MINISTERSTWO OBRONY NARODOWEJ

KWARTALNIK BELLONA

nr 3/2020 (702)

ISSN 1897-7065
E-ISSN: 2719-3853

Rocznik CII (XIV)

WOJSKOWY INSTYTUT WYDAWNICZY

KWARTALNIK BELLONA

Pismo naukowe

wydawane przez Ministerstwo Obrony Narodowej

1918–1950 Bellona

1950–2007 Myśl Wojskowa

KWARTALNIK BELLONA

Pismo naukowe

wydawane przez Ministerstwo Obrony Narodowej

Rocznik CII (XIV)

Nr 3/2020 (702)

Warszawa

Dyrektor Wojskowego Instytutu Wydawniczego: **Maciej Podczaski**
e-mail: sekretariat@zbrojni.pl
tel.: +48 261 849 007, +48 261 849 008, faks: +48 261 849 459
Al. Jerozolimskie 97, 00-909 Warszawa

Zastępca dyrektora: **Izabela Borańska-Chmielewska**
tel.: +48 261 849 212
e-mail: ibc@zbrojni.pl, e-mail: kwartalnikbellona@zbrojni.pl

Redaktor naczelny „Kwartalnika Bellona": **dr hab. Piotr Grochmalski**
e-mail: piotr.grochmalski@zbrojni.pl

Redaktor prowadzący „Kwartalnika Bellona": **dr Piotr Lewandowski**
e-mail: piotr.lewandowski@zbrojni.pl

Opracowanie redakcyjne: **Teresa Wieszczeczyńska**

Opracowanie graficzne: **Małgorzata Mielcarz**

Fotoedytor: **Andrzej Witkowski**

Tłumaczenie na jęz. ang.: **Anita Kwaterowska, Dorota Aszoff, autorzy artykułów**

Redakcja prosi o składanie manuskryptów przez stronę internetową www.kwartalnikbellona.com

Egzemplarze czasopisma są dostępne w wewnętrznym kolportażu wojskowym oraz w prenumeracie.

Czasopismo jest indeksowane w bazie *Index Copernicus.*

Na liście czasopism punktowanych MNiSW „Kwartalnikowi Bellona"przyznano 20 punktów.

Artykuły zamieszczone w „Kwartalniku Bellona" są recenzowane.

ISSN 1897-7065 | E-ISSN: 2719-3853

Oddano do druku w grudniu 2020 r.

Nakład 1200 egz.

Kolportaż i reklamacje: Poczta Polska Usługi Cyfrowe sp. z o.o.
ul. Dunikowska 9a
87-823 Włocławek
tel. : 542 315 201, 502 012 187
e-mail: elzbieta.kurlapska@poczta-polska.pl

Druk: Wojskowe Zakłady Kartograficzne
ul. Fort Wola 22
01-258 Warszawa

Elektroniczna wersja czasopisma na stronie www.kwartalnikbellona.com

Bezpieczeństwo i obronność

Sztuka wojenna

Praktyka i doświadczenia użycia sił zbrojnych

Artykuły poglądowe i recenzje

* * *

Security and Defense

Art of War

Practice and Experience in the Armed Forces Use

Review Papers and Reviews

Od redakcji

Szanowny Czytelniku,
w długiej, 102-letniej historii pisma Polska przeżyła wiele momentów krytycznych. Generał Tadeusz Rozwadowski, faktyczny twórca „Kwartalnika Bellona", widział jego główną rolę w odrodzeniu polskiej myśli strategicznej. Jej deficyt zawsze odbija się bowiem na jakości państwa i skutecznym zapewnieniu mu bezpieczeństwa. Edmund J. Osmańczyk napisał przed laty: „Żaden naród nie zapomina swych walk na śmierć i życie"[1]. To jest twarde jądro historycznego doświadczenia, które winno uczyć kolejne pokolenia Polaków odpowiedzialności za państwo. Narastająca współcześnie złożoność otoczenia Rzeczypospolitej Polskiej oraz agresywność Federacji Rosyjskiej wymagają jasnej oceny ryzyka, realnego szacowania naszych sił oraz wysokiej kultury strategicznej od społeczeństwa. Pod koniec 2020 roku Pakt Północnoatlantycki ujawnił raport wewnętrznej grupy ekspertów „United for a New Era" o wyzwaniach, przed jakimi stanie NATO do 2030 roku. Zwrócono w nim uwagę, że to ChRL będzie stanowić większe kompleksowe zagrożenie dla Sojuszu niż Rosja, obejmie ono bowiem kombinację działań Chin w wymiarze ekonomicznym, technologicznym i aksjologicznym. Państwo to próbuje też stworzyć nowy, globalny system łańcucha dostaw. Taki kształt rysujących się obszarów rywalizacji i związanych z nimi globalnych napięć już dziś wywołuje nowe zagrożenia bezpieczeństwa. Wymusza aktywną analizę naszych interesów i definiowania, w aktywnym środowisku międzynarodowym, polskiej racji stanu oraz wyznaczania naszych długofalowych celów.

„Kwartalnik Bellona" konsekwentnie wspiera wszelkie oznaki odradzania się polskiej myśli strategicznej, uznając, iż nadal pozostaje to jego zasadniczą misją. Z tego powodu przywiązujemy dużą wagę do tekstu gen. broni dr. Sławomira Wojciechowskiego pt. „21 Years of Polish Military NATO Membership – Glass Half Empty". W historii RP po 1989 roku jest to jeden z najważniejszych artykułów w tym obszarze, ukazuje bowiem poziom naszej refleksji nad zasadniczymi problemami: jak RP rozpoznała i rozwiązała współczesne dylematy strategiczne oraz jak ma przetrwać i prosperować w przyszłym świecie. Autor dokonuje rzetelnej oceny naszej aktywności w NATO, jest ona także punktem wyjścia do dalszej dyskusji nad kondycją rodzimej myśli strategicznej. Artykuł stanowi kontynuację wcześniejszych rozważań Autora, zawartych w tekście pt. „State Strategies in Contemporary Poland. Role, Importance, Needs", który został opublikowany na łamach „Kwartalnika Bellona" nr 695 w 2018 roku. W bieżącym numerze Autor przedstawia bodaj pierwszą tak poważną syntezę współczesnej polskiej myśli strategicznej. Wskazuje przy tym nie tylko na korzyści płynące z polskiej obecności w Sojuszu Północnoatlantyckim, lecz także na słabości w rodzimym myśleniu strategicznym oraz w podejmowanych działaniach. Artykuł prezentuje nowoczesne podejście do studiów strategicznych. Ukazuje, jak wielkim przedsięwzięciem naukowym, organizacyjnym i technologicznym jest zbudowanie silnej bazy

1 E.J. Osmańczyk, *Nasza Europa*, Poznań 1971, s. 10.

umożliwiającej wykreowanie potencjału, który będzie pozwalał na samodzielność strategiczną suwerennego państwa. Jest to ważny głos dotyczący budowy koncepcji bezpieczeństwa narodowego. Generał jako praktyk i dowódca Wielonarodowego Korpusu Północ-Wschód w Szczecinie dogłębnie analizuje szanse i wyzwania, jakie stoją przed polskimi siłami zbrojnymi. Jednocześnie konstatuje, że wstąpienie Polski do NATO spowodowało, iż zaniechano działań nad rozwojem rodzimej myśli strategicznej w zakresie bezpieczeństwa państwa.

Dział „Bezpieczeństwo i obronność" zamyka artykuł „Wpływ działalności gigantów technologicznych na globalne środowisku bezpieczeństwa. Studium przypadku spółki Amazon" autorstwa dr. Macieja Gurtowskiego i dr. Jana Waszewskiego. Tekst dotyczy zjawiska, które prof. Jan Kreft określa mianem „władzy algorytmów"[2] w przestrzeni globalnej. To typowe case study, w którym dogłębnej analizie został poddany jeden z podmiotów kształtujących układ międzynarodowy w modelu kapitalizmu nadzoru. Autorzy, wybitni analitycy Centrum Badań nad Bezpieczeństwem Akademii Sztuki Wojennej, ukazują istotny fragment współczesnego środowiska bezpieczeństwa, obserwowany z perspektywy oddziaływań technologicznych i rywalizacji jednego z podmiotów amerykańskiej złotej piątki big tech (Amazon, obok Google'a, Facebooka, Apple i Microsoftu tworzą grupę spółek popularnie zwanych GAFAM) na środowisko międzynarodowe. W tym ujęciu ich zasadniczym, strategicznym przeciwnikiem jest BATX, chińska grupa korporacji z obszaru nowoczesnych technologii, na którą składają się Baidu, Alibaba, Tencent i Xiaomi.

Naturalne dopełnienie tych rozważań stanowi tekst dr. hab. Macieja Siwickiego z Uniwersytetu Mikołaja Kopernika w Toruniu pt. „Przeciwdziałanie zagrożeniom w sieciach i systemach teleinformatycznych. Uwagi o działalności ABW i CSIRT". Autor analizuje, w jakiej mierze model działania bezpieczeństwa cybernetycznego sprawdza się w aktywności służb odpowiedzialnych za bezpieczeństwa państwa. Tu również mamy do czynienia ze studium przypadku dwóch instytucji: Agencji Bezpieczeństwa Wewnętrznego i Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego. W ramach tak zakreślonego obszaru badawczego, na podstawie wnikliwej analizy systemu legislacyjnego, Autor wskazuje, że panujący w Polsce model decentralizacji cyberbezpieczeństwa może okazać się niewystarczający w zderzeniu z coraz nowszymi metodami walki, tym bardziej że już teraz boryka się on z wieloma problemami na szczeblu organizacyjnym.

Wymiar zagrożeń cybernetycznych dobrze unaocznia artykuł płk. dr hab. inż. Piotra Deli pt. „Elementy systemu walki w cyberprzestrzeni". Tekst ten powstał na podstawie badań własnych autora oraz jako pokłosie publikacji jego monografii „Teoria walki w cyberprzestrzeni", wydanej nakładem Wydawnictwa Akademii Sztuki Wojennej na początku bieżącego roku. Autor syntetycznie ujmuje wiele zagrożeń cybernetycznych oraz odnosi się do teorii systemu walki w cyberprzestrzeni. Rozwija definicje, określa kontekst funkcjonowania zjawisk i zagrożeń w obszarze zdanetyzowanym, a także diagnozuje polską strategię cyberbezpieczeństwa.

Numer zamyka recenzja wspomnianej monografii profesora Piotra Deli. Krytycznej analizie poddaje ją prof. dr hab. Zbigniew Ścibiorek. Podkreśla istotność badań nad cyber-

2 J. Kreft, *Władza algorytmów. U źródeł potęgi Google i Facebooka*, Kraków 2019.

bezpieczeństwem i wysoko ocenia naukowy wymiar pracy. Zaznacza, że jest to pierwsza w Polsce tego typu publikacja, wskazuje, że powinni po nią sięgnąć zarówno decydenci, pracownicy służb wywiadu, jak i studenci oraz adepci bezpieczeństwa informacyjnego.

Szanowny Czytelniku, z szacunkiem i pokorą oddajemy w Twoje ręce 702 numer „Kwartalnika Bellona". Czynimy to w okresie, w którym druga fala pandemii koronawirusa nadal stanowi wyzwanie i zagrożenie dla świata, życzymy więc dużo zdrowia.

dr hab. Piotr Grochmalski, prof. ASzWoj,
redaktor naczelny „Kwartalnika Bellona"

dr Piotr Lewandowski,
redaktor prowadzący „Kwartalnika Bellona"

Editorial

Dear Reader,

in the long, 102-year-old history of the journal, Poland has gone through many critical moments. According to General Tadeusz Rozwadowski, the actual creator of the Bellona Quarterly, its main mission was to revive the Polish strategic thought, since its deficiency always reverberates in the state's quality and effectiveness in ensuring its own security. Years ago, Edmund J. Osmańczyk wrote: "No nation forgets its life-and-death struggles."1 It is the hard core of historic experience that should teach successive generations of Poles to feel responsible for their country. The currently growing complexity of Poland's surroundings and the aggressive attitude of the Russian Federation require a clear evaluation of risk, a realistic assessment of our strength and high strategic culture in the society. At the end of 2020, the North Atlantic Alliance revealed a report by an internal group of experts, entitled "United for a New Era," on the challenges that NATO will have to face up to the year 2030. The report states that China will pose a bigger comprehensive risk to NATO than Russia, as it will involve a combination of activities in the sphere of economy, technology and axiology. China is also trying to create a new, global supply chain system. The shape of these evolving areas of rivalry and global tensions connected with them are already creating new security risks. The situation requires us to actively analyze our interests, define the Polish raison d'état in the active international environment, and determine our long-term goals. The Bellona Quarterly consistently supports all signs of the rebirth of the Polish strategic thought, still considering it to be the journal's main role. Therefore, we attach great importance to the article written by Lt Gen. Sławomir Wojciechowski, PhD, entitled "21 Years of Polish Military NATO Membership – Glass Half Empty." It is one of the most important articles in the field in the post-1989 history of the Republic of Poland, as it presents the level of our consideration concerning essential problems: how Poland recognized and solved existing strategic dilemmas and how it is to survive and prosper in the future world. The author gives a reliable assessment of our activity in NATO, which is also the starting point for a further discussion on the condition of the Polish strategic thought. The article is a continuation of the earlier contemplations of the author in his article entitled "State Strategies in Contemporary Poland. Role, Importance, Needs," published in Bellona No. 695 in 2018. In the current issue, the author presents what is likely to be the first such substantial synthesis of Poland's contemporary strategic thought. He points to not only the advantages of Poland's membership in the North Atlantic Alliance, but also to the weaknesses in the Polish strategic thinking and undertaken actions. The article presents a modern approach to strategic studies. It shows how big of an undertaking – scientific, organizational and technological – is for Poland to create a strong enough ba-

1 E.J. Osmańczyk, *Nasza Europa*, Poznań 1971, p. 10.

sis for building potential that will ensure to it strategic independence of a sovereign state. It is an important voice concerning the development of a national security concept. The General, as a very experienced person and the Commander of the Multinational Corps Northeast in Szczecin, thoroughly analyzes the chances and the challenges awaiting the Polish Armed Forces. He also states that when Poland joined NATO, the work on developing our own strategic thought in the area of national security was abandoned.

We close the "Security and Defense" section with the article "Big Tech's Influence on Global Security Environment. The Case of Amazon.com" by Maciej Gurtowski, PhD, and Jan Waszewski, PhD. The text discusses a phenomenon which Prof Jan Kreft has described as the global "power of algorithms."2 It is a typical case study which thoroughly analyzes one of the entities shaping the international configuration in the surveillance capitalism model. The authors, outstanding analysts of the Center for Security Studies at the War Studies University, present an important fragment of the contemporary security environment, as seen from the perspective of rivalry and technological influences of one of the "Big Five" companies (Amazon, next to Google, Facebook, Apple and Microsoft, is a part of a group of companies referred to as the Big Five or GAFAM) on the international environment. In this context, their main, strategic adversary is BATX, a group of four biggest Chinese tech companies (Baidu, Alibaba, Tencent, Xiaomi).

A natural supplement to these reflections is a text by Prof Maciej Siwicki of the Nicolaus Copernicus University in Toruń, entitled "Counteracting threats in ICT networks and systems. A few remarks on the activities of the Internal Security Agency and the CSIRT." The author analyzes the extent in which the cyber security model of operation proves to be effective in the activity of services responsible for national security. It is also a case study concerning two institutions: Internal Security Agency and the Governmental Computer Security Incident Response Teams. Within this area of study, on the basis of a thorough analysis of the legislative system, the author indicates that the model of decentralizing cyber security that exists in Poland can prove insufficient when faced with more and more advanced methods of warfare, even more so that it is already struggling with numerous organizational problems.

The extent of cyber threats is clearly presented in the article by Col Piotr Dela, PhD, Eng, entitled "Elements of Cyberspace Warfare System." The text was written on the basis of the author's own studies and as a consequence of publishing his monograph Cyberspace Warfare Theory by Wydawnictwo Akademii Sztuki Wojennej (War Studies University Publishing House) at the beginning of this year. The author presents a synthesis of many cyber threats and refers to cyber warfare theory. He develops definitions, determines the context in which various phenomena and risks function in dataficated space, and diagnoses Poland's cyber security strategy.

We close the issue with a review of the mentioned monograph by Professor Piotr Dela. The critical analysis of the work has been written by Prof Zbigniew Ścibiorek, PhD. He emphasizes the importance of the studies on cyber security and gives high praise to the scientific aspect of the work. He underlines that it is the first publication of this kind in

2 J. Kreft, *Władza algorytmów. U źródeł potęgi Google i Facebooka*, Kraków 2019.

Poland, and encourages policy-makers, intelligence services agents, as well as information security students and trainees to read it.

Dear Reader, we respectfully and humbly present to you the Bellona Quarterly No. 702. We are doing it at a time when the second wave of the coronavirus pandemic still poses a big challenge and threat to the world, so we also want to wish you a lot of health.

Piotr Grochmalski, PhD,
associate professor at the War Studies University,
Editor-in-Chief of the Bellona Quarterly

Piotr Lewandowski, PhD,
Managing Editor of the Bellona Quarterly

THE BELLONA QUARTERLY ISSN: 1897-7065 | E-ISSN: 2719-3853

KWARTALNIK BELLONA

21 Years of Polish Military NATO Membership – Glass Half Empty

Lt Gen. Sławomir Wojciechowski, PhD

ORCID: 0000-0002-3017-3100
e-mail: s.wojciechowski@akademia.mil.pl
War Studies University (ASzWoj), Warsaw, Poland; Multinational Corps Northeast, Szczecin, Poland

ABSTRACT:

After the accession to NATO, Polish military should have adapted to new realities but the process coincided with the changes in security environment and with NATO strategic reorientation. In order to meet expectations and contribute to Allied requirements, the Polish Armed Forces faced the dilemma of keeping balance between transformation, the forces numerical decrease and modernization of the inventory. Due to the choice of direction with the focus on capability problems, the change has not brought expected effect until now. Applying existing terminology and notions, the article examines discrepancy between perceptions of the NATO accession and the state of the military effectiveness in the face of deepening the Polish-American military strategic partnership.

KEYWORDS:

NATO membership, fighting power concept, effectiveness, transformation, modernization, professionalization, expeditionary operations

Introduction

The beginning of the third decade of Polish membership in NATO, coupled with the plethora of articles summarizing previous 20 years of thereof, constitutes perfect opportunity to revisit the issue from different vantage point. NATO membership of the Republic of Poland (RP) is very often seen as political act summarizing years of diplomatic efforts that produced favorable strategic impact on the state's security in international system. From the military perspective, it is hardly possible to find opinion or the publication that argues against the motivating role of the Alliance for the change in the Polish Armed Forces (PAF) and particularly its major service – the Polish Land Forces (PLF). The process, habitually regarded as "the transformation of the armed forces,"[1] had focused on certain areas of the military organization and, by its very nature, has not been finished yet. Twenty one years is the age of maturity therefore, if the NATO accession had an authentically significant influence on the direction of the change in the Polish military, it seems justified to reiterate some questions and ask: How well Poland has performed in this respect? Were all of the important areas covered? Was the direction chosen rationally? Was the balance among the services maintained? Was the flexible approach applied in the case of changing demands?

Sources Review

The topic by its very nature is often classified. The basis for analysis and the research sources in Polish language is comprised of information available in: official strategic governmental documents and legal acts; PAF ratified and published doctrinal publications; opinions of independent experts, governmental officials and members of academia issued in books as well as in defense and security journals, periodicals and internet portals. Nowa Technika Wojskowa, Kwartalnik "Bezpieczeństwo Narodowe and Kwartalnik Bellona were the most frequent press platforms for discussion. To meet the aim of the article, the English language research sources included NATO Allied doctrinal publications; books that cover the notion of military effectiveness and fighting power, publications referring to NATO transformation in the security magazines; internet records of defense and security conferences, briefings and interviews with NATO military officials; NATO web page.

Method

For the purpose of the article, to discuss the problem of the degree of the influence of the NATO on the changes of the PAF, a following hypothesis was formulated: the Polish army, after 20 years of transformation as a result of NATO membership, is prepared for Allied operations with significant limitations. The author applied elements of the "fighting power" idea as the overarching structure for the discussion. Within the selected framework, the issue consideration was based on the comparison, the analysis and synthesis of available

1 Malec, M., "Dylematy transformacji Sił Zbrojnych RP," *Kwartalnik Bellona* 2010 No. 3, pp. 169–170.

statistics, official publications, recorded opinions, literature and recorded interviews with selected members of the Polish Armed Forces. That include officers representing NATO Command Structure, PAF strategic, operational and tactical commands and institutions, senior Non-Commissioned Officers (NCOs).

NATO Membership – Polish Military's Own Perspective[2]

The membership in NATO became the strategic objective for Polish political and military elites far before the actual accession in 1999, so that this process can be assessed as almost 30 years long. For the first time this intent was formalized in Security Policy and Defense Strategy of the Republic of Poland issued in 1992. In this publication, the ambition to join the Alliance symbolized new strategic orientations of the state and illustrated determination to seek security guarantees. The military establishment saw this strategic movement as the incentive and opportunity for inevitable change that could allow Poland to be in possession of higher quality modern armed forces equipped with the wide spectrum of modern capabilities.[3] In the following years, immediately after actual NATO accession, the security and defense strategic papers were amplifying the role of NATO and the demand that the change is consistent with its expectations. However, as a result of the Cold War order termination, the Alliance was in desperate search of its own identity and purpose. On the heels of the Balkan conflict of the 1990s, and redefinition of the threat for global order, NATO reorientation moved toward "out of area operations" and consequent expeditionary capabilities of the military force.[4] Despite the fact that requirement was in dire contradiction of the then expected role of PAF in the defense system of the country, NATO obligations took precedence. As a result, from the very outset of the process the Polish General Staff assumed that the integration with new organization will probably be conditional and it will require the increase of the personnel professionalization; the extending interoperability[5] with the Allied partners; establishment of the expeditionary capabilities and NATO standardization, and reorientation of defense planning.[6] In years to come, the narrative did not change by maintaining that the process of modernization of the military is determined not only by the changes in the security environment but also their involvement in the Allied

2 "Poland on NATO – more than 20 years," Ministry of National Defense, https://www.gov.pl/web/national-defence/poland-in-nato-20-years [access date: 28.07.2020]; Biuro Bezpieczeństwa Narodowego, https://www.bbn.gov.pl/pl/wydarzenia/15-lat-polski-w-nato/polska-w-sojuszu-polnoc/5295,Korzysci-i-inicjatywy.html [access date: 13.08.2020].

3 Lalka, J., "NATO – determinantem przemian w Siłach Zbrojnych RP," in: *10 lat Polski w NATO, materiały pokonferencyjne*, Skrabacz, A. (ed.), Centralna Biblioteka Wojskowa, Warszawa 2009, p. 89.

4 See: Sperling, J., Webber, M., "NATO: from Kosovo to Kabul," *International Affairs* 85:3, The Royal Institute of International Affairs 2009, p. 494; A. King, *The Transformation of Europe's Armed Forces. From the Rhine to Afghanistan,* Cambridge University Press, Cambridge 2014, p. 23; J. Simon, *NATO Expeditionary Operations: Impact Upon New Member and Partner*s, Institute for National Strategic Studies, National University Press, Washington D.C. 2005, pp. 12.

5 Then understood as minimal necessary capability to cooperate according to NATO requirements see Lalka, J., op. cit., p. 90.

6 Ibidem, p. 89.

operations, NATO Response Forces (NRF) packages,[7] UE membership[8] and the process of professionalization. Finally, this approach was codified in national security and defense strategies of 2000, 2003, 2007, and 2014. From today's perspective and the comfort of the observation of facts, critical examination of the respective areas may give us the answer to the question on how well NATO membership transformed the PAF.

Professionalization

The "professionalization" is often perceived as one of the greatest achievements and benefits motivated by the accession to NATO.[9] Starting from early 1990s, there was political will and economic realism to decide to decrease the size of the armed forces. In concert with the shift to follow NATO strategic orientation, compulsory military service soldiers were not adequate to expeditionary tasks. Degradation of the national draft system, amplified by the will to copy the overall tendencies of the Western armies,[10] motivated defense authorities to abandon conscription and invest in professional soldiers as the only solution.[11] Gradually implemented, introduction to all-professional armed forces was established in 2009, and aimed at changing the promotion of an officer to Non-Commissioned Officers (NCOs) and private soldiers.[12] In spite the fact that it was understood as the change in the military personnel structure, and mostly departure from conscription, this process should not be assessed only from this perspective.

As a significant factor of change and transformation,[13] the process was expected to provide adequately prepared personnel appropriate for the new model of the armed forces where professionally focused soldiers, airmen or sailors are to be the key element of military power. It was supposed to produce generational change that should surpass past legacies and by year 2020 these inheritances should have been non-existent. In some instances professionalization was viewed as integrated with the evolution in military education and training system which, by the purpose, should prepare expert officers, NCOs and privates of active and reserve duties to tasks with maximum efficiency. What is more, the system should have been able to respond to the changing demands of the operational environment and be able to meet the challenges of technological competition.[14] Was it more

7 Gocuł, M., "Współczesne uwarunkowania funkcjonowania i rozwoju Sił Zbrojnych RP," *Kwartalnik Bellona* 2014 No. 1, pp. 23–24.

8 The significant element of the discourse on the security and defence that dominated political and military elites is the tendency to position NATO inseparably with European Union.

9 Ojrzanowski, M., "Transformacja polskich sił zbrojnych – miara sił na zamiary," *Rocznik Bezpieczeństwa Międzynarodowego* 2013 No. 7, pp. 78–103; Gocuł, M., op. cit., p. 12; Cieniuch, M., "Piętnaście lat w NATO," *Bezpieczeństwo Narodowe* 2014 – I, p. 110; Pawłowski, M., "Cele i wyzwania profesjonalizacji Sił Zbrojnych RP," http://www.politykaglobalna.pl/2009/12/cele-i-wyzwania-profesjonalizacji-sil-zbrojnych-rp-4 [access date: 02.09.2020].

10 Chojnacki, W., *Profesjonalizacja wojska w teorii i badaniach socjologicznych*, Akademia Obrony Narodowej, Warszawa 2008, pp. 163–164.

11 See: Chojnacki, W., op. cit., pp. 165–167.

12 Korolczuk, A., "Transformacja Sił Zbrojnych RP 1999–2014. Aspekt finansowy," *Studia i Prace. Kwartalnik Kolegium Ekonomiczno-Społecznego* 2016, No. 3, pp. 195–196.

13 Ojrzanowski, M., op. cit., p. 44.

14 Cieniuch, M., op. cit., pp. 109–111.

than the change of the structure? In the opinion of the Operational Commander,[15] after more than twenty years we may experience complete differences that could be seen in the area of independence of commanders, command style and mentality. May this opinion be fully justified when compared with external observations and internal judgements?

According to the opinion of Thomas-Durell Young, based on his twenty-year research, even when "legacy armed forces" accept selected number of Allied-influenced reforms, junior and non-commissioned officers complain that NATO procedures are only respected during out of area operations but previous concepts still prevail at home environment. Younger generation of officers and NCOs, mainly those ones with deployment into operations experience, suffer cognitive dissonance.[16] Based on the excuse that these practices are the result of constitutional "national character" and as such should be exempted from allied responsibilities, they produce not only double military standards but also promote senior leaders who have little qualifications to command Allied formations at home.[17] Not to mention it creates discrepancies in the experience based on common assignments, understanding of military terminology[18] or application of similar command culture. It is worth noting that until today, there has been no codified set of principles or official reference documents that could define the PAF command principles. The notion of a "mission command" that appears in a few ratified NATO publications cannot fulfil the gap of conceptual identification of its own national style that would overlap with the overall Western military culture usually represented either by American, British, Canadian or German one.

The most vivid example of unfinished process of professionalization can be observed in the identification of the role of Senior NCOs[19] in the military Polish organization. Despite more than decade-old efforts, the structural change of proportion of number of officers to NCOs did not result in codified transition of NCO corps members to leadership positions. They mainly occupy functions of technical specialists. There is no clear career development system for them and the unpreparedness to recognize the need by officer's corps can be identified. The interviews with the several representatives of the corps revealed that as this is mostly a generational issue, it is a problem of education and experience, as well. The resistance to the change so far shows no signals that NCOs will finally gain their deserved role. Therefore, even slight examination of available facts, collected opinions and observations should not give everybody the reason to declare success unless we speak of termination of conscript services exclusively.

15 Lesiecki, R., *Dowódca Operacyjny: 20 lat Polski w NATO to przede wszystkim zmiana mentalności*, Defence24, 29.03.2019, https://www.defence24.pl/dowodca-operacyjny-20-lat-polski-w-nato-to-przede-wszystkim-zmiana-mentalnosci [access date: 28.10.2020].

16 Young, T.D., "What are Governments in Central and Eastern Europe not Buying with their Defense Budgets? The Readiness Clue*," The RUSI Journal*, Routledge, 164:2, May 2019, pp. 46, 55.

17 Young, T.D., "Legacy Concepts: A Sociology of Command in Central and Eastern Europe," *The US Army War College Quarterly: Parameters* 47(1), Carlisle, PA, USA, Spring 2017, p. 40.

18 Young, T.D., *Anatomy of Post-Communist European Defense Institutions. The Mirage of Military Modernity,* Bloomsbury, New York 2017, pp. 58–60.

19 Most often Senior NCOs are identified as: Command Sergeant Major (US) or Command Senior Enlisted Leader (NATO).

Expeditionary Operations

The NATO out-of-area operations had the ambiguous influence on the current PAF status. Resulting from the demands of the alliance adaptation to new realities[20] and the ambition of presenting itself as loyal and reliable ally,[21] the PAF significantly engaged its resources into expeditionary operations that, from the perspective of today, may be assessed as the pursuit for the "NATO standardization." This involvement is seen as positively influential to the quality of training and effectiveness of exercises. It was also to be the driving force of progress in achieving interoperability goals to serve as the testbed and source of needed lessons to correct standards of the equipment, doctrines and capacity of logistics, and helped gaining expertise to command multinational contingents.[22] Out-of-area missions, apart from having impact on the new directions of the forces development, were to shape the dynamic of the modernization to include enhanced procurement procedures, as well. Even if not all of them were NATO-led, those operations were to confirm the compatibility of Polish communications and information systems (CIS) with other NATO members on a tactical level. In capability terms, this involvement is measured as good opportunity for systemic refinement of tactics, techniques and procedures of command in real warfighting conditions.[23] Paired with the professionalization process, missions abroad were even seen as an important career stage by way of service in multinational formations,[24] and declared as the opportunity for verification of military qualifications of the higher military leadership.[25] In the sphere of military command culture,[26] this experience is seen as a source of significant mind-set changes[27] that is more adequate to demands of military combat realities.

Until today, contribution to NATO operations is viewed as platform to identify the capabilities necessary for Allied operations to include collective defense. Arguably, it includes such abilities as command and control of combined forces in a complex operating and informational environment (network enabled capability), intelligence, logistics and medical support.[28] However, proficiency in one or several areas of military mis-

20 *The 1999 NATO Strategic Concept*, https://www.nato.int/cps/en/natohq/topics_56626.htm [access date: 21.09.2020]; *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon*, https://www.nato.int/cps/en/natohq/official_texts_68580.htm [access date: 23.09.2020].

21 J.R. Hillison, *Stepping Up: Burden Sharing by NATO's Newest Members*, Strategic Studies Institute, United States Army War College, Carlisle, PA, USA, 2014, p. 179–216.

22 See for more *Międzynarodowe operacje pokojowe i stabilizacyjne w polskiej polityce bezpieczeństwa w XX i XXI wieku*, D. Kozerawski (red.), Warszawa 2016; R. Kupiecki, *NATO w polskiej perspektywie 1989–2019*, PISM, MSZ RP, Warszawa 2019.

23 Gocuł, M., op. cit., p. 16.

24 See: "Poland on NATO – more than 20 years...," op. cit.

25 According to internet open sources at 30.09.2020, 25% of the Army generals who served in Poland were not deployed to any military operations abroad. There is additional 10% of those without Iraq and Afghanistan experience. Very few among all of the number of nearly 50 occupied a commander position at any level.

26 As of nowadays, there is non-existent codified officially set of principles that could characterize command culture tenets in PAF. As a proxy notion serves ''mission command'' that appears in ratified NATO publications.

27 Lesiecki, R., op. cit.

28 See: "Poland on NATO – more than 20 years...," op. cit.

sions does not imply expertise in executing all of them. Good expeditionary units may not be efficient to defend its own territory. Effective home defense forces can be poor peacekeepers whereas forces that are focused mainly to defend national territory cannot necessary conquer their neighbors.[29] Following this argument, participation of the PAF in the expeditionary operations, no matter of which auspices they were executed,[30] and despite being the key element of national foreign policy, should not be seen as one of the sole precondition to maintain and develop the effective Armed Forces. Since 1996, PAF has taken part in 14 missions but only half of them were NATO-led, and took place in African, Middle East or Central Asian environment. By the very character they are focused on deployment abroad, and still constitute exception to Constitutional expectations. They could not serve the purpose because they were low-intensity, counter-insurgency, stability, peace or nation-building endeavors, focused on controlling foreign territories, against – in terms of international military conflict law – combatants or non-military local actors. To very extent they did not provide "warfighting experience" in "real combat enrollment" for combined arms effectiveness.[31] By that fact those missions could not serve the purpose. What is more, only recently, due to the change in NATO strategic concepts, Polish military operates in European theatre, and it is still too early to judge the value of Air Policing, NATO Standing Maritime groups, enhanced Forward Presence, and tailored Forward Presence to the PAF as a whole. Especially because they embrace lower tactical level units, and in some exceptions do not comprise the leading or framework nation role in them.

