Elżbieta Hodyr*

Cybersecurity of Air Force

Abstract

Cybersecurity of air force is new challenges topic in cyberspace. I would like to describe that challenges in my article. I think important is influence of Warsaw Summit 2016 and declaration, that Nato will be use in the future also Offensive Cyber Operation. I would like to describe them. Later I would like to focus how technology changes – satellite technologies should make an evolution in Air Force (maybe Air and Space Force should be). I will also describe India develop in cybersecurity of Air Force. In the and I will describe cybersecurity of Air Force objectives, gaps of cybersecurity of Air Force and try to give recommendation what to do to strengthen cybersecurity of Air Force.

Key words: cybersecurity, Offensive Cyber Operation, Defensive Cyber Operation, satellite technologies, Air Force, Air and Space Force

* Elżbieta Hodyr, PhD Student, War Studies University in Warsaw, e-mail: ehodyr@gmail. com, ORCID: 0000-0001-5045-093X.

In the beginning, what is cybersecurity? Cybersecurity comprises three planes of study:

– Operations adress the day-to day functioning of the information security tasks. Operational issues inclued staffing, implementation of policies and procedures, incident response, business continuity, disaster recovery, systems management, tool acquisition and deployment, investigations and more;

– Governence function includes the development of organizational structure and command chain that oversees, manages and handles information and information systems. Governence include the development of policies and procedures that drive the operational aspects, the laws and policies that set the societal expectations of individual and organization activities. Categories of law include crimnal law (statutes guiding actions that are deemed to threaten harm public safety or welfare), civil law and administrative law;

– Training refers to teaching indivduals specific skills and competencies that are usually task-or project-oriented[1].

According to the US approach cyber security includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster[2].

How to position the air force in cybersecurity. They are one of the most important components of the security system.

In terms of systems, most generally, air defense can be defined as separated forces and measures organized in a specific structure aimed at ensuring safety in the airspace. The challenge for the air defense system in question is the implementation of tasks in the area of state air security by ensuring an appropriate degree of reaction of the assigned forces to emerging threats. It is important that this guarantor is the constant search for optimal solutions in the organizational sphere, as well as technical, technological and procedural modernization[3].

[1] E. Hodyr, *Cybersecurity – new challenges in international law*, „Journal of Polish American – Science and Technology" 2016, vol. 10.

[2] Ibidem.

[3] *Wyzwania i rozwój obrony powietrznej Rzeczpospolitej Polskiej – obronność RP XXI wieku*, eds. K. Dobija, S. Maślanka, D. Żyłka, Warszawa 2018, p. 102.

The source of threats in the air force are threats such as: air attack measures, air terrorism, continuous increase in speed, intensity and, consequently, air traffic density, dangerous weather phenomena, unreliability of human activity[4].

Recently, however, it should be noted that air forces, in particular, rely heavily on cyberspace's Computer and Information Systems CIS and Information Technology to carry out their missions. From the strategic to the tactical level and from Command and Control (C2) systems to mission systems, air forces are, arguably, both more vulnerable to breaches in their defenses and greater benefactors of successful attacks on adversaries'systems[5].

The defense of its CIS/IT has always been one of NATO's principle responsibilities in order to protect its ability to connect the Alliance, support projects and conduct operations and missions. The overall responsibility to protect NATO's CIS/IT was shared for decades among several agencies up until 1 July 2012 when the NATO Communication and Information Agency (NCIA) was formed from amalgamation of several agencies, principally: the NATO Consultation Command and Control Agency NC3A, the NATO CIS Services Agency (NCSA), the NATO Air Command and Control systems (ACCS) Management Agency (NACMA) and the Active Layered Theatre Ballistic Missile Defense BMD Programme office[6].

At this point I would like to mention, Computer Incident Response Capability (NCIRC) and Computer Emergency Response Team of the European Union (CERT-EU) – all these activities were developed within the framework of NATO's mission and core tasks of collective defense, crisis management and cooperative security[7].

As I wrote in the introduction, the Air Force needs technical and technological modernization, which is why the Air and Space Power in NATO Future Vector project is worth attention. The project was initiated in 2002. The justification of the project stated that space and the power of cyberspace enable the extraordinary precision of modern weapons. Cybernetic capabilities give you a chance to neutralize your opponent without firing a shot. The ideal

[4] A. Glen, *Podstawy poznawcze bezpieczeństwa powietrznego państwa*, Warszawa 2013, p. 43.

