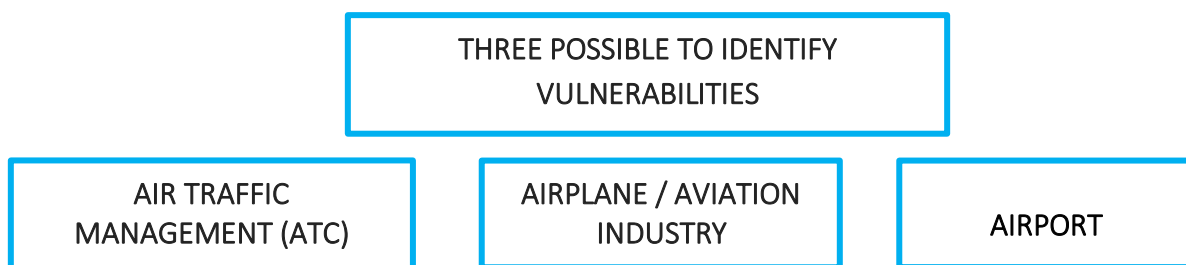
relatively rarely modified due to the fact that each of the components must be certified before being installed on the aircraft, and this process is time consuming and expensive.

For the above reasons, air carriers are trying to introduce any modifications in bulk to cut financial costs. Installed packages, however, are usually unmodified. It is often the case that some systems and programs installed on passenger aircraft are ten years old or older. The DHS report states that over the last several years there have been no significant changes regarding the guidelines of installed systems in passenger aircraft.

When analyzing threats from Cyberspace to passenger aviation, they should be divided (see Fig. 3.) into; threats of cyberattacks by the Air Traffic Management area, the aircraft itself and all its IT, and Airports together with all its ground infrastructure.

WHY ARE CYBER THREATS IMPORTANT IN THE FIELD OF AVIATION SECURITY, THE ENTIRE AVIATION ECOSYSTEM?

Fig. 3. Threats to cyberattacks for passenger aviation.



Source: Own study

The aviation ecosystem consists of three main areas (see Figure 3):

➤ Air Traffic Management, Air Traffic Control (ATC³¹), controllers provide ground air traffic services, operate aircraft on the ground and in controlled airspace, they can also advise aircraft moving in uncontrolled airspace. The main task of Air Traffic Control is to prevent collisions, organize and accelerate the flow of air traffic and provide information and other support for pilots. The controllers use complicated software that, subjected to cyberattacks, can cause a total mess and can

³¹ ATC (Air Traffic Control) - a service established to prevent dangerous approach of aircraft to each other, both during a flight and at airports. Air traffic control also aims to improve and maintain an orderly flow of air traffic. https://pl.wikipedia.org/wiki/Kontrola_ruchu_lotniczego access. on 21.08.2021.

lead to a number of disasters, which is why this cell is such an important element in the entire civilian carrier traffic.

- Aircraft - the cyber security of aircraft of an air carrier can be defined as prevention and response to intentional, intentional and malicious actions using Cyberspace, which may mean direct exposure to aircraft systems, or indirect, where these systems play a leading role in the aviation ecosystem.

- Airport / Airfield - airport security can be defined as actions to prevent cyberattacks, responding to intentional and malicious actions performed through cyberattacks that may directly or indirectly expose airport systems and the entire airport to disruption or complete elimination from ongoing operation of those systems that play a key, critical role in the broad aviation ecosystem. It should be noted that the airport is an intermediate link connecting the air traffic corridor with the aircraft creating a network of interconnections. Take into account measures to protect airports and the entire airport against attacks that can lead to degradation of aviation, security measures, e.g. security control, access control, etc. Cyberattacks are aimed at disrupting the operation of airports or entire airlines, mainly dedicated in the area of facilitation for passengers, e.g. departure control, baggage handling, etc.

Robert Hickey, Head of Aviation Programs in Cybersecurity at DHS Science & Technology (S&T), as well as a staff officer at the Office of the Director of National Intelligence stated that "... despite the fact that although aviation is a subsector of the National Security Plan component Infrastructure and the emphasis is mainly on traditional ground security systems, but passenger aviation is another part, another type of Critical Infrastructure that is in motion, and which is an important part of National Critical Infrastructure". He further stated that passenger aircraft, or all passenger aviation, is a major challenge for cyber security (cybersecurity) and traditional terrestrial networks. He stressed that regardless of whether it is military air forces or the commercial sector, so far there are no specialized maintenance teams that could cope with cybernetic extortion, cyberattacks or the general threat of cyberattacks by commercial aircraft.