The participation of the PAF in NATO, EU, UN or coalition out-of-area operations did not and could not prepare its personnel, equipment, weapon platforms and structures to European theatre, high-intensity and peer-to-peer adversary warfighting. They did not practice on greater scale than sub-unit level tactics, joint fires, river crossing operations, brigade maneuvers or close air support and combat service support, etc. It cannot be even denied by unquestionable sacrifice of individual soldier and the low level of leadership proficiency shown during those deployments.

Technical Modernization

The last but definitely not least element to scrutinize NATO membership influence on the PAF is "technical modernization" of the armed forces. This ought to be the process of replacing old generation of weapons and platforms for new, more effective models within the ramification of strategic aims and the economic condition of the state.[32] Technological

29 Biddle, S., *Military Power. Explaining Victory and Defeat in Modern Battle*, Princeton University Press, Princeton and Oxford 2004, p. 5.

30 Polish contingents operating within the framework of NATO (SFOR, KFOR, ISAF, Active Endeavour, Baltic Air Policing, Iraq), European Union (EUFOR „Althea", EUFOR RD Congo, MINURCAT, Mali), United Nations (UNDOF, UNIFIL, Sudan, Chad) and Coalition operations (OEF Afghanistan, OIF Iraq).

31 There is little evidence that may prove the argument that Polish military did introduce significant lessons from abroad missions to everyday practice.

32 Bączyk, N., „Modernizacja techniczna sił zbrojnych RP – przyszłość a dekada 2001–2010. Cz. I. Uwarunkowania strategiczne," *Nowa Technika Wojskowa* 2011 No. 3, p. 22.

advantage remains one of the very foundations of successful defense strategies, and ability to dominate and exploit warfare space by way of integration all available combat assets is the attribute of modern armed forces.[33] Despite the ambition from the outset – a transformation towards the NATO-focused and compatible armed forces – and when assessing the technological modernization of the PAF, the results appear to be negative. The process is the most quantifiable, and by that its effects are seen as both unanimously and unsatisfactory in Poland. That may be proved by the comparative analysis, which is based on data collected and published regularly in The Military Balance[34] and focused on weapon platforms and key equipment procured along the last twenty years in Poland.

The Polish Land Forces, to start with the largest branch, cut the number of its Main Battle Tanks nearly in 50% but significant majority of those left in the fleet have Soviet conceptual origins, and only more than 250 are modern platforms. In the reconnaissance and infantry inventory, the Warsaw Pact BRDM-2 makes early 90% of all the number of recce vehicles whereas armored fighting platforms BMP-1of the same generation make three quarters of all infantry mobility assets available for the infantry. More than 350 modern Rosomaks alone make military effectiveness limited among over 1,000 of elderly combat platforms. In the field of artillery ordnance, all towed assets were discarded, however, nearly 50% decrease in overall numbers of guns since 2000 still have not influenced the presence 122-mm guns 2S1 in artillery ranks. They still make more than 50% of the number of the general fire support artillery. The parallel situation occurs in tube artillery assets. The worst situation, from the perspective of the modernization, is in the Ground-Based Air Deference (GBAD). This branch experienced no changes in its short- and medium-range assets procurement. Upgraded versions of SA-8 and SA-6 still dominate, and the army heavy investment was directed into very short air defense (VSHORAD) missile systems. In the field of rotary wings, despite not very significant changes in number military helicopters, only 25% of air frames are of non-Soviet background. The fleet of attack helicopters remains unchanged for the last two decades, and consists of Mi-24 HIND.

In the case of other services, the Air Force combat air platforms shrunk in half but the service was able to acquire 48 F-16s that consist 50% of air-to-air and air-to-ground capabilities. Unfortunately, surface-to-air missile equipment belongs entirely to legacy armed forces, and shares the fate of the army air defense. The SA-3 modernized version remains still in service. The Polish Navy, as the smallest of the three branches, especially with reference to surface combat vessels, is four times smaller than at the NATO accession. With two frigates, no destroyers, one corvette-class ship and three fast patrol boats armed with rocket system, procurement achievements are minimal. Fortunately, mine warfare vessels potential is maintained and improved with additional modern platforms. In spite of the fact of the purchase of coastal defense missiles AShM 12 NSM, the Navy as a branch did not succeed in the effort of technical modernization.

33 Cieniuch, M., op. cit., p. 111.

34 *The Military Balance 2001–2002*, Oxford University Press, London 2001, pp. 68–69; *The Military Balance 2020*, Routledge, London 2020, pp. 134–135.

From today's perspective, the Polish Armed Forces did not transform from quantity to quality as military tool of national policy. After the cuts to 50% of the equipment numbers, only about the half of the remained ones have been modernized since 1990s. NATO membership was the decisive factor in the change of defense planning practices, and consequently had significant influence on the direction alteration of the whole process of technical modernization in the years 1999-2018. Paradoxically, the process was influenced by two parallel factors, namely: the expeditionary requirements of conflicts in Iraq and Afghanistan, and the transition from big conscript army into the smaller one, consisting of professional soldiers. Those endeavors consumed significant portion of the defense budget dedicated for procurement of modern equipment. Additionally, in order to respond to frequent changes to the state fiscal policy, there were eight PAF modernization and development plans published[35] within twenty years, but none of those plans was fully completed. In some areas they were not completed at all. Unstable financial foundations and demands of current operations could not help in balanced and steady rebuilding forces. However, the failure of all the programs can only partially be attributed to economic or even defense industry capacities. The political and strategic factors should be taken into account. As early as ten years after the accession, it has been suggested that initial assumptions were overoptimistic and decision-makers' choices were too focused on everyday practice rather than on national assumptions which were focused on the middle-European theatre[36] of possible conflict put in the context of geopolitical changes.

The Alliance, in a very different way than the Warsaw Pact, did not impose on its members the obligation of mass armament, and it was – and still is – that the Alliance member states that had real independence in what should be procured. The fluctuation of concepts,[37] contradictory expectations of the Ministry of National Defense (MoND) departments versus the General Staff, and the will to integrate effectively with NATO resulted in changes in initial standing defense development plans. In reality, the most driving factors of the direction of the modernization were needs to meet transforming NATO goals with second priority to national local character.[38] However, even nowadays, one may have difficulty in gaining more confidence in the change of the effectiveness of the forces rebuilding. There are still opinions that Polish modernization plans remain rather ambiguous especially with the country's ambitions to play more significant role in Europe. This may be proved by the Polish Chief of Defense (CHOD) who admitted that the military is making investments and changes where it can, but, more importantly, is to be flexible and ready to change direction, speed and priorities; the adaptation as such is more important than the end state.[39]

35 See: Dmitruk, T., "Dwie dekady w NATO – modernizacja techniczna Sił Zbrojnych," *Nowa Technika Wojskowa* 2018, No. 2, pp. 16–20.

36 Bączyk, N., op. cit., p. 23.

37 Ojrzanowski, M., op. cit., pp. 87–89.

38 Bączyk, N., op. cit., p. 23.

39 McLeary, P., *Defense Chief: With Giant Exercise Looming, Poland Looks To Lead Central Europe*, https://breakingdefense.com/2019/12/defense-chief-with-giant-exercise-looming-poland-looks-to-lead-central-europe/ [access date: 28.10.2020]. See also: Cieniuch, M., op. cit., p. 108.

This statement does not signal the military strategic approach to change compared to previous leadership.

Despite the fact that the effects of the accession are periodically discussed, particularly on the occasion of anniversaries, and are perpetually seen as indisputably positive[40], no holistic assessment of the checks and balances is visible. Arguably, in the light of discussed areas, the membership alone gave Polish military opportunity to be prepared "to react to a full spectrum of threats and maintain capabilities for effective operations"[41] or that the fulfillment of Allied obligations "guarantees constant, rational and high standard of the technological development of PAF."[42] Even from today's perspective it is difficult to measure that in the military appeared "revolutionary changes in the mentality and habits of the personnel."[43] Without the shadow of a doubt, the accession had stimulating and inspirational role in the transformation of the PAF[44] but at the same time, despite nearly unanimous opinions of military experts that NATO membership influenced contemporary shape of the PAF and still is a motivating factor for its internal transformation, there is little reflection on its outcome or even the envisioned end state.

The witnessed effects of NATO participation are often attributed to inaccurate political and military-strategic decisions that did not take into account real capabilities of the state. The contradiction between perceived all area success,[45] and only one field of a significant disappointment, may suggest that from the beginning of the accession the assumptions might have had weak foundations and not necessarily were correctly identified. The lack of balanced approach may result from deficiency of overall vision of the armed forces as designed to win wars or conflicts in the context of the contemporary threats and possible future challenges.[46] There is imperative that armed forces and the effectiveness are seen as one integral whole, but the problem will remain until the PAF are seen as the "armed forces in being"[47] focused on peace time existence instead of serving the purpose – be effective in warfighting. Although the most critique usually goes to technical modernization, it is difficult to deny the impression that most of the efforts was put just on "westernizing" the military.

Fighting Power

The quest for military effectiveness should be governing attitude of people in arms since there is no second place in the struggle when opposing sides decide to revert to combat to

40 See: Klich, B., *NATO – wyzwania i zadania*, in: A. Skrabacz (ed.), op. cit., p. 11.

41 Cieniuch, M., op. cit., p. 108.

42 Ibidem, p. 114.

43 Ibidem, p. 108.

44 Zieliński, T., "Transformation of the Polish Armed Forces: A Perspective on the 20th Anniversary of Poland's Membership in the North-Atlantic Alliance," *Kwartalnik Bellona* 2020 No. 1, p. 33.

45 See: "Poland on NATO – more than 20 years...", op. cit.

46 Bączyk, N., op. cit., p. 28.

47 This notion relates to original comments of Admiral Lord Torrington about "fleet in being" introduced the year 1690 and it refers to deterrent effect of High Seas Fleet in the face of stronger enemy. See A. Gordon, *The Tule of the Game*, Penguin Books, Great Britain 2014, p. 21.

solve the conflict. With finite resources armed forces conceptualize, invest, experiment, and exercise to be prepared to win if fight comes. The introduction of the concept of "fighting power" may be one of tools to achieve the goal of maximizing the effect and to optimize the efforts to be militarily competitive. Accordingly, before theoretical and practical considerations it is advisable to analyze the origins of the "fighting power" concept first.

The first traces of the term "fighting power" might be found in publications of the British military theorist J.F.C. Fuller, dated on 1920s. He applied it when reflecting on the instruments of war and the description of a physical sphere. However, in that context, he recognized nine basic elements of the armed forces, grouped under three main areas that comprise mental, moral and physical aspects of military activities.[48] In his opinion, the most crucial factor were inter-relations and interdependencies between the selected elements of the military organization. Different perspective on the term was proposed by Martin van Creveld who identified fighting power as key feature of the forces building process that consists of organization, training and leadership.[49] For him it "is the multiplying factor that equals the quality and quantity of equipment of the given armed forces that are assessed, within the limits of their size, as a worthwhile military instrument"[50]. It is built on organizational, mental, and intellectual grounds and is demonstrated as combination of discipline, cohesion, morale, initiative, courage and the willingness of the military to fight.[51] Indeed, he focused his attention mainly on the domain of will and motivation. In this regard, Jim Storr – when discussing the issue of warfare as armed violence between states – invokes British military doctrine that utilizes the notion of fighting power.[52] Divided into three components, again physical, conceptual and moral, Storr explains that the first reflects the means (the equipment, the soldiers, and the logistics to sustain them), the second involves methods (ways and intellectual processes to solve the problem how to utilize means) and the third element is about the military culture (motivation, leadership, morale, and ethos). He focuses his attention on the domain of thought as the dominant among the three,[53] but, more importantly, in his view fighting power should be assessed as relative to the identified adversary.

More formal version of the fighting power idea is utilized in the education process of Danish Defense Academy. Designed by K.V. Nielsen, taught and known as "the Circuit of Warfare," it attempts to describe the association between military doctrine, technology and organization and the social surroundings depicted by its ideology, political structure

48 Fuller, J.F.C., *The Foundations of the Science of War*, A Military Classic Reprint, US Army General and Staff College Press, Fort Leavenworth, Kansas, USA, 1993. pp. 91, 173 and 325.

49 Creveld van, M., *More on War*, Oxford University Press, Oxford 2017, pp. 62–75.

50 Idem, *Fighting Power. German and US Army Performance, 1939-1945,* Greenwood Press, Westport, US, 1982, pp. 3 and 174.

51 Ibidem, p. 174.

52 *Design of Military Operations. The British Military Doctrine*, 1996, Army Code 71451, pp. 4–6.

53 Storr, J., *The Human Face of War*, Continuum, London 2009, pp. 8 and 16.

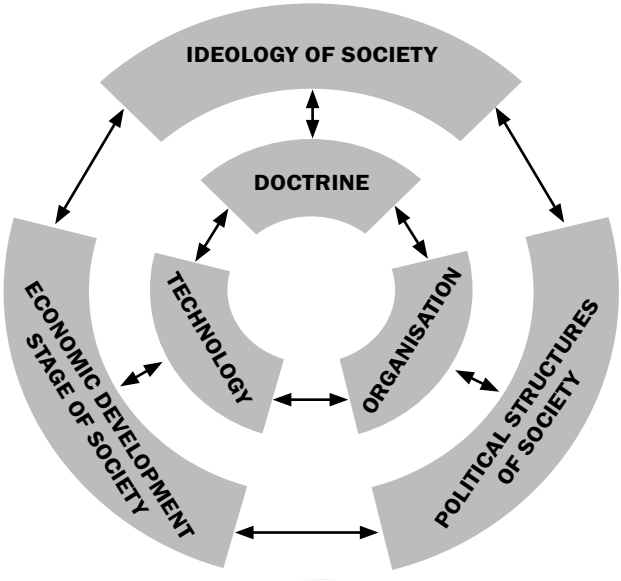


Figure 1. The Circuit of Warfare
Source: Danish Army Military Academy, 1994

and the economic status[54] (see Figure 1). The universal nature and purpose of the Circuit is based on the assumption that in any society, regardless of the moment of time, one can predict or explain the nature of its elements,[55] and even decide on the course of their development. The author of a proposed model strongly suggests applying it as a tool to be applied with reference to specified opponent.

Certainly, among national military organizations, the most formalized approach to the notion we may find in British Army doctrinal publications, where the emphasis is put on military effectiveness and the judgment norm applicable to all levels of the organizational structure. The concept of Fighting Power is the tool by which effectiveness is explained in relation to other armies. Only throughout the components of the concept, the intellectual and practical justification of the Army structures take place including its "ability to fight and to succeed."[56] Fighting power then comprises conceptual component (the ideas how), a moral component (the ability to motivate people) and a physical one (the means)[57] to operate and fight or engage in combat (see Figure 2). The concept describes the operational effectiveness of

54 The model of that shape was formulated by K.V. Nielsen and it was introduced at the Defense Academy since mid-1960s. See: Bergstein, S., "The Technology of Violence," *Military Journal* 1985 No. 2; Jensen, M.S., *Strategy. The Circuit of Warfare*, https://krigsvidenskab.dk/emne/krigsforelsens-kredslob [access date: 15.09.2020].

55 Jensen, M.S., op. cit.

56 *Design of Military Operations...,* op. cit., pp. 4-2.

57 *Army Doctrinal Publication, Operations*, Development, Concepts and Doctrine Centre, Shrivenham (UK) 2010, p. 2-2.

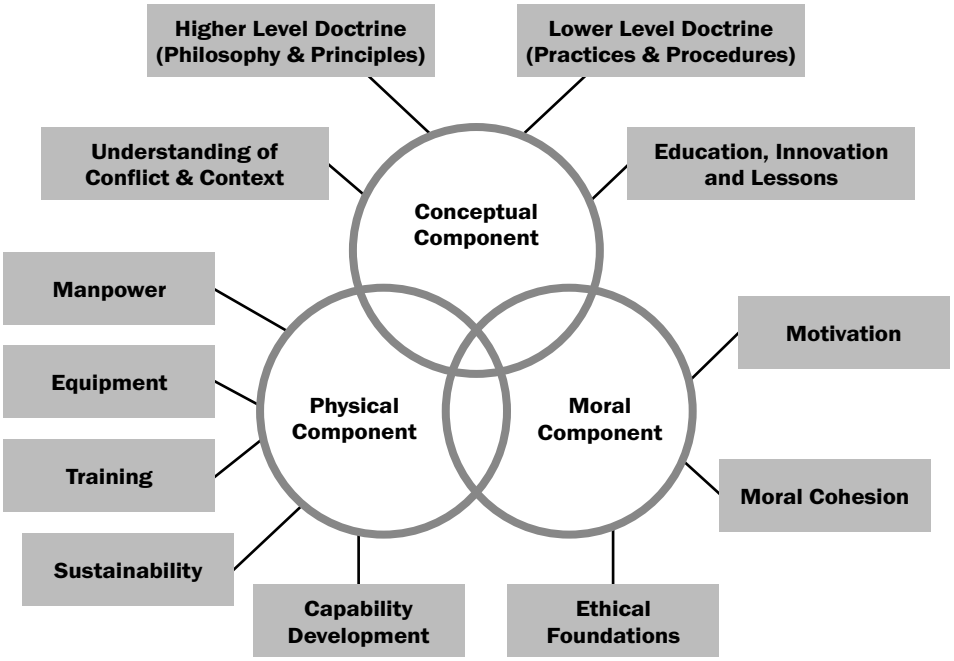


Figure 2. Concept of Fighting Power
Source: UK Army Doctrinal Publication, *Operations*

armed forces, or any element of them, and guides force development and preparation.[58] It is worth noting that British military doctrine recognizes that physical component may be recognized as the equivalent of the term "combat power" defined by NATO publications as "total means of destructive and/or disruptive force which a military unit/formation can apply against the opponent at a given time."[59] They include the organization of its main elements that consist of Manpower, Equipment, Logistics, Training and Readiness.[60] But the utility of fighting power concept is more common and ranges beyond British Army.

NATO doctrinal publications for more than a decade recognize and promote the concept of fighting power.[61] They explain its contextual characteristics and identify again that it consists of three components: conceptual, moral and physical. The trinity of equal, over-

58 See: Army Field Manual, AFM, A5, *Land Operations*, Land Warfare Development Centre, Army Doctrine Publication AC 71940.

59 AAP-6.

60 *Design of Military Operations...*, op. cit., pp. 3–5.

61 See: North Atlantic Treaty Organization Allied Joint Publication: *Allied Joint Doctrine for Land Operations AJP-3.2*, Edition A, Version 1, Published by the NATO Standardization Office (NSO), March 2016, pp. 2–13 to 2–14, and *Allied Joint Doctrine, AJP-01 Edition E, Version 1*, February 2017, pp. 1–17.

lapping and interrelated components recognizes that the degree of technological advancement of combat platforms, weapons and sensors means little if the personnel operating them is not motivated and supported by doctrine, training, or adequate leadership. Its value derives from harmonized process of forces preparation.

The conceptual part in the allied publications emphasizes the role of commanders as well as all members of the organization in observing security environment. Usually accumulated over long time, the strength of this component is based on experience, experimentation, education, research and knowledge gained through lessons learned. It establishes the ground to design the shape of future organization and operations. Its importance may illustrate situation when decision-makers choose the course of action made on misplaced information, alternate perception of reality or misjudged assumptions that may subsequently disrupt the use or development of other components. Deficiencies in this component will inexorably lead to ineffective application of fighting power or imbalance between its elements. Exemplified in doctrine and theories of war and warfare that form part of the component, it provides intellectual framework within which members of military personnel are able to build understanding of profession demands, the missions and tasks to fulfil. If properly managed, it equips commanders of all levels with the ability to comprehend the context of their activities and sets the base favorable for innovation and initiative that is necessary in complex situations. The moral element recognizes that fighting power is generated by the power of human factor. NATO publications maintain that forces are time, effort, and resources driven particularly in the case that they are to be developed, sustained, and employed effectively. The component pertains to motivation and the ability to persuade people to fight. It changes on the status of morale, the sense of purpose and on what is morally and ethically acceptable, and the determination to achieve the aim. To maximize its effect it requires quality leadership and efficient management that will lead to confidence in the course of preparations to warfare and produces organizational cohesion. The most dangerous in this respect is insufficiency of the qualified leadership. The physical component of fighting power stands for the means to fight. It consists of manpower, equipment, collective performance and training, readiness, and sustainability of forces. It is understood as a combination of people and training, both individual and in teams, in relation with the combat platforms. The component efficiency is measured by the quality of link between the people, weapons and sensors, in time of deployment, operations, sustainment and recovery. Therefore physical element of the concept cannot be measured by procurement policies alone.

Fighting power concept is well established in NATO doctrinal publications, however; they are focused on forces that already exist to be generated to warfighting rather than being developed. Nonetheless, despite the recognition of the importance of balance between its elements, they give pre-eminence to the conceptual component, while the others are derived from it. Without a theory that can assist in deriving from it a model of reality, there is no foundation for formulation of assumptions, or opinions, and there is little probability to identify relationships necessary to assess their own actions that are indispensable to accomplish anticipated state of affairs.[62] There is no possibility to achieve desired goal or

62 Jensen, M.S., op. cit.

to arrive to expected destination point, without envisioned end-state resulting from the power of mastermind.

Fighting Power – The Polish Armed Forces' Perspective

The effectiveness of forces in warfare and combat should matter most for any military organization and leadership. This will be true only if the whole organizational culture is focused on the effectiveness as the measure to judge critically its own performance. NATO as the organization utilizes the term occasionally, and does not have agreed definition that might have serve as a point of reference for the development fighting potency of forces. Having in mind the fact that for Polish military leadership within NATO membership was the reference on which doctrines, standards and conceptual documents were developed and are currently being internalized,[63] it should not be a surprise that this applies to notion of effectiveness in PAF.

As stated by one of the former Polish Chief of the General Staff[64], unquestionable but measurable attribute and quality of every army is its ability for quick and agile adjustment of its organization, concepts and operating capabilities, from current to foreseen demands, to fulfill allied, coalition or national obligations. The problem of the scale and direction of change starts with the chosen framework and conceptual or theoretical reference. If Polish political leadership decided that it was to be NATO, it must have become the frame for the military.

Having applied the induction as the scientific method that can assist in the search of objective knowledge and draw general conclusions about the state of theoretical foundations of forces development, it is time to examine the concept understanding from the perspective of the PAF.

Conceptual Component

The analysis of the language plays a significant role in identification of social phenomena. The symbolic convergence that takes place in public sphere pertains to the language traits in the process of communication. The selection of the words, due to fact of their meaning, has decisive influence on the expression of ideas. Scientifically considered, the examinations revealed that the defense and military realm suffers from the lack of its language precision.[65] The notion of „fighting power" in Polish doctrinal publications is mentioned but "hidden" in the operational standardization documents under the name *możliwości bojowe*.[66] Following NATO interpretation, the first priority is given to combat power. This is exemplified by mathematical equation where fighting power multiplied by combat functions equals to combat power. Fighting power is the ability to fight, measured

63 Lesiecki, R., op. cit.

64 Gocuł, M., op. cit., p. 12.

65 Stańczyk, J., *Formułowanie kategorii pojęciowej bezpieczeństwa*, Wydawnictwo FENCE, Poznań 2017, pp. 209–211.

66 Based on the recorded opinion of the Head of Centrum Doktryn i Szkolenia located in Bydgoszcz.

by assessment of operational capability.[67] By definition, however, combat power is defined as the total means of destructive, and/or disruptive force which a military unit/formation can apply against the opponent at a given time.[68] This may lead to the conclusion that fighting power has lower tactical role in Polish forces and especially the Army. The concept is not even mentioned in standardization document D-01 (E), Polish equivalent of NATO AJP 01(E) that incidentally raises the idea. Polish document, like its NATO originators, focuses the attention of a commander on the process of forces generation and that may echo the Alliance adherence to expeditionary mindset and reaction forces.

Conceptual sphere of the idea of fighting power in the PAF is still exposed to new challenges when at the same time old ones are not properly intellectually embraced. Not having been the part of conceptual development, experimentation and exercising, there will still be difficulty to see joint mindset among the organization. Without active contribution to past concepts such as Air-Land Battle or the idea of Joint Operations Doctrine, the concept of the Comprehensive Approach and Multi-Domain Operations will for long be alien to the whole body of military thinking. Until today, conceptually Polish doctrinal publications do not recognize clear division between strategic, operational and tactical level of national command levels and still operates within politico-military legacy. Even in terms of doctrine, it is difficult to argue with the opinion that Polish operational thinking is torn by two needs: the deployability in support of allies abroad, and the fixed territorial mission – with the consequences for training, procurement, etc.

Theory of warfare and concepts of how to fight in wars should be exemplified in doctrinal solutions and concept. The requirement of military doctrine comes from its role as crucial element of national security strategy, or grand strategy, if such exists. If grand strategy is the personification of national sovereign view on the world, the military doctrine, as its sub element should reflect the chosen way for fighting wars. It is based on the judgements of military professionals and civilian leaders about what is or is not militarily possible and necessary. Judgements based on assessment of military technology, national geography, opponent capabilities, and own fighting power efficiency provide, with relation to combat, the level of forces required, their posture, equipment, platforms and other inventory items.[69] Therefore, there is desperate need to develop national military doctrine in Poland. Doctrine understood as not only holy truth and dogma but, as Geoffrey Solan[70] notes, also the bridge between theory and practice, the connection between thought and action that expounds the idea of war.

Physical Component

The problem of application of chosen conceptual framework complicates when capability driven process of the forces development is taken into account. Capability (*zdolność*) is

67 AJP-3.2 definition – not NATO Agreed.

68 APP-6, AJP 3.2., DT-3.2.1_1PS.

69 Posen, B.R., *The Sources of Military Doctrine*, Cornell University Press, Ithaca and London 1984, pp. 13–14.

70 Sloan, G., "Military doctrine, command philosophy and the generation of fighting power: genesis and theory," *International Affairs* (Royal Institute of International Affairs 1944-) 2012, Vol. 88, No. 2, pp. 243–244.

the system of mutually related elements, such as doctrine, organization, training, materiel, leadership, personnel, facilities or interoperability (DOTMLPFI), which enables the reach of required goals.[71] NATO publication AJP-3(C) and national doctrine for the conduct of joint operations marginally mention DOTMLPFI. Even if they refer to operational level in the context of integration of forces into operation and mention the synergy of effort,[72] they serve as a NATO comparison tool with respect to capabilities in the process of lessons learned.

In order to better harmonize and energize PAF modernization efforts, there was concept of „operational capabilities"[73] in the strategic planning applied. It has been, and still is, defined as the capacity of given entity that results from its very characteristic feature or specificity that allows it undertaking expected actions. The functional components of them are: doctrines, organization, training, equipment, personnel, leadership, infrastructure and interoperability.[74] Labeled as the "defense planning based on capabilities," it was recognized as systemized items list of the operational capabilities raging from the main capability area to a single tactical capability. For the management of the capabilities, there were established functional systems which can be understood as logically selected and interconnected subsystems, as well as responsibility areas.[75] There were identified seven functional systems namely: CIS support, intelligence, fires, survivability and force protection, logistics, mobilization and personnel resupply and training,[76] common to all functional DOTMLPFI components. Those functional components, though, were not seen as interrelated to each other throughout a functional system, and the whole process crested a silo effect. Yet again, the whole effort was disconnected from the effectiveness that should be understood as the ability to deliver an intended result – forcers able to win. Technical modernization effectively lacks clear prioritization, and is still based on a variety of conflicting factors, because changing Allied obligations and permanent societal expectations may for long be different.

Moral Component

Command philosophy and command culture with reference to a fighting power idea should receive special attention from the perspective of the PAF. A human factor, but particularly commanders' professionalism, intellectual agility, innovative attitudes or adherence to the code of conduct will always be the decisive agent of the efficient employment of forces according to a given doctrine. The reason for that may be found in the opinion of LtGen Piotrowski who admitted that throughout the last twenty years of NATO member-

71 *Katalog zdolności Sił Zbrojnych RP*, SG WP 2012; *Doktryna prowadzenia operacji połączonych,* D-3 (C).

72 D-3 (C), p. 12.

73 *Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022*, adopted on the 9th of April 2013, p. 19.

74 *Metodyka planowania i programowania rozwoju Sił Zbrojnych Rzeczypospolitej Polskiej w latach 2013–2022*, Sygn. Wewn. 14/4/2011, p. 11.

75 *Koncepcja ustanowienia organizatorów systemów funkcjonalnych*, Sztab Generalny WP, Warszawa 2012, p. 4.

76 Gocuł, M., op. cit., p. 16.

ship, the most difficult thing was to change mentality. That pertains mainly to a decision-making and a command style, since there was a significant difference in what the Warsaw Pact practiced, and what were the Western models.[77] Hence, the fundamental question is: Was "the Western model" internalized by military leadership?

The quality of leadership comes from education and selection to ranks. Transparency, competition based on equal chances, balanced management of human resources, competitiveness of an organization in the social system, real experience driven and 360-degree assessment principles ought to suffice to make foundation for quality leadership. Despite the fact that military education system was restructured and military personnel was more often educated abroad in best educational centers, and the curricula of all military academies and training centers embraced the NATO and the new allies' military and warfare theoretical considerations, it is obvious that it could not be sufficient without any organizational culture change.

It is hard to presume that senior leaders shall comprehend spontaneously new concepts just by sheer exposure to Western philosophies of command during combined operations. The problem lays in a recognition, in spite of the fact that there are some commonalities, that there exists one single Western command idea. NATO efforts to have one ended up on the strategic and operational level. Polish experience shows that little effort was done and no effect was achieved to identify it. NATO itself will not solve this problem on a national level. The introduction of modern combat platforms and weapon systems will not naturally be catalyst for new practices. Contemporary expectations may be difficult to achieve, since the existence of collective decision-making was designed to avoid responsibility; lack of delineation between leadership, command, and management; and very centralized higher-level decision-making.[78] Fighting power, as approximately all concepts accepted by the PAF, has NATO origins, and is derived from experiences of the Alliance individual armies. This applies to command culture and philosophy. Without full acceptance and real unhampered introduction of new practices at all levels of command, and without "intellectual interoperability," all the efforts will, regardless of any intellectual recognition of the existence of a fighting power idea, as experience has shown, be yet again futile.

US Military Presence – Transformation 2.0

The United States Army's presence, which has been the fact since 2014 and recently reinforced by a bilateral strategic agreement, shall have significant impact on the transformation or further evolution of the Polish Armed Forces. Notwithstanding from the very beginning of Polish efforts to join NATO, US military provided significant assistance[79] in all possible areas. For the last twenty years it resulted in the participation of Polish forces as a member of coalition assisted and commanded by US wars and operations. The estab-

77 Lesiecki, R., op. cit.

78 See: Young, T.D., "Legacy Concepts: A Sociology...," op. cit., p. 31.

79 See: Lalka, J., op. cit., p. 90; R. Kupiecki, op. cit., pp. 183–185.

lishment of the elite Special Operations Forces (SOF) as an additional branch of the Armed Forces would not be so effective without the help from over the Atlantic. Realization of strategic procurement programs as well as intensive education in US academies should make natural backdrop for development of common interoperability, procedures or even acceptance of selected doctrinal solutions.

NATO membership and dedication to follow the Alliance's demands on one hand, and vast experience gained in operations and exercises with US participation on the other hand, yet again make the PAF exposed to a dilemma of choice. Poland's firm commitment to NATO is non-negotiable, and remains a central element of the country's security and foreign policy agenda. Nonetheless, as it was voiced by the Polish chief of defense, it is the Polish national interest to build own bilateral relations with the Americans as one of options or even the alternative to NATO.[80] If bilateral relations between the two states are chiefly about capability, effectiveness, readiness and should not worry the Alliance, shall they be the source of worry for the Polish military establishment?

From the perspective of a discussed concept of fighting power and US military, it is worth noting that US Army do not recognize using this model in its doctrine.[81] Emblematic to NATO-US relations is the situation when doctrinally own American regulation take precedence over the Allied ones. Often it is for a good reason, since the organization has still gaps in standardization among its members. More often we may find a previously discussed term of "capability." According to S. Biddle, capability is the ability to achieve success at a given mission. Since there is no single universal indistinguishable concept of "military capability" applicable to all conflicts, in all places and times, different military actors will assess capability in a very different way for the same forces.[82] In the face of intensified bilateral military cooperation between Poland and USA, by analogy, there may be various aspects that could be the source of different perceptions or expectations.

Conceptually, both countries belong to different worlds. It is by many reasons to name the size of forces, their role and capabilities, organization, and strength and ability to operate independently. Expeditionary by their mindset, they emphasize strongly and tend to practice "jointness" and their doctrine is based on destructive role of firepower oriented into deep battle. In physical aspect, if there is no technical interoperability with allied partners, they provide their own abilities applying it according to their own US doctrines, consequently and obviously. Their power comes not only from a single branch source, which for the army-centric PAF may be the challenge. Logistically sustainable, materiel independent, deployed or stationed into Europe as to operations, American military will be readiness-focused and high-intensity-training-oriented. And it may require immediate adaptations as those that pertain to the capabilities of a division as the Army is a formation in Poland.[83] The strength requires leadership and delineation and allocation of roles and clear

80 Opinion of General Rajmund Andrzejczak.

81 United States Army doctrine does not use model of fighting power however sporadically mentions idea of DOTMLPFI.

82 Biddle, S., op. cit., pp. 5–6.

83 Hodges, B., Bugajski, J., Wojcik, R., Schmiedl, C., *One flank, One Threat, One Presence, A Strategy for NATO Eastern Flank,* CEPA, Washington DC 2020, pp. 2 and 57–59.

command relations designed for crisis and conflict, already in peace time. This includes recognition of the existence of NATO force structure, formations, Headquarters. It is hard to argue that doctrines, force and leadership education, selection and training, at least within military service branches, are for sure more cohesive than Polish military ones. Organizational culture really matters.

The success in the transformation of the US Army after the Vietnam War is sometimes attributed to three key factors:[84] reorganization of NCO corps education system and career development, creation and further refinement of Combat Training Centers with the ability to objectively assess forces capabilities; and application of After Action Review as self-analysis to find what went wrong, why and how to fix it. So little, and still so much.