[5] P. MacKenzie, *NATO Joint Air Power and Offensive Cyber Operations*, Kalcar 2017, p. 2.

[6] *NATO Communications and Information Agency NCIA*, http://www.nato.int/cps/en/natolive/topics_69332.htm [access: 20.04.2022].

[7] *North Atlantic Treaty Organization*, http:/ www.nato.int/cps/en/natohq/topics_133127.htm [access: 15.03.2022].

of winning without extensive on-the-spot fighting and with minimal human cost is nothing new, but recent improvements to Air, Space and Cyber Power technology open up new avenues for using the armed forces without sending large numbers of troops[8].

Continuing, it should be mentioned that the implementation of the Air and Space Power in Nato Future Vector project faced numerous obstacles from the very beginning. It was not until the NATO summit in Warsaw in July 2016 that the organization's leadership officially declared that it would also use offensive operations in cyberspace in the future[9].

As I wrote in the introduction, I would like to describe the difference between OCO offensive operations and DCO defensive operations. DCO are considered those actions undertaken to ensure the confidentiality, integrity and availability of NATO systems and/or data. OCO are those activities undertaken via digital means, to infiltrate, reconnoiter, exploit, disrupt, deny access to and/or destroy the adversaries systems and/or data. Furthermore, since the focus is OCO as the pertain to Joint Air Power it is necessary to understand Joint Air Power as synergetic application of air, space and information systems from and for all services to project military power and includes the use of military force in air or space by or from an air platform or missile operating above the surface of the earth[10].

In accessing cyber targeting Michael N. Schmitt attest that'it is quite simply unimaginable that a contemporary conflict would not involve some manner of cyber operations' even for something as complicated as bringing down the enemy's Integrated Air Defense Systems and it is very possible the preferred method may turn out to be cyber means instead of conducting kinetic attacks. Adversaries' civilian Air Traffic Control and Airspace Management Systems are also potential targets if employed even partially by the military[11].

That's why, with respect to incorporating OCO at the operational level, a solutions may be found in options purposed for integrating cyberspace into USAF Air Operations Centers (AOC)[12].

[8] M. Polkowska, *Bezpieczeństwo w przestrzeni kosmicznej. Prawo, zarządzanie, polityka*, Warszawa 2021, p. 98.

[9] Ibidem.

[10] Concept for the Joint Air Power Competence Centre (JAPCC) MOD Bonn, 31 July 2003, p. 3.

[11] P. MacKenzie, op. cit., p. 9–10.

[12] A. Bradley, *Cyber Integration within the Air Operations Center*, *May 2013*, *Graduate Research Project*, Wright-Patterson, OH 2013.

In this model AOC provides operational level C2 of air, space and cyberspace operations and is the focal point for planning, directing and accessing air, space and cyberspace operations to meet JFACC (Joint Force Air Component Commander) operational objectives and guidance[13].

The AOC would be organized, trained and equipped to provide cyber planning and operation expertise in order to coordinate and synchronize cyberspace operations activities with other domains and would ensure all cyber tasking are deconflicted, integrated and coordinated into the Air Tasking Order (ATO)[14].

In the next part of the article I would like to analyze the development of technologies for cybersecurity. I think that one should therefore ask whether the Air Force or the Air and Space Force.

On the ground-segment side of satellite control, the debut of privately owned communication antennas for rent and a move to cloud-based operations or mission centers will bring new requirements for cyber protection for both Department of Defense (DOD) and commercial satellite operations alike. It is no longer a matter of whether automation will be introduced to satellite operations, but how quickly satellite operators can adapt to the onset of control automation and promote cybersecurity in an increasingly competitive, contested, and congested space domain[15].

An additional operational distinction is made between satellite automation — the self-contained system process of conducting repetitive tasks — and satellite autonomy, which gives the satellite the ability to implement changes with limited to no human-in-the-loop actions[16].

This distinction will add a level of complexity to the cybersecurity of satellite control. Placing tasks previously controlled by humans under the control of a computer-executed algorithm may be the only viable way

[13] Ibidem, p. 6.