Experts in the subject of cyber aviation security say that the entire aviation sector is not as resistant to cyber threats as other industries. It is a generally known truth that passenger planes such as the Boeing 777 are very complex IT systems that are based on many systems, including on many transponders to illustrate the position of aircraft for air traffic control.

Performing a cyberattack on this type of device is a difficult task, and in particular cyberattacks on all systems simultaneously, including on-board devices such as two-way radios and air

communication addressing and reporting systems (ACARS), which are used to send messages or information about aircraft as a substitute for voice transmission. In such an environment, "an attack with a deep understanding of the specifics of passenger aircraft systems and their IT can cause serious problems with operational standards." (Paganini, 2014).

The modern world, social communication environment, globalization of our lives, communication between people and devices, computerization of our lives, price erosion and software development are factors increasing the need for serious and continuous consideration of cyber threats in the communications aviation sector. The safety of communication aviation remains a key topic of protection against cyberattacks, despite some actions in this field, but this threat exists and it is not a new trend at all. Subject experts see increased activation with the avalanche use of computer systems; from sophisticated air navigation systems installed on aircraft, control and air communication systems, from ground airport service systems.

It wasn't just the navigation systems that were subject to cyberattacks. Attack on the Internet in 2006, he forced the US Federal Aviation Authority to close some of Alaska's air traffic control systems. In July 2013, the attack led to the deactivation of passport control systems at departure terminals at Istanbul airport, causing a delay in many flights. Finally, it is possible that the 2013 attack involved 75 malicious hackers and phishing agents in the US. In April 2015, mass media reported that it was confirmed by the FBI³², that Chris Roberts³³ provocatively showed during a flight with a Boeing 737 that you can have full control over the aircraft by controlling, among others engine throttle as well as other aircraft systems. The means to take control of the aircraft systems was on-board Wi-Fi. It was found that Roberts was able to use the entertainment control system in the aircraft by connecting his MacBook Pro to the hidden Ethernet port in the seat and then used the Vortex software. Following such actions, he was also able to monitor data flowing into the cockpit and had control over the aircraft systems listed. As a result of his "experiment" he was banned for life from United Airline.

Experts in the subject of cybersecurity of passenger aviation have long signaled that an average capable hacker is able to take control of the basic systems of the aircraft along with all its avionics. Cyber security specialists in passenger aviation claim that by exploiting vulnerabilities in the on-board

³² FBI – Federal Bureau of Investigation, Federal Bureau of Investigation. www.dictionaty.com/browse/fbi access. on 21/08/2021.

³³ Chris Roberts – security systems expert, business owner

software of Boeing or Airbus aircraft in 2011-2014, it was possible to break into aircraft systems computers, e.g. climb systems.

A German Hugo Teso, who is a programmer and has a pilot license, claims that he created his program called PlaneSploit (in free translation "exploiting the weakness of the aircraft") for a smartphone equipped with the Android system, which creates the possibility of taking control of a passenger plane. According to Teso, the PlaneSploit device has the ability to establish communication with the passenger ship's electronics and take control over it. The created program has the ability to modify everything that is related to navigation systems, to change all data displayed on the remote control displays, or to control the lights in the pilot's cockpit.

In this situation, it means that using a smartphone it is possible to modify the data on board a passenger aircraft entered e.g. to the navigation system and creating a situation that causes the passenger ship to ground³⁴.

CAN HACKERS THREATEN THE SAFETY OF PASSENGER FLIGHTS?

Kaspersky Lab experts and other experts on cybersecurity claim that this is possible and cite numerous examples of attempts to perform cyberattacks on passenger planes. They further claim that e.g. the security of the communication system between the flight control tower and the aircraft has not been changed since 1978³⁵. Also the European Aviation Safety Agency (EASA) reports increased activity of hackers and their attempts to launch cyberattacks on passenger planes. According to the head of the new technologies department of the Kaspersky Lab group, Andrei Nikiszyn, hackers are already able to deceive the ACARS (Aircraft Communication Addressing and Reporting System), a system of communication with aircraft based on messages and acknowledgment of receipt, i.e. a two-sided system), which sends text messages between the airport and the plane, which can lead to a disaster in a straight line. Hackers can confuse the GPS system by entering their data and thus deceive the pilot and lead to disaster.