Conclusions

From the grand strategy point of reference, still absent in Poland, NATO accession was unquestionable a success. Equipped with the Allied authority and guarantees, the Republic could realize its national ambitions in a more confident way and the membership is commonly seen as the source of an increase in the position and prestige of Poland on the international stage. With the unquestionable political and strategic impact on the national security matters, in the defense sphere, the positive role of accession is often paired with unilaterally declared achievements of the Polish military in the process of its adaptation. Those self-recognized accomplishments usually comprise the successful adaptation to "NATO standards," armed forces technical modernization, the transition from a military force based on conscription to an all-volunteer force, and the rise of interoperability level as a result of the participation in the expeditionary missions. Selected at the beginning of the process, the items mentioned earlier were on the list of the areas to change and, along the years of the membership, had become the PAF's creed. They reflected not only the subjective perception of trends dominating in the alliance, but also may illustrate military establishment confidence in own forces high military potential.

Labeled as the 'transformation," the process is seen by professionals and academics mostly through the lenses of "technical modernization" and "operational experience." The first pertains to the efforts of procurement of the equipment other than with post-Soviet origins, and other with expeditionary operations, however, not always under auspices of NATO as such. Most of the changes were focused on "hardware" and organizational adjustments to mirror NATO countries' military structures – a physical part of the force. And still, the only area that is definitely recognized as a fiasco is the process of technical modernization. The attention that was paid to a conceptual factor of the change was dominated by outer incorporation of doctrinal solutions, so today they have imitative nature. Command culture and philosophy did not undergo dramatic changes in the past twenty

84 Statement of LtGen Ben Hodges during the Land Warfare Conference in London, 2017, www.youtube.com [access date: 06.09.2020]

years, and wait for finalization. Yet, the deficiency in intellectual transformation or modernization is not questioned.

Fighting power as a notion, idea or a reference model hardly exists in Polish military conceptual and intellectual sphere. Applying the model, we should assume that the change in the doctrines and theory developments should have had an impact on procurement plans, training, behavior and leadership culture. If procurement plans are not executed and corrected, doctrinal and theoretical adjustments should respond to it. Equipment and doctrine influence training methods, intensity, and quality with the reference to command philosophy. Having "Western" trained and experienced leaders, and still possessing Soviet-school concepts and inventory should impact doctrinal gradual evolution rather than indiscriminate copying from other nation's manuals. Equipment readiness and capabilities stay with tight association to drills and tactical practices rooted in doctrines based on strategy and security policy. Consequently the last thirty years of the military integration with NATO (Western militaries) cannot be announced as successful. Capability-driven thinking as the only facto has its price.

Wargaming past battles without awareness of the conditions and pressures in which they were fought in is unfair, and will rarely bring objective conclusions. Strategic military choices of the past and their effects on the present time, however, should mobilize current leaders to learn from the lessons of the last thirty years. The application of the idea of fighting power was to illustrate the need for more holistic model that will emphasize the demand for balance between tangible and intangible areas of military force. This is particularly important and time is really urgent at the beginning of more intensive bilateral strategic cooperation with the US armed forces. The might, understanding of space and distances, technological sophistication, security perceptions, political objectives and strategic choices alone, expose decision-makers again to set course for the future: the inevitable transformation of the Polish Armed Forces 2.0. ■

STRESZCZENIE:

Po wejściu Polski do NATO należało przystosować Siły Zbrojne RP do nowej rzeczywistości, jednak proces ten zbiegł się w czasie ze zmianami w środowisku bezpieczeństwa oraz strategii NATO. Aby sprostać oczekiwaniom oraz dokonać wkładu na rzecz Sojuszu, polskie wojsko stanęło przed problemem zachowania równowagi między transformacją, zmniejszeniem liczebności wojsk i modernizacją wyposażenia. W wyniku określonych wyborów, które skupiły się głównie na kwestiach „zdolności", okazało się że do dzisiaj zmiany nie przyniosły oczekiwanego rezultatu.

W artykule przeanalizowano, z wykorzystaniem istniejących terminów i pojęć, niezgodność między postrzeganiem członkostwa w NATO a faktycznym stanem efektywności militarnej sił zbrojnych w świetle wyzwań wynikających z pogłębiającej się polsko-amerykańskiej strategicznej współpracy obronnej.

SŁOWA KLUCZOWE:

członkostwo w NATO, siła bojowa, efektywność, transformacja, modernizacja, profesjonalizm, operacje ekspedycyjne

Bibliography

Army Field Manual, AFM, A5, Land Operations, Land Warfare Development Centre, Army Doctrine Publication AC 71940.

Army Doctrinal Publication, Operations, Development, Concepts and Doctrine Centre, Shrivenham (UK) 2010.

Bączyk, N., "Modernizacja techniczna sił zbrojnych RP – przyszłość a dekada 2001-2010. Cz. I. Uwarunkowania strategiczne," *Nowa Technika Wojskowa* 2011 No. 3.

Bergstein, S., "The Technology of Violence," *Military Journal* 1985 No. 2.

Biddle, S., *Military Power. Explaining Victory and Defeat in Modern Battle*, Princeton University Press, Princeton and Oxford 2004.

Chojnacki, W., *Profesjonalizacja wojska w teorii i badaniach socjologicznych*, Akademia Obrony Narodowej, Warszawa 2008.

Cieniuch, M., "Piętnaście lat w NATO," *Bezpieczeństwo Narodowe* 2014 – I.

Creveld, M.V., *Fighting Power. German and US Army Performance, 1939–1945,* Greenwood Press, Westport, US, 1982.

Creveld, M.V., *More on War*, Oxford University Press, Oxford 2017.

Design of Military Operations. The British Military Doctrine, 1996, Army Code 71451.

Dmitruk, T., "Dwie dekady w NATO – modernizacja techniczna Sił Zbrojnych," *Nowa Technika Wojskowa* 2018 No. 2.

Doktryna prowadzenia operacji połączonych, D-3 (C).

Fuller, J.F.C., *The Foundations of the Science of War*, A Military Classic Reprint, US Army General and Staff College Press, Fort Leavenworth, Kansas, USA, 1993.

Gocuł, M., "Współczesne uwarunkowania funkcjonowania i rozwoju Sił Zbrojnych RP," *Kwartalnik Bellona* 2014 No. 1.

Gordon, A., *The Tule of the Game*, Penguin Books, Great Britain 2014.

Hillison, J.R., *Stepping Up: Burden Sharing by NATO's Newest Members*, Strategic Studies Institute, United States Army War College, Carlisle, PA, USA, 2014.

Hodges, B., Bugajski, J., Wojcik, R., Schmiedl, C., *One flank, One Threat, One Presence, A Strategy for NATO Eastern Flank*, CEPA, Washington DC 2020.

Jensen, M.S., *Strategy. The Circuit of Warfare*, https://krigsvidenskab.dk/emne/krigsforelsens-kredslob [access date 15.09.2020].

Katalog zdolności Sił Zbrojnych RP, SG WP 2012.

King, A., *The Transformation of Europe's Armed Forces. From the Rhine to Afghanistan*, Cambridge University Press, Cambridge 2014.

Klich, B., *NATO – wyzwania i zadania*, in: *10 lat Polski w NATO, materiały pokonferencyjne*, Skrabacz, A. (ed.), Centralna Biblioteka Wojskowa, Warszawa 2009.

Koncepcja ustanowienia organizatorów systemów funkcjonalnych, Sztab Generalny WP, Warszawa 2012.

Korolczuk, A., "Transformacja Sił Zbrojnych RP 1999–2014. Aspekt finansowy," *Studia i Prace. Kwartalnik Kolegium Ekonomiczno-Społecznego* 2016 nr 3.

Kupiecki, R., *NATO w polskiej perspektywie 1989-2019*, PISM, MSZ RP, Warszawa 2019.

Lalka, J., "NATO – determinantem przemian w Siłach Zbrojnych RP," in: *10 lat Polski w NATO, materiały pokonferencyjne*, Skrabacz, A. (ed.), Centralna Biblioteka Wojskowa, Warszawa 2009, p. 89.

Lesiecki, R., *Dowódca operacyjny: 20 lat Polski w NATO to przede wszystkim zmiana mentalności*, Defence24, 29.03.2019, https://www.defence24.pl/dowodca-operacyjny-20-lat-polski-w-nato-to-przede-wszystkim-zmiana-mentalnosci [access date: 28.10.2020].

Malec, M., "Dylematy transformacji Sił Zbrojnych RP," *Kwartalnik Bellona* 2010 nr 3.

McLeary, P., *Defense Chief: With Giant Exercise Looming, Poland Looks To Lead Central Europe*, https://breakingdefense.com/2019/12/defense-chief-with-giant-exercise-looming-poland-looks-to-lead-central-europe/ [access date: 28.10.2020].

Metodyka planowania i programowania rozwoju Sił Zbrojnych Rzeczypospolitej Polskiej w latach 2013–*2022*, Sygn. Wewn. 14/4/2011.

Międzynarodowe operacje pokojowe i stabilizacyjne w polskiej polityce bezpieczeństwa w XX i XXI wieku, Kozerawski, D. (ed.), Warszawa 2016.

*Ministry of National Defense, "*Poland on NATO – more than 20 years," https://www.gov.pl/web/national-defence/poland-in-nato-20-years [access date: 28.07.2020].

National Security Bureau, https://www.bbn.gov.pl/pl/wydarzenia/15-lat-polski-w-nato/polska-w-sojuszu-polnoc/5295,Korzysci-i-inicjatywy.html [access date: 13.08.2020].

NATO, *The 1999 NATO Strategic Concept*, https://www.nato.int/cps/en/natohq/topics_56626.htm [access date: 21.09.2020].

NATO, *Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization adopted by Heads of State and Government in Lisbon*, https://www.nato.int/cps/en/natohq/official_texts_68580.htm [access date: 23.09.2020].

North Atlantic Treaty Organization Allied Joint Publication, *Allied Joint Doctrine, AJP-01 Edition E, Version 1*, February 2017.

North Atlantic Treaty Organization Allied Joint Publication, *Allied Joint Doctrine for Land Operations AJP-3.2*, Edition A, Version 1, Published by the NATO Standardization Office (NSO), March 2016.

Ojrzanowski, M., "Transformacja polskich sił zbrojnych – miara sił na zamiary," *Rocznik Bezpieczeństwa Międzynarodowego* 2013 nr 7.

Pawłowski, M., "Cele i wyzwania profesjonalizacji Sił Zbrojnych RP," http://www.politykaglobalna.pl/2009/12/cele-i-wyzwania-profesjonalizacji-sil-zbrojnych-rp-4/ [access date: 02.09.2020].

Posen, B.R., *The Sources of Military Doctrine*, Cornell University Press, Ithaca and London 1984.

Simon, J., *NATO Expeditionary Operations: Impact Upon New Member and Partners*, Institute for National Strategic Studies, National University Press, Washington D.C. 2005.

Sloan, G., "Military doctrine, command philosophy and the generation of fighting power: genesis and theory," *International Affairs* (Royal Institute of International Affairs 1944-) 2012, Vol. 88, No. 2.

Sperling, J., M. Webber, "NATO: from Kosovo to Kabul," *International Affairs* 85:3, The Royal Institute of International Affairs 2009.

Stańczyk, J., *Formułowanie kategorii pojęciowej bezpieczeństwa*, Wydawnictwo FENCE, Poznań 2017.

Storr, J., *The Human Face of War*, Continuum, London 2009.

Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022, adopted on the 9th of April 2013.

The Military Balance 2001–2002, Oxford University Press, London 2001.

The Military Balance 2020, Routledge, London 2020.

Young, T.D., *Anatomy of Post-Communist European Defense Institutions. The Mirage of Military Modernity,* Bloomsbury, New York 2017.

Young, T.D., "Legacy Concepts: A Sociology of Command in Central and Eastern Europe," *The US Army War College Quarterly: Parameters* 47(1), Carlisle, PA, USA, Spring 2017.

Young, T.D., "What are Governments in Central and Eastern Europe not Buying with their Defense Budgets? The Readiness Clue," *The RUSI Journal*, Routledge, 164:2, May 2019.

Zieliński, T., "Transformation of the Polish Armed Forces: A Perspective on the 20th Anniversary of Poland's Membership in the North-Atlantic Alliance," *Kwartalnik Bellona* 2020 No. 1.

Article history:	Received: 5.11.2020; Reviewed: 15.11.2020; Accepted: 27.11.2020
DOI:	10.5604/01.3001.0014.5496
Corresponding author:	Lt Gen. Sławomir Wojciechowski, PhD, War Studies University (ASzWoj), Warsaw, Poland; Multinational Corps Northeast, Szczecin, Poland; ORCID: 0000-0002--3017-3100; e-mail: s.wojciechowski@akademia.mil.pl
Cite this article as:	Wojciechowski S., Lt. Gen., PhD, "21 Years of Polish Military NATO Membership – Glass Half Empty". bellona quart. 2020(3): 13–36
Policy:	The content of the journal is circulated on the basis of the Open Access which means free and limitless access to scientific data.
Competing interests:	The authors declare that they have no competing interests.
Table of content URL:	https://kwartalnikbellona.com/issue/12943

THE BELLONA QUARTERLY ISSN: 1897-7065 | E-ISSN: 2719-3853

KWARTALNIK BELLONA

Wpływ działalności gigantów technologicznych na globalne środowisko bezpieczeństwa. Studium przypadku spółki Amazon

dr Maciej Gurtowski

ORCID:0000-0002-2990-9088
e-mail: m.gurtowski@akademia.mil.pl
Akademia Sztuki Wojennej, Centrum Badań nad Bezpieczeństwem, Warszawa

dr Jan Waszewski

ORCID:0000-0002-7370-3714
e-mail: j.waszewski@akademia.mil.pl
Akademia Sztuki Wojennej, Centrum Badań nad Bezpieczeństwem, Warszawa

ABSTRACT:

The article analyses the influence of the American Big Tech companies, commonly known as GAFAM (Google, Amazon, Facebook, Apple, and Microsoft), on the global security environment. It indicates the influence is determined by the phenomenon of a 'surveillance capitalism,' and that GAFAM companies are not only the top multinational companies, but they are also closely cooperating with their home countries. The analysis shows the emergence of the new powerful actors in the global security environment. In crisis situations, such as pandemic or a military conflict, the Big Tech companies operate not only in the informational area, they are also becoming central elements in the present-day critical infrastructure.

KEYWORDS:

Big Tech, security environment, surveillance capitalism, critical infrastructure, crisis situations

Wstęp

Celem niniejszego artykułu jest scharakteryzowanie jednego z aspektów globalnego, w konsekwencji także polskiego, środowiska bezpieczeństwa, kierunku jego przemian, podmiotów mających wpływ na te przemiany oraz metod (w tym także zasobów) wywierania wpływu. W artykule wskazano, że coraz większą rolę we współkształtowaniu istotnej części globalnego środowiska bezpieczeństwa odgrywają firmy z grupy gigantów technologicznych (od ang. *big tech*), które wykorzystują zasoby podmiotów działających zgodnie z modelem właściwym dla kapitalizmu nadzoru.

Przegląd literatury

Kapitalizm nadzoru jest to koncepcja rozwinięta systematycznie przez Shoshanę Zuboff, emerytowaną profesor Uniwersytetu Harvarda. Sedno jej namysłu dotyczy systemowych przyczyn i konsekwencji masowego zbierania i przetwarzania danych przez gigantów technologicznych[1]. Według Zuboff pojęcie kapitalizmu nadzoru określa aktualne stadium rozwoju dominującego na świecie modelu gospodarki kapitalistycznej. Obecnie istotną rolę odgrywa w niej czerpanie zysków o znacznej wartości z ciągłej inwigilacji ludzi oraz z kształtowania ich zachowań.

Zdaniem Zuboff w kapitalizmie nadzoru kluczowe jest uznanie danych o zachowaniach ludzi za swobodnie dostępny materiał, który można bez ich wiedzy i zgody zbierać, przetwarzać i sprzedawać[2]. Wartość takich przetworzonych danych wynika z ich dwóch właściwości. Po pierwsze, umożliwiają one trafne przewidywanie zachowań ludzi w przyszłości, a po drugie, dzięki nim można także wpływać na przyszłe działania ludzi.

Wraz z kapitalizmem nadzoru wyłonił się globalny rynek, na którym giganci technologiczni w zamian za udostępnianie „nieodpłatnych usług" zbierają o użytkownikach maksymalną dostępną im ilość danych, następnie analizują je i wykorzystują w celach marketingowych. Dzięki analizie danych można idealnie dostosować ofertę marketingową do indywidualnego profilu użytkownika. Firmy *big tech* krzyżują dane z różnych źródeł – to, czego użytkownik poszukuje w sieci, na co patrzy, z kim się kontaktuje, jakim posługuje się językiem, w jaki sposób się przemieszcza, gdzie i z kim mieszka, ile ma środków na koncie, jak drogi ma komputer, telefon i samochód, na co choruje, co go podnieca itp. Na podstawie tego typu informacji giganci technologiczni mogą przewidywać, co dany użytkownik w danej chwili robi, gdzie przebywa, na co będzie skłonny wydać pieniądze i w jakiej kwocie. Z dużym prawdopodobieństwem można na podstawie danych ze smartfona czy komputera przewidzieć także to, o czym użytkownik myśli[3]. Masowo zbierane dane służą również do ciągłego i często zautomatyzowanego doskonalenia mechanizmów pozwalających na dalsze zbieranie, przetwarzanie i spieniężanie danych.

Rośnie liczba badań i analiz dotyczących problemu wykorzystywania coraz liczniejszych urządzeń do zbierania danych o zachowaniach użytkowników[4]. W opracowaniach wskazuje się

1 S. Zuboff, *The Age of Surveillance Capitalism. The Fight for the Future at the New Frontier of Power*, London 2019, s. 9.

2 Ibidem.

3 J. Waszewski, *„Nie ukryjesz się". Konsekwencje synergii big data, mediów społecznościowych i neuronauki* [w druku].

4 Ibidem.

wprost, że zachowania śledzą już nie tylko smartfony i komputery, ale także urządzenia Internetu rzeczy, czyli domowe RTV, AGD, samochody, sieci kamer na ulicy, drony stróżujące, smartwatche itd. Następuje gwałtowna ekspansja infrastruktury permanentnie zbierającej i wysyłającej do firm technologicznych informacje na temat ludzi, zwierząt, roślin i materii nieożywionej. W konsekwencji powstają wielkie bazy danych o poszczególnych ludziach, całych społeczeństwach i innych obszarach drobiazgowo rejestrujące stan i aktywność poszczególnych osób oraz grup społecznych, a także ich otoczenia.

Warto zwrócić uwagę na analizy poświęcone wpływom politycznym i potencjałowi masowej manipulacji przez gigantów technologicznych. Dotyczą one między innymi tego, w jaki sposób największe medium społecznościowe na świecie – Facebook – testowało, czy jest w stanie zachęcić ludzi do wzięcia udziału w wyborach[5]. Facebookowi zarzucono również przyczynienie się do ludobójstwa w Mjanmie (Birmie)[6]. Z kolei Google, który ma 90% rynku wyszukiwarek na świecie, może współdecydować już nie tylko o tym, co ludzie kupią, lecz także o tym, czego mogą dowiedzieć się o świecie i o sobie samych. Znany jest przykład, gdy monitorowanie zapytań kierowanych do wyszukiwarki na temat symptomów choroby pozwalało na przewidzenie epidemii chorób zakaźnych[7]. Giganci kapitalizmu nadzoru już dziś mogą wpływać na decyzje i działania dosłownie miliardów ludzi na świecie.

Coraz bogatsza jest literatura poświęcona problemowi zwiększania się obszarów aktywności współczesnego człowieka zapośredniczonych cyfrowo[8]. Istotnie wzrasta rola gigantów technologicznych w kontrolowaniu infrastruktury, za pomocą której pojedynczy ludzie, firmy, podmioty pozarządowe i instytucje zaspokajają swoje potrzeby i wykonują zadania. Osłabia się znaczenie państwa, czy też szerzej – podmiotów politycznych, jako współregulatorów życia zbiorowego. Zwiększa się za to rola pozapaństwowych aktorów w postaci amerykańskich gigantów technologicznych, którzy mają wpływy polityczne, gospodarcze i kulturowe o globalnym zasięgu.

W kontekście relacji między kapitalizmem nadzoru a instytucjami bezpieczeństwa państwa Zuboff pisze o rozległej współpracy wywiadowczej po atakach z 11 września 2001 roku i roli amerykańskich gigantów technologicznych w programach Total Information Awareness, a później także w programie PRISM[9]. Warto nieco szerzej omówić wątek przejęcia przez kapitalistów nadzoru metody wywiadowczej stosowanej przez armię, określanej jako analiza wzorców życiowych (*patterns of life analysis*)[10]. Jej powstanie i rozwój łączą się z amerykańską operacją „Cedar Falls", którą przeprowadzono podczas wojny w Wietnamie. Metoda ta miała pomóc w ustalaniu powtarzalnych cykli codziennego funkcjonowania partyzantów Wietkongu,

5 Z. Corbyn, *Facebook experiment boosts US voter turnout*, Nature [online] 12.09.2012, https://www.nature.com/news/facebook-experiment-boosts-us-voter-turnout-1.11401 [dostęp: 9.11.2020].

6 T. Miles, *U.N. investigators cite Facebook role in Myanmar crisis*, Reuters [online] 12.03.2018, https://www.reuters.com/article/us-myanmar-rohingya-facebook-idUSKCN1G02PN [dostęp: 9.11.2020].

7 J. Ginsberg et al., *Detecting influenza epidemics using search engine query data*, „Nature" 2009, Vol. 457, Issue 7233, s. 1012–1014.

8 Vide: J. Waszewski, *„Nie ukryjesz się". Konsekwencje synergii...,* op. cit.

9 S. Zuboff, *The Age of Surveillance...*, op.cit., s. 85, 116–122.

10 Ibidem, s. 243.

tego, gdzie się ukrywają i śpią, jak się przemieszczają, z kim się kontaktują itp.[11] Dane te miały istotne znaczenie wywiadowcze i militarne, ponieważ umożliwiały precyzyjne planowanie niszczenia siły żywej przeciwnika, unikanie zasadzek oraz oszczędzanie własnych sił i środków. Źródłami informacji były dane wywiadu oraz dane zbierane z wykorzystaniem metod etnograficznych.

W warunkach kapitalizmu nadzoru metoda analizy wzorców życiowych zyskuje jakościowo nowy poziom. Dane o codziennej aktywności wielu ludzi na świecie są zbierane automatycznie, w czasie zbliżonym do rzeczywistego, z cyfrową precyzją, są stale aktualizowane i możliwe jest ich filtrowanie oraz przetwarzanie za pomocą algorytmów sztucznej inteligencji. Pozwala to na bezprecedensowo trafny wgląd w sposób funkcjonowania pojedynczych ludzi oraz całych społeczeństw.

Z niektórych wypowiedzi szefów amerykańskich gigantów technologicznych wynika, że mają oni świadomość znaczenia działalności ich firm dla bezpieczeństwa narodowego. Przykładowo, w październiku 2018 roku szef Amazona Jeff Bezos stwierdził, że […] *jeśli przedsiębiorstwa big tech odwrócą się od Departamentu Obrony USA, to ten kraj znajdzie się w poważnych tarapatach*[12]. Z kolei szef Facebooka podczas przesłuchania przed amerykańskim Senatem powiedział: […] *są w Rosji ludzie, których praca polega na próbie eksploatacji naszych systemów, innych systemów Internetu* […]. *Więc to jest wyścig zbrojeń, tak? Chodzi mi o to, że oni będą w tym coraz lepsi i my musimy również zainwestować, by to ulepszyć* […][13]. Podobny sens mają ujawnione przez media strategie komunikacyjne stosowane przez byłego szefa Google'a, obecnie członka zarządu holdingu Alphabet, Erica Schmidta. Zasiada on w komisjach doradczych amerykańskiej administracji, między innymi w National Security Commission on Artificial Intelligence. W ujawnionych przez media materiałach Schmidt przekonuje, że jeśli władze USA nie złagodzą regulacji dotyczących ochrony konkurencji i prywatności obywateli, to amerykańskie firmy technologiczne nie wytrzymają konkurencji z chińskimi, co w konsekwencji zagrozi bezpieczeństwu narodowemu Stanów Zjednoczonych[14].

Nie tylko amerykańscy giganci technologiczni, lecz także inne wielkie firmy międzynarodowe próbują intencjonalnie współkształtować procesy globalne. W opracowaniach poświęconych temu zagadnieniu stawiane są pytania, w jakich sytuacjach pewna grupa podmiotów może zmienić warunki brzegowe działania innych globalnych podmiotów – w tym państw[15]. Niniejsza analiza jest ograniczona głównie do wymiaru związanego z tym, jak giganci technologiczni współkonstruują globalne środowisko bezpieczeństwa.

11 R.R. Tomes, *Socio-Cultural Intelligence and National Security*, „Parameters" 2015, Vol. 45 No. 2, s. 63–64.

12 L. Sumagay, *Jeff Bezos Says Tech Shouldn't Turn Against the Federal Government*, Government Technology [online], 17.10.2018, https://www.govtech.com/civic/Jeff-Bezos-Says-Tech-Shouldnt-Turn-Against-the-Federal-Government.html [dostęp: 17.12.2019].

13 *Transcript of Mark Zuckerberg's Senate hearing*, The Washington Post [online], 11.04.2018, https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing [dostęp: 30.03.2019].

14 N. Klein, *How big tech plans to profit from the pandemic*, op.cit.

15 Vide: J. Szalacha-Jarmużek, *Instrumentarium globalnego panowania. O podmiotowych aspektach globalizacji*, Poznań 2013.

Środowisko bezpieczeństwa

W artykule przyjęto systemową perspektywę analizy środowiska bezpieczeństwa autorstwa Shiping Tanga[16]. Ten chiński badacz argumentuje, że koncentrowanie się na bezpośrednio i konkretnie rozumianym zagrożeniu bezpieczeństwa jest w dużym stopniu obciążone redukcjonizmem. Jeśli ktoś skupia się na konkretnym zagrożeniu, to będzie przygotowany tylko na to konkretne zagrożenie, nie zaś na zagrożenia, których nie przewiduje. Ujęcie kwestii zagrożeń w sposób bardziej systemowy pozwala przygotować się na różnego rodzaju zagrożenia. Zdaniem Tanga przyczyną wielu historycznych porażek w dziedzinie bezpieczeństwa państwa było właśnie zbyt wycinkowe identyfikowanie wyzwań.

Środowisko bezpieczeństwa ma bowiem systemową naturę i trudno ująć je, skupiając się wyłącznie na ograniczonej liczbie czynników i nie uwzględniając sieci dynamicznych interakcji między nimi. Za jedyną zaletę oglądu bezpieczeństwa przez pryzmat konkretnych zagrożeń Tang uznaje subiektywne poczucie dokładnego rozumienia problemu oraz jego rozwiązań. Podejście systemowe jest bardziej wymagające poznawczo niż to tradycyjne, skupiające się na konkretnych zagrożeniach, gdyż często każe posługiwać się wnioskowaniem zarówno pośrednim, jak i przybliżonym.

W swojej koncepcji Tang jest nastawiony pragmatycznie. Wskazuje, że kryterium jakości środowiska bezpieczeństwa danego państwa określają prawdopodobieństwo wystąpienia konfliktu oraz szansa na zwycięstwo w nim. W kontekście bezpieczeństwa regionalnego Tang dodaje, że dodatkowym kryterium będzie prawdopodobieństwo rozprzestrzeniania się konfliktu.

Wśród najważniejszych wymiarów środowiska bezpieczeństwa w systemowym ujęciu Tanga znajduje się technologia. Jego zdaniem […] w *historii ludzkości technologie militarne (lub technologie podwójnego zastosowania) były największą siłą zdolną do penetracji barier geograficznych państw i każda rewolucja w wojskowości przynosiła nowy rodzaj uzbrojenia i kalkulacje państw w zakresie wojny zmieniały się wraz z nią*[17].

Zaletą koncepcji Tanga jest dobre zdefiniowanie pola problemowego, wskazuje się w nim bowiem na potrzebę ujęcia holistycznego, odejście od skupienia uwagi na oczywistych i bezpośrednich zagrożeniach oraz kluczową rolę technologii w kształtowaniu środowiska bezpieczeństwa.

Dość często pojęcia środowiska bezpieczeństwa używa się zbyt swobodnie – w znaczeniu swoistego imponderabilium mającego ujmować zbiór czynników, które intuicyjnie są uznawane za istotne dla bezpieczeństwa, jednak trudno je bliżej określić. Jako ogólny problem teoretyczny z zakresu teorii bezpieczeństwa można w tym kontekście wskazać trudności z rozstrzygnięciem tego, na podstawie jakich kryteriów należałoby oceniać stan bezpieczeństwa, a dokładniej, jakie czynniki nie są w ogóle istotne z punktu widzenia bezpieczeństwa.

Metodologia

Niniejszą analizę przeprowadzono z zastosowaniem głównie metodologii białego wywiadu – wykorzystania danych jawnych, powszechnie dostępnych, tak niewywoływanych przez ba-

16 S. Tang, *A Systemic Theory of the Security Environment*, „Journal of Strategic Studies" 2004, No 27, s. 1–34.

17 Ibidem, s. 7

dacza, jaki i wywoływanych przez niego. W metodologii tej kluczowe jest traktowanie każdego źródła informacji jako instrumentu zbliżenia się do pełniejszego poznania przebiegu określonych procesów. Niezbędne są ciągła krytyka źródeł i weryfikowanie ich z dużą pieczołowitością. Często jednak istotniejsze od absolutnej pewności jest wskazanie dopiero wyłaniających się zjawisk. Część tekstu dotycząca analizy wpływu gigantów technologicznych na środowisko bezpieczeństwa została zbudowana z zastosowaniem metody studium przypadku[18]. Przyjęto jej instrumentalną odmianę[19]. Studium przypadku stanowi w niej ilustrację pewnych zjawisk i procesów. Chodzi o znalezienie przykładów, często jak najbliższych typu idealnego[20]. W tym sensie uzasadnione jest skupienie się w badawczej części artykułu na spółce Amazon i dwóch wybranych aspektach jej funkcjonowania. Po pierwsze, są to działania wywołane pandemią SARS-CoV-2 i przejmowanie przez firmę prywatną niektórych funkcji państwa. Po drugie, opisane zostają ślady tworzenia przez Amazon organizacji o charakterze służby specjalnej. Obie części studium przypadku wiążą się ze sobą bezpośrednio i stanowią ilustrację dążeń giganta technologicznego do kształtowania środowiska bezpieczeństwa w warunkach kapitalizmu nadzoru.

Wyniki i dyskusja

Amerykańscy giganci technologiczni mają coraz większe wpływy na gospodarkę i pośrednio również na państwową politykę wewnętrzną oraz międzynarodową. W sposób nieunikniony przekłada się to na kształtowanie środowiska bezpieczeństwa. Przedstawiciele *big tech* dążą do zdobycia i utrzymania pozycji monopolistycznej na wybranych rynkach. Świat cyfrowy – nie tylko w USA – właściwie już został podzielony i choć wejście na ten rynek jest nadal możliwe, to napotyka trudne do przekroczenia bariery. Mimo że twórcy start-upów, innowacyjnych podmiotów biznesowych, wciąż mają szansę włączyć się do wyścigu i stworzyć własną niszę na rynku, to giganci technologiczni mają jednak sposoby na radzenie sobie z taką konkurencją. Jak wykazuje raport amerykańskiej komisji, która badała działania monopolistyczne amerykańskiego *big tech*, dwie podstawowe techniki neutralizacji konkurencji polegają na przejęciu konkurencji oraz kopiowaniu jej rozwiązań[21]. W pierwszym przypadku twórcy start-upu są najczęściej kooptowani i stają się razem ze swoimi firmami częścią giganta. Kopiowanie polega na włączeniu do modelu działalności giganta nowych rozwiązań, które mają być oczywiste i niezwiązane z pojawieniem się innowacyjnego start-upu. Z drugiego sposobu korzysta się zazwyczaj wtedy, gdy nie powiodły się rozmowy dotyczące sposobu pierwszego.

18 R.E. Stake, *Studium przypadku*, w: *Ewaluacja w edukacji*, L. Korporowicz (red.), Warszawa 1997, s. 120–143; R.E. Stake, *Jakościowe studium przypadku*, w: *Metody badań jakościowych*, N.K. Denzim i Y.S. Lincoln (red.), Warszawa 2009, t. 1, s. 623–654.

19 R.K. Yin, *Case Study Research. Design and Methods*, Londyn 2009.

20 W rozumieniu Weberowskim. Vide: G. Psathas, *The Ideal Type in Weber and Schutz*, w: *Explorations of the Life-World. Contributions to Phenomenology (In Cooperation with the Center for Advanced Research in Phenomenology)*, M. Endress, G. Psathas, H. Nasu (red.), Dordrecht 2005, s. 143–169.

21 Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, *Investigation of competition...*, op. cit., s. 279.

Podobnie jak GAFAM, działa BATX, chińska grupa *big tech*, na którą składają się: Baidu – wyszukiwarka, Alibaba – handel internetowy, Tencent – rozrywka, media i płatności (WeChat) oraz Xiaomi – producent elektroniki i oprogramowania. Reszta świata, poza USA i Chinami, i w pewnym zakresie także Rosją, wydaje się nieustannym polem bitwy między podmiotami z grupy GAFAM a jej odpowiednikami z Państwa Środka. Jest to oczywiście pewne modelowe uproszczenie. W Rosji i rosyjskojęzycznym Internecie w dalszym ciągu funkcjonują grupy Yandex i Mail.ru. Na niektórych polach, np. w mediach społecznościowych i wyszukiwaniu, są one w stanie rywalizować z GAFAM i BATX.