[14] Ibidem, p. 14.

[15] C. Poole, R. Bettinger, M. Reith, *Shifting Satellite Control Paradigms.Operational Cybersecurity in the Age of Megaconstellations*, „Air and Space Power Journal – Technology" 2021, vol. 35, no. 3, p. 46.

[16] J.B. Hartley, P.M. Hughes, *Automation of Satellite Operations: Experiences and Future Directions at NASA GSFC* [in:] *Space Mission Operations and Ground Data Systems – SpaceOps'96, Proceedings of the Fourth International Symposium held 16–20 September 1996 in Munich, Germany*, ed. T.D. Guyenne, Paris 1996, p. 1262−1269.

to manage the development of future megaconstellations and enable effective space-traffic management[17].

The control architecture for satellites has remained nearly constant since the beginning of the Space Age in the mid-twentieth century. Starting with the launch of the first artificial satellites, each on-orbit system has mostly featured a unique design, function, and mode of operation. This uniqueness has led to self-contained and independent operating procedures controlled by the satellite owner. In the typical satellite-control structure, a satellite downlinks information such as payload data and spacecraft state-of-health information when it is within view of a ground based receiver. From the receiver, the information is processed and passed to the satellite operations center (SOC), which reviews it for faults and assesses the need for required operating adjustments and/or new system instructions[18].

In Asia, China Telecom reportedly plans to create a 10,000-satellite megaconstellation called „China StarNet" in the next 5−10 years[19]. In late 2020, the European Union revealed plans to initiate a program to develop a telecommunications megaconstellation to establish „European digital sovereignty"[20].

While automation will play a large role in handling satellite functions, the main changes for cybersecurity will come from the evolutionary shifts made in the ground-control segments and associated security implementation requirements. In the 2020 Space Capstone Publication Spacepower: Doctrine for Space Forces, the foundation for cybersecurity is defined in the cyber operations spacepower discipline as the „knowledge to defend the global networks upon which military space power is vitally dependent", the „ability to employ cybersecurity and cyber defense of critical space networks and systems", and the „skill to employ future offensive capabilities"[21].

The goal of any satellite system is to maintain mission functionality for the planned mission lifetime; this requires satellite survivability. Satellite

[17] S.J. Butow et al., *State of the Space Industrial Base 2020: A Time for Action to Sustain US Economic & Military Leadership in Space*, Washington, DC 2020.

[18] C. Poole, R. Bettinger, M. Reith, op. cit., p. 47.

[19] D. Swinhoe, *China's Moves into Mega Satellite Constellations Could Add to the Space Debris Problem*, April 20, 2021, https://www.datacenterdynamics.com/ [access: 20.04.2022].

[20] J. O'Callaghan, *Europe Wants to Build Its Own Satellite Mega Constellation to Rival SpaceX's Starlink*, Forbes, December 23, 2020, https://www.forbes.com/ [access: 20.04.2022].

[21] J.W. Raymond, *Space Capstone Publication Spacepower: Doctrine for Space Forces*, Washington, DC 2020, p. 52.

survivability is a function of three time-separated phases: susceptibility, vulnerability, and recoverability[22].

The USSF is in the crucial position to make this happen starting at the ground level. As mentioned in the Space Capstone Publication, increased education will add to the understanding of the „network dimension". Optimally, this education would result in embedding cyberoperations members at key SOCs, in addition to having increased cybersecurity and monitoring training at all levels of satellite operations. This approach will facilitate a highly digitally capable satellite-operations cadre[23].

Satellite systems and controls architectures are in a rapid state of change. Satellite automation could significantly alter the current hands-on satellite-operations mission to one of key-event monitoring, with a consolidated human-in-the-loop team present to react to and resolve issues that cannot be directly handled by the satellite itself or by the megaconstellation. Additionally, the introduction of a more capable and increasingly flexible mission-operations system, one using emerging technologies such as cloud-based networks and services like privately owned and networked ground stations, will make it possible for true 24/7 global access to and control of satellite systems. To ensure the continued safety and security of on-orbit satellite systems, both the defense and commercial space sectors must adapt to the rapidly changing digital landscape of future space operations. The introduction of the CMMC has already demonstrated such an adaptation, along with the alignment of emergent USSF doctrine and strategy with cyber-mindedness. The final step will be to shape the future of the USSF and USAF space and cyberspace cadre to be better prepared as a digital force synergistically working to remain at the forefront of protection in the increasingly competitive, contested, and congested domain of space[24].

