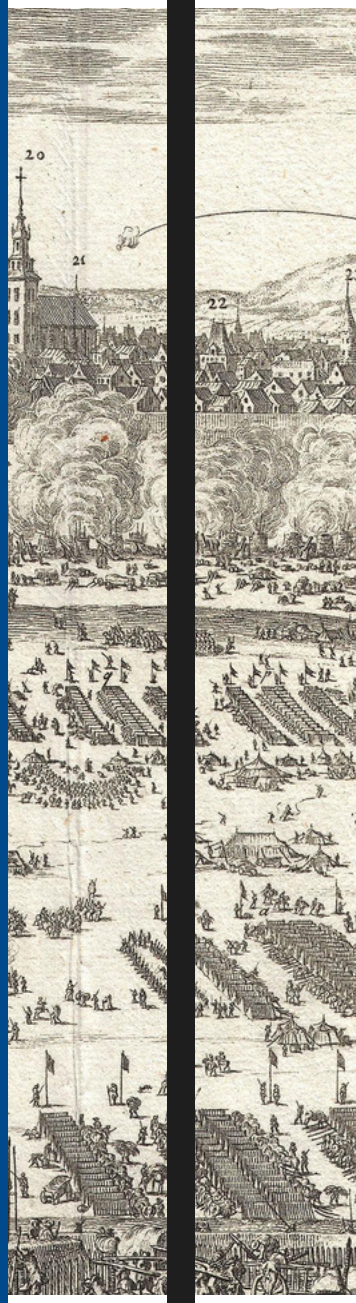
JAGIELLOŃSKI PRZEGLĄD BEZPIECZEŃSTWA



1

2016

Zakład Bezpieczeństwa Narodowego UJ

JAGIELLOŃSKI PRZEGLĄD BEZPIECZEŃSTWA

The Jagiellonian Security Review

Jagielloński Przegląd Bezpieczeństwa jest recenzowanym czasopismem naukowym wydawanym przez Zakład Bezpieczeństwa Narodowego Instytutu Nauk Politycznych i Stosunków Międzynarodowych Uniwersytetu Jagiellońskiego w Krakowie.

Zakład Bezpieczeństwa Narodowego został utworzony w 2015 r. Tworzą go naukowcy i praktycy o szerokiej wiedzy i doświadczeniu w zakresie bezpieczeństwa narodowego i międzynarodowego, konfliktów regionalnych, studiów strategicznych i prawnych aspektów współczesnego bezpieczeństwa.

Więcej informacji na stronie internetowej: http://www.zbn.inp.uj.edu.pl/

The Jagiellonian Security Review is a double-blind peer reviewed open access scholarly journal published by the National Security Chair at the Institute of Political Science and International Relations of Jagiellonian University in Krakow.

The National Security Chair was established in 2015. It is constituted by the team of scholars with extensive expertise in national and international security, regional conflicts, strategic studies and legal affairs.

More information on the webpage: http://www.zbn.inp.uj.edu.pl/en_GB/

JAGIELLOŃSKI PRZEGLĄD BEZPIECZEŃSTWA

The Jagiellonian Security Review

Informacje dla Autorów

Zapraszamy pracowników naukowych i doktorantów oraz specjalistów i ekspertów z ośrodków naukowych i analitycznych w kraju i za granicą do składania oryginalnych, dotąd niepublikowanych i nierozpatrywanych w tym samym czasie przez inną redakcję artykułów naukowych oraz recenzji książek. Przyjmujemy artykuły napisane zarówno w języku polskim, jak i angielskim. Ostateczna decyzja Redakcji o przyjęciu artykułu do publikacji zależy od uzyskania pozytywnego wyniku anonimowego procesu recenzyjnego. Recenzenci są wyznaczani przez Redakcję spośród specjalistów zajmujących się daną dziedziną.

Wytyczne dla Autorów są dostępne na stronie internetowej: http://www.przeglad.uj.edu.pl/dla-autorow

Contributions

The Jagiellonian Security Review welcomes original submission of scholarly and scientific research from academic specialists, security policymakers and analysts from Poland and abroad.
Submission guidelines are available at: *http://www.zbn.inp.uj.edu.pl/en_GB/*
Submit articles for consideration to the address below.

Adres redakcji / Correspondence to: Jagielloński Przegląd Bezpieczeństwa, INPiSM UJ, ul. Jabłonowskich 5, 31-114 Kraków; e-mail: jpb@uj.edu.pl.

Strona internetowa / Webpage: http://www.przeglad.uj.edu.pl/

Pierwotną formą czasopisma jest wersja elektroniczna.