Amerykański Kongres oraz Departament Sprawiedliwości próbują ukrócić potęgę gigantów technologicznych z USA za pomocą postępowań antymonopolowych. Oznacza to, że amerykańskie instytucje dostrzegają problemy związane z rosnącą potęgą *big tech*. Ze względu na przyjętą przez instytucje regulacyjne optykę – dążenie do usunięcia monopolistycznej pozycji rynkowej – mogą one jednak nie zauważać istoty problemu. A stanowią ją rosnące role – polityczna i geopolityczna – gigantów cyfrowych.

W artykule przedstawiono dwa przykłady, które demonstrują, w jaki sposób jeden z gigantów cyfrowych – Amazon – kształtuje swoje, a w rezultacie, pośrednio, globalne środowisko bezpieczeństwa. Opisano działania tej spółki będące reakcją na wybuch pandemii SARS-CoV-2, a także pokazano, jakich narzędzi Amazon używa do zdobywania informacji na temat środowiska bezpieczeństwa i – również pośrednio – do kształtowania go zgodnie z własnymi potrzebami oraz planami. Jako pytanie badawcze do dalszych dociekań pozostawiono kwestię, w jakim stopniu inni giganci technologiczni prowadzą podobne do Amazona działania.

Warto krótko przedstawić historię Amazona. Spółka ta została założona przez Jeffreya (Jeffa) P. Bezosa w 1994 roku i nazywała się Cadabra. Już w 1995 roku zmieniła nazwę na Amazon.com, od rzeki Amazonki, co według niektórych interpretacji miało oddawać ambicje twórcy dotyczące skali przepływu dóbr przez tę firmę. Początkowo była to głównie księgarnia internetowa. Z biegiem czasu Amazon poszerzał ofertę handlową i zaczął sprzedawać własne produkty. Najpierw były to czytniki książek elektronicznych. Obecnie Amazon tworzy również inne linie produktów, między innymi inteligentne głośniki, tablety oraz systemy bezpieczeństwa (kamery i oprogramowanie do nich). Urządzenia te, podobnie jak sprzęt produkowany przez innych gigantów technologicznych, tworzą zamknięty ekosystem powiązanych ze sobą towarów i usług. Za pomocą urządzeń Amazona można korzystać z jego usług streamingowych, filmów, seriali, gier, muzyki i audiobooków. Amazon przejął nawet sieć sklepów spożywczych i zajął się dostawami żywności. Z biegiem lat spółka stała się emblematycznym przykładem detalicznego sklepu internetowego. Jej ambicją – obecnie zaspokojoną – było zostać sklepem, w którym można kupić wszystko (*everything store*)[22].

Do swojej oferty Amazon dołączył również usługi sieciowe – jest największym dostawcą chmury obliczeniowej na świecie. W lipcu 2020 roku spółka miała 31% światowego rynku na tym polu[23]. I to mimo porażki poniesionej podczas próby zdobycia kontraktu na zapewnienie

22 Nawiązanie do tytułu książki o Amazonie oraz jej założycielu i szefie J. Bezosie: B. Stone, *The Everything store*, New York 2013.

23 *Global cloud services market Q2 2020*, Canalys [online], 30.07.2020, https://www.canalys.com/newsroom/worldwide-cloud-infrastructure-services-Q2-2020 [dostęp: 4.11.2020].

usług chmurowych amerykańskiemu Departamentowi Obrony. Kontrakt na realizację wartego 10 mld i planowanego na 10 lat programu JEDI (Joint Enterprise Defense Infrastructure) wygrał w październiku 2019 roku Microsoft. Amazon zadecydował, że będzie walczył przed sądami o unieważnienie tej decyzji[24]. Jako argument na potwierdzenie swojej wiarygodności wskazuje fakt świadczenia usług na rzecz 6500 innych amerykańskich agencji rządowych – w tym wojskowych i wywiadowczych.

Już w 2013 roku Amazon ogłosił, że zawarł kontrakt z Centralną Agencją Wywiadowczą (CIA)[25]. Przedmiotem zamówienia było przygotowanie usług chmurowych – zdalnego dostępu do mocy obliczeniowej komputerów oraz zdalnego dostępu do zasobów cyfrowych przechowywanych w centrach danych – dla 17 amerykańskich służb wywiadowczych zrzeszonych we Wspólnocie Wywiadowczej[26]. Kontrakt został zawarty na cztery lata, z możliwością przedłużenia go dwa razy – łącznie o 5 lat. Maksymalna płatność za wykonane usługi wyniosła 600 mln dolarów[27]. Dla Amazona był to kontrakt przełomowy, i to z kilku powodów. Po pierwsze, spółka kojarzona powszechnie jako „detaliczny sklep internetowy" po raz pierwszy wygrała rywalizację o kontrakt federalny z wielkimi firmami informatycznymi o ustalonej reputacji[28]. Protest walczącego o kontrakt IBM został odrzucony, ponieważ to Amazon zapewnił lepsze rozwiązania technicznie. Po drugie, w przeciwieństwie do poprzednich umów gigant handlu internetowego zgodził się na zbudowanie infrastruktury u swojego klienta. Wcześniejsze kontrakty – również rządowe – wiązały się z wykorzystywaniem zasobów, z których korzystano za pośrednictwem ogólnodostępnego Internetu.

Kontrakt dla CIA pokazuje, jak poszerzała się ekspansywna działalność Amazona. Spółka tworząc infrastrukturę informatyczną dla amerykańskich służb, zyskała w relacjach z państwem ekskluzywną pozycję. Jest już podmiotem, który stał się jednym z kluczowych węzłów dla działania znacznej części Internetu. To w chmurze Amazona i dzięki niej działa wiele portali społecznościowych oraz serwisów internetowych (np. Netflix). W pewnym stopniu awarie chmury tej spółki stają się awariami Internetu[29]. Jednak nawet coraz bardziej centralne dla korporacji usługi chmurowe w ogólnodostępnej sieci przestały być wystarczające. Mniej więcej od czasu kontraktu dla CIA Amazon zaczął pracować również nad zwiększaniem swojego znaczenia dla infrastruktury federalnej USA. Pewnym ukoronowaniem tych planów była właśnie próba zdobycia kontraktu JEDI.

24 *JEDI: Why we will continue to protest this politically corrupted contract award*, AWS [online], 4.09.2020, https://aws.amazon.com/blogs/publicsector/jedi-why-we-will-continue-protest-politically-corrupted-contract-award [dostęp: 4.11.2020].

25 C. Metz, *Amazon's Invasion of the CIA Is a Seismic Shift in Cloud Computing*, Wired [online], 18.06.2013, https://www.wired.com/2013/06/amazon-cia [dostęp: 6.11.2020].

26 Wspólnota Wywiadowcza (ang. intelligence community) – grupa 17 służb specjalnych lub podmiotów o charakterze służb specjalnych wchodzących w skład innych instytucji rządowych, powołana do życia w USA w 1981 r. i kierowana przez dyrektora wywiadu narodowego.

27 United States Government Accountability Office, *Decision*, GAO [online], 6.06.2013, https://www.gao.gov/assets/660/655241.pdf [dostęp: 5.11.2020].

28 C. Metz, *Amazon's Invasion of the CIA...*, op.cit.

29 A.C. Estes, *Amazon Just Broke the Internet*, Gizmodo [online], 28.02.2017, https://gizmodo.com/amazon-just-broke-the-internet-1792827856 [dostęp: 6.11.2020].

Jeff Bezos jest uznawany za najbogatszego człowieka na świecie, głównie dzięki posiadaniu pakietu ponad 11% akcji Amazona[30]. Przykładowo, 4 listopada 2020 roku wartość majątku Bezosa była szacowana na ponad 180 mld dolarów[31]. W tym samym dniu kapitalizacja rynkowa Amazona wyniosła ponad 1,5 bln dolarów[32]. Jeśli wskazać tylko jeden wskaźnik finansowy Amazona, to w samym trzecim kwartale 2020 roku zyski spółki wyniosły 6,3 mld dolarów. W porównaniu z trzecim kwartałem 2019 roku oznacza to wzrost o ponad 4 mld dolarów zysku.

Jeszcze przed wybuchem pandemii koronawirusa Amazon próbował pokazać, że może być ważnym partnerem dla władz samorządowych i lokalnych organizacji policyjnych w USA (biur szeryfów, policji miejskich itp.). Bliską z nimi współpracę nawiązała i tworzenie relatywnie taniej infrastruktury bezpieczeństwa zaoferowała jedna ze spółek zależnych tego amerykańskiego giganta. Chodzi o Amazon Ring, start-up kupiony przez Amazon w 2018 roku[33]. W ramach współpracy z nim aż 1300 lokalnych organizacji policyjnych zachęcało obywateli do kupowania flagowego produktu Amazon Ring i udostępniania organom ścigania nagrań wideo pozyskanych w trakcie jego użytkowania. Ten produkt to „inteligentne dzwonki" do drzwi, które są wyposażone w kamerę i podłączone do Internetu. W USA kurierzy często pozostawiają paczki na gankach domów lub w specjalnych skrzynkach. Kamera Amazon Ring obserwująca miejsce pozostawienia przesyłki ma przede wszystkim odstraszyć potencjalnych złodziei.

Zakup produktów z serii Ring stał się jednak czymś więcej niż tylko narzędziem ratującym paczki przed kradzieżą. Obecnie jest jedną ze ścieżek budowy względnie taniego „inteligentnego domu" z wykorzystaniem urządzeń (inteligentne głośniki Amazon Echo itp.) i oprogramowania Amazona oraz jego usług przechowywania danych w chmurze. Oprócz „inteligentnych dzwonków" do drzwi Amazon Ring sprzedaje również kamery monitoringu wewnętrznego i zewnętrznego oraz rozwija wspomagające je oprogramowanie (aplikację na smartfony, systemy rozpoznawania twarzy).

Jednym z rozwiązań wprowadzanych wraz z „inteligentnymi dzwonkami" jest swoiste medium społecznościowe – przedstawiane jako straż sąsiedzka[34] – w którym mieszkańcy tej samej okolicy dzielą się informacjami na temat przestępczości i poszczególnych jej sprawców[35]. Dostęp do danych zgromadzonych przez Amazon Ring nie tylko ułatwia współpracę między sąsiadami, lecz także ma usprawniać pracę policji[36].

30 Dane z listopada 2020 r.

31 *Jeff Bezos*, Forbes [online], https://www.forbes.com/profile/jeff-bezos [dostęp: 4.11.2020].

32 Dane giełdy NASDAQ, https://www.nasdaq.com/market-activity/stocks/amzn [dostęp: 4.11.2020].

33 Vide: J. Kelley, M. Guariglia, *Amazon Ring Must End Its Dangerous Partnerships With Police*, Electronic Frontiers Foundation [online], 10.06.2020, https://www.eff.org/deeplinks/2020/06/amazon-ring-must-end-its-dangerous-partnerships-police [dostęp: 6.11.2020]; E. Kim, *Amazon buys smart doorbell maker Ring for a reported $1 billion*, CNBC [online], 27.02.2018, https://www.cnbc.com/2018/02/27/amazon-buys-ring-the-smart-door-bell-maker-it-backed-through-alexa-fund.html [dostęp: 6.11.2020]; D. Harwell, *Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns*, The Washington Post [online], 28.08.2019, https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach [dostęp: 6.11.2020].

34 *Neighborhood security in your hands*, Ring [online], https://ring.com/neighbors [dostęp: 6.11.2020].

35 B.F. Rubin, *How Ring's Neighbors app is making home security a social thing*, CNET [online], 3.12.2018, https://www.cnet.com/news/how-rings-neighbors-app-is-making-home-security-a-social-thing [dostęp: 6.11.2020].

36 M. Guariglia, *Five Concerns about Amazon Ring's Deals with Police*, Electronic Frontiers Foundation [online], 30.08.2019, eff.org/pl/deeplinks/2019/08/five-concerns-about-amazon-rings-deals-police [dostęp: 6.11.2020].

Po wybuchu pandemii wirusa SARS-CoV-2 Amazon podjął wiele skoordynowanych działań. Mają one umożliwić mu przetrwanie kryzysu oraz służyć zwiększeniu pozycji rynkowej[37]. Warto wskazać przykłady tych działań, unaoczniają one bowiem, na jak wielu polach Amazon reaguje na potrzeby otoczenia społecznego i instytucjonalnego, tym samym wpływa na swoje środowisko bezpieczeństwa. Nie można zapomnieć, że ze względu na globalną pozycję Amazona (i innych gigantów technologicznych) globalne są również jego wpływy na to środowisko.

Amazon podejmuje decyzje o priorytetowym wysyłaniu niektórych produktów i wstrzymaniu wysyłki innych, uznanych za mniej priorytetowe w warunkach pandemii koronawirusa[38]. W rezultacie firma samodzielnie reguluje opanowaną przez siebie część rynku i rozstrzyga, którzy z jego z dostawców będą narażeni na straty, a które ze współpracujących z nią firm w dłuższej perspektywie czasowej będą zagrożone upadłością[39]. Ponadto amerykański gigant handlu internetowego próbuje zapanować nad spekulacjami współpracujących z nim i korzystających z jego infrastruktury sprzedawców[40]. Przeprowadzone w lutym i marcu 2020 roku interwencje dotyczyły głównie maseczek i środków do dezynfekcji skóry[41]. Amazon odgrywa również rolę cenzora i blokuje możliwość sprzedawania na swojej platformie handlowej książek o COVID-19 zawierających niezweryfikowane lub fałszywe informacje oraz teorie spiskowe[42].

Firma podjęła się rozprowadzania testów do wykrywania zakażenia SARS-CoV-2[43]. Początkowo dostawy dotyczyły Seattle, miasta, w którym znajduje się jej główna siedziba, i były realizowane przez spółkę zależną Amazon Care (wcześniej zajmowała się ona zdrowiem pracowników centrali Amazona i ich rodzin). Amazon także w Wielkiej Brytanii był jednym z podmiotów, którym tamtejszy rząd powierzył zadanie dostarczania testów na COVID-19 pracownikom służby zdrowia[44].

37 J.P. Mandalindan, *Can Amazon handle the coronavirus pressure?,* Protocol [online], 22.03.2020, https://www.protocol.com/amazon-delivery-coronavirus-high-demand [dostęp: 1.04.2020]; aktualizowana regularnie lista działań Amazona znajduje się na oficjalnym blogu spółki: https://blog.aboutamazon.com/company-news/amazons-actions-to-help-employees-communities-and-customers-affected-by-covid-19 [dostęp: 20.10.2020].

38 L. Matsakis, *Amazon Warehouses Will Now Accept Essential Supplies Only*, Wired [online], 17.03.2020, https://www.wired.com/story/amazon-warehouse-essential-goods-only/ [dostęp: 25.03.2020], G. Marks, *Amazon Warehouses Are Accepting Only The Essentials...And Other COVID-19 Small Business Tech News*, Forbes [online], 22.03.2020, https://www.forbes.com/sites/quickerbettertech/2020/03/22/amazon-warehouses-are-accepting-only-the-essentialsand-other-covid-19-small-business-tech-news/#6b8ca46ef678 [dostęp: 25.03.2020].

39 Vide: D. Lee, P. Nilsson, *Amazon auditions to be 'the new Red Cross' in Covid-19 crisis*, 31.03.2020, ft.com/content/220bf850-726c-11ea-ad98-044200cb277f [dostęp: 1.04.2020].

40 J. Dastin, *Amazon bars one million products for false coronavirus claims*, Reuters [online], 27.02.2020, https://uk.reuters.com/article/us-china-health-amazon-com/amazon-bars-one-million-products-for-false-coronavirus-claims-idUKKCN20L2ZH [dostęp: 25.03.2020]; C. Osborne, *eBay and Amazon are losing the battle against coronavirus profiteering*, ZDNet [online], 25.03.2020, zdnet.com/article/ebay-and-amazon-are-losing-the-battle-against-coronavirus-profiteering [dostęp: 25.03.2020].

41 L. Matsakis, *As Covid-19 Spreads, Amazon Tries to Curb Mask Price Gouging*, Wired [online], 25.02.2020, wired.com/story/covid-19-amazon-curb-face-mask-price-gouging [dostęp: 25.03.2020].

42 Idem, *Amazon Quietly Removes Some Dubious Coronavirus Books*, Wired [online], 11.03.2020, https://www.wired.com/story/amazon-quietly-removes-coronavirus-books [dostęp: 25.03.2020].

43 *Government launches new drive on coronavirus tests for frontline NHS staff*, GOV.UK [online], 27.03.2020, https://www.gov.uk/government/news/government-launches-new-drive-on-coronavirus-tests-for-frontline-nhs-staff [dostęp: 9.11.2020].

44 I.A. Hamilton, *Amazon is reportedly in talks to help deliver COVID-19 tests in the UK*, Business Insider [online], 23.03.2020, https://www.businessinsider.com/amazon-in-talks-to-help-deliver-covid-19-tests-uk-2020-3 [dostęp: 25.03.2020].

Wyzwaniem dla planów spółki były paraliżujące działalność centrów logistycznych zakażenia pracowników koronawirusem oraz strajki pracowników, którzy domagali się, między innymi, skutecznych środków ochrony osobistej[45]. Protestowali również polscy pracownicy spółki[46]. Grupa zasiadających w amerykańskim Kongresie członków Partii Demokratycznej zażądała, żeby Amazon wyjaśnił, w jaki sposób chroni zdrowie swoich pracowników i jakie zamierza poczynić w tym celu kroki[47].

Podsumowując, na przykładzie Amazona widać, że w warunkach amerykańskich przejmuje on wprost zadania dotychczas wykonywane przez państwo i samorządy[48]. Spółka próbuje się pokazać jako instytucja, która spełnia kluczową funkcję publiczną i że zamknięcie jej centrów logistycznych poważnie zagroziłoby utrzymywaniu dystansu społecznego[49]. Taka postawa to oczywiście jeden z podstawowych czynników decydujących o sukcesie biznesowym Amazona. Jednocześnie takie przechwytywanie funkcji państw i samorządów jest jednym z wymiarów kształtowania środowiska bezpieczeństwa. Spółka stara się nie tylko pokazać siebie jako niezbędny element infrastruktury krytycznej, lecz także dąży do tego, by stać się nim realnie. W tym celu korzysta w USA i w innych państwach ze swojej monopolistycznej pozycji. Sprzedaż własnych produktów Amazona oraz zapewnienie kanału dystrybucji współpracującym z nim sprzedawcom staje się głównym narzędziem również dla państw wprowadzających lockdown lub inne formy obostrzeń w celu zwiększenia dystansu społecznego. Inne działania Amazona związane z pandemią – zdrowotne, cenzorskie – wydają się służyć utrzymaniu pozycji niezbędnego elementu infrastruktury krytycznej. Taka pozycja może dotyczyć i innego typu kryzysów.

Druga sprawa warta omówienia w niniejszym studium przypadku unaocznia, jakie jest podejście Amazona do analizy zebranych przez niego danych i zarazem ukazuje, jakie mogą być konsekwencje eskpansji kapitalizmu nadzoru. Dzięki niespodziewanej i przejściowej „szczerości" amerykańskiej spółki można zorientować się, jak Amazon postrzega środowisko bezpieczeństwa. Nie chodzi tylko o rozpoznanie wyzwań, tj. zagrożeń i szans, istotne wydają się bowiem możliwość oddziaływania na środowisko bezpieczeństwa i ambicja kształtowania go zgodnie z interesem spółki, jej kierownictwa oraz właścicieli.

45 Vide: informacje o sytuacji we francuskich oddziałach Amazona: A. Publie, *Coronavirus: la gronde s'intensifie contre Amazon*, Les Echos [online], 20.03.2020, https://start.lesechos.fr/travailler-mieux/flexibilite-travail/coronavirus-la-gronde-s-intensifie-contre-amazon-17659.php [dostęp: 1.04.2020]; relacja o obawach amerykańskich pracowników spółki: A. Palmer, *'They're putting us all at risk': What it's like working in Amazon's warehouses during the coronavirus outbreak*, CNBC [online], 26.03.2020, https://www.cnbc.com/2020/03/26/amazon-warehouse-employees-grapple-with-coronavirus-risks.html [dostęp: 1.04.2020].

46 Vide: P. Drabik, *Amazon nie zamyka swoich magazynów pomimo epidemii*, Radio Zet [online], 26.03.2020, https://biznes.radiozet.pl/News/Covid-19.-Amazon-nie-zamyka-swoich-magazynow.-Dlaczego [dostęp: 6.04.2020].

47 A. Holmes, *Ilhan Omar and Bernie Sanders are demanding that Amazon come up with a safety plan for workers as online orders soar amid coronavirus*, Business Insider [online], 27.03.2020, https://www.businessinsider.com/ilhan-omar-bernie-sanders-amazon-worker-safety-coronavirus-2020-3 [dostęp: 1.04.2020].

48 Vide: J.C. Wong, *'The US of Amazon': how the coronavirus has created a governance vacuum the tech giant is quickly filling*, The Guardian [online], 24.03.2020, theguardian.com/technology/commentisfree/2020/mar/24/the-us-of-amazon-how-the-coronavirus-has-created-a-governance-vacuum-the-tech-giant-is-quickly-filling [dostęp: 25.03.2020].

49 J. Bezos, *A message from our CEO and founder*, Amazon [online], 21.03.2020, https://blog.aboutamazon.com/company-news/a-message-from-our-ceo-and-founder [dostęp: 1.04.2020].

W styczniu 2020 roku na stronie internetowej Amazona informującej o procesach rekrutacyjnych firmy pojawiło się ogłoszenie o poszukiwaniu pracownika na stanowisko analityka wywiadowczego (*intelligence analyst*)[50]. W lipcu dodano ogłoszenie o poszukiwaniu starszego analityka wywiadowczego. Są to pierwsze tego typu ogłoszenia w historii spółki. Z archiwalnych ogłoszeń o wolnych stanowiskach[51] wynika, że w przeszłości również poszukiwano analityków mających doświadczenie w analizowaniu danych. Z pewnością zatrudniano weteranów służb specjalnych i organów ścigania. Jak wynika z dalszej części analizy, od analityków wywiadowczych Amazon oczekiwał jednak dosyć precyzyjnie określonych umiejętności, doświadczenia oraz gotowości do podejmowania konkretnych działań.

Na ogłoszenia rekrutacyjne o poszukiwaniu analityków wywiadowczych zwrócono uwagę w mediach społecznościowych 1 września 2020 roku. Ogłoszenia wywołały serię komentarzy. Po niespełna trzech godzinach od pierwszych wypowiedzi i zainteresowaniu się sprawą przez media tradycyjne ogłoszenia zostały usunięte ze strony rekrutacyjnej Amazona[52]. Na pytania dziennikarzy rzecznik prasowy firmy odpowiedziała, że […] *ogłoszenie o pracy nie było dokładnym opisem roli pracownika – było wynikiem błędu, który został już poprawiony*[53]. Między 4 a 8 września na stronie rekrutacyjnej Amazona pojawiła się wersja oferty pracy dla analityka wywiadowczego pozbawiona kwestii, które budziły zdziwienie i niepokój mediów[54].

Ważnym kontekstem sprawy wydaje się fakt, że 9 września 2020 roku Amazon ogłosił, iż do jego jedenastoosobowej rady dyrektorów dołączył generał rezerwy US Army Keith B. Alexander[55]. W latach 2005–2014 był on dyrektorem Narodowej Agencji Bezpieczeństwa (National Security Agency – NSA). To właśnie Alexander nadzorował rozwój amerykańskich systemów globalnego nadzoru elektronicznego. Również w okresie jego pracy w NSA miało dojść – zgodnie z informacjami ujawnionymi przez sygnalistę Edwarda Snowdena – do bliskiej współpracy USA z gigantami technologicznymi w tworzeniu tego systemu. We wchodzącym w jego skład programie PRISM Amazon miał jednak nie brać udziału[56]. Ale już samo zatrudnienie osoby mającej takie doświadczenie i sieć kontaktów jak Alexander może świadczyć o ambicjach i planach tego giganta technologicznego.

50 Amazon usunął ogłoszenia po ich nagłośnieniu. Są dostępne na portalu archive.org, który archiwizuje m.in. strony WWW: https://web.archive.org/web/20200901142713/https://www.amazon.jobs/en/jobs/1213610/sr-intelligence-analyst/; https://web.archive.org/web/20200901153123/https://www.amazon.jobs/en/jobs/1026060/intelligence-analyst [dostęp: 4.09.2020].

51 https://www.amazon.jobs [dostęp: 1.11.2020].

52 J. Wakefield, *Amazon withdraws job adverts for union 'spies'*, BBC News [online], 3.09.2020, www.bbc.com/news/technology-53998201 [dostęp: 4.09.2020].

53 L. Franceschi-Bicchierai, *Amazon Is Hiring an Intelligence Analyst to Track 'Labor Organizing Threats'*, VICE [online], 1.09.2020, https://www.vice.com/en_us/article/qj4aqw/amazon-hiring-intelligence-analyst-to-track-labor-organizing-threats [dostęp: 4.09.2020].

54 Na portalu archive.org 8 września br. zarchiwizowana została nowa wersja oferty pracy, https://web.archive.org/web/20200908152053/https://www.amazon.jobs/en/jobs/1026060/intelligence-analyst [dostęp: 24.09.2020].

55 Zgłoszenie dla Securities and Exchange Commission (Komisji Papierów Wartościowych i Giełd), 9.09.2020, https://sec.report/Document/0001018724-20-000026 [dostęp: 11.09.2020].

56 R. Brandom, *Former NSA chief Keith Alexander has joined Amazon's board of directors*, The Verge [online], 9.09.2020, https://www.theverge.com/2020/9/9/21429635/amazon-keith-alexander-board-of-directors-nsa-cyber-command [dostęp: 11.09.2020].

Wspomnianych analityków wywiadowczych rekrutował dział Amazona o nazwie Globalny Program Wywiadowczy (Global Intelligence Program – GIP), który jest częścią Globalnych Operacji Bezpieczeństwa (Global Security Operations – GSO). Oba ogłoszenia są bardzo podobne, różnią się głównie tym, że starszy analityk miał wykonywać więcej zadań kreatywnych, związanych z kierowaniem zespołem i tworzeniem nowych narzędzi, oraz miał utrzymywać bezpośrednie kontakty z kierownictwem Amazona, również najwyższego szczebla.

Starszy analityk miał nie tylko wykazywać się umiejętnościami kierowniczymi, lecz także mieć doświadczenie w kwestiach technicznych. Oczekiwano od niego tworzenia […] *metodologii i produktów służących ocenie najnowszego wpływu na określone produkty dynamicznie rozwijających się sytuacji – w tym protestów, geopolitycznych kryzysów oraz konfliktów*.

Starszy analityk ds. wywiadu miał blisko współpracować z działem personalnym oraz z działem zarządzania zasobami ludzkimi i współtworzyć z nimi narzędzia oraz procedury wykrywania zagrożeń, a także innych wrażliwych kwestii. Od analityków oczekiwano pomocy dla prawników, którzy przygotowywali pozwy przeciwko aktywistom i ich grupom prowadzącym nielegalne działania wymierzone w Amazona.

W ogłoszeniu wprost wskazano, że monitorowanie zagrożeń będzie obejmować między innymi *działalność związków zawodowych, grup aktywistycznych oraz wrogich przywódców politycznych*. Analitycy mieli nawiązywać kontakty ze specjalistami od zjawisk uznawanych za istotne dla Amazona. Należą do nich […] *grupy nawołujące do nienawiści, akcje polityczne, kwestie geopolityczne, terroryzm, wymiar sprawiedliwości oraz związki zawodowe*.

Ponadto od analityków oczekiwano umiejętności zbierania danych z zachowaniem bezpieczeństwa operacyjnego, czyli – jak można sądzić – niepozostawiania śladów tego, że dane w ogóle były pozyskiwane. Wśród wskazanych technik i metod wywiadowczych znalazły się: biały wywiad, analiza obrazu i nagrań, analiza powiązań, wizualizacja danych oraz korzystanie z systemów informacji przestrzennej.

W części ogłoszenia o obowiązkach starszego analityka znalazło się zastrzeżenie, że będzie on musiał […] *zrozumieć i nauczyć się bogatego zestawienia różnych typów danych Amazona, współpracować z kontrolującymi je zespołami [data owners] i tak wykorzystywać zbiory danych, żeby odkrywać nowe kwestie, które mogą być istotne dla kierownictwa spółki*. Jeśli chodzi o kwalifikacje, to na stanowisko starszego analityka wywiadowczego poszukiwani byli ludzie z doświadczeniem wyniesionym ze służb specjalnych, sił zbrojnych, organów ścigania oraz z sektora prywatnego, jeśli zajmowali się w nim zagrożeniami globalnymi.

Amerykańskie media skupiły się głównie na tej części zadań poszukiwanych pracowników, która dotyczy walki z próbami stworzenia związków zawodowych i inwigilowania już działających związków[57]. Choć działalność antyzwiązkowa jest w USA nielegalna, to Amazon często bywa publicznie oskarżany o działania tego typu[58]. Tym bardziej przyciągały uwagę mediów

57 K. Cox, *Amazon deletes anti-union listing, watches workers "secret" social groups*, Ars Technica [online], 2.09.2020, https://arstechnica.com/tech-policy/2020/09/amazon-deletes-anti-union-listing-watches-workers-secret-social-groups [dostęp: 4.09.2020]; L.K. Gurley, J. Cox, *Inside Amazon's Secret Program to Spy Onę Workers' Private Facebook Groups*, VICE [online], 2.09.2020, https://www.vice.com/en_us/article/3azegw/amazon-is-spying-on-its-workers-in-closed-facebook-groups-internal-reports-show [dostęp: 4.09.2020].

58 L. Matsakis, *Amazon Deletes Job Posts Seeking Analysts to Track 'Labor Organizing Threats'*, Wired [online], 1.09.2020, https://www.wired.com/story/amazon-deletes-job-posts-labor-organizing-threats [dostęp: 4.09.2020].

takie sformułowania z ogłoszeń jak to, że […] *analityk musi umieć informować i zainteresować kierownictwo wrażliwymi tematami, które są wysoce poufne, w tym o zagrożeniach dla spółki wynikających z powstawania związków zawodowych*. Ujawnienie ogłoszeń rekrutacyjnych zbiegło się w czasie z publikacją raportu poświęconego inwigilacji pracowników przez Amazon[59].

W komentarzach medialnych przeważało zaskoczenie, że Amazon otwarcie przyznaje, iż sam prowadzi działania, które inne podmioty biznesowe zlecają podwykonawcom[60]. Samodzielne rekrutowanie pracowników do pracy wywiadowczej i kontrwywiadowczej – szczególnie antyzwiązkowej – uznano za ewenement. Komentatorzy wyrażali przekonanie, że działania Amazona ze względu na dotychczasową historię firmy i jej kierownictwa są jednak oczywistością. Jeff Bezos w przeszłości stał się ofiarą ataku hakerskiego, który przeprowadzono, jak wynika z doniesień medialnych, na zlecenie saudyjskiego następcy tronu Muhammada ibn Salmana[61]. W związku z tym zasadne miało być podjęcie przez Amazon działań o charakterze kontrwywiadowczym i przeciwdziałanie zagrożeniom ze strony niechętnych firmie lub Bezosowi podmiotów, w tym także przywódców politycznych.

Pewne elementy ogłoszeń wskazują, w jakim stopniu Amazon jest zainteresowany zrozumieniem i kształtowaniem globalnego środowiska bezpieczeństwa. Poszukuje punktów konfliktowych – we własnych strukturach oraz w swoim otoczeniu – i stara się zapobiec konfrontacjom. To właśnie pod takim kątem poszukiwani analitycy wywiadowczy mają przetwarzać dane zebrane przez Amazon. Ogłoszenia sugerują, że w firmie dochodzi do powoływania odpowiednika służby specjalnej. Upraszczając problem, można stwierdzić, że Amazon korzysta ze swojej pozycji rynkowej i zebranych danych, żeby lepiej zrozumieć globalne środowisko bezpieczeństwa i móc albo się do niego dopasować, albo je zmieniać zgodnie ze swoimi potrzebami.

Wszyscy giganci cyfrowi masowo zbierają dane wrażliwe lub dane, które po przetworzeniu za pomocą systemów analitycznych i zestawieniu z innymi danymi mogą się stać wrażliwe[62]. W analizowanym przypadku, w odróżnieniu od innych spółek *big tech*, Amazon tylko otwarcie przyznał, że prowadzi aktywną działalność wywiadowczą i kontrwywiadowczą oraz udostępnia do tych celów swoje systemy analityczne odpowiednim komórkom wewnętrznym. Z analizowanych ogłoszeń wynika, że gigant handlu wysyłkowego i największy dostawca usług chmurowych oczekuje od swoich analityków wywiadowczych umiejętności budowania nowych systemów zautomatyzowanej analizy danych i wykorzystywania systemów już istniejących. Wszystkie te narzędzia można wykorzystywać do celów wywiadowczych i kontrwywiadowczych poprzez analizę danych zebranych w innych częściach firmy.

59 D.A. Hanley, S. Hubbard, *Eyes Everywhere: Amazon's Surveillance Infrastructure and Revitalizing Worker Power*, [online], September 2020, https://static1.squarespace.comstatic/5e449c8c3ef68d752f3e70dc/t/5f4cffea23958d79eae1ab23/1598881772432/Amazon_Report_Final.pdf [dostęp: 9.09.2020].

60 C. Cimpanu, *Amazon is hiring intelligence analysts to watch organized labor, hostile political leaders, more*, ZDNet [online], 1.09.2020, www.zdnet.com/article/amazon-is-hiring-intelligence-analysts-to-watch-organized-labor-hostile-political-leaders-more [dostęp: 9.09.2020].

61 Ibidem; M. Murphy, *Why Jeff Bezos is hiring ex-spooks to keep tabs on his employees*, The Telegraph [online], 2.09.2020, https://www.telegraph.co.uk/technology/2020/09/02/jeff-bezos-hiring-ex-spooks-keep-tabs-employees [dostęp: 9.09.2020].