I think it is worth noting here that the threat of countries with cyber attacks meant that the European members of this organization, who had so far used the SSA system – the space situational awareness program (which did not treat military issues as the main issue), had to turn to the American SDA program, intended primarily for the military (which, in its assumptions, is to combat cyber attacks[25].

[22] C. Poole, R. Bettinger, M. Reith, op. cit., p. 52.
[23] Ibidem, p. 54.
[24] Ibidem.
[25] M. Polkowska, op. cit., p. 97–98.

It should also be mentioned here that a few years ago the Panel on Concepts and Integration of Systems of Science and Technology Organizations (STO) was created, which supports NATO activities in space. In STO was created Research Task Group: Collaborative Space Domain Awareness Data Collection and Fusion Experiment for data collection and experimental activities and the exchange of information between Member States[26].

That's why I think it must by analyze Air Force or Air and Space Force.

Although the nature of air and space as distinct domains make independent services desirable, they remain intimately linked. Secretary of the Air Force Frank Kendall stated, only the „Air and Space Forces have the ability to control the high ground [...] can project power on short notice to anywhere that it is needed [...] have the ability to confront and defeat aggression immediately, wherever it occurs [...] [and] have the ability to come to the aid of our global Allies and partners with little or no notice wherever aggression occurs"[27]. The Air and Space Forces share a common operating border – the air domain ends and the space domain begins at the point atmospheric effects become negligible[28].

The last time the DAF had an opportunity to change its name to embrace space was in 1981, when Congressman Ken Kramer recognized the advancing Soviet space threat required a new focus. Kramer introduced House Resolution 5130, the Aerospace Force Act that would have renamed the department and service to the Department of the Aerospace Force and US Aerospace Force and granted Title 10 authorities for space operations – something that only recently occurred with the Space Force's establishment. At the hearing, Kramer testified that the suggestion of a name change is to stimulate thinking about the fact that our Air Force ought to be involved in both air and space in coequal roles, that too much emphasis to date has been placed on air and not enough emphasis on space. If we had an Aerospace Force as opposed to an Air Force, implicit in that name would be a recognition of the importance of space as another theater[29].

[26] Ibidem.

[27] F. Kendall, *VIDEO: Kendall on the State of the Forces at AFA's Air, Space & Cyber '21*, „Air Force Magazine" (website), September 23, 2021, https://www.airforcemag.com/ [access: 22.04.2022].

[28] *Chairman of the Joint Chiefs of Staff (CJCS), Joint Air Operations, Joint Publication (JP) 3-30*, Washington, DC 2021, p. I-1; *Space Operations, JP 3-14*, Washington, DC 2020, p. vii.

[29] K. Kramer, *Hearing on H.R. 5130 Aerospace Force Act before the Investigations Subcommittee of the Committee on Armed Services House of Representatives*, 97th Cong.

The DAF's point of opposition in 1981 provides a benchmark to measure the relative justification for renaming today with a simple question: is space a coequal partner with air in the department? Fortunately, the department itself has already provided the answer, stating in a 2020 report to Congress that it is „one department with two coequal services and service chiefs", justifying a name that accurately reflects its composition and purpose[30].

Renaming would affect the DAF headquarters elements, Air and Space Forces awards and decorations, and joint Air and Space Forces field organizations that support both services – whether they are situated within the Air Force, Space Force, or the Office of the Secretary of the Air Force. This is not a revolution but rather marks a singular moment in the ongoing evolution of these organizations from air to air and space.

- Department of the Air Force (DAF) – Department of the Air and Space Forces (DASF);
- Secretary of the Air Force (SecAF/SAF) – Secretary of the Air and Space Forces (SecASF/SASF);
- US Air Force Academy (USAFA) – US Air and Space Forces Academy (USASFA/ASFA;
- Air Force Reserve Officer Training Corps (ROTC) – Air and Space Forces ROTC;
- Air Force Research Laboratory (AFRL) – Air and Space Forces Research Laboratory (ASFRL);
- Air Force Cross – Air and Space Forces Cross;
- Airman's Medal – Airman and Guardian's Medal

The Air and Space Forces should also ensure aerospace and air and space do not describe single-domain or single-service functions. For instance, the Air Force's 2A aerospace maintenance enlisted career fields, including aerospace ground equipment and aerospace propulsion, deal almost exclusively with aircraft[31].