The expert claims that the ACARS system does not have verification of data packets sent from the airport to the aircraft, which is why cheating this system is possible by inserting a foreign data packet between information sent to the aircraft. In this way, an attacking hacker can influence the pilot's decisions regarding e.g. the course of the aircraft by sending false information about an approaching storm. In a similar way, an attacking hacker can deceive the GPS system and can influence the pilot's

³⁴ Source; CNN (<http://www.tvn24.pl>), access. on 21.08.2021.

³⁵ technology.dziennik.pl/.../502623,ekspert-ostrezega-hackers-moga-zaatakowac-samol access. on 21/08/2021

decision by misinterpreting the position of the aircraft. The solution to this problem is to change the outdated system (operated since 1978) to one that will fully protect the system from cyberattacks³⁶..

Another expert in the field of security against cyberattacks, Bruno Nouzille, head of the avionics department of the Thales consortium, stated on the basis of analyzes carried out by the company that in 2025 over 70% of the fleet of communication aircraft will allow access to the Internet for its passengers, and this creates a kind of threat access to aircraft control systems. Earlier, the author demonstrated cases of attempts to take control of an airplane, even when the laptop is in airplane mode after disabling access to Wi-Fi or bluetooth. It is stated that this situation requires a quick response of the carrier and the aircraft industry so that a special interface that would provide access only to carry out maintenance or to connect the so-called Electronic Flight Bag (EFB, electronic navigation aids and maintenance, FlySmart for Peach Aviation, which Ryanair introduced in 2015³⁷..

Currently, Thales is proposing the implementation of special programs that would counteract cyberattacks, and in addition signal the need to create a special team of specialists who would constantly monitor the condition of the aircraft, e.g. power unit, avionics, etc., which would also be responsible for timely software updates.

Also, the American FAA³⁸ agency in its special report is demanding that Boeing eliminate its problems with securing the latest Boeing 787 Dreamliner products against cyberattacks. The agency points to the fact that Boeing 787 may be vulnerable to cyberattacks as a result of using a network that provides passengers with internet access during their flight. This network is connected with systems that control the functioning of the aircraft, which creates a very high threat of Dreamliner cyberattacks as a result of unconscious or deliberate activity aimed at destroying or disrupting the work of systems installed on the aircraft.

WHAT MEASURES TO COMBAT CYBERATTACKS ON AIRCRAFT MUST AIR CARRIERS TAKE?

"People talk about the power of the water element during the floods, about the tornadoes, about earthquakes, about fires. The crisis management strategy in each country is based on the fight against the elements. But now a new element has emerged, unknown to the ancients - Cyberspace. How to control it? How to keep her in notches? How to minimize the effects of disasters caused in the virtual space of global economies and attacks on Critical Infrastructure ranging from water intakes through

³⁶Source: Kaspersky Lab

³⁷ http://www.altair.com.pl/news/view?news_id=18466

³⁸ FAA - Federal Aviation Administration. <https://www.faa.gov/> access. on 21.08.2021.

energy and telecommunications networks to financial systems?" - Sławomir Kisieliński wonders when discussing the assumptions of the Cyberspace program³⁹.

The examples of cyberattacks carried out or likely to occur as a result of vulnerabilities in IT software for the aviation ecosystem justify the need to prevent just such threats to civil aviation that cause or could lead to dramatic consequences. Interpersonal and human-to-device communication, as well as a sharp increase in computer performance, as well as price erosion and software development are components of the aviation ecosystem that increase the need for serious consideration of cyber threats in the civil aviation sector. Strategies for the development of transport aviation see cyber security as a really key topic, despite all the investments and measures involved in its prevention or elimination of its effects.

This new type of threat in the aviation sector is explained by the increased use of computer systems, sophisticated air navigation systems on board aircraft, control systems and air communication, systems used at airports, including flight information and ground security control at airports, common data management systems.