62 B. Lubarsky, *Re-Identification of 'Anonymized' Data*, „Georgetown Law Technology Review" April 2017, https://georgetownlawtechreview.org/wp-content/uploads/2017/04/Lubarsky-1-GEO.-L.-TECH.-REV.-202.pdf [dostęp: 24.09.2020].

Amazon znany jest z nacisku, jaki kładzie na gromadzenie i analizowanie danych. Mają one służyć lepszemu zrozumieniu decyzji i działań klientów, a dzięki temu zwiększeniu zysków. Ogłoszenia o pracy dla analityków wywiadowczych wskazują, że dane i narzędzia do ich analizy mają być wykorzystywane nie tylko do walki ze związkami zawodowymi oraz innymi przeciwnikami Amazona. Chodzi również o polityków, urzędników oraz obywateli zainteresowanych zmianą regulacji, którym podlega amerykański gigant handlu internetowego. Podobnie zresztą działają również inni giganci cyfrowi, i to nie tylko amerykańscy. W taki sposób działa wiele firm poszukujących dla siebie niszy – także tych, które pracują dla służb specjalnych lub organów ścigania. Najbardziej znanym przykładem jest firma Palantir.

Właściwie wszystkie amerykańskie firmy z sektora *big tech* dążą do zdobywania kontraktów rządowych w USA. Zdają sobie sprawę z tego, że współpraca z instytucjami federalnymi, służbami specjalnymi i siłami zbrojnymi może im ułatwiać obronę, na przykład, przed działaniami antykoncentracyjnymi. Zatrudnianie byłych funkcjonariuszy służb specjalnych i organów ścigania może sprzyjać budowaniu kanałów komunikacyjnych – formalnych i nieformalnych – między spółką a wcześniejszymi miejscami pracy tych osób.

Wnioski

Perspektywą, która pozwala szerzej spojrzeć na analizowaną problematykę, jest proces sekurytyzacji działalności *big tech*. Zgodnie z koncepcją Ole Waevera, ważnego przedstawiciela tzw. szkoły kopenhaskiej, określony problem zostaje poddany procesowi sekurytyzacji, kiedy definiuje się go jako stwarzający zagrożenie dla bezpieczeństwa. Proces ten jest dwustopniowy. Początkowo to przedstawiciele elit w swoich wypowiedziach wskazują, że coś zagraża bezpieczeństwu. Domknięcie procesu sekurytyzacji polega na względnie powszechnym przejęciu tej narracji przez opinię publiczną[63].

W wypadku działalności *big tech* można mówić o globalnej makrosekurytyzacji w sensie zaproponowanym przez innego reprezentanta szkoły kopenhaskiej, Barry'ego Buzana. Wskazywał on, że wcześniej takim procesem objęto rywalizację zimnowojenną w połowie XX wieku oraz islamski terroryzm na początku XXI wieku[64]. W tradycyjnych analizach z zakresu bezpieczeństwa międzynarodowego skupiano się zazwyczaj na roli państw. Po atakach z 11 września 2001 roku uznano potrzebę szerszego uwzględnienia także pozapaństwowych aktorów, takich jak organizacje terrorystyczne. Obecnie pozapaństwowymi aktorami mającymi przemożny wpływ na globalne środowisko bezpieczeństwa stają się giganci technologiczni.

Proces sekurytyzacji problemu działalności *big tech* właśnie się domyka. Wskazuje na to zakończone w październiku 2020 roku postępowanie amerykańskiej parlamentarnej podkomisji ds. ochrony konkurencji, która *expressis verbis* wskazała, że monopol GAFAM zagraża amerykańskiej demokracji[65]. Inny argument na poparcie tezy o makrosekurtyzacji

63 O. Waever, *Securitization and Desecuritization*, w: *On Security*, R. Lipschutz (red.), New York 1995, s. 6.

64 B. Buzan, *The 'War on Terrorism' as the new Macro-Securitization*, Oslo Workshop papers, Oslo, 2006.

65 Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, *Investigation of competition in digital markets*, 2020, https://int.nyt.com/data/documenttools/house-antitrust-report-on-big-tech/b2ec22cf340e1af1/full.pdf [dostęp: 2.11.2020], s. 7.

działalności GAFAM dotyczy kluczowej roli tych podmiotów w rywalizacji chińsko-amerykańskiej, o czym wspominał Eric Schmidt, były szef Google'a, w materiałach ujawnionych przez dziennikarzy[66]. Jako doradca w komisjach doradczych administracji amerykańskiej wskazywał on na wielką rolę amerykańskich firm technologicznych w amerykańskiej infrastrukturze bezpieczeństwa. Próbował przekonywać, że jeśli nie zostaną złagodzone pewne obostrzenia regulacyjne dotyczące konkurencji i prywatności, to amerykańskie firmy nie zdołają konkurować z chińskimi, to zaś może zagrażać amerykańskiemu bezpieczeństwu narodowemu.

Na podstawie rozstrzygnięć teoretycznych i przedstawionego studium przypadku można przyjąć, że działalność *big tech* wpływa na globalne środowisko bezpieczeństwa w trzech wymiarach. Po pierwsze, już sama skala działania biznesowego amerykańskich gigantów technologicznych, w tym bezprecedensowa historycznie koncentracja różnego typu kapitału oraz ciągła ekspansja, istotnie oddziałuje na ład globalny i pośrednio, w sposób niezamierzony, współkształtuje globalne środowisko bezpieczeństwa. Po drugie, giganci technologiczni także w sposób intencjonalny dążą do wywołania wrażenia, że są niezbędni dla utrzymania bezpieczeństwa państwa i że w sytuacjach kryzysowych są w stanie zastąpić je na wybranych polach. W pewnym sensie firmy te w sposób skoordynowany i zamierzony współuczestniczą w procesie sekurytyzacji swojej działalności. Przed skierowanym przeciwko nim działaniom antymonopolowym bronią się, próbując pokazać, że mogą istotnie wspierać również funkcje państw i organizacji międzynarodowych. Sekurytyzacja ich działalności jest prawdopodobnie także instrumentalnie wykorzystywana jako działalnie osłonowe dla kontrowersyjnej działalności biznesowej. Po trzecie, Amazon ogłaszając nabór analityków do swojej komórki o zadaniach służby specjalnej – jak się wydaje przypadkowo – ujawnił wprost swoją wewnętrzną strategię dotyczącą rozpoznawania, analizowania i wpływania na globalne środowisko bezpieczeństwa. Wrodzy liderzy polityczni, niechętni korporacjom transnarodowym lub broniący prawa do prywatności działacze oraz organizatorzy związków zawodowych mają być obserwowani (czy wręcz inwigilowani) przez grupę wyspecjalizowanych pracowników Amazona. Doświadczenie tych ludzi oraz narzędzia, którymi się posługują dzięki zasobom typowym dla kapitalizmu nadzoru, sprawiają, że giganci technologiczni mogą wpływać na warunki globalnego środowiska bezpieczeństwa. Nie tylko ostrzegając przed zagrożeniami, lecz także wskazując, w jaki sposób można je zneutralizować. Trudno określić, jak duże możliwości przewidywania i sterowania zachowaniami ludzi dają narzędzia informatyczne stosowane przez Amazon. Takie pytania muszą sobie stawiać przywódcy polityczni, działacze niechętni gigantom technologicznym oraz inne osoby postrzegane przez nich jako przeciwnicy[67]. ■

66 N. Klein, *How big tech plans to profit from the pandemic*, The Guardian [online], 13.05.2020, https://www.theguardian.com/news/2020/may/13/naomi-klein-how-big-tech-plans-to-profit-from-coronavirus-pandemic [dostęp: 20.05.2020].

67 Warto pamiętać, co na temat programów współpracy wywiadu sygnałowego USA z gigantami technologicznymi ujawnił Edward Snowden. (T.H. Edgar, 2017, *Beyond Snowden. Privacy, Mass Surveillance, and the Struggle to Reform the NSA*, Brookings Institution Press, Washington, D.C.; G. Greenwald, *Snowden. Nigdzie się nie ukryjesz*, Agora, Warszawa 2014; D. Lyon, *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique*, „Big Data & Society" July–December 2014, s. 1–14).

STRESZCZENIE:

W artykule przeanalizowano wpływ działalności amerykańskiego *big tech*, czyli spółek popularnie zwanych GAFAM (Google, Amazon, Facebook, Apple i Microsoft), na globalne środowisko bezpieczeństwa oraz wskazano, w jaki sposób wpływ ten determinuje zjawisko kapitalizmu nadzoru. Rozważono argumentację na poparcie tezy, że spółki z grupy GAFAM nie tylko należą do kluczowych międzynarodowych podmiotów gospodarczych, lecz także ściśle współpracują z państwem, z którego się wywodzą. Z analizy wynika, że wyłaniają się nowi, potężni aktorzy globalnego środowiska bezpieczeństwa. W czasie sytuacji kryzysowych – między innymi pandemii i konfliktów zbrojnych – spółki *big tech* zarówno działają w sferze informacyjnej, jak i stają się centralnymi elementami infrastruktury krytycznej.

SŁOWA KLUCZOWE:

big tech, środowisko bezpieczeństwa, kapitalizm nadzoru, infrastruktura krytyczna, sytuacje kryzysowe

Bibliografia

Brandom R., *Former NSA chief Keith Alexander has joined Amazon's board of directors*, The Verge [online], 9.09.2020, https://www.theverge.com/2020/9/9/21429635/amazon-keith-alexander-board-of-directors-nsa-cyber-command/.

Buzan B., *The 'War on Terrorism' as the new Macro-Securitization*, Oslo Workshop papers, Oslo 2006.

Chong C., *Blockbuster's CEO once passed up a chance to buy Netflix for only $50 million*, Business Insider [online], 17.07.2015, https://www.businessinsider.com/blockbuster-ceo-passed-up-chance-to-buy-netflix-for-50-million-2015-7?r=US&IR=T/.

Cimpanu C., *Amazon is hiring intelligence analysts to watch organized labor, hostile political leaders, more*, ZDNet [online], 1.09.2020, www.zdnet.com/article/amazon-is-hiring-intelligence-analysts-to-watch-organized-labor-hostile-political-leaders-more/.

Corbyn Z., *Facebook experiment boosts US voter turnout*, Nature [online] 12.09.2012, https://www.nature.com/news/facebook-experiment-boosts-us-voter-turnout-1.11401/.

Cox K., *Amazon deletes anti-union listing, watches workers' "secret" social groups*, Ars Technica [online], 2.09.2020, https://arstechnica.com/tech-policy/2020/09/amazon-deletes-anti-union-listing-watches-workers-secret-social-groups/.

Dastin J., *Amazon bars one million products for false coronavirus claims*, Reuters [online], 27.02.2020, https://uk.reuters.com/article/us-china-health-amazon-com/amazon-bars-one-million-products-for-false-coronavirus-claims-idUKKCN-20L2ZH/.

Drabik P., *Amazon nie zamyka swoich magazynów pomimo epidemii*, Radio Zet [online], 26.03.2020, https://biznes.radiozet.pl/News/Covid-19.-Amazon-nie-zamyka-swoich-magazynow.-Dlaczego/.

Edgar T.H., *Beyond Snowden. Privacy, Mass Surveillance, and the Struggle to Reform the NSA*, Brookings Institution Press, Washington, D.C 2017.

Estes A.C., *Amazon Just Broke the Internet*, Gizmodo [online], 28.02.2017, https://gizmodo.com/amazon-just-broke-the-internet-1792827856/.

Executive Order on Addressing the Threat Posed by WeChat, Zarządzenie wykonawcze Prezydenta USA z 6.08.2020, https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/.

Franceschi-Bicchierai L., *Amazon Is Hiring an Intelligence Analyst to Track 'Labor Organizing Threats'*, VICE [online], 1.09.2020, https://www.vice.com/en_us/article/qj4aqw/amazon-hiring-intelligence-analyst-to-track-labor-organizing-threats/.

Ginsberg J. et al., *Detecting influenza epidemics using search engine query data*, „Nature" 2009, Vol. 457, Issue 7233, s. 1012–1014.

Global cloud services market Q2 2020, Canalys [online], 30.07.2020, https://www.canalys.com/newsroom/worldwide-cloud-infrastructure-services-Q2-2020/.

Government launches new drive on coronavirus tests for frontline NHS staff, GOV.UK [online], 27.03.2020, https://www.gov.uk/government/news/government-launches-new-drive-on-coronavirus-tests-for-frontline-nhs-staff/.

Greenwald G., 2014, *Snowden. Nigdzie się nie ukryjesz*, Warszawa 2014.

Guariglia M., *Five Concerns about Amazon Ring's Deals with Police*, Electronic Frontiers Foundation [online], 30.08.2019, eff.org/pl/deeplinks/2019/08/five-concerns-about-amazon-rings-deals-police/.

Gurley L.K., Cox J., *Inside Amazon's Secret Program to Spy Onę Workers' Private Facebook Groups*, VICE [online], 2.09.2020, https://www.vice.com/en_us/article/3azegw/amazon-is-spying-on-its-workers-in-closed-facebook-groups-internal-reports-show/.

Hamilton I.A., *Amazon is reportedly in talks to help deliver COVID-19 tests in the UK*, Business Insider [online], 23.03.2020, https://www.businessinsider.com/amazon-in-talks-to-help-deliver-covid-19-tests-uk-2020-3/.

Hanley D.A., S. Hubbard, *Eyes Everywhere: Amazon's Surveillance Infrastructure and Revitalizing Worker Power*, [online], September 2020, https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/5f4cffea23958d79eae1ab23/1598881772432/Amazon_Report_Final.pdf/.

Harwell D., *Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns*, The Washington Post [online], 28.08.2019, https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/.

Holmes A., *Ilhan Omar and Bernie Sanders are demanding that Amazon come up with a safety plan for workers as online orders soar amid coronavirus*, Business Insider [online], 27.03.2020, https://www.businessinsider.com/ilhan-omar-bernie-sanders-amazon-worker-safety-coronavirus-2020-3/.

JEDI: Why we will continue to protest this politically corrupted contract award, AWS [online], 4.09.2020, https://aws.amazon.com/blogs/publicsector/jedi-why-we-will-continue-protest-politically-corrupted-contract-award/.

Kelley J., *Amazon Ring Must End Its Dangerous Partnerships With Police*, Electronic Frontiers Foundation [online], 10.06.2020, https://www.eff.org/deeplinks/2020/06/amazon-ring-must-end-its-dangerous-partnerships-police/.

Kim E., *Amazon buys smart doorbell maker Ring for a reported $1 billion*, CNBC [online], 27.02.2018, https://www.cnbc.com/2018/02/27/amazon-buys-ring-the-smart-door-bell-maker-it-backed-through-alexa-fund.html/.

Klein N., *How big tech plans to profit from the pandemic*, The Guardian [online], 13.05.2020, https://www.theguardian.com/news/2020/may/13/naomi-klein-how-big-tech-plans-to-profit-from-coronavirus-pandemic/.

Lee D., P. Nilsson, *Amazon auditions to be 'the new Red Cross' in Covid-19 crisis*, 31.03.2020, https://www.ft.com/content/220bf850-726c-11ea-ad98-044200cb277f/.

Lubarsky B., *Re-Identification of 'Anonymized' Data*, „Georgetown Law Technology Review" April 2017, https://georgetownlawtechreview.org/wp-content/uploads/2017/04/Lubarsky-1-GEO.-L.-TECH.-REV.-202.pdf/.

Lyon D., 2014, *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique*, „Big Data & Society" July–December 2014, s. 1–14.

Mandalindan J.P., *Can Amazon handle the coronavirus pressure?,* Protocol [online], 22.03.2020, https://www.protocol.com/amazon-delivery-coronavirus-high-demand/.

Marks G., *Amazon Warehouses Are Accepting Only The Essentials... And Other COVID-19 Small Business Tech News*, Forbes [online], 22.03.2020, https://www.forbes.com/sites/quickerbettertech/2020/03/22/amazon-warehouses-are-accepting-only-the-essentialsand-other-covid-19-small-business-tech-news/#6b8ca46ef678/.

Matsakis L., *Amazon Quietly Removes Some Dubious Coronavirus Books*, Wired [online], 11.03.2020, https://www.wired.com/story/amazon-quietly-removes-coronavirus-books/.

Matsakis L., *Amazon Warehouses Will Now Accept Essential Supplies Only*, Wired [online], 17.03.2020, https://www.wired.com/story/amazon-warehouse-essential-goods-only/.

Matsakis L., *As Covid-19 Spreads, Amazon Tries to Curb Mask Price Gouging*, Wired [online], 25.02.2020, wired.com/story/covid-19-amazon-curb-face-mask-price-gouging/.

Matsakis, L., *Amazon Deletes Job Posts Seeking Analysts to Track 'Labor Organizing Threats'*, Wired [online], 1.09.2020, https://www.wired.com/story/amazon-deletes-job-posts-labor-organizing-threats/.

Metz C., *Amazon's Invasion of the CIA Is a Seismic Shift in Cloud Computing*, Wired [online], 18.06.2013, https://www.wired.com/2013/06/amazon-cia/.

Miles T., *U.N. investigators cite Facebook role in Myanmar crisis*, Reuters [online] 12.03.2018, https://www.reuters.com/article/us-myanmar-rohingya-facebook-idUSKCN1GO2PN/.

Murphy M., *Why Jeff Bezos is hiring ex-spooks to keep tabs on his employees*, The Telegraph [online], 2.09.2020, https://www.telegraph.co.uk/technology/2020/09/02/jeff-bezos-hiring-ex-spooks-keep-tabs-employees/.

Osborne C., *eBay and Amazon are losing the battle against coronavirus profiteering*, ZDNet [online], 25.03.2020, zdnet.com/article/ebay-and-amazon-are-losing-the-battle-against-coronavirus-profiteering/.

Palmer A., *'They're putting us all at risk': What it's like working in Amazon's warehouses during the coronavirus outbreak*, CNBC [online], 26.03.2020, https://www.cnbc.com/2020/03/26/amazon-warehouse-employees-grapple-with-coronavirus-risks.html.

Psathas G., *The Ideal Type in Weber and Schutz*, w: *Explorations of the Life-World. Contributions to Phenomenology (In Cooperation with the Center for Advanced Research in Phenomenology)*, M. Endress, G. Psathas, H. Nasu (red.), Dordrecht 2005, s. 143–169.

Publie A., *Coronavirus: la gronde s'intensifie contre Amazon*, Les Echos [online], 20.03.2020, https://start.lesechos.fr/travailler-mieux/flexibilite-travail/coronavirus-la-gronde-s-intensifie-contre-amazon-17659.php/.

Rubin B.F., *How Ring's Neighbors app is making home security a social thing*, CNET [online], 3.12.2018, https://www.cnet.com/news/how-rings-neighbors-app-is-making-home-security-a-social-thing/.

Stake R.E., *Jakościowe studium przypadku*, w: *Metody badań jakościowych*, N.K. Denzim, Y.S. Lincoln (red.), Warszawa 2009, t. 1, s. 623–654.

Stake R.E., *Studium przypadku*, w: *Ewaluacja w edukacji*, L. Korporowicz (red.), Warszawa 1997, s. 120–143.

Stone B., *The Everything store*, New York 2013.

Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, *Investigation of competition in digital markets*, 2020, https://int.nyt.com/data/documenttools/house-antitrust-report-on-big-tech/b2ec22cf340e1af1/full.pdf/.

Sumagay Say L. *Jeff Bezos Says Tech Shouldn't Turn Against the Federal Government*, Government Technology [online], 17.10.2018, https://www.govtech.com/civic/Jeff-Bezos-Says-Tech-Shouldnt-Turn-Against-the-Federal-Government.html/.

Sun D., *More than $11 million in grants available for small business, nonprofits impacted by COVID-19*, [online], 12.03.2020, kiro7.com/news/local/more-than-11-million-grants-available-small-business-nonprofits-impacted-by-covid-19/MFJ5SRSRARAKHGJJA6JS7FDNYI/.

Szalacha-Jarmużek J., *Instrumentarium globalnego panowania. O podmiotowych aspektach globalizacji*, Poznań 2013.

Tang S., *A Systemic Theory of the Security Environment*, „Journal of Strategic Studies" 2004 No 27, s. 1–34.

Tomes R.R., *Socio-Cultural Intelligence and National Security*, „Parameters" 2015, Vol. 45 No. 2.

Transcript of Mark Zuckerberg's Senate hearing, The Washington Post [online], 11.04.2018, https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/.

United States Government Accountability Office, *Decision*, 6.06.2013, https://www.gao.gov/assets/660/655241.pdf/.

Waever O., *Securitization and Desecuritization*, w: *On Security*, R. Lipschutz (red.), New York 1995.

Wakefield J., *Amazon withdraws job adverts for union 'spies'*, BBC News [online], 3.09.2020, www.bbc.com/news/technology-53998201/.

Waszewski J., *„Nie ukryjesz się". Konsekwencje synergii big data, mediów społecznościowych i neuronauki* [w druku].

Wong J.C., *'The US of Amazon': how the coronavirus has created a governance vacuum the tech giant is quickly filling*, The Guardian [online], 24.03.2020, theguardian.com/technology/commentisfree/2020/mar/24/the-us-of-amazon-how-the-coronavirus-has-created-a-governance-vacuum-the-tech-giant-is-quickly-filling/.

Yin R.K., *Case Study Research. Design and Methods*, Londyn 2009.

Zuboff S., *The Age of Surveillance Capitalism. The Fight for the Future at the New Frontier of Power*, London 2019.

Article history: Received: 20.11.2020 ; Reviewed: 29.11.2020; Accepted: 22.12.2020

DOI: 10.5604/01.3001.0014.6159

Corresponding author: Maciej Gurtowski, PhD, War Studies University (ASzWoj), Warsaw, Poland; ORCID:0000-0002-2990-9088; e-mail: m.gurtowski@akademia.mil.pl

Jan Waszewski, PhD, War Studies University (ASzWoj), Warsaw, Poland; ORCID:0000-0002-7370-3714; e-mail: j.waszewski@akademia.mil.pl

Cite this article as: Maciej Gurtowski, PhD; Jan Waszewski, PhD, "Big Tech's Influence on Global Security Environment. The Case of Amazon.com". bellona quart. 2020(3): 37–56

Policy: The content of the journal is circulated on the basis of the Open Access which means free and limitless access to scientific data.

Competing interests: The authors declare that they have no competing interests.

Table of content URL: https://kwartalnikbellona.com/issue/12943

Author's bio: Maciej Gurtowski, PhD
PhD in Social Sciences in sociology. He works at the War Studies University (ASzWoj) Centre for Security Research in Warsaw. He's an expert in security at the Jagiellonian Club's Center for Analysis.

Jan Waszewski, PhD
PhD in Social Sciences in sociology. He works at the War Studies University (ASzWoj) Centre for Security Research in Warsaw. He authored the PhD thesis on privacy in the context of new social control techniques.

THE BELLONA QUARTERLY ISSN: 1897-7065 | E-ISSN: 2719-3853

KWARTALNIK BELLONA

Przeciwdziałanie zagrożeniom w sieciach i systemach teleinformatycznych. Uwagi o działalności ABW i CSIRT

dr hab. Maciej Siwicki, LL.M., prof. UMK

ORCID: 0000-0002-3120-0211
e-mail: msiwicki@umk.pl
Wydział Nauk o Polityce i Bezpieczeństwie Uniwersytetu Mikołaja Kopernika w Toruniu

ABSTRACT:

The necessity of comprehensive and multifaceted protection of electronically processed information is beyond doubt. Despite the fact that new technical and software solutions are systematically improve in security systems, the number of attacks aimed at unlawful access , disrupting automatic processing or preventing access by authorized persons continues to grow at an alarming rate. There are also numerous attacks on a technical device used for automatic processing, collection or transmission of IT data. In response to the above-mentioned challenges, many countries decided to establish special units to prosecute perpetrators of such crimes. Some countries, due to the frequent linking of attacks from the territory of another country, also decided to use intelligence services for this purpose.

This study is devoted to the answer the question whether the model of cyberspace security system organization adopted in Poland properly provides the relevant services with the appropriate competences enabling quick and effective counteracting of threats and incidents. Due to the limited framework, this study focuses on the activities of the Internal Security Agency and Computer Security Incident Response Teams.

KEYWORDS:

cybersecurity, critical infrastructure, ABW, CSRIT, cybercrime

Wstęp

Działalność przestępczą w cyberprzestrzeni podejmują nie tylko pospolici przestępcy czy zorganizowane grupy i organizacje przestępcze, lecz także służby wywiadowcze, które pozyskują informacje w celu sabotowania i destabilizowania innych państw. Według niemieckiego Federalnego Ministerstwa Spraw Wewnętrznych (Bundesministerium des Innern) tego rodzaju działania prowadziły rosyjskie służby wywiadowcze w czasie konfliktu na Ukrainie. Także chińskie i irańskie służby wywiadowcze przeprowadzają ataki w celu szpiegowania innych państw. Od 2005 roku niemieckie agencje rządowe, firmy oraz instytucje badawcze były szpiegowanie za pomocą złośliwego oprogramowania Uroburos (również Snake lub Turla), które pozyskiwało informacje ważne z punktu widzenia innego państwa, dotyczące między innymi technologii energetycznej, rentgenowskiej i nuklearnej, technologii pomiarowej, emisji gazu czy badań w kosmosie[1]. Oprogramowanie to zostało wykorzystane również w maju 2016 roku do przeprowadzenia ataku na berneńską grupę zbrojeniową i technologiczną RUAG Holding AG, z której pozyskano ponad 23 GB informacji[2]. W połowie czerwca 2016 roku w Stanach Zjednoczonych przeprowadzono atak na sieć Demokratycznego Komitetu Narodowego (Democratic National Committee – DNC) Partii Demokratycznej, w wyniku którego pozyskano informacje z ponad 19 tys. wewnętrznych e-maili. Opublikowała je później witryna WikiLeaks[3]. Podobnych ataków było oczywiście więcej[4].

Skuteczne przeciwdziałanie zagrożeniom związanym z cyberprzestępczością wymaga znacznego zaangażowania państwa i jego służb specjalnych. Pojawia się jednak pytanie, jaki wariant działania w tym obszarze będzie najskuteczniejszy: czy wariant zdecentralizowany (rozproszony), polegający na wykorzystaniu już istniejących podmiotów i instytucji przez zwiększenie ich kompetencji w dziedzinie ochrony cyberprzestrzeni, czy też wariant scentralizowany, zakładający powołanie nowego podmiotu, który skupiałby funkcje zarówno koordynujące, jak i wykonawcze.

W niniejszej pracy skoncentrowano się głównie na działalności organów państwa powołanych do ochrony cyberbezpieczeństwa, w tym w szczególności na Agencji Bezpieczeństwa Wewnętrznego oraz Zespołach Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzonych przez ministra obrony narodowej (CSIRT MON), szefa Agencji Bezpieczeństwa Wewnętrznego (CSIRT GOV) oraz Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (CSIRT NASK).

1 *Verfassungsschutzbericht 2016*, Bundesministerium des Innern [online], https://www.verfassungsschutz.de/download/vsbericht-2016.pdf [dostęp: 5.11.2019].

2 *Cyber attack on RUAG: major damage averted*, RUAG [online], 12.05.2016, https://www.ruag.com/en/news/cyber-attack-ruag-major-damage-averted [dostęp: 5.11.2019].

3 A. Parlapiano, *Cyberattack on democratic politicians DNC*, „The New York Times" [online], 16.08.2016, https://www.nytimes.com/interactive/2016/08/16/us/politics/cyberattack-on-democratic-politicians-dnc.html [dostęp: 5.11.2019].

4 Vide: *Verfassungsschutzbericht 2018*, Bundesministerium des Innern [online], https://www.verfassungsschutz.de/download/vsbericht-2018.pdf [dostęp: 5.11.2019].

Przegląd literatury

W literaturze przedmiotu problematyka działalności służb specjalnych ukierunkowanej na przeciwdziałanie cyberprzestępczości nie znajduje szerszego odzwierciedlenia. Większość autorów analizuje działalność ABW w kontekście statusu służb specjalnych i ich funkcjonariuszy[5], zadań i uprawnień tych służb[6] oraz podejmowanych przez nie konkretnych działań w celu wyeliminowania określonych zagrożeń[7]. Cześć autorów koncentruje uwagę na poszczególnych zagrożeniach internetowych i w znikomym stopniu odnosi się do roli Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego[8]. Tematyka poruszona w niniejszym opracowaniu zachęca więc do dalszych badań i analiz.

Metodologia

W trakcie badań zastosowano metody właściwe dla nauk prawnych i nauk o bezpieczeństwie. Jako podstawową metodę badawczą przyjęto analizę formalno-dogmatyczną. Przeanalizowano wybrane regulacje normatywne oraz dostępną literaturę przedmiotu. W badaniach nad obowiązującymi przepisami odwołano się także do metody prawnoporównawczej.

Wyniki analizy i dyskusja

Agencja Bezpieczeństwa Wewnętrznego i Agencja Wywiadu

Służby wywiadowcze wielu państw wykorzystują sieć nie tylko do zbierania dowodów przestępstw czy rozwijania współpracy międzynarodowej, lecz także do masowego zbierania wszelkich przydatnych informacji. Krótko po wydarzeniach z 11 września Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności (Defense Advanced Research Projects Agency – DARPA) amerykańskiego Departamentu Obrony rozpoczęła projekt Total Information Awareness, którego celem jest gromadzenie i pozyskiwanie

5 Vide: M. Liwo, *Status służb mundurowych i funkcjonariuszy w nich zatrudnionych*, Warszawa 2012; K. Walczuk, M. Bożek, *Konstytucyjne i ustawowe uwarunkowania organizacji i funkcjonowania Agencji Bezpieczeństwa Wewnętrznego*, Siedlce 2015, s. 113.

6 Vide: *Poczucie bezpieczeństwa obywateli w Polsce. Identyfikacja i przeciwdziałanie współczesnym zagrożeniom*, Guzik-Makaruk Ewa Monika (red.),Warszawa 2011; M. Bożek, *Zwalczanie przestępstw jako ustawowe zadanie Agencji Bezpieczeństwa Wewnętrznego. Stan obecny i postulaty de lege ferenda*, „Studia Iuridica Lublinensia" 2015 Vol. XXIV, t. 1, s. 35–66; P. Herbowski, *Pozyskanie tajnego współpracownika przez służby kontrwywiadowcze na podstawie materiałów obciążających — rozważania o sensie instytucji*, „Nowa Kodyfikacja Prawa Karnego" 2019 nr 51, s. 83–102; M. Białuński, *Odstąpienie od obowiązku zawiadomienia prokuratora o przestępstwie – analiza nowego uprawnienia Szefa Agencji Bezpieczeństwa Wewnętrznego*, „Palestra" 2018, nr 3, s. 72–80.

7 Vide: G. Materna, *Zmowy przetargowe w prawie ochrony konkurencji i prawie karnym*, Warszawa 2016; P. Chlebowicz, *Nielegalny handel bronią*, Warszawa 2015; J.W. Wójcik, *Przeciwdziałanie przestępczości zorganizowanej. Zagadnienia prawne, kryminologiczne i kryminalistyczne*, Warszawa 2011; R. Lizak, *Kontrolowane przyjęcie lub wręczenie korzyści majątkowej*, „Wojskowy Przegląd Prawniczy" 2011 nr 1, s. 27–42; M.R. Tużnik, *Udział Agencji Bezpieczeństwa Wewnętrznego w postępowaniu karnym skarbowym*, „Studia Prawnicze i Administracyjne" 2018 nr 24(2), s. 57–62.

8 Vide: K. Czaplicki, A. Gryszczyńska, G. Szpor, *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019; A. Szkurłat, *Kompetencje Prezesa UODO w zakresie cyberbezpieczeństwa w świetle polskich i unijnych regulacji prawnych*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2020 nr 2, s. 54–60.

informacji o społeczeństwie amerykańskim w celu identyfikacji terrorystów. Gromadzone są między innymi dane telefoniczne, bankowe, dokumentacja medyczna oraz dane edukacyjne i podróżne[9]. Również inne państwa w celu ochrony przed cyberatakami wprowadzają rozwiązania umożliwiające masową inwigilację użytkowników w sieci. Na przykład w Rosji tego rodzaju regulacje zostały przyjęte w listopadzie 2019 roku[10]. Konieczność pozyskiwania w sieciach teleinformatycznych informacji i ich gromadzenia przez organy ścigania raczej nie budzi wątpliwości. Trzeba jednak zapytać o podstawy prawne takiej działalności oraz o to, jakie służby powinny mieć kompetencje w tym zakresie.

Do zadań Agencji Wywiadu wymienionych w *Ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j. DzU z 2018 r. poz. 2387), zgodnie z art. 5, należy: […] *rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa* (ust. 1 pkt 1). Ponadto: rozpoznawanie, zapobieganie i wykrywanie przestępstw szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa (ust. 1 pkt 2). Wśród zadań ABW wymieniono także […] *rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa, systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych* […] (ust. 1 pkt 2a). Jednocześnie podkreślono, że poza granicami Rzeczypospolitej Polskiej ABW może prowadzić działania na terytorium innego państwa wyłącznie w zakresie wykonywania zadań określonych w ust. 1 pkt 2.

W swojej działalności ABW może uzyskiwać dane niestanowiące treści odpowiednio: przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w art. 180c i art. 180d *Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne* (DzU z 2018 r. poz. 1954), w art. 82 ust. 1 pkt 1 *Ustawy z dnia 23 listopada 2012 r. Prawo pocztowe* (DzU z 2017 r. poz. 1481 oraz z 2018 r. poz. 106, 138, 650, 1118 i 1629), w art. 18 ust. 1–5 *Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (DzU z 2017 r. poz. 1219 oraz z 2018 r. poz. 650), a także może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

Pozyskiwanie danych drogą monitorowania listów, poczty czy też telekomunikacji przez służby wywiadowcze musi wynikać z wykonywania obowiązków ustawowych w celu ochrony przed zagrożeniami bezpieczeństwa wewnętrznego państwa oraz jego porządku konstytucyjnego, w tym także przed zagrożeniami cybernetycznymi. Wymaga to każdorazowo uzasadnienia konieczności przetwarzania i gromadzenia takich danych oraz ich związku z prowadzonym postępowaniem. Wynika to z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji RP, w którym stwierdza się, że […] *władze publiczne nie mogą pozy-*

9 *More about Department of Defense/NSA spying*, ACLU [online], https://www.aclu.org/other/more-about-department-defensensa-spying [dostęp: 5.11.2019].