Continuing, and as it is in India. This is also where the cybersecurity of the air force is developing. IAF chief addresses Central Air Command, urges

2nd Sess. (May 19, 1982) (9) (Statement of Congressman...), https://www.congress.gov/bill/97th-congress/house-bill/5130/all-info?r=84&s=1 [access: 20.04.2022].

[30] S. Erwin, *U.S. Space Force Organizational Plan Delivered to Congress*, SpaceNews, February 3, 2020, https://spacenews.com [access: 20.04.2022].

[31] *Air Force Enlisted Classification Directory: The Official Guide to the Air Force Enlisted Classification Codes*, San Antonio, TX 2021, p. 116, 142, 144.

stronger physical, cyber security. He directed the Commanders to ensure the readiness of all platforms weapon systems and assets are kept at the highest level. The chief appreciated the role of Central Air Command in the recent flood relief efforts and aid to civil administration. Urging the Commanders to continue their efforts in ensuring a safe operational flying environment, the Air Chief Marshal stressed the need to augment the combat capability in Indian Air Force through innovation, self – reliance and indigenisation[32].

In the end, cybersecurity objectives are:

1. Organizational design should be flexible and decentralized. The cybersecurity environment is inherently dynamic and complex. The literature suggests that well managed organizations cope with such environments by choosing organizational designs that favor solutions obtained through decentralized coordination and collaboration of workers over those prescribed by standardized and formalized controls.

2. Outcome-based feedback is more valuable than compliance-based feedback. Organizations tend to focus on readily observable metrics, such as compliance with policies and directives, to indicate their level of cybersecurity. However, compliance does not, in itself, reflect the actual state of cybersecurity, especially in complex and rapidly changing threat environments. Organizations should instead focus on whether their policies and practices are achieving the desired outcomes (e.g., mission assurance in the face of adaptive cyberattacks) and should be ready to adapt as needed[33].

Follow I would like to describe Air Force gabs. They reveals number of them. The vulnerabilities are as follows:

Current policies are better suited to simple, stable, and predictable environments than to the complex, rapidly changing, and unpredictable reality of today's cybersecurity environment. DoD has sought to standardize cybersecurity by applying the National Institute of Standards and Technology's (NIST's) security controls to all systems, including weapon systems. But these controls are designed to mitigate security issues in designs that the Air Force inherits, such as in COTS systems. Weapon systems, in contrast, present opportunities for designers to build systems that are more inherently secure.

[32] https://www.aninews.in/news/national/general-news/iaf-chief-addresses-central-air-command-urges-stronger-physical-cyber-security20210917105036/ [access: 20.04.2022].

[33] *Cybersecurity of Air Force Weapon Systems. Ensuring Cyber Mission Assurance Throughout a System's Life Cycle. Research Brief*, p. 1–2, https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9800/RB9835/RAND_RB9835.pdf [access: 25.04.2022].

Sound system security engineering during the early design phase of a weapon system would be more effective than security controls that are applied as overlays to designs created without cybersecurity as an integral priority.

Implementation of cybersecurity is not continuously vigilant throughout the life cycle of a military system. Attention to cybersecurity is generally triggered by acquisition events, which mostly occur during procurement. As a result, policy does not cover the full range of cybersecurity issues that affect a system over its life cycle. This shortfall has several important consequences. First, programmatic triggers for cybersecurity come late in the design process and, therefore, have little leverage to influence critical design decisions that affect cybersecurity. Second, systems in programs beyond the procurement phase (i.e., in sustainment or disposal) receive less attention than those in procurement. As noted above, this underemphasizes the majority of Air Force systems, which are in sustainment. Third, this policy structure tends to favor vulnerability assessments (prevalent in the design phase) over mission impact and threat assessments (which affect the entire life cycle). Finally, management, oversight, and budgeting within DoD are strongly structured around programs, whereas cybersecurity vulnerabilities cross program boundaries. This creates a misalignment between cybersecurity challenges in specific systems and how they can be managed.