The 2009 NASA report highlights the dynamic development of software and its complexity in all industries:

- In the years 1960–2000 the use of pilot software increased z 8% do 80%. Despite this complexity, aviation systems are not fully prepared for cyberattacks. At the time the first flight aviation network was created, these systems operated in an isolated environment and were designed more for high availability than security. Of course, air carriers took a number of actions, but they turned out to be insufficient. With the new software, the complexity of the software increases, and along with it should increase its user security, which, in fact, is not completely guaranteed. It is also the reason for increasing searches to close loopholes in the aviation sector software system and thus prevent cyberattacks by frequently testing security-critical civil aviation ecosystem.

Subject experts warn that the complexity of the civil aviation ecosystem produces a large number of violations of unauthorized access to its IT systems,

and determining who is responsible for the violation or cyberattack is difficult. Previous cases of unauthorized access in the civil aviation sector have led to some observations, e.g.

³⁹ S. Kisieliński, *The government wants to protect the cyberspace of the Republic of Poland*, "Computerworld.pl", 5 February 2009.

✓ When a software vulnerability or breach is discovered, software providers do not eliminate this type of threat, do not feel responsible for the software breach or vulnerability, and blame each other (e.g. Airbus, Boeing).

✓ The main internal on-board communication protocol is embedded in duplex avionics (Avionics Full-Duplex Switched Ethernet, AFXD), which does not completely protect against unauthorized access and cyberattacks on the entire aviation industry has definitely increased, which forces the cooperation of all elements of the aviation ecosystem to prevent cybercrime and cyberattacks.

The entire civil aviation ecosystem makes efforts and activities that are as follows:

- Following the increase in cyberattacks in the entire aviation ecosystem, the implemented solutions are based on computers, which is why ICAO⁴⁰ calls to work closely together with stakeholders to identify these threats and risks as much as possible.

- The same organization suggests that its members implement strong cyber security and cyber security management strategies. The main purpose of these activities is to implement a decidedly greater number of rules and measures that should prevent cyberattacks, and which will protect our society against drama.

- Airports implement modern measures that are designed to secure every IT system already installed in the aviation ecosystem.

- IATA⁴¹ has proposed annual audits that provide airlines with the opportunity to counteract cyberattacks.

- The aviation industry has made attempts and some effort to implement additional security measures on Boeing 777 aircraft to prevent cyberattacks on critical civil aviation computer systems.

Security specialists against unauthorized access to aircraft IT systems say that manufacturers have long known the situation of software shortcomings, despite this fact they did not consider it important enough to intervene and inform their customers about it, e.g. Boeing has treated this information provided by experts as valuable, but with low practicality. Cyberattacks on aircraft IT

⁴⁰ ICAO - (International Civil Aviation Organization), an organization dealing with the development and implementation of international regulations governing the safety of international air navigation and supports the development of air transport to ensure safe and orderly development. <https://www.icao.int/> access. on 21.08.2021

⁴¹ IATA - (International Air Transport Association), a global trade organization based in Montreal and Geneva) gathering today 260 carriers using airlines. https://pl.wikipedia.org/.../Międzynarodowe_Zrzeszenie_Przewoźników_Powietrznych. access. on 21.08.2021

systems require specialized knowledge that the average person does not have, which is why the opinion of specialists has not been treated as a common security threat.

The aviation industry is currently facing a major challenge, having links with other industry sectors, whose task is to look for a way to secure aircraft IT systems against cyberattacks and which were developed at a time when we didn't realize

threats coming from Cyberspace.

The aviation ecosystem and transport in it is assessed as the safest means of transport, therefore it is the duty of the person concerned to consider all possibilities of counteracting cyber threats in order to preserve and even increase the efficiency, security and resilience of civil aviation systems. Travelers are looking for a safe means of transport, which is why air carriers have to deal with these types of threats and maintain a very high rate of trust and interest in air transport. In order to meet these requirements, air carriers and the entire aviation ecosystem must take the following actions:

- The entire aviation ecosystem is forced to rapidly evolve and introduce very stringent cyber-threat level checks and the fact that these new tests must be compatible with existing ones. The conclusion is that all components should be tested regardless of the time of assembly. Systems in passenger aviation consist of isolated systems, which unfortunately are susceptible to cyberattacks, therefore it is necessary to ensure a very quick response to discovered vulnerabilities in security systems.

- Critical systems should be tested by independent external companies with extensive experience in cybersecurity.

- Critical systems should have high security priority, such as communication system, radio, which should ensure strong authentication, confidentiality, accessibility and integrity. The philosophy in checking security against cyberattacks should be the following approach, other unsecured systems should be considered as a potential threat.