10 Laty, *Rosja wprowadza cenzurę internetu*, GRY – Online.pl [online], 4.11.2019, https://www.gry-online.pl/hardware/rosja-wprowadza-cenzure-internetu/z11cf1f [4.11.2019].

skiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

W kontekście przytoczonych regulacji pojawia się pytanie, czy aktywność ABW poza granicami państwa powinna obejmować także czynności operacyjne określane jako cyberobrona (Cyber Defence), polegające między innymi na zbieraniu strategicznych informacji związanych z monitorowaniem aktywności międzynarodowych grup terrorystycznych oraz przeciwdziałaniem cyberatakom na infrastrukturę krytyczną, w tym w szczególności za pomocą złośliwego oprogramowania lub innych podobnie szkodliwych technologii (włamania na serwery rządowe w celu manipulowania informacjami tam gromadzonymi i przetwarzanymi bądź dezinformacji). Na gruncie polskiego ustawodawstwa uprawnienia ABW w tym zakresie są jednak ograniczone do rozpoznawania, zapobiegania i wykrywania przestępstw szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa.

W tej kategorii znajdują się działania obejmujące cyberterroryzm, definiowany w literaturze przedmiotu jako bezprawny atak lub groźba ataku na komputery, sieci lub systemy informacyjne, będący rezultatem działań grup subnarodowych, podmiotów niepaństwowych bądź obcych służb specjalnych, w celu zastraszenia albo wymuszenia na rządzie lub społeczeństwie danego kraju spełnienia daleko idących żądań polityczno-społecznych[11]. Do kategorii przestępstw godzących w bezpieczeństwo państwa ściganych przez ABW zalicza się także wszelkiego rodzaju kodeksowe i pozakodeksowe przestępstwa, których przedmiotem ochrony jest bezpieczeństwo państwa[12]. Są to przede wszystkim przestępstwa przeciwko Rzeczypospolitej Polskiej wymienione w rozdziale XVII kodeksu karnego, czyli wszelkie działania skierowane przeciwko niepodległemu bytowi i suwerenności państwa oraz porządkowi publicznemu. Czy – i ewentualnie w jakim zakresie – będzie to dotyczyło także przestępstw godzących w bezpieczeństwo systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych czy też infrastruktury krytycznej, istotnych z punktu widzenia ciągłości funkcjonowania państwa? Przeciwko takiej możliwości przemawia fakt, że art. 5 ust. 1 pkt 2 o tym elemencie w ogóle nie wspomina, ustawodawca zaś wyraźnie tę kategorię zagrożeń umieścił w osobnym punkcie – 2a, co stanowi poważny błąd.

Artykuł 79 *Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*[13] (t.j. DzU z 2020 r. poz. 1369.) dodał do ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu art. 32aa, który nałożył na ABW obowiązek wdrażania u właścicieli, posiadaczy samoistnych i posiadaczy zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, zwany systemem ostrzegania. Do obowiązków ABW należy także prowadzenie takiego systemu i koordynowanie jego funkcjonowania.

11 A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm jako nowe zagrożenie dla bezpieczeństwa międzynarodowego w dobie globalizacji*, w: *Terroryzm w świecie współczesnym*, E. Haliżak (red.), Warszawa 2004, s. 324.

12 K. Walczuk, M. Bożek, *Konstytucyjne i ustawowe uwarunkowania organizacji i funkcjonowania Agencji Bezpieczeństwa Wewnętrznego*, Siedlce 2015, s. 113.

13 Dalej: u.KSC.

Jednocześnie podmioty wymienione w tym przepisie zostały zobowiązane do przystąpienia do systemu ostrzegania oraz przekazania ABW informacji umożliwiających wdrożenie takiego systemu.

Ponieważ art. 32aa odnosi się jedynie do zdarzeń o charakterze terrorystycznym, przepis ten nie będzie dotyczył przypadków ataków, które zostaną podjęte nie w celu zastraszenia danej grupy ludności i wymuszenia na niej lub na państwie określonych ustępstw, lecz w innym celu, na przykład bezprawnego ujawnienia lub wykorzystania informacji niejawnych, godzących w podstawy ekonomiczne państwa, w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa.

ABW podejmując decyzję o wydaniu ostrzeżenia użytkownikom IT, musi dokonać oceny uwzględniającej różnego rodzaju interesy (interes publiczny, prywatny, dobro służby itp.), w tym także te wynikające z obowiązku dyskrecji. Przedmiotowe ograniczenie jedynie do zdarzeń o charakterze terrorystycznym budzi jednak wątpliwości. Wynikają one głównie z faktu, że na gruncie międzynarodowym brakuje globalnej definicji terroryzmu. Oprócz wątpliwości terminologicznych pojawia się pytanie o podstawy takiego ograniczenia. To ABW powinna ocenić, czy wydanie konkretnego ostrzeżenia jest konieczne dla ochrony bezpieczeństwa wewnętrznego państwa oraz jego porządku konstytucyjnego. Także ABW, uwzględniając różne interesy, może wydać ostrzeżenie w odpowiedniej formie czy rodzaju, z dołączeniem stosowanych zaleceń.

Przeciwdziałanie międzynarodowej cyberprzestępczości, w tym tzw. „kampaniom" obejmującym ataki jeden po drugim na kilka państw, oraz rozwijanie współpracy międzynarodowej przez ABW wymaga *de lege ferend*a objęcia zakresem przepisu art. 5 ust. 3 także pkt 2a. Zasadne jest również rozszerzenie zakresu działania ABW – powinna ona nie tylko rozpoznawać, zapobiegać i zwalczać, lecz także ostrzegać o zagrożeniach i bezpośrednio brać udział w tworzeniu skutecznej cyberobrony, w tym w zacieśnianiu współpracy z innymi podmiotami odpowiedzialnym za bezpieczeństwo sieci i systemów teleinformatycznych.

Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego

Dyrektywa NIS zobowiązuje państwa członkowskie do wyposażenia swoich organów odpowiedzialnych za bezpieczeństwo systemów i sieci informatycznych w odpowiednie instrumenty *zarówno pod względem zdolności technicznych, jak i możliwości organizacyjnych*, pozwalające na *zapobieganie incydentom i ryzykom dotyczącym sieci i systemów informatycznych*[14]. Jednocześnie podkreślono, że ze względu na znaczenie współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa CSIRT powinny mieć *możliwość uczestniczenia w międzynarodowych sieciach współpracy, niezależnie od współpracy w ramach sieci CSIRT ustanowionej na mocy* […] *dyrektywy*[15]. Co oczywiste, ochrona ta powinna wykraczać poza kontrolę z rekomendacjami przewidzianymi w ustawie o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu.

14 Pkt 34 *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.* DzU UE L 194/1 z 19.7.2016.

15 Ibidem.

W celu ułatwienia współpracy międzynarodowej organy właściwe do spraw cyberbezpieczeństwa mogą współdziałać z właściwymi organami państw członkowskich Unii Europejskiej za pośrednictwem pojedynczego punktu kontaktowego (art. 42 ustawy), w tym mogą wymieniać z nimi także informacje o incydentach poważnych (art. 26 ust. 1 pkt 11 i 12 ustawy). Operatorzy usług kluczowych są zobowiązani do notyfikacji incydentu poważnego oraz określenia zasięgu geograficznego obszaru, którego ten incydent dotyczy (art. 12 ust. 1 pkt 4).

Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV, oprócz współpracy operacyjnej z innymi państwami członkowskimi, należy także reagowanie na zgłoszone incydenty (art. 26 ust. 3 pkt 5 ustawy). W celu uniknięcia sporów kompetencyjnych ustawodawca określił właściwość poszczególnych zespołów, w tym wskazał katalogi obsługiwanych podmiotów, tworzących krajowy system cyberbezpieczeństwa. Decyzja co do tego, czy określony zespół podejmie działania oraz jaki będą one miały charakter, jest decyzją uznaniową tego organu. Na gruncie tej ustawy obowiązek współpracy podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV został nałożony na operatorów usług kluczowych (art. 11 ust. 1 pkt 5 u.KSC) Obowiązku współpracy nie przewidziano w art. 18 ust. 1 u.KSC w odniesieniu do dostawcy usługi cyfrowej. Organy CSIRT będą jednak miały ogólne obowiązki związane z ochroną danych osobowych (użytkowników, pracowników operatora) czy poufności (tajemnica przedsiębiorstwa, handlowa, ryzyko utraty reputacji i poniesienia szkód handlowych) zgodnie z obowiązującymi przepisami.

Reagowanie na incydent będzie obejmowało wiele czynności, między innymi: jego weryfikację, analizę, klasyfikację, udokumentowanie, politykę informacyjną (kontakt z użytkownikami, wymiana informacji z innymi CSIRT itp.), badanie urządzenia informatycznego lub oprogramowania w celu wykrycia przyczyny i usunięcia ewentualnych luk oraz podatności, koordynowanie obsługi incydentów, rozliczenie odpowiedzialności, uszczelnienie systemów, a także inne czynności związane ze zwalczaniem zagrożenia. Ustawodawca w art. 26 ust. 3 pkt 5 ustawy nie wskazał jednak konkretnie tych czynności ani nie określił ich zakresu. Brak takiej regulacji stanowi naruszenie obowiązku państwa zapewnienia bezpieczeństwa prawnego swoim obywatelom. Operator nie zna bowiem w pełni przesłanek działania tych organów. Nie wie, za jakiego rodzaju czynności związane z reagowaniem na incydent poniesie koszty, zwłaszcza gdy będzie to wymagało zaangażowania wykwalifikowanej kadry z zewnątrz. Oprócz postulatu *de lege ferenda* dotyczącego uregulowania tej kwestii celowe byłoby przyjęcie wymogu niezbędności podjęcia określonych czynności w celu przywrócenia bezpieczeństwa lub funkcjonalności danego systemu informatycznego. Wydaje się, że za pierwsze działania podjęte przez CSIRT w celu ograniczenia szkód i zapewnienia działania awaryjnego operator nie powinien ponosić żadnych opłat ani wydatków. Kwestia ta musi być jednak rozstrzygnięta przez ustawodawcę.

Art. 26 ust. 3 u.KSC wśród zadań CSIRT MON wymienia także wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa (pkt 4). Takie same możliwości wydawania komunikatów przewidziane zostały dla CSIRT GOV i CSIRT NASK. Ostrzeżenia, które mogą być wydawane przez te podmioty, nie są ograniczone tylko do

zdarzeń o charakterze terrorystycznym, mogą obejmować między innymi informacje o utracie danych lub nieautoryzowanym dostępie do danych czy też o innych zdarzeniach, szczególnie w przypadkach, gdy takie informacje mogą przyczynić się do ograniczenia szkód powstałych w wyniku ataku (np. o uzyskaniu przez sprawcę danych dostępowych do konta użytkownika). Ustawodawca nałożył na te podmioty obowiązek informacyjny, ale nie określił, w jaki sposób i w jakiej formie powinien on być spełniony. Jest oczywiste, że organy wypełniając ten obowiązek muszą chronić bezpieczeństwo i interesy państwa, organów publicznych, przedsiębiorców lub/i osób fizycznych oraz w odpowiedni sposób doradzać użytkownikom IT, jednocześnie jednak muszą uwzględniać poufność informacji przekazanych w ostrzeżeniu.

Ostrzeżenia powinny być wydawane jedynie wówczas, gdy dany zespół ma odpowiednią wiedzę o incydencie. Dlatego operatorzy są zobowiązani do zgłaszania incydentów poważnych (art. 11 ust. 1 pkt 4 u.KSC), a dostawcy usług – incydentów istotnych (art. 18 ust. 1 pkt 4 u.KSC). Dodatkowo właściwy organ lub CSIRT został zobowiązany do poinformowania innego państwa członkowskiego o incydencie, który go dotyczy (art. 28 ustawy oraz art. 14 ust. 5 dyrektywy NIS). Informacje te mogą być pozyskiwane także w wyniku współpracy z innymi podmiotami – czy to w ramach administracyjnej sieci CERT, centrów cyberobrony, czy współpracy międzynarodowej (np. SISSDeN[16], system ARAKIS Enterprise 2.0[17], n6 – network security incident exchange[18]).

Stosowanie do art. 33. ust 1 u.KSC CSIRT MON, CSIRT NASK lub CSIRT GOV może przeprowadzić badanie urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, tym samym może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. W wypadku identyfikacji podatności CSIRT składa do pełnomocnika do spraw cyberbezpieczeństwa wniosek dotyczący rekomendacji. Pełnomocnik po uzyskaniu opinii kolegium wydaje, zmienia lub odwołuje rekomendacje. Jeżeli rekomendacje nie zostaną uwzględnione, to informację o tym pełnomocnik przekazuje organowi sprawującemu nadzór nad podmiotem. Rekomendacje wiążą wszystkie podmioty będące w krajowym systemie cyberbezpieczeństwa. I choć wskazany przepis nie przewiduje żadnej sankcji za nieuwzględnienie rekomendacji, to fakt jej nieuwzględnienia może stanowić podstawę do przeprowadzenia kontroli u operatora usługi kluczowej w celu potwierdzenia istnienia podatności. W takim wypadku za niewypełnienie obowiązku jej usunięcia (art. 11 ust. 1 pkt 6 u.KSC) może być nałożona kara finansowa do 20 tys. zł za każdą nieusuniętą podatność (art. 73 ust. 3 pkt 8 u.KSC). Warto nadmienić, że art. 32e (wydawanie rekomendacji) ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu daje szefowi ABW możliwość wydania rekomendacji zmierzającej do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych w celu zapewnienia ich integralności, poufności, rozliczalności i dostępności.

16 https://sissden.eu/.

17 https://www.arakis.pl/.

18 https://n6.cert.pl/.

Wskazane przepisy nie przewidują możliwości badania urządzeń lub oprogramowania u ich producenta, a jedynie u podmiotów krajowego systemu cyberbezpieczeństwa. Nie został także przewidziany żaden system ani schemat certyfikacji tych produktów, który mógłby ułatwić podejmowanie decyzji co do instalacji i wdrożenia odpowiedniego oprogramowania lub/i sprzętu IT. Obowiązek certyfikacji został przewidziany tylko w stosunku do środków ochrony elektromagnetycznej przeznaczonych do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej (art. 50 *Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,* t.j. 15.3.2019 r., DzU z 2019 r. poz. 742). Wprowadzenie certyfikacji także w odniesieniu do innych urządzeń byłoby korzystne dla producentów, którzy chcieliby stworzyć nowe rozwiązania lub wprowadzić określony towar czy usługę na polski rynek. Takie badania mogłyby się stać skutecznym narzędziem cyberobrony. System certyfikacji powinien być adekwatny do zagrożeń, a także uwzględniać specyfikę poszczególnych grup podmiotów odpowiedzialnych za cyberbezpieczeństwo (uwzględniać wielkość podmiotu, jego zadania i obowiązki).

Oczywiście sprzęt i oprogramowanie są objęte przepisami dotyczącymi odpowiedzialności za produkt. Jeżeli w wyniku błędów lub usterek powstanie szkoda, z roszczeniami będzie można wystąpić na ogólnych zasadach. Na przykład podstawę roszczeń z tytułu odszkodowania może stanowić art. 471 kodeksu cywilnego (t.j. DzU z 2020 r. poz. 1740), normujący tzw. odpowiedzialność kontraktową w związku z niewykonaniem lub nienależytym wykonaniem zobowiązania umownego.

Wnioski

W kontekście dotychczasowych rozważań pojawiają się pytania o to, czy w wypadku złożonych ataków szybka reakcja nie będzie utrudniona ze względu na możliwe spory kompetencyjne bądź różnego rodzaju trudności wynikające z odmiennego funkcjonowania poszczególnych podmiotów (różne uprawnienia, zasoby budżetowe, doświadczenie, wiedza, zakres współpracy międzynarodowej). W odniesieniu do złożonych ataków skierowanych na kilka podmiotów problemy mogą się pojawić już na etapie wydania ostrzeżenia lub poinformowania społeczeństwa. Liczne wątpliwości budzi także samo określenie, jakie organy i w jakim zakresie są uprawnione do podjęcia działań w celu przywrócenia bezpieczeństwa lub funkcjonalności danego systemu informatycznego po ataku. Trudności mogą pojawić się również podczas oceny charakteru ataku: kto powinien ocenić, czy zagrożenie ma charakter terrorystyczny, czy zagraża bezpieczeństwu wewnętrznemu państwa oraz jego porządkowi konstytucyjnemu, czy może stanowi zagrożenie godzące w bezpieczeństwo systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych, istotnych z punktu widzenia ciągłości funkcjonowania państwa, a może podlega CSIRT MON, bo zostało zgłoszone przez podmioty wskazane w art. 26 ust. 5 u.KSC. Kolejne wątpliwości – ze względu na brak jednolitego systemu certyfikacji – dotyczyć będą tego, jakie rozwiązania techniczne i programowe uznaje się na danym poziomie za bezpieczne i kto o tym decyduje. Problemy te wynikają nie tylko ze złożoności ataków cyberprzestępców, lecz także z tego, że obecnie wiele podmiotów prowadzi działalność na kilku obszarach, podlegających kompetencjom różnych podmiotów.

Przyjęty na gruncie polskiego ustawodawstwa wariant zdecentralizowany obejmuje wykorzystanie istniejących podmiotów odpowiedzialnych za ochronę cyberprzestrzeni. Nie zakłada centralizacji zadań ani przez powołanie jednej instytucji koordynującej, na przykład w postaci jednego ministerstwa (np. Ministerstwa Spraw Wewnętrznych), ani też jednej nadrzędnej instytucji, która reagowałaby w warstwie operacyjnej. Ten model może być skuteczny, jeśli wyraźnie zostaną określone kompetencje poszczególnych organów odpowiedzialnych za przeciwdziałanie cyberprzestępczości. Pozytywnym aspektem decentralizacji jest możliwość lepszego przystosowania się (specjalizacji) do potrzeb związanych z przeciwdziałaniem określonemu zagrożeniu (szybsza reakcja, lepsze zarządzanie). Natomiast wadą takiego rozwiązania jest większe obciążenie poziomego przepływu informacji między poszczególnymi jednostkami oraz brak klarownego rozdziału kompetencji w wypadku złożonych zagrożeń, co może utrudniać szybkie i właściwe określenie źródła oraz celu zagrożenia, tym samym jego zwalczanie.

Za zasadne należy uznać powołanie instytucji koordynującej[19], która zapewni zarówno odpowiednie funkcjonowanie systemu w warstwie strategiczno-legislacyjnej, jak i właściwe koordynowanie działań w warstwie operacyjnej. W tym wypadku pojawiają się jednak pytania o to, jaką część uprawnień decyzyjnych przenieść na niższe szczeble kierownicze, w jaki sposób w danych warunkach kontrolować niższe szczeble oraz w jakim zakresie dokonać przesunięć w dół hierarchii. ■

19 W tym kontekście należy w pełni zgodzić się z rekomendacją przygotowaną przez Naukową i Akademicką Sieć Komputerową instytutu badawczego (NASK) z zespołem CERT Polska funkcjonującym w ramach NASK. Vide: *System bezpieczeństwa cyberprzestrzeni RP*, Warszawa 2015, https://www.cert.pl/wp-content/uploads/2015/12/nask_rekomendacja.pdf [dostęp: 18.12.2019].

STRESZCZENIE:

Konieczność kompleksowej i wielopłaszczyznowej ochrony informacji przetwarzanej elektronicznie nie budzi wątpliwości. Mimo wprowadzania różnorodnych rozwiązań technicznych i programowych służących zapewnieniu bezpieczeństwa informatycznego wciąż zwiększa się liczba zamachów mających na celu bezprawne uzyskanie dostępu do informacji, zakłócenie jej automatycznego przetwarzania czy też uniemożliwienie dostępu do niej osobom uprawnionym. Nasilają się także ataki na urządzenia do automatycznego przetwarzania, gromadzenia i przekazywania danych informatycznych. Dlatego wiele państw tworzy specjalne jednostki, a nawet wykorzystuje służby wywiadowcze do ścigania sprawców takich przestępstw.

W artykule podjęto próbę odpowiedzi na pytanie, czy przyjęty w Polsce model organizacji systemu bezpieczeństwa cyberprzestrzeni zapewnia odpowiednim służbom kompetencje pozwalające szybko i skutecznie przeciwdziałać zagrożeniom, a także incydentom związanym z naruszeniem bezpieczeństwa systemów i sieci komputerowych oraz użytkowników korzystających z usług świadczonych drogą elektroniczną. Analizę ograniczono do działalności Agencji Bezpieczeństwa Wewnętrznego oraz Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego.

SŁOWA KLUCZOWE

cyberbezpieczeństwo, infrastruktura krytyczna, ABW, CSRIT, cyberprzestępczość

Bibliografia

Białuński M., *Odstąpienie od obowiązku zawiadomienia prokuratora o przestępstwie – analiza nowego uprawnienia Szefa Agencji Bezpieczeństwa Wewnętrznego*, „Palestra" 2018, nr 3, s. 72–80.

Bożek M., *Zwalczanie przestępstw jako ustawowe zadanie Agencji Bezpieczeństwa Wewnętrznego. Stan obecny i postulaty de lege ferenda*, „Studia Iuridica Lublinensia" 2015 Vol. XXIV, t. 1, s. 35–66.

Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm jako nowe zagrożenie dla bezpieczeństwa międzynarodowego w dobie globalizacji*, w: *Terroryzm w świecie współczesnym*, E. Haliżak (red.), Warszawa 2004.

Chlebowicz P., *Nielegalny handel bronią*, Warszawa 2015.

Czaplicki K., Gryszczyńska A., Szpor G., *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.

Herbowski P., *Pozyskanie tajnego współpracownika przez służby kontrwywiadowcze na podstawie materiałów obciążających — rozważania o sensie instytucji*, „Nowa Kodyfikacja Prawa Karnego" 2019 nr 51, s. 83–102.

Liwo M., *Status służb mundurowych i funkcjonariuszy w nich zatrudnionych*, Warszawa 2012.

Materna G., *Zmowy przetargowe w prawie ochrony konkurencji i prawie karnym*, Warszawa 2016.

Lizak R., *Kontrolowane przyjęcie lub wręczenie korzyści majątkowej*, „Wojskowy Przegląd Prawniczy" 2011 nr 1, s. 27–42.

Poczucie bezpieczeństwa obywateli w Polsce. Identyfikacja i przeciwdziałanie współczesnym zagrożeniom, Guzik-Makaruk Ewa Monika (red.), Warszawa 2011.

Szkurłat A., *Kompetencje Prezesa UODO w zakresie cyberbezpieczeństwa w świetle polskich i unijnych regulacji prawnych*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2020 nr 2, s. 54–60.

Tużnik M.R., *Udział Agencji Bezpieczeństwa Wewnętrznego w postępowaniu karnym skarbowym*, „Studia Prawnicze i Administracyjne" 2018 nr 24(2), s. 57–62.

Walczuk K., Bożek M., *Konstytucyjne i ustawowe uwarunkowania organizacji i funkcjonowania Agencji Bezpieczeństwa Wewnętrznego*, Siedlce 2015.

Wójcik J.W., *Udział Agencji Bezpieczeństwa Wewnętrznego w postępowaniu karnym skarbowym*, „Studia Prawnicze i Administracyjne" 2018 nr 24(2), s. 57–62.

Article history: Received: 15.12.2020; Reviewed: 16.12.2020; Accepted: 23.12.2020

DOI: 10.5604/01.3001.0014.6160

Corresponding author: Maciej Siwicki, PhD, LLM, Faculty of Political Science and Security Studies at the Nicolaus Copernicus University in Toruń, Poland; ORCID: 0000-0002-3120-0211, e-mail: msiwicki@umk.pl

Cite this article as: Maciej Siwicki, PhD, LLM, "Counteracting threats in ICT networks and systems. A few remarks on the activities of the Internal Security Agency and the CSIRT". bellona quart. 2020(3): 57–68

Competing interests: The authors declare that they have no competing interests.

Table of content URL: https://kwartalnikbellona.com/issue/12943

Author's bio: Maciej Siwicki, PhD, LLM
Associate Professor in Legal Sciences, Professor at the Nicolaus Copernicus University in Toruń. Holder of a postgraduate Master's degree from the Goethe University in Frankfurt am Main, where he obtained the title of Lex Legum Master (LLM). He has written over 60 works concerning new technologies law, drawing particular attention to computer criminal law, the functioning of the mass media in Poland, and some aspects of intellectual property protection.

the bellona quarterly issn: 1897-7065 | e-issn: 2719-3853

KWARTALNIK BELLONA

Elementy systemu walki w cyberprzestrzeni

płk dr hab. inż. Piotr Dela

ORCID: 0000-0003-3643-3759
e-mail: delson@wp.pl
Akademia Kaliska, Kalisz

ABSTRACT:

The author attempts to identify essential elements for building the competence of a security subject, which is the state, in the area of activities (armed conflict) in cyberspace. He characterizes contemporary conflicts, and puts special attention on cyberspace activities. He draws attention to the necessity of a systematic approach to the problem, presenting the most important elements of a combat system in cyberspace. He discusses the principles of art of war, which – in his opinion – should form the basis for building the state's competence in cyberspace. He analyzes the potential course of armed conflict which uses cyberspace.

KEYWORDS:

system, cyberspace, cyberspace security, armed conflict, armed forces

Wstęp

Państwo jako podmiot prawa międzynarodowego i zarazem podmiot bezpieczeństwa powinno być zdolne do przeciwdziałania wszelkim zagrożeniom, zarówno wewnętrznym, jak i zewnętrznym. W zagrożenia te wpisuje się cyberprzestrzeń – środowisko, w którym trudno wyznaczyć granice. Z tego względu dla każdego nowoczesnego państwa staje się ona wyzwaniem, zmusza je do budowania odpowiednich kompetencji, struktur oraz procedur mających na celu zapewnienie bezpieczeństwa własnego i obywateli. Jednym z wielu narzędzi państwa do zapewnienia pożądanego stanu bezpieczeństwa, w głównej mierze ukierunkowanego na bezpieczeństwo militarne, są siły zbrojne. Wysiłki wielu podmiotów zmierzające do przeniesienia wyścigu zbrojeń w cyberprzestrzeń powodują, że stworzenie systemu walki w tej przestrzeni staje się koniecznością, a nawet obowiązkiem państwa.

Budowanie kompetencji, zdolności do prowadzenia walki w przestrzeni cybernetycznej, powinno być oparte na podejściu systemowym, tak by każdy element miał swoje miejsce i przeznaczenie. Istotne są sposób tworzenia i budowania kompetencji państwa w tym zakresie oraz określenie ich podstawy. Punktem wyjścia powinien być zbiór zasad, który będzie służył podmiotowi do budowania odpowiedniego, skutecznego systemu bezpieczeństwa. Zbiór ten należy wywieść z prakseologii i zasad sztuki wojennej. Działalność podmiotów w cyberprzestrzeni jest bowiem elementem współczesnej kooperacji negatywnej, noszącej znamiona wojny asymetrycznej, hybrydowej. Dobrze oddają to słowa Tadeusza Kotarbińskiego, który w rozważaniach nad systemem walki, podkreślił, że zawsze występują co najmniej dwie strony (dwa podmioty) nawzajem bezpośrednio lub pośrednio się zwalczające, czyli *cele działających są niezgodne i jedni drugim usiłują przeszkodzić w działaniach*[1]. Aby odnieść zwycięstwo, nie wystarczy przeszkodzić stronie przeciwnej w osiągnięciu jej celów cząstkowych. Należy doprowadzić do sytuacji, w której realizacja zakładanego celu będzie zależała tylko od własnych działań, nie zaś od poczynań strony przeciwnej oraz jej możliwości oddziaływania. Drogą do osiągnięcia tego jest stworzenie systemu walki w cyberprzestrzeni.

Celem badań było określenie podstawowych uwarunkowań tworzenia systemu walki w cyberprzestrzeni z punktu widzenia podmiotów bezpieczeństwa, jakimi są państwa. W osiągnięciu tego celu pomocne okazały się metody teoretyczne, takie jak analiza, synteza i porównanie. Wykorzystano także obserwację – uczestnictwo autora w wielu ćwiczeniach z obszaru bezpieczeństwa i ochrony cyberprzestrzeni.

Inspiracją do badań była chęć wypełnienia pewnej luki tematycznej, brakuje bowiem opracowań poświęconych problematyce walki w cyberprzestrzeni, postrzeganej przez pryzmat działań ofensywnych i defensywnych. Większość opracowań dotyczących bezpieczeństwa cyberprzestrzeni nie uwzględnienia aspektów kooperacji negatywnej, rozumianej jako walka. Zagadnienie to ma duże znaczenie, tym bardziej że szybko zmienia się podejście do wykorzystania cyberprzestrzeni jako środowiska, w którym są realizowane interesy narodowe[2]

1 T. Kotarbiński, *Hasło dobrej roboty*, Warszawa 1975, s. 127.

2 Artykuł został przygotowany w 2019 r. Wiosną 2020 r. ukazała się monografia mojego autorstwa *Teoria walki w cyberprzestrzeni*, w której podjęty w artykule problem wykorzystania cyberprzestrzeni do realizacji interesów narodowych został szerzej omówiony.

Charakterystyka walki zbrojnej i współczesnych konfliktów zbrojnych

Termin „walka" ma wiele znaczeń, zwłaszcza współcześnie, używa się go bowiem do opisu walki zarówno zbrojnej, jak i sportowej, politycznej czy jakikolwiek innej formy rywalizacji. Walka, tym bardziej walka zbrojna, stanowi podstawową kategorię w sztuce wojennej. Także w prakseologii walka i walka zbrojna mają swoje odzwierciedlenie w ogólnej teorii walki i często są określane jako kooperacja negatywna[3].

W artykule uwagą badawczą skupiono na walce zbrojnej. Jest ona różnorodnie definiowana. Zdaniem Stanisława Kozieja stanowi bezpośrednie starcie zgrupowań wojsk, *wzajemne destrukcyjne oddziaływanie za pomocą posiadanych środków rażenia,*[…] *przede wszystkim fizyczne niszczenie i psychologiczne obezwładnianie przeciwnika jako przeszkody na drodze do celu*[4]. Z takiego rozumowania wynika, że warunkiem walki zbrojnej w cyberprzestrzeni jest posiadanie sił zdolnych do jej prowadzenia (wojsk cybernetycznych) oraz odpowiednich środków rażenia, mogących fizycznie i psychologicznie obezwładnić przeciwnika (logicznych, kinetycznych i informacyjnych), a także przyjęcie rozwiązań organizacyjno-funkcjonalnych (doktryny i regulaminy). Również w definicji zawartej w *Małej encyklopedii wojskowej* stwierdza się, że […] *walka to zorganizowane starcie zbrojne stron wojujących; wszelaka akcja sił zbrojnych stron przeciwnych, z których każda dąży do zniszczenia nieprzyjaciela wszystkim dostępnymi środkami rażenia*[5]. Patrząc przez pryzmat historii wojen i wojskowości, cyberprzestrzeń stała się kolejnym obszarem walki zbrojnej, równie ważnym – jeśli nie ważniejszym – jak ląd, woda, powietrze i kosmos.

Nie wydaje się celowe przytaczanie innych definicji walki zbrojnej, ponieważ w większości wskazują one pewne wspólne cechy tego pojęcia, mianowicie: zorganizowaną formę, posiadanie sił i środków oraz dążenie do pokonania przeciwnika. Dlatego każdą walkę, także walką zbrojną w cyberprzestrzeni, należy utożsamiać z systemem, składającym się z elementów wewnętrznych będących ze sobą w odpowiedniej relacji oraz elementów zewnętrznych znajdujących się w otoczeniu i warunkujących funkcjonowanie elementów wewnętrznych (wskutek odpowiednich powiązań zwrotnych i relacji), działającym celowo. W walce tej nie można ograniczać się tylko do cyberprzestrzeni i tylko do obrony. System walki w przestrzeni cybernetycznej musi być integralnym elementem systemu walki sił zbrojnych, zdolnym do działań zarówno defensywnych, jak i ofensywnych.

Współczesne konflikty zbrojne i wojny różnią się od wojen i konfliktów znanych nam z przeszłości. Każda epoka ma bowiem swoje wojny, uwarunkowane poziomem rozwoju technologicznego i społecznego. W wyniku ekspansji środków przekazu oraz przechowywania, wytwarzania i przetwarzania informacji zmienił się sposób funkcjonowania współczesnych społeczeństw. Dostęp do informacji, możliwość jej szybkiego przesyłania i przechowywania w środowisku określanym jako cyberprzestrzeń, dał społeczeństwom nową jakość, polegającą na możliwości funkcjonowania i pełnienia funkcji społecznych w sposób, jaki jeszcze do niedawna trudno było sobie wyobrazić. Pozwala to nie tylko na szyb-

3 Idem, *Traktat o dobrej robocie*, Wrocław–Warszawa–Kraków–Gdańsk–Łódź 1982, s. 221.

4 S. Koziej, *Teoria sztuki wojennej*, Warszawa 1993, s. 16–17.

5 *Mała encyklopedia wojskowa*, Warszawa 1979, s. 472.

szy rozwój społeczeństw, lecz także ma istotny wymiar ekonomiczny, objawiający się redukcją kosztów funkcjonowania państwa i jednoczesnym skróceniem czasu pełnienia tych funkcji. Wnioski ze zdarzeń w Estonii z 2007 roku, konfliktów w Gruzji z 2008 roku i na Ukrainie z 2014 roku uświadamiają, że nowy wymiar współczesnego życia, jakim jest funkcjonowanie w cyberprzestrzeni, będzie miał ogromny wpływ na przebieg przyszłych konfliktów zbrojnych i wojen.