Control of and accountability for military system cybersecurity is spread over numerous organizations and is poorly integrated. This results in diminished accountability and unity of command and control for cybersecurity. These overlapping roles, and particularly the presence of a cybersecurity-focused authorizing official, create ambiguities in decision authority and accountability. For example, who can make the final decision regarding risk to a mission: the commander or the authorizing official? And should a cybersecurity incident occur, who is ultimately to be held accountable: the program manager, the authorizing official, or the operational commander?

Monitoring and feedback for cybersecurity is incomplete, uncoordinated, and insufficient for effective decision making or accountability. Current feedback does not capture all systems, does not probe the consequences of cybersecurity shortfalls, and is not produced in a form that informs effective decision making. The lack of comprehensive program- or system-oriented feedback on cybersecurity and the impact of cybersecurity on operational missions stands in contrast to the abundance of feedback on cost and schedule. This imbalance creates an incentive structure for program managers and program executive officers to favor cost and schedule over cybersecurity performance. These deficiencies in feedback on cybersecurity also further inhibit individual accountability[34].

In the conclusion, there are steps the Air Force can take to strengthen cybersecurity for weapon systems:

1. Define cybersecurity goals for military systems within the Air Force around desired outcomes while remaining consistent with DoD issuances. As a working objective, keep the impact of adversary cyber exploitation and offensive cyber operations to an acceptable level, as guided by a standardized process for assessing risk to mission assurance.

2. Realign functional roles and responsibilities for cybersecurity risk assessment around a balance of system vulnerability, threat, and operational mission impact, and empower the authorizing official to integrate and adjudicate among stakeholders. For example, the life-cycle management community (specifically the program manager) would be responsible for program and system vulnerability assessments, the intelligence and counterintelligence communities would be responsible for threat assessments, and the mission owner (e.g., core function lead integrator, lead major command) would be responsible for operational mission assurance assessments. The authorizing official would integrate and balance these viewpoints based on an acceptable level of cybersecurity risk.

3. Assign each authorizing official a portfolio of systems and ensure that all systems explicitly fall under some authorizing official throughout their life cycles.

4. Encourage Air Force program offices to supplement the required DoD security controls (which focus on closing vulnerabilities) with more comprehensive cybersecurity measures, including sound system security engineering (which focuses on making the system robust and resilient in the face of successful attacks).

5. Foster innovation and adaptation in cybersecurity by decentralizing, in any new Air Force policy, how system security engineering is implemented within individual programs.

6. Explicitly assess the trade-offs between cybersecurity risks and functional benefits associated with interconnecting military systems in cyberspace. This would reverse the default culture of connecting systems whenever possible and would reduce the complexity of cybersecurity.

[34] Ibidem, p. 2.

7. Create a group of experts in cybersecurity who can be matrixed as needed within the life-cycle community, making resources available to small programs and to programs in sustainment.

8. Establish an enterprise-directed prioritization for assessing and addressing cybersecurity issues in legacy systems.

9. Close feedback gaps and increase the visibility of cybersecurity by producing a regular, continuous assessment that summarizes the state of cybersecurity for every program in the Air Force. Hold program managers accountable for a response to issues.

10. Create cybersecurity red teams that are dedicated to acquisition/life-cycle management within the Air Force.

11. Hold individuals accountable for willful infractions of cybersecurity policies.

12. Develop mission threat data to support program managers and authorizing officials in assessing acceptable risks to missions caused by cybersecurity deficiencies in systems and programs[35].

I think it's important to conclude that air force cybersecurity is a big challenge in the world around us. The 2016 NATO summit in Warsaw was of great importance for the development of cybersecurity of the air force, where it was decided that offensive operations in cyberspace would also be used in the future. The space and cyber domains of the air force should also not be forgotten, which is of utmost importance for their development, despite the air force cybersecurity gaps described at the end of the article. I think that the further development of air force cybersecurity is extremely important for international cyber defense and the future.

Bibliography

Air Force Enlisted Classification Directory: The Official Guide to the Air Force Enlisted Classification Codes, San Antonio, TX 2021.

Butow S.J. et al., *State of the Space Industrial Base 2020: A Time for Action to Sustain US Economic & Military Leadership in Space*, Washington, DC 2020.