- Each element of the aviation ecosystem should raise awareness among all employees related to cyberattack threats and procedures to counter them. You should know and understand in depth the threats and risks, know who the attackers can be, what their motivations can be and how and where they can possibly attack. In such a situation, priority should be given to the protection of air carrier system components.

- Each of these elements must know its weaknesses in order to implement effective measures to reduce or completely eliminate the possible effects of cyberattacks.

- The next step in securing yourself from cyberattacks should be to build a recovery plan and increase response flexibility.

Nowadays, passenger aviation can be much safer by using Cyberspace by strengthening the security of its systems, whereas technologies are evolving very dynamically, both those used in transport and those used to perform cyberattacks.

PROTECTION OF AIRPORTS AND PASSENGER AIRCRAFT AGAINST UNAUTHORIZED INTRUSION OF DRONES INTO THE AIRPORT AREA

Unmanned aerial vehicles, often called drones, have become one from the technological wonders of our reality. Drones are easy to manufacture, relatively cheap, easy to fly, but difficult to detect. Drones are also a rapidly evolving technological threat to aviation, both military and civil aviation. Unmanned aviation creates a lot of new opportunities, but adequately to them also creates new threats that are not fully appreciated. The use of drones has become a common phenomenon in the public domain. Easy accessibility means that many people are unaware of the danger that goes with ignoring regulations and the basic requirements of aviation safety, which causes a huge threat and risk to aviation.

Currently, drones have the ability to collect confidential data, transport explosives, drugs, weapons, cell phones, chemical bombs, drugs, various types of jammers, etc. and question security systems.

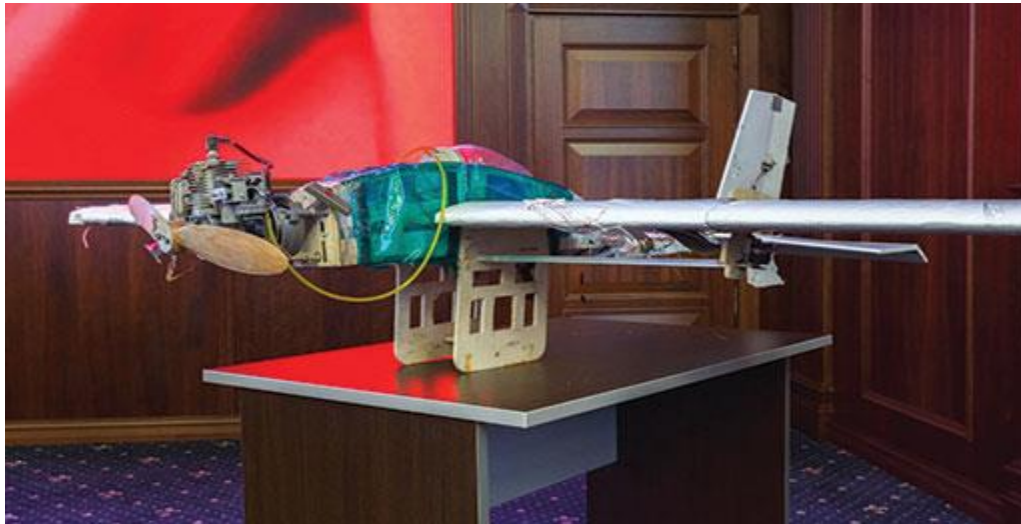
Modern life brings examples of the mass use of drones thanks to their ease of use, accessibility, cost savings, but also to perform tasks that are dangerous to people without risk of losing their lives. Non-state actors have also found application in, among others surveillance, attack. The possibilities of using drones are only limited by human imagination.

In addition to the benefits of using drones, they can become an increasing threat to aviation, including communication aviation. Terrorist organizations can use drones to inflict mass injuries and life sacrifices. Therefore, many companies have built anti-drone systems, e.g. NO-DRONE, HOLOGARDE, ArbitorShield, DroneShield, etc. These systems are integrated and are designed to detect, monitor, identify and classify drones that work for the airport, but also those which are inoperative and approaching the airport.

A big danger from drones is the attack on the airport, all airport infrastructure. Such an example is the terrorist attack on four Russian bases in Syria, on January 10, 2018. The attack was made with the help of thirteen drones, manufactured at home. Each of the drones was equipped with GPS and

powered by gas engines from mowers, and on board were placed half a kilogram of explosives (PETN⁴²) and metal ball bearings.