Z punktu widzenia współczesnych konfliktów zbrojnych ważne jest określenie istoty wojny, ta zaś w jej obecnym ujęciu jest trudna do zdefiniowania. Składają się na to różnego rodzaju czynniki, związane między innymi z nieprawdopodobnym przyspieszeniem rozwoju ekonomicznego świata, zwiększeniem się populacji ludności oraz zmianami geopolitycznymi na arenie międzynarodowej. Pojęcia wojny często używają politycy i decydenci w celu wyrażenia swojego stosunku do zaistniałej sytuacji. Zyskało ono wymowę retoryczną i ma służyć wywarciu określonego wrażenia społecznego i międzynarodowego.

Z definicji Carla von Clausewitza[6] mówiącej o wojnie jako o *przedłużeniu polityki* i *czynie politycznym państwa* można wysnuć wniosek, że wojna stanowi domenę głównie podmiotów państwowych dążących do osiągnięcia swoich celów politycznych metodami niepokojowymi. W dziele *O wojnie* Clausewitz uznaje wojnę za czyn polityczny, […] *dalszy ciąg stosunków politycznych przejawiających się w aktach przemocy, mający na celu zmuszenie przeciwnika do spełnienia naszej woli.* […] *celem działań wojennych jest obezwładnienie wroga, jego rozbrojenie: doprowadzenie jego sił zbrojnych do stanu, w którym nie będą one zdolne do walki*. Zdaniem Bolesława Balcerowicza w przytoczonych definicjach daje się zauważyć ścisły związek między polityką, państwem, wojną i wojną (przemocą) ujętą jako instrument polityki[7]. Jest to swoista gra siły, władzy i ludu lub – w innym ujęciu – rozumu, siły i (ślepego) żywiołu. Wojna jako forma rozwiązywania konfliktów między stronami będzie się więc charakteryzowała stosowaniem przemocy odpowiedniej do sytuacji, posiadanych możliwości i rozwoju społecznego.

Interesującą definicję wojny przedstawił Carl Schmitt[8], stwierdził, że jest to *konflikt między jednostkami zorganizowanymi politycznie, prowadzony za pomocą uzbrojenia*. Każda era ma swoje wojny, tym samym swoje uzbrojenie i metody jej prowadzenia. Także era informacyjna, czyli ta, w której żyjemy, ma swoje nowe uzbrojenie. Jednym z jej elementów są narzędzia wykorzystywane do prowadzenia walki w szeroko rozumianej cyberprzestrzeni.

Ostatnimi czasy widoczna jest asymetryczność stron konfliktu. Termin „konflikt asymetryczny"[9] pojawił się w latach dziewięćdziesiątych XX wieku w Stanach Zjednoczonych. Najczęściej oznacza konflikt, […] *w którym państwo i jego siły zbrojne konfrontowane są z przeciwnikiem, którego cele, organizacja, środki walki i metody działania nie miesz-*

6 B. Balcerowicz, *Czym jest współczesna wojna*? wersja HTML pliku, http://dlibra.kul.pl/Content/31109/34038__Balcerowicz-Bolesla_0000.pdf [dostęp: 29.06.2018].

7 Ibidem

8 Ibidem.

9 K. Piątkowski, *Wojna nowego typu*, „Polska w Europie" 2002, nr 1, s. 23–24.

czą się w konwencjonalnym ujęciu wojny. W takim rozumieniu wojny (konfliktu zbrojnego) nie występuje pojęcie frontu, a walka jest prowadzona w rozproszeniu geograficznym i czasowym. Przeciwnik asymetryczny unika bezpośredniego starcia z przeciwnikiem – państwem, posługuje się metodami niekonwencjonalnymi, tj. terroryzmem i jego bardziej wyrafinowaną formą – cyberterroryzmem. Działania te są ukierunkowane głównie na oddziaływanie na społeczeństwo w sferze informacyjnej, psychologicznej i ekonomicznej. Podział stron konfliktu asymetrycznego odzwierciedla status stron na arenie międzynarodowej, stanowiącej swoistą asymetrię legitymizacji opartych na prawie międzynarodowym[10].

Do najistotniejszych cech konfliktów asymetrycznych należy zaliczyć: cele odmienne od klasycznych, organizację, technikę, metody działania oraz zasięg[11]. Cele nowych wojen skupiają się na uzyskaniu (wzmocnieniu) tożsamości politycznej (ideologicznej) pojmowanej w nowy sposób, nie zawsze zorientowanej na budowę nowego państwa[12]. I choć celem takiej wojny nie jest osiągnięcie pełnej kontroli nad danym terytorium, np. drogą pozbycia się niechcianej ludności, to jest ona prowadzona totalnie, na całym terytorium i w sposób jak najdotkliwszy dla zamieszkującego go społeczeństwa. Kluczowymi elementami konfliktu asymetrycznego są: skrytość, zmienność, zaskoczenie, wysoki stopień intensywności oraz niegraniczony zasięg[13]. W takim ujęciu cyberprzestrzeń staje się nowym wymiarem konfliktów asymetrycznych. Ze względu na wrogie zastosowanie technologii informatycznych konflikty asymetryczne mogą przybrać formę wojny informatycznej, w której stronami konfliktu będą nie tylko podmioty asymetryczne, lecz także państwa z całą swoją potęgą ekonomiczną, gospodarczą i militarną.

Ze współczesnymi konfliktami zbrojnymi wiąże się hybrydowość. Jest to nowe (choć dobrze znane z przeszłości) podejście poznawcze w nauce o konfliktach zbrojnych[14], rozumiane jako współistnienie starych i nowych elementów wojen, klasycznych konfliktów zbrojnych i wojen ponowoczesnych, starcia narodowych sił zbrojnych i konfliktów asymetrycznych, supernowoczesnych technologii wojskowych i prymitywnych narzędzi walki, walki o terytoria i zasoby naturalne oraz sporów o tożsamość i wartości[15]. Wynika ona z jednoczesnego współistnienia w czasie i przestrzeni wojen odmiennych generacji, które na współczesnym polu walki wzajemnie się przenikają[16].

Hybrydowość konfliktów zbrojnych polega na równoczesnym istnieniu dwóch głównych płaszczyzn konfliktu: terytorialnej i wirtualnej. Pierwsza odnosi się do klasycznie pojmowanego państwa lub grup etnicznych stale zamieszkujących określony obszar, natomiast druga do struktury transgranicznej, ponadterytorialnej, umożliwiającej

10 H. Munkler, *Wojny naszych czasów*, Kraków 2004, s. 10.

11 K. Piątkowski, *Wojna nowego typu…*, op.cit., s. 24–26.

12 B. Balcerowicz, *Wojna. Kwestie nie tylko terminologiczne*, „Myśl Wojskowa" 2003 nr 2, s. 70–71.

13 K. Piątkowski, *Wojna nowego typu…*, op. cit., s. 25.

14 A. Gruszczak, *Hybrydowość współczesnych konfliktów zbrojnych – analiza krytyczna*, wersja HTML pliku, www.bbn.gov.pl/download/1/8755/Hybrydowoswspolczesnychwojenanalizakrytyczna.pdf/, s. 10 [dostęp: 27.06.2018].

15 Ibidem, s. 11.

16 Ibidem.

komunikowanie się w obrębie danej sieci oraz propagowanie w niej wartości, zasad i idei[17]. Wojny w wymiarze terytorialnym mają na celu głównie rozciągnięcie i utrzymanie kontroli nad określonym obszarem, ochronę granic oraz egzekwowanie norm prawnych w stosunku do ludności zamieszkującej ten obszar. Wojny w wymiarze wirtualnym redefiniują parametry konfliktu i eliminują takie determinanty jak terytorium, zasoby naturalne, porządek publiczny czy nawet państwo. Na płaszczyźnie wirtualnej powstają nowe pseudopaństwa, pozbawione tradycyjnych elementów władzy państwowej, takich jak podmiotowość międzynarodowa czy hierarchiczność organizacji, mające jednak skuteczne instrumenty pomnażania zasobów finansowych, prowadzenia kampanii informacyjnych i oddziaływania na środowisko zarówno lokalne, jak i międzynarodowe[18].

System walki

Podobnie jak walka, system jest różnie definiowany. Ta złożona problematyka została omówiona w publikacji Piotra Sienkiewicza *Podstawy teorii systemów*[19]. W artykule zostały przeanalizowane tylko najważniejsze definicje systemu, najbardziej przydatne do dalszych rozważań. Piotr Sienkiewicz postrzegał system jako […] *pojęcie desygnujące pewną całość, tworzoną przez określony zbiór obiektów (elementów) i powiązań (relacji) między nimi, rozpatrywaną z określonego punku widzenia (aspektu badań)*[20]. Wynika z tego, że system walki w cyberprzestrzeni powinien stanowić swoistą całość, zbiór elementów będących ze sobą w relacjach, rozpatrywaną z punku widzenia walki, jaką ten system ma prowadzić. Walka jest wyznacznikiem funkcjonalności systemu. A skoro walka obejmuje działania ukierunkowane na pokonanie (zniszczenie) przeciwnika, to nie można mówić (jak twierdzą w oficjalnych wystąpieniach decydenci) tylko i wyłącznie o obronie cyberprzestrzeni (wojskach obrony cyberprzestrzeni). System w rozpatrywanym ujęciu stanowi skończony zbiór elementów M i relacji R, określonych na zbiorze elementów[21]. Wobec tego zidentyfikowanie (stworzenie) systemu walki w cyberprzestrzeni wymaga określenia zbioru elementów tego systemu i relacji między nimi. Określenie celu działania systemu wynika z samej nazwy systemu – walki.

Podejście systemowe, systemowość, nie jest domeną teraźniejszości. Problemem tym zajmowali się już starożytni filozofowie – Platon i Arystoteles. Ten ostatni wskazał, że *całość to więcej niż część*[22]. Twórca ogólnej teorii systemów Ludwig von Bertalanffy stwierdził, że […] *organizm stanowi system, w którym rola poszczególnych części jest uzależniona od ich miejsca w całości tego systemu*[23]. Podejście Bertalanffy'ego opierało się na nowych zasadach poznania naukowego, takich jak[24]:

17 Ibidem, s. 14.

18 Ibidem.

19 P. Sienkiewicz, *Podstawy teorii systemów*, Warszawa 1993.

20 Ibidem, s. 16.

21 Ibidem, s. 14.

22 M. Blaug, *Teoria ekonomii. Ujęcie retrospektywne*, Warszawa 1994, s. 711.

23 P. Sienkiewicz, *Podstawy teorii...*, op.cit., s. 19.

24 Ibidem.

– rozpatrywanie organizmu jako całości, czyli zorganizowanego układu oddziałujących na siebie wzajemnie składników;

– rozpatrywanie organizmu jako zjawiska dynamicznego, mającego charakter procesualny;

– rozpatrywanie organizmu jako aktywnego uwzględnienia zależności losowych w opisie jego zachowania.

W teorii systemów można znaleźć wiele innych podejść, jednak nie będą one przedmiotem analizy.

W podejściu systemowym duże znaczenia ma to, czym naprawdę są systemy i jak je odróżnić od niesystemów. Odpowiedź daje Piotr Sienkiewicz: […] *coś stanowi całość wtedy, gdy stanowi zbiór pełny (zamknięty), w jakiś sposób jest wyróżniony z otoczenia, a co istotniejsze – składa się z części, które dadzą się oddzielić, lecz są ze sobą w pewien szczególny sposób. Całość jest obiektem różnym w stosunku do tego, co stanowi prostą sumę poszczególnych części*[25].

Określenia wymaga również termin „system walki". Z analizy literatury wynika, że pojęcie to jest definiowane niejednoznacznie i ma różnorodne odpowiedniki: system ognia, system obrony, system operacji, system obrony i natarcia[26]. W 1970 roku Józef Konieczny w publikacji *Cybernetyka walki*[27] przedstawił teorię niszczenia (teorię walki), w której obiekty każdej walczącej strony A i B podzielił na niszczycieli oraz obiekty niszczone. Wyróżnił także obiekty będące niszczycielami i obiektami niszczenia zarazem. Dowolny obiekt każdej strony może należeć bądź do systemu niszczenia, bądź do systemu zabezpieczenia, tym samym każdy obiekt należy do systemu walki, którego podsystemami są system niszczenia i system zabezpieczenia[28]. W swojej teorii walki Konieczny wskazał, że system niszczenia zawiera wszystkie łańcuchy niszczenia, w których obiekty danej strony tworzą niszczyciele. Walka ze stroną przeciwną jest prowadzona przez proces niszczenia na drodze zasileniowej i informacyjnej. System zabezpieczenia odpowiada za właściwe działanie obiektów należących do systemu niszczenia. Są to wszelkiego rodzaju procesy (łańcuchy) zaopatrzenia w broń, amunicję, materiały pędne i smary, żywność, wsparcie medyczne, części zamienne, a także w informację (co w przypadku walki w cyberprzestrzeni jest chyba najważniejsze). Strony mogą niszczyć i swoich niszczycieli, i ich łańcuchy zabezpieczenia[29]. A to wpisuje się w możliwości prowadzenia działań zbrojnych w cyberprzestrzeni w oderwaniu od miejsca i czasu. Odcięcie niszczycieli od zasilania w wyniku obezwładnienia ich infrastruktury krytycznej – zarówno cywilnej, jak i militarnej – jest najlepszym sposobem osiągnięcia celu walki. Historycznym dowodem na to mogą być trudności armii niemieckiej z dostępem do benzyny pod koniec drugiej wojny światowej. Oczywiście było to spowodowane zmasowanymi nalotami aliantów na

25 P. Sienkiewicz, *Inżynieria systemów*, Warszawa 1983, s. 7–8.

26 Szerzej: M. Huzarski, *Działania taktyczne (materiał do studiowania)*, Warszawa 1992; S. Koziej et al., *Działania taktyczne wojsk lądowych*, Warszawa 1992; Idem, *Działania operacyjne*, Warszawa 1993; Z. Ścibiorek, *Działania taktyczne wojsk lądowych*, Warszawa 1996; R. Bojarski, *Operacja obronna*, Warszawa 1999.

27 J. Konieczny, *Cybernetyka walki*, Warszawa 1970.

28 Ibidem, s. 103–104.

29 Ibidem.

zakłady produkujące benzynę. W XXI wieku podobne rezultaty można osiągnąć drogą oddziaływania w cyberprzestrzeni.

Podsumowując, w obowiązującej w Siłach Zbrojnych RP definicji systemu walki wskazano, że jest to […] *skoordynowany wewnętrznie zbiór wzajemnie powiązanych sił, środków i działań, ukierunkowany na osiągnięcie celu walki zgodnie z zamiarem dowódcy*[30]. Dodatkowo określono elementy systemu walki jako […] *współdziałające ze sobą części systemu/podsystemu walki, znajdujące się w określonych relacjach między sobą*[31]. W skład systemu walki zaliczono osiem podsystemów[32]: dowodzenia, rozpoznania, rażenia, wsparcia inżynieryjnego, obrony przed bronią masowego rażenia, obrony przeciwlotniczej, zabezpieczenia logistycznego oraz zabezpieczenia medycznego.

W kontekście przedstawionych uwarunkowań zasadne wydaje się wskazanie elementów (podsystemów) systemu walki w cyberprzestrzeni. Poszukiwanie najlepszego rozwiązania wymaga uwzględnienia całości dorobku sztuki wojennej, współczesnych zmian technologicznych i społecznych, posiadanego potencjału oraz – co najważniejsze – interesu narodowego. Oczywiście jest to proces złożony, czaso- i kosztochłonny. Niemniej jednak na podstawie analizy własnego potencjału, rozwiązań stosowanych w krajach wysoko rozwiniętych i pożądanych kompetencji można określić elementy krytyczne. Należą do nich: dowództwo wojsk cybernetycznych, pododdziały wojsk cybernetycznych, elementy zabezpieczenia i wsparcia, przemysł oraz komórki naukowo-badawcze. Dowództwo wojsk cybernetycznych w swojej strukturze powinno zawierać między innymi takie elementy jak: rozpoznanie, prowadzenie operacji cybernetycznych, planowanie operacji oraz szkolenie i rozwój. Oczywiście zbiór ten nie jest zbiorem zamkniętym i w dowództwie mogą występować także inne elementy. Poddziały wojsk cybernetycznych, podległe bezpośrednio dowództwu wojsk cybernetycznych, powinny charakteryzować się wysoką specjalizacją i być zdolne do wykonywania zadań z wykorzystaniem narzędzi (środków walki) dostarczonych przez rodzimy przemysł oraz komórki naukowo-badawcze. Elementy wsparcia i zabezpieczenia, zgodnie z koncepcją Józefa Koniecznego, stanowią podsystem zasilający, bez którego dowództwo i pododdziały cybernetyczne nie są zdolne do prowadzenia działań (funkcjonowania).

Uzasadnione wydają się rozważania nad stworzeniem nowego, samodzielnego rodzaju sił zbrojnych – wojsk cybernetycznych i odpowiedniego umieszczenia ich w otoczeniu (podsystemie militarnym państwa).

Zasady sztuki wojennej

Budowanie kompetencji państwa związanych ze zdolnością do prowadzenia działań w cyberprzestrzeni powinno być oparte na uniwersalnych zasadach, gwarantujących osiągnięcie sukcesu. Wywodzą się one z dobrze znanych i sprawdzonych przez stulecia zasad sztuki wojennej. Za najważniejsze w tym obszarze należy uznać: przewagę, swobodę działania,

30 *Instrukcja zgrywania systemów walki w SZ RP, DD/7.1.2*, Warszawa 2011, s. 7.

31 Ibidem.

32 Ibidem, s. 6.

zaskoczenie, ekonomię sił, aktywność i synergiczność[33]. Jest to zbiór otwarty i w toku dalszych badań można wskazać jeszcze inne, nie mniej ważne zasady.

Przewaga, w klasycznym ujęciu, sprowadza się do konstatacji, że w celu pokonania przeciwnika należy uzyskać nad nim dominację w różnych aspektach, od możliwości intelektualnych dowódców i oficerów sztabu, teorii taktyki, sztuki operacyjnej i strategii, przez lepsze uzbrojenie, lepsze wykorzystanie terenu, po większą liczbę żołnierzy. Uzyskanie przewagi lub zminimalizowanie przewagi przeciwnika wymaga wykorzystania wszystkich możliwych sposobów. Jak zatem rozpatrywać przewagę w cyberprzestrzeni i w czym może się ona wyrażać?

Niezbędnym warunkiem budowania przewagi w przestrzeni cybernetycznej jest posiadanie odpowiednich zasobów intelektualnych, wysoko wykwalifikowanych specjalistów z zakresu zarówno informatyki, jak i bezpieczeństwa informacyjnego, psychologii oraz socjologii, a także dowódców i specjalistów potrafiących planować i prowadzić działania w cyberprzestrzeni w połączeniu z działaniami konwencjonalnymi. Zasobem, który niejednokrotnie stanowił o przewadze w decydujących momentach konfliktów zbrojnych, jest potencjał ludzki. Dlatego należy dążyć do stworzenia odpowiednich programów edukacyjnych, adresowanych i do społeczeństwa – w celu zwiększenia jego świadomości zagrożeń płynących z cyberprzestrzeni, i do specjalistów, którzy mają prowadzić walkę w cyberprzestrzeni.

W dążeniu do osiągania przewagi duże znaczenie ma uniezależnienie się od obcych technologii dzięki posiadaniu i rozwojowi własnych (narodowych) systemów, opartych na rodzimym sprzęcie i oprogramowaniu. W obecnych uwarunkowaniach doprowadzenie do takiego stanu jest niezwykle trudne ze względu na całkowitą i bezkrytyczną zależność od technologii zachodnich i dalekowschodnich. Można nawet stwierdzić, że Polska, tak jak wiele innych krajów, całkowicie straciła suwerenność w cyberprzestrzeni. Z analizy zjawisk zachodzących w przestrzeni cybernetycznej jednoznacznie wynika, że wykorzystywanie w niej obcych rozwiązań sprzętowych i programowych wiąże się z ryzykiem. Powszechnie znana podatność owych rozwiązań na ataki czy potencjalne backdoory skazują stronę korzystającą z obcych technologii na porażkę w możliwej, przyszłej wojnie w cyberprzestrzeni i powodują, że wszelkie działania tej strony będą działaniami już z niekorzystnej pozycji. Dlatego należy dążyć do uzyskania oraz rozwoju technologii umożliwiających opracowanie własnych rozwiązań sprzętowych i programowych na potrzeby zastosowania w cyberprzestrzeni, zdolnych do zachowania swojej funkcjonalności niezależnie od infrastruktury bazującej na rozwiązaniach czysto komercyjnych.

Ważnym zagadnieniem jest ochrona własnych zasobów informacyjnych oparta na narodowych rozwiązaniach kryptograficznych. Bez tego nie można zapewnić jakiejkolwiek ochrony informacji, tym samym nie można zdobyć przewagi.

Swoboda działania, podobnie jak przewaga, jest bezpośrednio związana z wykorzystaniem nowoczesnych, narodowych technologii do tworzenia własnych systemów teleinformatycznych. Ma to na celu wzmocnienie ich odporności na potencjalne oddziaływanie

33 Szerzej: S. Koziej, *Teoria sztuki...*, op.cit., s. 68–90; A. Polak, *Sztuka wojenna. Kontekst teoretyczny i praktyczny*, „Zeszyty Naukowe Akademii Obrony Narodowej" 2013 nr 3, s 219–228.

przeciwnika i w rezultacie zwiększenie swobody działania we własnej przestrzeni cybernetycznej. Dodatkowym elementem uzyskania swobody działania jest ochrona własnych zasobów informacyjnych i zdobywanie informacji o stronie przeciwnej, co umożliwi prowadzenie działań z korzystnej pozycji, z wykorzystaniem automatyzmów rzeczywistości.

Zaskoczenie, w potocznym rozumieniu, stanowi zasadę sztuki wojennej polegającą na zapewnieniu określonej przewagi nad przeciwnikiem oraz racjonalnym jej spożytkowaniu, po to by osiągnąć cele minimalnym kosztem. Warunkiem uzyskania efektu zaskoczenia są działania podejmowane w sposób nieoczekiwany i nagły, nieprzewidywany przez stronę przeciwną. W wyniku zaskoczenia zostaje naruszona równowaga psychiczna, czego bezpośrednią konsekwencją jest czasowa utrata zdolności do podejmowania trafnych decyzji i ich sprawnego wykonania.

W cyberprzestrzeni zaskoczenie będzie związane głównie z informacją i tzw. bronią cybernetyczną. Walka o informację w przestrzeni cybernetycznej powinna być prowadzona stale, niezależnie od fazy konfliktu. Z jednej strony należy koncentrować się na zdobyciu informacji o zamiarach przeciwnika, jego potencjale i planowanych operacjach, z drugiej zaś podejmować działania dezinformujące, polegające na preparowaniu fałszywego obrazu rzeczywistości. Istotą wykorzystania broni cybernetycznej jako narzędzia walki w cyberprzestrzeni powinno być całkowite zaskoczenie strony przeciwnej, jeśli chodzi o czas i cel użycia tej broni oraz skutki i zakres jej rażenia. Broń tego typu powinna być przygotowywana w ścisłej tajemnicy, z założeniem jednorazowego charakteru tego typu uzbrojenia. Aby uzyskać zaskoczenie w cyberprzestrzeni, trzeba dysponować arsenałem narzędzi zdolnych do skutecznego paraliżowania przeciwnika w tym środowisku walki.

Zasada ekonomii sił polega na racjonalnym dysponowaniu siłami i środkami, tak aby osiągnąć cel działania w możliwie jak najkrótszym czasie, małymi nakładami i z jak najmniejszymi stratami. Do każdego zadania należy użyć tylko tylu sił i środków, ilu potrzeba, tylko wtedy, gdy jest to niezbędne, i tylko w taki sposób, w jaki jest to konieczne. Walka w cyberprzestrzeni idealnie wpisuje się w tę zasadę. Warunkuje to wiele czynników. Po pierwsze, koszty prowadzenia walki są nieproporcjonalnie niższe w stosunku do kosztów ponoszonych w konfliktach konwencjonalnych. Po drugie, skutki oddziaływania w cyberprzestrzeni mogą być większe niż skutki wykorzystania broni konwencjonalnej. Po trzecie, broń cybernetyczna charakteryzuje się nieograniczonym zasięgiem w stosunku do broni konwencjonalnej. Po czwarte, właściwości broni cybernetycznej gwarantują maksymalne bezpieczeństwo własnym wojskom. Strona przeciwna, w myśl zasady ekonomii sił, także będzie dążyła do przeniesienia konfliktu w obszar cyberprzestrzeni, co warunkuje posiadaniem odpowiedniej struktury, narzędzi i procedur pozwalających zmniejszyć podatność własnej cyberprzestrzeni na wrogie ataki, a jeżeli już do nich dojdzie, umożliwiających szybkie odtworzenie funkcjonalności własnego systemu informacyjnego i zapewnienie ciągłości działania elementom infrastruktury krytycznej.

Aktywność – zasada ta polega na nieustannym dążeniu do narzucenia własnej woli, własnych reguł gry. Należy nie tylko przeciwstawić się działaniom przeciwnika, lecz także zmierzać do realizacji własnych interesów narodowych. W cyberprzestrzeni aktywność powinna wyrażać się w ciągłej dążności państwa, w wielu obszarach, do doskonalenia własnego systemu walki. Chodzi przede wszystkim o tworzenie własnych rozwiązań systemo-

wych, pozwalających na szybkie i skuteczne zapewnienie narodowych interesów w cyberprzestrzeni. Ponadto konieczne jest stworzenie odpowiednich narzędzi prawnych, edukacyjnych, proceduralnych i strukturalnych, które dadzą organom odpowiedzialnym za bezpieczeństwo cyberprzestrzeni stosowne narzędzia oddziaływania, zarówno defensywne, jak i ofensywne.

Zasada synergiczności sprowadza się do wzajemnego zespolenia działań różnych elementów systemu obronnego państwa, ukierunkowanego na osiągnięcie wspólnego celu. Działania w cyberprzestrzeni powinny być zespolone z działalnością takich organów jak: wywiad i kontrwywiad (zarówno cywilny, jak i wojskowy), organów odpowiedzialnych za ład i porządek publiczny, organów ścigania i wymiaru sprawiedliwości oraz systemu edukacyjnego na wszystkich poziomach organizacyjnych. Synergiczność dotyczy również konwencjonalnych działań zbrojnych, które powinny być zintegrowane z oddziaływaniem w cyberprzestrzeni.

Przebieg konfliktu z wykorzystaniem cyberprzestrzeni

Konflikt zbrojny jako wojna w ujęciu klasycznym będzie ostateczną fazą rozwiązywania sporów, po wyczerpaniu wszystkich możliwych form oddziaływania na stronę przeciwną. W pierwszej kolejności zostaną wykorzystane formy przemocy niewymagające dużych nakładów finansowych, dotkliwe dla strony przeciwnej oraz akceptowalne przez własne społeczeństwo i społeczność międzynarodową. Między innymi będzie to oddziaływanie w cyberprzestrzeni obejmujące: dezinformację i propagandę; informatyczne blokowanie, niszczenie i modyfikację informacji posiadanej przez przeciwnika; informatyczne obezwładnianie infrastruktury krytycznej; informatyczne obezwładnianie systemu informacyjnego przeciwnika; fizyczne niszczenie informacji; fizyczne obezwładnianie infrastruktury krytycznej oraz fizyczne obezwładnianie systemu informacyjnego przeciwnika. Narzędzia do tego wykorzystywane są tanie (w stosunku do kosztów broni konwencjonalnej), natomiast przewidywanie celu ataku, czasu i potencjalnego sprawcy jest niezwykle skomplikowane.

Istotnym zagrożeniem stała się możliwość oddziaływania informatycznego na elementy infrastruktury krytycznej, której sprawność i niezawodność jest kluczowa w wymiarze ekonomicznym i społecznym dla każdego wysoko rozwiniętego państwa. Infrastrukturę tę w coraz większym stopniu determinują informatyczne systemy sterujące. Ich wadliwe funkcjonowanie może skutkować awariami infrastruktury technicznej i w konsekwencji katastrofami technicznymi. Jako przykład takiego zagrożenia można przypomnieć atak na ukraińską sieć energetyczną[34] z grudnia 2015 roku.

Oddziaływanie fizyczne to nic innego jak kinetyczne niszczenie tych elementów, które mają duże znaczenie dla sprawności funkcjonowania systemu obronnego państwa. Są nimi zasoby informacyjne, obiekty infrastruktury krytycznej oraz poszczególne składowe systemu informacyjnego, z decydentami włącznie. Tego rodzaju oddziaływanie będzie niejako uzupełnieniem oddziaływania informatycznego na elementy, które zachowają funkcjonalność i żywotność po ataku informatycznym.

34 *Analysis of the Cyber Attack on the Ukrainian Power Grid*, E-ISAC, Washington DC 2016.

Wymienione działania powinny być skoordynowane z tworzeniem pozytywnego wizerunku strony konfliktu zarówno we własnym społeczeństwie, jak i na arenie międzynarodowej. Ilustracją takiej aktywności może być propaganda uprawiana w czasie konfliktu na Ukrainie[35] (rys. 1).

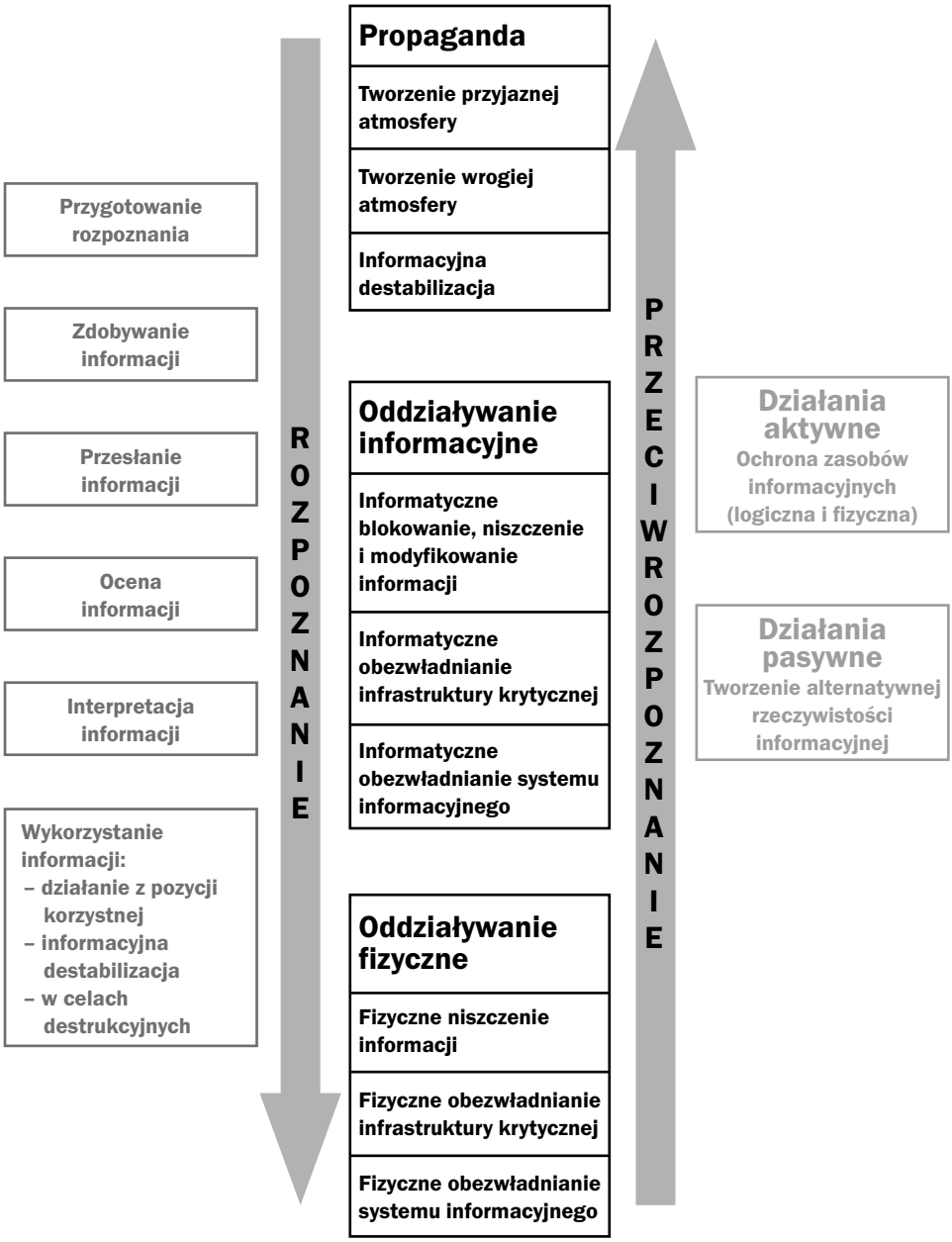
Walka w cyberprzestrzeni to nic innego jak walka o zdobycie przewagi informacyjnej nad drugą stroną. Polega na dążeniu do ukrycia własnej informacji, własnych zamiarów oraz stworzenia ich fałszywego obrazu i równocześnie usiłowaniu zdobycia informacji o zamiarach strony przeciwnej, a także na zapewnieniu funkcjonalności własnego systemu informacyjnego i infrastruktury krytycznej oraz sparaliżowaniu (obezwładnieniu) systemu informacyjnego i infrastruktury krytycznej strony przeciwnej.

Wiarygodność posiadanej informacji zależy od jakości zarówno systemu rozpoznania, jak i czynności przeciwstawnych, czyli przeciwrozpoznania. Te dwa procesy rywalizujące o informację dążą do uzyskania przewagi informacyjnej nad stroną przeciwną. Strona, która zdobędzie przewagę w dziedzinie informacji, osiągnie swój cel mniejszym kosztem, w rezultacie oznacza to zmaksymalizowanie kosztów strony przeciwnej. Przeciwrozpoznanie powinno zapewniać nie tylko ukrycie własnych zamiarów (informacji), lecz także stanowić podstawowy rodzaj ochrony własnych zasobów informacyjnych przed obezwładnieniem, modyfikacją lub zniszczeniem.