Cybersecurity of Air Force Weapon Systems. Ensuring Cyber Mission Assurance Throughout a System's Life Cycle. Research Brief, https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9800/RB9835/RAND_RB9835.pdf [access: 25.04.2022].

Erwin S., *U.S. Space Force Organizational Plan Delivered to Congress*, SpaceNews, February 3, 2020, https://spacenews.com [access: 20.04.2022].

Glen A., *Podstawy poznawcze bezpieczeństwa powietrznego państwa*, Warszawa 2013.

[35] Ibidem.

Hartley J.B., Hughes P.M., *Automation of Satellite Operations: Experiences and Future Directions at NASA GSFC* [in:] *Space Mission Operations and Ground Data Systems – SpaceOps'96, Proceedings of the Fourth International Symposium held 16–20 September 1996 in Munich, Germany*, ed. T.D. Guyenne, Paris 1996.

https://www.aninews.in/news/national/general-news/iaf-chief-addresses-central-air-command-urges-stronger-physical-cyber-security20210917105036/ [access: 20.04.2022].

Kendall F., *VIDEO: Kendall on the State of the Forces at AFA's Air, Space & Cyber'21*, „Air Force Magazine" (website), September 23, 2021, https://www.airforcemag.com/ [access: 22.04.2022].

Kramer K., *Hearing on H.R. 5130 Aerospace Force Act before the Investigations Subcommittee of the Committee on Armed Services House of Representatives*, 97th Cong. 2nd Sess. (May 19, 1982) (9) (Statement of Congressman...), https://www.congress.gov/bill/97th-congress/house-bill/5130/all-info?r=84&s=1 [access: 20.04.2022].

MacKenzie P., *NATO Joint Air Power and Offensive Cyber Operations*, Kalcar 2017.

NATO Communications and Information Agency NCIA, http://www.nato.int/cps/en/natolive/topics_69332.htm [access: 20.04.2022].

North Atlantic Treaty Organization, http:/ www.nato.int/cps/en/natohq/topics_133127.htm [access: 15.03.2022].

O'Callaghan J., *Europe Wants to Build Its Own Satellite Mega Constellation to Rival SpaceX's Starlink*, Forbes, December 23, 2020, https://www.forbes.com/ [access: 20.04.2022].

Polkowska M., *Bezpieczeństwo w przestrzeni kosmicznej. Prawo, zarządzanie, polityka*, Warszawa 2021.

Poole C., Bettinger R., Reith M., *Shifting Satellite Control Paradigms. Operational Cybersecurity in the Age of Megaconstellations*, „Air and Space Power Journal – Technology" 2021, vol. 35, no. 3.

Raymond J.W., *Space Capstone Publication Spacepower: Doctrine for Space Forces*, Washington, DC 2020.

Swinhoe D., *China's Moves into Mega Satellite Constellations Could Add to the Space Debris Problem*, April 20, 2021, https://www.datacenterdynamics.com/ [access: 20.04.2022].

Wyzwania i rozwój obrony powietrznej Rzeczpospolitej Polskiej – obronność RP XXI wieku, eds. K. Dobija, S. Maślanka, D. Żyłka, Warszawa 2018.

Cyberbezpieczeństwo sił powietrznych

Streszczenie

Cyberbezpieczeństwo sił powietrznych to nowe wyzwania w cyberprzestrzeni. Tych wyzwań dotyczy niniejszy artykuł. Ważny jest wpływ szczyt NATO w Warszawie w 2016 roku i deklaracja, że NATO będzie w przyszłości wykorzystywać także ofensywną operację Cyber. Autorka skupiła się na zmianach technologicznych – technologie satelitarne powinny ewoluować w siłach powietrznych (a może powinny być siły powietrzne i kosmiczne?). Na przykładzie Indii opisała rozwój cyberbezpieczeństwa sił powietrznych. Następnie omówiła cele cyberbezpieczeństwa sił powietrznych oraz luki w nim. W zakończeniu zawarła rekomendacje – co zrobić, żeby wzmocnić cyberbezpieczeństwo sił powietrznych.

Słowa kluczowe: cyberbezpieczeństwo, ofensywna operacja cybernetyczna, defensywna operacja cybernetyczna, technologie satelitarne, siły powietrzne, siły powietrzne i kosmiczne