Fig. 4. Drone used during the attack in Syria on Russian bases



Source: (Credit: Russian Ministry of Defense)

The aviation ecosystem fighting the possibilities of unauthorized entry of drones in the airport area or with the possibility of a terrorist attack using drones, develops anti-drone systems, which can include SIM cards mounted in drones, as well as are detected by radars, acoustics, radio frequency (RF⁴³), heat detection, as well as pistols, which turn off UAVs or properly trained for capturing drones during flight birds of prey.

UNMANNED AERIAL VEHICLES AS TOOLS SUPPORTING THE PROTECTION OF AIRPORT INFRASTRUCTURE

Unmanned aerial vehicles (drones), in addition to the threats that appear along with unauthorized access to airport infrastructure, play a very important role in its protection. Drones supporting and protecting airport infrastructure can support Airport Rescue and Fire Fighting Services, monitoring

⁴² PETN (Pentrite) - a limited chemical compound from the group of nitroesters. Pentrite is one of the strongest known blasting explosives. It was used during World War II, today it is used in the production of explosive mixtures. <https://pl.wikipedia.org/wiki/Pentryt> access. on 21/08/2021

⁴³ RF is short for radio frequency. RF means any frequency in the electromagnetic spectrum associated with radio wave propagation. When RF current is supplied to the antenna, an electromagnetic field is created, which can then spread in space. Many wireless technologies rely on RF field propagation. These frequencies are part of the electromagnetic spectrum. m.pl.relyrfwireless.com/info/rf-testing-definition-description-22424659.html access. on 21/08/2021

and also recording accidents and disasters, support airport maintenance services, support various departments of airport infrastructure operation by monitoring and inspecting buildings, various types of equipment, road surfaces, installations. Drones are often used to support operational and duty departments, providing very good quality imagery for situational and operational awareness.

Airbus presented the capabilities of airport drones to the civil aviation environment by showing them the inspection of the aircraft, which lasted only fifteen minutes. Numerous research and development centers have shown that:

- the drone can effectively fulfill the innovative role of an airport security management element, monitoring the technical condition of aircraft, the entire infrastructure of the airport, the fence, or detecting other unmanned aerial vehicles that perpetrate unauthorized intrusion into the airspace of the airport, thus preventing collisions or acts of terrorism from the air,
- drones can contribute to improving the safety of old aircraft and landings by detecting potential threats,
- airport drones have detection systems that are based on active ones and passive radars capable of detecting radio signals emitted by apparatus and controllers,
- it is recommended to create at least three airstrips at the airport for drones belonging to airport services,
- unmanned aerial vehicles in the airport service should show high flight speed, good camera separation, very short take-off time from the occurrence of a negative phenomenon to the moment of arrival by UAV, high resistance to adverse weather conditions,
- a system should be created to ensure image transfer from an airport drone to the units and services responsible for safety and security at the airport, e.g. Airport Security Guard, Border Guard, Airport Rescue and Fire Fighting Service, Customs Service, various departments of duty, operational or police. Integration of airport drones with the work of the crisis staff is a required necessity.

Nevertheless, airport drones can be attacked by hackers, and used to perform a cyberattack on airport infrastructure using drone disruption technique, i.e. the possibility of interrupting GPS signal reception is at stake. In this case, the unmanned platform could potentially lose the ability to monitor its flight and may lose the ability to calculate its position, altitude and direction of flight⁴⁴. After the takeover of the airport drone by cyber hackers, they can perform a terrorist attack on any object of

⁴⁴ W. Leśnikowski, *Unmanned platforms in cyberspace*, "Adam Marszałek Toruń", 2017, p. 222

the airport infrastructure, or directed to perform an attack on taking off or landing aircraft with a large number of passengers on board.

CONCLUSIONS

Our society in which we live is called a global information society that operates in a certain climate of uncertainty and risk. Subject experts define our age as a world of crises and security shortages, as a world dominated by cyberattacks on all areas of life, including Critical Infrastructure and civil aviation.