Walka informacyjna określa całokształt działań ofensywnych i defensywnych, koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów. Obecnie stała się ona niejako preludium do walki zbrojnej w ujęciu klasycznym. Zanim dojdzie do starcia zbrojnego, polem bitwy będzie cyberprzestrzeń, obejmująca nie tylko terytorium stron konfliktu, lecz także przestrzeń cybernetyczną społeczności międzynarodowej. Bitwa taka może przebiegać w sposób zarówno pełzający, jak i gwałtowny. W pierwszym przypadku oddziaływanie na stronę przeciwną będzie rozwijało się stopniowo, bez zauważalnego początku ataku, może nawet być niedostrzeżone lub potraktowane jako zjawisko występujące na co dzień w Internecie. Dla ataku gwałtownego natomiast charakterystyczne będą duża intensywność oddziaływania na cyberprzestrzeń strony przeciwnej oraz dotkliwie odczuwalne tego skutki.

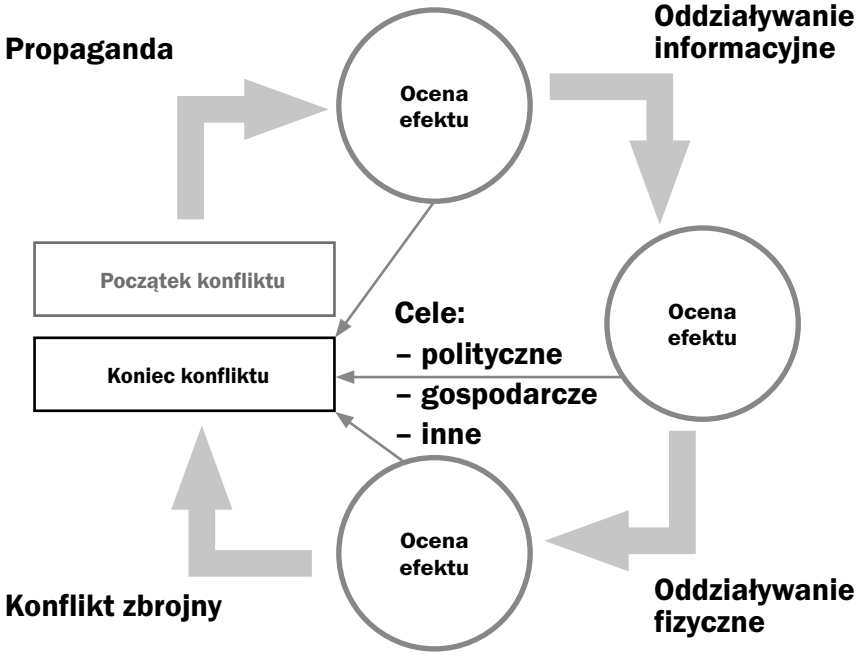
Można przyjąć, że konflikt w cyberprzestrzeni obejmie kilka zasadniczych etapów (rys. 2). Pierwszy – budowanie przewagi informacyjnej – będzie polegał na kreowaniu pozytywnego własnego wizerunku na arenie międzynarodowej oraz we własnym społeczeństwie, a także w społeczeństwie przeciwnika, z jednoczesnym oczernianiem strony przeciwnej. Drugi etap – rozpoznanie systemu informacyjnego przeciwnika – zostanie ukierunkowany na elementy składowe tego systemu, zasoby informacyjne, procedury postępowania oraz infrastrukturę krytyczną. Jednocześnie będzie prowadzone przeciwrozpoznanie, czyli będą wykonywane czynności polegające na myleniu i dezinformowaniu przeciwnika oraz zapewnianiu ochrony własnego systemu informacyjnego. W ostatnim etapie zostanie obezwładniony system informacyjny strony przeciwnej w wyniku oddziaływania informatycznego i fizycznego (kinetycznego).

35 P. Dela, P. Stobiecki, *Przestrzeń informacyjna współczesnych konfliktów zbrojnych*, Warszawa 2017, s. 63.



Rys. 1. Elementy walki w cyberprzestrzeni

Opracowanie własne autora



Rys. 2. Etapy konfliktu zbrojnego z wykorzystaniem cyberprzestrzeni
Opracowanie własne autora

Celem walki w cyberprzestrzeni jest przejście do klasycznych działań zbrojnych z pozycji uprzywilejowanej lub też zmuszenie przeciwnika do uległości na drodze samego oddziaływania w cyberprzestrzeni. Etapy tej walki mogą się wzajemnie przenikać i uzupełniać i będą występowały, z różnym nasileniem, przez cały czas trwania konfliktu.

Podsumowanie

Budowanie kompetencji państwa potrzebnych do prowadzenia działań zbrojnych w cyberprzestrzeni jest procesem złożonym i czasochłonnym. Wymaga uwzględnienia różnorodnych czynników, choćby takich jak podsiadane zasoby fizyczne i osobowe czy uwarunkowania doktrynalne, sojusznicze i ekonomiczne. Niemiej jednak na podstawie analizy współczesnych konfliktów zbrojnych oraz innych niekorzystnych zjawisk w cyberprzestrzeni można skonstatować, że takie państwo jak Polska powinno jak najszybciej nadrobić zaległości i zbudować kompetencje niezbędne do prowadzenia działań zbrojnych w cyberprzestrzeni. Budowanie tego rodzaju kompetencji powinno cechować się systemowością i być oparte na wcześniej zdefiniowanym zbiorze zasad[36]. ■

36 Wprawdzie jesienią 2020 r. została przyjęta doktryna DD 3.20, dotycząca operacji w cyberprzestrzeni, to jeszcze daleka droga do stworzenia rodzaju sił zbrojnych zdolnego do prowadzenia działań w cyberprzestrzeni.

STRESZCZENIE:

W artykule podjęto próbę określenia zasadniczych elementów służących do budowania kompetencji podmiotu bezpieczeństwa, jakim jest państwo, w obszarze działań (walki zbrojnej) w cyberprzestrzeni. Scharakteryzowano współczesne konflikty oraz walkę zbrojną, z uwzględnieniem zwłaszcza działań w cyberprzestrzeni. Zwrócono uwagą na konieczność systemowego ujęcia problematyki oraz przedstawiono najważniejsze elementy systemu walki w cyberprzestrzeni. Omówiono zasady sztuki wojennej, które powinny stanowić podstawę do budowania kompetencji państwa w przestrzeni cybernetycznej. Przeanalizowano potencjalny przebieg konfliktu zbrojnego z wykorzystaniem cyberprzestrzeni.

SŁOWA KLUCZOWE

system, cyberprzestrzeń, bezpieczeństwo cyberprzestrzeni, walka zbrojna, siły zbrojne

Bibliografia

Analysis of the Cyber Attack on the Ukrainian Power Grid, E-ISAC, Washington DC 2016.

Balcerowicz B., *Czym jest współczesna wojna*? wersja HTML pliku, http://dlibra.kul.pl/Content/31109/34038__Balcerowicz-Bolesla_0000.pdf/.

Balcerowicz B., *Wojna. Kwestie nie tylko terminologiczne*, „Myśl Wojskowa" 2003 nr 2, s. 53–74.

Blaug M., *Teoria ekonomii. Ujęcie retrospektywne*, Warszawa 1994.

Bojarski R., *Operacja obronna*, Warszawa 1999.

Dela P, Stobiecki P., *Przestrzeń informacyjna współczesnych konfliktów zbrojnych*, Warszawa 2017.

Gruszczak A., *Hybrydowość współczesnych konfliktów zbrojnych – analiza krytyczna*, www.bbn.gov.pl/download/1/8755/Hybrydowoswspolczesnychwojenanalizakrytyczna.pdf/.

Huzarski M., *Działania taktyczne (materiał do studiowania)*, Warszawa 1992.

Instrukcja zgrywania systemów walki w SZRP, DD/7.1.2, Warszawa 2011.

Konieczny J., *Cybernetyka walki*, Warszawa 1970.

Kotarbiński T., *Hasło dobrej roboty*, Warszawa 1975.

Kotarbiński T., *Traktat o dobrej robocie*, Wrocław–Warszawa–Kraków–Gdańsk–Łódź 1982.

Koziej S., *Teoria sztuki wojennej*, Warszawa 1993.

Koziej S. et al., *Działania taktyczne wojsk lądowych*, Warszawa 1992.

Koziej S. et al., *Działania operacyjne*, Warszawa 1993.

Mała encyklopedia wojskowa, Warszawa 1979.

Munkler H., *Wojny naszych czasów*, Kraków 2004.

Piątkowski K., *Wojna nowego typu*, „Polska w Europie" 2002 nr 1, s. 19–46.

Polak A., *Sztuka wojenna. Kontekst teoretyczny i praktyczny*, „Zeszyty Naukowe Akademii Obrony Narodowej" 2013 nr 3, s. 219–228.

Sienkiewicz P., *Inżynieria systemów*, Warszawa 1983.

Sienkiewicz P., *Podstawy teorii systemów*, Warszawa 1993.

Ścibiorek Z., *Działania taktyczne wojsk lądowych*, Warszawa 1996.

Article history: Received: 24.11.2020; Reviewed: 29.11.2020; Accepted: 10.12.2020

DOI: 10.5604/01.3001.0014.6161

Corresponding author: Col Piotr Dela, PhD, Eng., Kalisz Academy (Akademia Kaliska), Kalisz, Poland; ORCID: 0000-0003-3643-3759, e-mail: delson@wp.pl

Cite this article as: Dela P., Col., PhD, Eng., "Elements of Cyberspace Warfare System". bellona quart. 2020(3): 69–84

Competing interests: The authors declare that they have no competing interests.

Table of content URL: https://kwartalnikbellona.com/issue/12943

Author's bio: Col Piotr Dela, PhD, Eng.
He's a research academic at War Studies University (ASzWoj). He is a graduate of the Faculty of Military Cybernetics at Military University of Technology (WAT), and of postgraduate studies at National Defense University (AON) and the Institute of World Politics in Washington. He authors over 100 articles, essays, manuals, monographies, and scientific publications. His scientific interests focus on decision-support systems, ICT systems and networks, and on informational and cyberspace security.

THE BELLONA QUARTERLY ISSN: 1897-7065 | E-ISSN: 2719-3853

KWARTALNIK BELLONA

O potrzebie strukturalnych przemian w systemie bezpieczeństwa cyberprzestrzeni

Recenzja monografii płk. dr. hab. inż. Piotra Deli *Teoria walki w cyberprzestrzeni*

płk w st. spocz. prof. dr hab. Zbigniew Ścibiorek

ORCID: 0000-0002-7408-4302
e-mail: zbscibi@wp.pl
Międzynarodowa Wyższa Szkoła Logistyki i Transportu we Wrocławiu

ABSTRACT:

The book covers the most important issues related to the cyber threat. It presents the basics of the combat in cyberspace, primarily focused on the security of ICT networks and critical infrastructure systems. It is a publication that also organizes the concepts related to the combat in cyberspace.

KEYWORDS:

cyberspace, cyberspace combat, security, system, armed forces

Dla osób zawodowo zajmujących się utrzymaniem sieci teleinformatycznych i systemów infrastruktury krytycznej coraz większym problemem staje się zapewnienie bezpieczeństwa cyberprzestrzeni. Przekłada się ono bowiem wprost na bezpieczeństwo jego użytkowników – tych, którzy wykorzystują to środowisko w pracy zawodowej czy w życiu codziennym. Niemal każdego dnia docierają do nas informacje o zagrożeniach polegających na kradzieży pieniędzy czy tożsamości. Słyszymy o atakach na infrastrukturę krytyczną – jako przykłady można wskazać atak na sieć energetyczną na Ukrainie z 2015 roku czy ataki na instalacje naftowe w Arabii Saudyjskiej, w tym także kinetyczne. Coraz częściej mówi się o oddziaływaniu informacyjnym na decydentów i społeczeństwa prowadzonym w cyberprzestrzeni za pomocą portali społecznościowych. Pojawiają się doniesienia o wpływaniu na wyborców oraz o szerzeniu niepokojów społecznych koordynowanym przez tego rodzaju portale. Skala zagrożeń płynących z cyberprzestrzeni, mimo niezaprzeczalnych zalet użytkowych, gospodarczych i społecznych tej sfery, jest coraz większa i staje się wyzwaniem dla współczesnego świata. Tym bardziej że oprócz aktywności pojedynczych graczy, potocznie nazywanych hakerami, w cyberprzestrzeni dostrzegalne jest zjawisko usystematyzowania wrogiej działalności prowadzonej przez zorganizowane grupy na zlecenie państw czy też przez same państwa, dążące do osiągnięcia swoich celów strategicznych. Dlatego niezbędne staje się budowanie kompetencji państwa w zakresie prowadzenia w przestrzeni cybernetycznej własnych interesów oraz osiągania w niej celów strategicznych. Tym zagadnieniom jest poświęcona monografia *Teoria walki w cyberprzestrzeni* autorstwa płk. dr. hab. inż. Piotra Deli.

Pułkownik Dela od wielu lat zajmuje się problematyką wojskowych sieci teleinformatycznych, ich funkcjonowaniem oraz strukturą organizacyjną, a także bezpieczeństwem. Ma bogate doświadczenie badawczo-dydaktyczne, zdobyte w Akademii Sztuki Wojennej w Warszawie oraz Akademii Kaliskiej w Kaliszu. Swoje dociekania naukowe koncentruje na obszarze sztuki wojennej oraz nowoczesnych technologii teleinformatycznych wykorzystywanych na potrzeby bezpieczeństwa i obronności państwa. Wiele opracowań naukowych Autora zostało zastosowanych w praktyce. Przykładem – koncepcja domen informacyjnych zaimplementowana w wojskowych sieciach teleinformatycznych czy koncepcja zarządzania informacją w środowisku o niskiej przepływności wykorzystana w systemie zarządzania polem walki. Płk dr hab. inż. Piotr Dela uczestniczył w pracach zespołów eksperckich, które opiniowały normy i doktryny na potrzeby Sił Zbrojnych RP, oceniał krajowe projekty badawcze w ramach współpracy z Narodowym Centrum Badań i Rozwoju, a także recenzował międzynarodowe projekty badawcze w ramach współpracy z Komisją Europejską.

Z zaciekawieniem więc sięgnąłem po najnowszą publikację pułkownika Deli – monografię *Teoria walki w cyberprzestrzeni*, wydaną przez Akademię Sztuki Wojennej na początku bieżącego roku. Jak Autor zaznaczył we wstępie, tytuł publikacji jest nieprzypadkowy i kontrowersyjny. Chodzi o określenie „teoria". W pracy zostały omówione istotne kwestie bezpieczeństwa państwa w cyberprzestrzeni, w środowisku, które zmieniło funkcjonowanie ludzkości w sposób dotychczas niespotykany. Z jednej strony cyberprzestrzeń ma pozytywne aspekty, związane z możliwością wymiany informacji, dostępem do niej, kształtowaniem nowych form organizacyjnych i społecznych. Z drugiej strony stanowi zagrożenie, co wynika z niedoskonałości zarówno jej samej, jak i jej użytkowników. Owo zagrożenie staje się tym

większe, im bardziej w sposób celowy przestrzeń ta jest wykorzystywana przez podmioty państwowe do realizacji własnych interesów narodowych.

Monografia stanowi jedną z nielicznych publikacji porządkujących pojęcia związane z kooperacją negatywną w cyberprzestrzeni, postrzeganą jako walka. Autor w sposób przemyślany identyfikuje cztery obszary, w których dochodzi do walki. Są to: zagrożenia naruszające bezpieczeństwo samej cyberprzestrzeni (zagrożenia informatyczne), zagrożenia wynikające z wykorzystania cyberprzestrzeni do dezinformacji i propagandy (zagrożenia informacyjne), zagrożenia wynikające z uzależnienia od działania cyberprzestrzeni (zagrożenia techniczno-technologiczne) oraz zagrożenia związane z wykorzystaniem sztucznej inteligencji (zagrożenia nieznane – prognozowane). Problemy poruszone w monografii, choć w pewnej mierze już określone, nie są jednak trywialne, przeciwnie – zostały przedstawione w sposób unikatowy. Ma to szczególną wartość, ponieważ inni naukowcy często te zagadnienia pomijają i skupiają się wyłącznie na obszarze zagrożeń oraz bezpieczeństwie cyberprzestrzeni.

Autor stawia fundamentalne pytania o funkcjonowanie państwa i państwowości w przestrzeni cybernetycznej, wysuwa propozycję stworzenia w niej podwalin państwowości, która pozwoli przetrwać państwu w razie utraty niepodległości i terytorium. Trafnie zauważa, że walkę w cyberprzestrzeni należy postrzegać przez pryzmat systemu złożonego z elementów wewnętrznych wzajemnie powiązanych realizacjami oraz elementów zewnętrznych, znajdujących się w otoczeniu warunkującym funkcjonowanie elementów wewnętrznych oraz celowość działania systemu. Podkreśla – co uznaję za niezwykle cenne – że w walce tej nie można ograniczać się tylko do cyberprzestrzeni i tylko do obrony. Poruszając się w materii, która z jednej strony powinna być dobrze zbadana (sztuka wojenna), a z drugiej podlega ciągłym i dynamicznym przemianom (cyberprzestrzeń) Autor precyzyjnie formułuje myśli, posługuje się językiem prostym, zwięzłym i zrozumiałym. Nie wprowadza nowych terminów, które miałyby zastąpić powszechnie używane i akceptowane w imię – jak to określa – nowoczesności i naukowości. Zwraca uwagę, że nowoczesne państwo musi prowadzić walkę w cyberprzestrzeni, w warunkach pokoju ograniczoną do rozpoznania, odziaływania informacyjnego i stałego budowania zdolności do rażenia.

Autor umiejętnie korzysta z dorobku uznanych naukowców, głównie z dziedziny sztuki wojennej i teorii systemów, dokonuje transpozycji ich poglądów w wielu wymiarach do cyberprzestrzeni. Świadczy to o jego znakomitym rozumieniu technicznych aspektów przestrzeni cybernetycznej, ale to zrozumiałe, wszakże jest absolwentem Wydziału Cybernetyki Wojskowej Akademii Technicznej. Zwraca uwagę na aspekty, rolę i znaczenie systemu prawnego, który umożliwia prowadzenie działań w cyberprzestrzeni, oraz systemu edukacyjnego, odpowiedzialnego za kształcenie specjalistów. Cenne i warte uwzględnienia w trakcie tworzenia wojsk cybernetycznych w Polsce są rozważania dotyczące systemu walki, przedstawione w szóstym rozdziale.

Podsumowując, monografia *Teoria walki w cyberprzestrzeni* jest pierwszą publikacją porządkującą pojęcia związane z walką w cyberprzestrzeni. Powinna być traktowana jako punkt wyjścia do dalszych rozważań w tym obszarze badawczym, dla zainteresowanych walką w cyberprzestrzeni oraz cyberbezpieczeństwem może stanowić zaś swego rodzaju słownik pojęć i zaleceń. Publikacja jest adresowana przede wszystkim do decydentów odpowiedzialnych za budowanie systemów bezpieczeństwa cyberprzestrzeni. Także do

menedżerów, którzy w swojej działalności biznesowej powinni uwzględniać elementy walki informacyjnej ukierunkowanej na działanie z pozycji dodatniej. Ze względu na przystępny język i czytelny układ, mający znamiona systemowości, dzieło to powinno wejść do kanonu prac wykorzystywanych w edukacji z zakresu bezpieczeństwa państwa. ■

STRESZCZENIE:

W monografii omówiono najistotniejsze kwestie dotyczące zagrożenia cybernetycznego. Przedstawiono podstawy walki w cyberprzestrzeni, ukierunkowanej głównie na bezpieczeństwo sieci teleinformatycznych i systemów infrastruktury krytycznej. Uporządkowano także pojęcia związane z walką w przestrzeni cybernetycznej.

SŁOWA KLUCZOWE:

cyberprzestrzeń, walka w cyberprzestrzeni, bezpieczeństwo, system, siły zbrojne

Article history: Received: 7.12.2020; Reviewed: 20.12.2020; Accepted: 22.12.2020

DOI: 10.5604/01.3001.0014.6162

Corresponding author: Col (ret) Prof Zbigniew Ścibiorek, PhD, The International University of Logistics and Transport in Wrocław, Poland; ORCID: 0000-0002-7408-4302; e-mail: zbscibi@wp.pl

Cite this article as: Zbigniew Ścibiorek, Col (ret) Prof, PhD, "On the Need for Structural Changes in the Cyberspace Security System. Review of a monograph by Col Eng Piotr Dela, PhD, entitled »Teoria walki w cyberprzestrzeni« (Cyberspace Warfare Theory)". bellona quart. 2020(3): 85–88

Policy: The content of the journal is circulated on the basis of the Open Access which means free and limitless access to scientific data.

Competing interests: The authors declare that they have no competing interests.

Table of content URL: https://kwartalnikbellona.com/issue/12943

Author's bio: Col (ret) Prof Zbigniew Ścibiorek, PhD
Professor at the International University of Logistics and Transport in Wrocław. He has performed many didactic functions and held many military staff and command positions. Author of numerous publications concerning the battlefield, the geopolitical situation, control and command, as well as security studies methodology. Science editor of a series of publications entitled "Education for Security."

Wskazówki redakcyjno-techniczne dotyczące przygotowania prac do opublikowania w „Kwartalniku Bellona”

Redakcja przyjmuje oryginalne artykuły naukowe, artykuły przeglądowe, artykuły i komunikaty badawcze, artykuły recenzyjne w języku angielskim i polskim (lub innym języku autora korespondencyjnego). Redakcja zastrzega sobie możliwość tłumaczenia wybranych artykułu na język angielski.

1. Przygotowanie tekstu

Edytor MS Word, czcionka Times New Roman 12 pkt (przypisy – 10 pkt), odstęp między wierszami – 1,5, marginesy normalne (górny, dolny, lewy, prawy – 2,5 cm). Objętość artykułu – 20 000–30 000 znaków. Artykuł powinien zawierać streszczenie w języku polskim i angielskim (maksymalnie 1200 znaków) oraz pięć słów kluczowych.

Do pracy należy dołączyć:

– pismo, w którym autor zwraca się do redakcji o wydrukowanie artykułu w czasopiśmie (jest to formalna zgoda autora na publikację pracy), podaje swój dokładny adres, zatrudnienie, numer telefonu, adres e-mailowy oraz składa podpis z podaniem tytułu naukowego i stanowiska;

– pisemne oświadczenie, że artykuł dotychczas nie był ogłoszony drukiem i nie został złożony w innej redakcji. W przypadku wykorzystywania rysunków wcześniej opublikowanych lub pochodzących od innych autorów należy dołączyć pisemną zgodę autorów i wydawnictwa na ich wykorzystanie.

Wojskowy Instytut Wydawniczy zastrzega sobie prawo do dokonywania poprawek, skracania lub uzupełniania artykułów bez naruszenia zasadniczych myśli autora, do wprowadzania własnych tytułów oraz zamieszczania publikacji, w języku polskim i angielskim, na stronie internetowej www.kwartalnikbellona.pl

2. Struktura artykułu

Każdy składany manuskrypt, z wyjątkiem recenzji i dyskusji naukowych, powinien być przygotowany w międzynarodowym standardzie naukowym, w schemacie AIMRaD (Abstract, Introduction, Materials and Methods, Results, and Discussion):

– wstęp – przedstawiający cele i przyczyny powstania artykułu oraz znaczenie tematu, który podejmuje;

– przegląd literatury – przedstawiający dotychczasowy dorobek nauki w zakresie badania danego zagadnienia. W przypadku artykułów innowacyjnych dopuszczalne jest stwierdzenie o braku literatury dotyczącej omawianego tematu;

– metodologia – opis metod badawczych stosowanych przez autora oraz źródeł danych i informacji wykorzystanych w czasie tworzenia manuskryptu wraz z uzasadnieniem;

– wyniki i dyskusja – opis najważniejszych wyników oraz ich interpretacja, także na tle istniejącej literatury. Dopuszczalne jest przedstawienie wyników i dyskusji w osobnych sekcjach;

– wnioski – przedstawienie najważniejszych wniosków i rekomendacji autora dotyczących badanego zagadnienia. Ta sekcja powinna stanowić samodzielny tekst, pozwalający na zrozumienie zagadnienia bez konieczności lektury reszty artykułu;

– bibliografia.

Abstrakt i strona tytułowa są wprowadzane osobno przez system składania artykułów dostępny w zakładce. Abstrakt i słowa kluczowe powinny być napisane w języku angielskim oraz polskim (i/lub języku narodowym autora korespondencyjnego).

3. Sporządzanie przypisów

– poszczególne elementy opisu oddzielamy przecinkami;

– nazwę autora podajemy w formie: inicjał imienia z kropką (w wypadku kilku inicjałów imion zapisujemy je bez spacji, np. D.M.), spacja, nazwisko. Pomijamy tytuły naukowe i zawodowe. Jeśli autorów jest dwóch lub trzech, podajemy ich nazwiska, oddzielając je przecinkami. Jeśli autorów jest wię-

cej niż trzech, to podajemy nazwisko pierwszego i zamieszczamy dopisek et al. (*et alli* – i inni);
– tytuł pracy zapisujemy kursywą;
– stosujemy skróty łacińskie: *op.cit.* (dzieło cytowane), *vide* (zobacz), *ibidem* (tamże), *idem* (tenże), *eadem* (taż), *eidem* (ci sami), *passim* (w różnych miejscach);
– oznaczamy brak: roku wydania – [s.a.] – *sine anno*, miejsca wydania – [s.l.] – *sine loco*, miejsca i roku wydania – [s.a.e.l.] – *sine anno et loco*.
Przykłady:
K. Ficoń, *Międzynarodowe standardy zarządzania ryzykiem*, „Kwartalnik Bellona" 2013 nr 3, s. 31–50.
Idem, *Ryzyko etapowe w zarządzaniu kryzysowym*, „Kwartalnik Bellona" 2015 nr 1, s. 11–30.
B. Balcerowicz, *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010, s. 12.
Ibidem, s. 16.
A. Polak, *Bibliografia teorii sztuki wojennej w latach 1945–1989*, Warszawa 2009, s. 119.
B. Balcerowicz, *Siły zbrojne*…, op.cit., s. 13.
Źródła do dziejów powstań śląskich, t. 1. *Październik 1918–styczeń 1920*, cz. I, H. Zieliński (oprac.), Wrocław–Warszawa–Kraków 1963, s. 178.
E. de Amicis, *Serce. Książka dla chłopców*, tłum. M. Konopnicka, Warszawa [s.a.], s. 36.

Opis wydawnictw zwartych
– podajemy kolejno: inicjał(y) imienia (imion), nazwisko, tytuł zapisany kursywą (przy tłumaczeniach podajemy nazwisko tłumacza poprzedzone skrótem tłum.), miejsce i rok wydania, numer strony, np.:
R.A. Heinlein, *Kawaleria kosmosu*, Warszawa 1994, s. 54.

Opis wydawnictwa zbiorowego
podajemy: tytuł publikacji, inicjał(y) imienia (imion) i nazwisko redaktora z oznaczeniem: red. w nawiasie, miejsce i rok wydania, stronę, np.:
Ekonomia a wojna. Studia i szkice, M. Franz (red.), Toruń 2011, s. 9.

Opis artykułu w wydawnictwie zbiorowym
podajemy: inicjał(y) imienia (imion) i nazwisko autora, tytuł zapisany pismem pochyłym, przyimek w z dwukropkiem, tytuł wydawnictwa zapisany pismem pochyłym, inicjał imienia i nazwisko redaktora, skrót red. w nawiasie, miejsce i rok wydania, stronę, np.:
I. Clark, *Globalizacja i ład pozimnowojenny, w: Globalizacja polityki światowej. Wprowadzenie do stosunków międzynarodowych*, J. Baylis, S. Smith (red.), Kraków 2008, s. 912–913.

Opis czasopism i gazet
podajemy: inicjał imienia i nazwisko autora, tytuł zapisany pismem pochyłym, nazwę czasopisma w cudzysłowie (polski cudzysłów ma postać: „ … "), bezpośrednio po niej (bez rozdzielania przecinkiem) rok wydania, tom, zeszyt lub numer i stronę. W wypadku gazet codziennych podajemy nazwę gazety w cudzysłowie i dalej, bez przecinka, dzień, miesiąc i rok wydania, np.:
W.S. Lind, *Understanding the fourth generation war*, „Military Review" 2004 No. 10, s. 12–16.
Ł. Kamieński, *Nieuświadomiona percepcja, czyli neurobiologia na usługach amerykańskiej armii*, „Kwartalnik Bellona" 2014 nr 3, s. 196–206.
A. Słojewska, *Dwa tygodnie na porozumienie z Grecją*, „Rzeczpospolita" 15.05.2015.

Opis dokumentów elektronicznych
podajemy: inicjał(y) imienia (imion) i nazwisko autora, tytuł zapisany pismem pochyłym, w nawiasie prostokątnym typ nośnika i wersję, następnie miejsce i rok wydania. W przypadku dokumentów na stronach WWW podajemy adres sieciowy oraz datę dostępu w nawiasie kwadratowym, np.:
W. Kopaliński, *Wielki multimedialny słownik Władysława Kopalińskiego* [CD-ROM, wersja 1.00.00], Warszawa 2000.
L. Sly, *Al-Qaeda force captures Fallujah amid rise in violence in Iraq*, „The Washington Post" [online], 3.01.2014, http://www.washingtonpost.com/world/al-qaeda-force-captures-fallujah-amid-

rise-in-violence-in-iraq/2014/01/03/8abaeb2a-74aa-11e3-8def-a33011492df2_story.html [dostęp: 9.01.2015].

Cytowanie archiwaliów
podajemy: nazwę instytucji przechowującej dany dokument, jej skrót lub akronim z określeniem siedziby (miejscowości), nazwę jednostki archiwalnej (zespołu akt) lub tematykę opisywanej jednostki, sygnaturę lub inne oznaczenie identyfikacji dokumentu, liczbę i numer strony (karty), np.:
Centralne Archiwum Wojskowe w Warszawie (dalej: CAW), Oddział II SGWP, sygn. I.303.4.5755, Sprawozdanie Malskiego z akcji „Łom", k. 8–9.

4. Tabele, rysunki i fotografie
– materiał graficzny (fotografie, mapy) należy dostarczać jako osobne pliki, zapisane w formacie JPG lub TIF (w rozdzielczości nie mniejszej niż 300 dpi). Warunkiem umieszczenia ich w wydaniu jest posiadanie przez autora artykułu zgody na ich wykorzystanie (dotyczy to również materiałów ze stron internetowych; nie wystarczy podanie daty dostępu). W danym artykule rysunki i fotografie powinny mieć numerację ciągłą;
– określenie „Tabela" z numerem zapisanym liczbą arabską i tytułem umieszczamy nad tabelą. Pod tabelą należy wskazać źródło;
– przypisy do tabeli zamieszczamy pod tabelą (nie w tekście głównym). Jako odsyłaczy używamy gwiazdek, a w przypadku większej liczby odsyłaczy – małych liter;
– określenie „Rys." umieszczamy pod rysunkiem. Każdy rysunek powinien mieć numer i tytuł. Pod rysunkiem podajemy źródło;
– rysunki powinny być przygotowane w pliku edytowalnym w formacie AI, EPS lub PDF.

5. Bibliografia
W bibliografii obowiązuje układ alfabetyczny według nazwiska autora. Dopuszcza się podział bibliografii na: źródła/archiwalia, monografie, artykuły, artykuły elektroniczne, jednak nie jest to wymagane. Podajemy: nazwisko autora, inicjał(y) imienia, tytuł, miejsce wydania, rok wydania.
Balcerowicz B., *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010.

6. Kontrola jakości
Wszystkie artykuły składane do „Kwartalnika Bellona" przechodzą procedurę recenzencką *double blind peer-review*. W związku z tym prosimy o składanie artykułów pozbawionych cech pozwalających na identyfikację autora.

7. Standardy etyczne
Redakcja „Kwartalnika Bellona" stosuje zasady etyki publikacyjnej zgodne z wytycznymi Komitetu do spraw Etyki Publikacyjnej COPE (Committee on Publication Ethics).
Link: https://publicationethics.org/.

8. Opłaty za publikację
Redakcja nie pobiera opłat na żadnym etapie publikacji artykułów.

9. Składanie artykułów
Do publikacji przyjmujemy wyłącznie artykuły składane przez zakładkę „Złóż manuskrypt" na naszej stronie www.kwartalnikbellona.pl.

10. Publikacja
Po pozytywnym przejściu procesu recenzenckiego artykuł ukazuje się w wersji drukowanej, a także cyfrowej na stronie www.kwartalnikbellona.pl. Każdy otrzymuje numer DOI i jest kierowany do zamieszczenia w międzynarodowych bazach naukowych.

Wszelkie zmiany od ww. zasad należy uzgadniać z redaktorem prowadzącym. Zastrzegamy sobie prawo do redakcyjnego opracowania tekstów.

SZANOWNI CZYTELNICY!

Zapraszamy do składania zamówień na prenumeratę „Kwartalnika Bellona”
Jej koszt w 2021 roku wynosi 100 zł (cztery wydania w cenie 25 zł każde)

Prenumeratę można zamówić:
– e-mailem: prenumerata@zbrojni.pl
– listownie: Wojskowy Instytut Wydawniczy, 00-909 Warszawa, Aleje Jerozolimskie 97
– telefonicznie: +48 261 849 494
Warunkiem wysyłki kwartalnika jest wpłata na konto: 23 1130 1017 0020 1217 3820 0002

Cena 25 zł (w tym 8% VAT)

ISSN 1897-7065
E-ISSN: 2719-3853