The increasing automation of civil aviation means a greater risk of cyberattack. The more comprehensive the systems, the more potential unauthorized "entrances". IT systems and networks in passenger aircraft are very different from "normal" computers and the network infrastructure known to us. Fixing any gaps in the software for the aviation industry is an extremely complicated task, and besides, or perhaps above all, this procedure costs a fortune. According to one member of the DHS (*Department of Homeland Security*) team, repairing one line of code in such a program can cost from a million dollars upwards, and its inclusion in production can take years.

The days are over when the biggest threat during the flight or at the airport was a weapon. Modern cyber threats are already much more serious, which is why the Civil Aviation Authority (ULC) has set up a new body dealing with IT security 24 hours a day, seven days a week. Thus, ULC joined the system of sharing information about accidents, incidents and cybersecurity with the signing of the agreement with EASA⁴⁵.

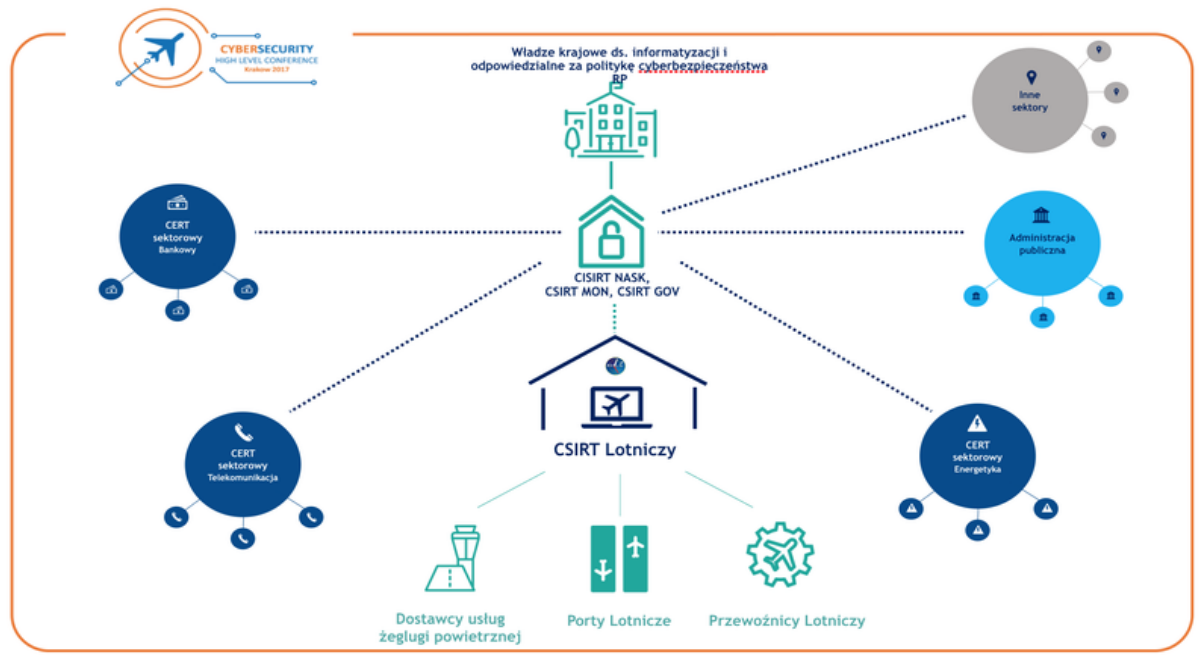
Cybersecurity is not identified only with IT, first of all it is information. Even the smallest safety signals, including civil aviation safety, should not be underestimated. Along with the information, conclusions should be drawn which should be forwarded to the interested institutions and cells of the aviation ecosystem.

Information is the basis. The key is exchange of information. The resulting cybersecurity center in civil aviation, i.e. the Cyberinformatic Threat Response Center, which has been included in the national cybersecurity system, as did the energy industries and the financial sector. The center is to employ both IT specialists and analysts.

"In the current century, the main threat is the smartphone, Internet, cyber threats," said ULC president Piotr Samson.

⁴⁵ EASA - (European Aviation Safety Agency). www.ulc.gov.pl/pl/urząd/kierownictwo/248-wazne/1482-easa access. on 21/08/2021.

Fig. 5. ULC activities to protect against cyberattacks and other unauthorized access to civil aviation



Source: Photo, Civil Aviation Authority

Fig. 6. Airport infrastructure detection and protection system built by Airbus DS. Electronic and Border Security (EBS) Dedrone. The system detects and disarms or destroys small drones that have obtained unauthorized access to the critical airspace of the airport.



Source: <https://www.recode.net/2017/2/14/14600030/dedrone-disarm-illegal-drones-15-million-funding> access. on 21.05.2021

BIBLIOGRAFIA

REFERENCES LIST

PIŚMIENICTWO LITERATURE

- Bógadał-Brzezińska A., Gawrycki F. M., *Cyberterrorism and the problem of IT security in the modern world*, ASPRA-JR, Warsaw 2003
- Borowik, R., *Transformations of cultural awareness in the era of the information society*, <http://www.uci.agh.edu.pl/agh/dep/wsss/konferencja/doc>
- Dobrzeński K., *Law and ethos of cyberspace*, Adam Marszałek, Toruń 2021, p. 11
- Gagnon B., *Are We Headed for a "Cyber-9/11?": The American Failure in Cyberstrategy*, Center for United States Studies of the Raoul Dandurand Chair of Strategic and Diplomatic Studies, Occasional Paper no 5, Quebec, 2004
- Gibson W., *Neuromancer*, ed. II, Poznań 1999
- Horoszkiewicz J., *Internet - uncontrolled zone in cyberspace*, *Political Review*, 2001. No. 2 (62)
- Kisielewski S., *The government wants to protect the cyberspace of the Republic of Poland*, *Computerworld.pl*, February 5, 2009
- Janowska A., *Cyberterrorism - reality or fiction ?*, [in:] *Information society - vision or reality ?*, Kraków 2003, <http://www.angelfire.com/az/sthurston/Cyberwar.html>
- Jasper S., *Conflict and Cooperation in the Global Commons. A Comprehensive Approach for International Security*, Georgetown University Press/Washington, DC, 2012
- Koziej S., *Security: Essence, basic categories and historical evolution*, *National Security*, 2011, No. 18
- Leśnikowski W., *Unmanned platforms in cyberspace*, Adam Marszałek Toruń, 2017
- Leśnikowski W., *Welcome to the cyberwar world*, *Air Force Review*, 2011, No. 4 (046)
- Leśnikowski W., *Military use of cyberspace and conventional combat operations*, Monograph, *Contemporary bioterrorist and cyberterrorist threats and Polish national security*, Warsaw, December 2013
- Leśnikowski W., *Cyberattacks against critical infrastructure as cheap and effective means to paralyze developed countries*, *Air Force Review*, September 2012 No. 02 (059), (electronic version)
- Leśnikowski W., *Welcome to the world of cyberwar part. one*; *Air Force Review*, 2011 No. 4 (046)
- Rattray J. Gregory *Strategic war in cyberspace. Secret - Attack - Defense*. Scientific and Technical Publishing House, Warsaw 2004
- The governmental cyberspace protection program of the Republic of Poland for 2011-2016, version 1.1, June 2010)
- Sienkiewicz P., *25 lectures*, AON, 2013
- Sienkiewicz P., Świeboda H., Lichoński E., *System analysis of the phenomenon of cyberterrorism*, National Defence Academy.. <http://www1.aon.edu.pl/zen2/index.php?option=content&task=view&id=571>

ŹRÓDŁA

SOURCES

Directions of development of the command system of the Polish Armed Forces - selected aspects,

<http://www.angelfire.com/az/sthurston/Cyberwar.html>

<https://rcb.gov.pl/infrastruktura-krytyczna/>

<https://www.aiaa.org/>

"ecosystem" of aviation - www.rynekinfrastruktury.pl/.../nowa-strategia-rozkieta-europejskiego-lotnictwa-52198....

www.dictionary.com/browse/fbi

www.dictionary.com/browse/fbi

Technologia.dziennik.pl/.../502623,expert-warns-hackers-can-attack-plane

http://www.altair.com.pl/news/view?news_id=18466

<https://www.icao.int/>

https://pl.wikipedia.org/.../International_association_of_air_carriers

m.pl.relyrfwireless.com/info/rf-testing-definition-description-22424659.html

www.ulc.gov.pl/pl/urząd/kierownictwo/248-wazne/1482-easa

<https://www.recode.net/2017/2/14/14600030/dedrone-disarm-illegal-drones-15-million-funding>



Copyright (c) 2021 Władysław LEŚNIKOWSKI



This work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.