JAGIELLOŃSKI PRZEGLĄD BEZPIECZEŃSTWA

The Jagiellonian Security Review

nr 1 (1) • 2016

Od Redaktora

Współczesne bezpieczeństwo jest tym wymiarem rzeczywistości, który stale rozszerza się, przenika życie polityczne, społeczne, gospodarcze, kulturalne, religijne. Wkracza w liczne i różnorodne dziedziny: zarówno tradycyjne, jak obronność, ład publiczny, produkcja przemysłowa, jak i współczesne, takie jak informatyka, telekomunikacja, środki masowego przekazu. Bezpieczeństwo przestało być domeną państwa: jego instytucji, służb i organów. W coraz większym zakresie kształtowane jest przez podmioty pozapaństwowe, te działające z pozytywnymi skutkami oraz te, które wywołują negatywne konsekwencje, dysfukcyjne wobec istniejącego ładu ustrojowego i porządku publicznego.

Głównym elementem dzisiejszej refleksji nad bezpieczeństwem jest świadomość rosnącej mnogości i różnorodności zagrożeń, które tworzą liczne i rozproszone źródła ryzyka oraz prowadzą do rozprzestrzenienia lęku i niepewności we współczesnych społeczeństwach. Międzynarodowe konflikty zbrojne, wojny domowe, terroryzm i ekstremizm, zorganizowana przestępczość międzynarodowa, niekontrolowane migracje, cyberprzestępczość, wojna informacyjna, dysfunkcyjność państw, osłabienie norm i instytucji praworządności to najważniejsze pozycje obszernego katalogu aktualnych zagrożeń i problemów bezpieczeństwa. Stawiają one przed badaczami wymóg pogłębionej refleksji, dociekliwości poznawczej, wnikliwej analizy oraz nowatorstwa metodologicznego.

Zespół naukowców, nauczycieli akademickich i ekspertów o ogromnym doświadczeniu praktycznym w zakresie bezpieczeństwa działających w ramach Zakładu Bezpieczeństwa Narodowego Instytutu Nauk Politycznych i Stosunków Międzynarodowych Uniwersytetu Jagiellońskiego od kilku lat podejmuje działania naukowo-badawcze, dydaktyczne i popularyzatorskie służące zgłębianiu wiedzy teoretycznej i praktycznej o mechanizmach, regułach, instytucjach i obszarach bezpieczeństwa. Są one ujmowane w perspektywie historycznej i współczesnej, a nawet prognostyczno-planistycznej, odnoszą się do aspektów bezpieczeństwa wewnętrznego, narodowego i międzynarodowego. Zmierzają do interdyscyplinarnego, pogłębionego, analitycznego spojrzenia na odmiany i formy bezpieczeństwa występujące w różnych wymiarach przeszłości i współczesności.

Jagielloński Przegląd Bezpieczeństwa jest nowym czasopismem naukowym, które zrodziło się z potrzeby wzbogacenia współczesnej debaty o bezpieczeństwie toczonej w Polsce i za granicą. Wychodząc od bieżącej aktywności naukowej pracowników Zakładu Bezpieczeństwa Narodowego INPiSM UJ, otwiera możliwość i zachęca do udziału w tej debacie przedstawicieli ośrodków akademickich, naukowych i eksperckich z kraju i zagranicy. Będzie towarzyszyć innym ważnym cyklicznym przedsięwzięciom Zakładu Bezpieczeństwa Narodowego: międzynarodowej (globalnej) Jagiellonian Interdisciplinary Security Conference; krajowej Jagiellońskiej Konferencji Bezpieczeństwa; wykładom otwartym Zakładu Bezpieczeństwa Narodowego UJ.

Zapraszam do włączenia się do debaty na łamach Jagiellońskiego Przeglądu Bezpieczeństwa z pożytkiem dla rozwoju polskich badań nad bezpieczeństwem oraz ich wkładu w międzynarodową refleksję nad współczesnymi problemami bezpieczeństwa.

Artur Gruszczak

Redaktor Naczelny

Editorial

Contemporary security is that realm of reality which is constantly expanding, penetrating political, social, economic, cultural and religious life. It is embedded in numerous and varied fields: traditional, such as defence, public order, industrial production as well as modern, such as information technologies, telecommunication, mass media. Security no longer is the domain of the state along with its institutions, services and bodies. It is increasingly shaped by non-state actors, those which produce positive effects, and those which have negative repercussions, dysfunctional with regard to the existing political and public order.

The main element of today's reflection on security is the awareness of the growing multiplicity and variety of threats which generate numerous and scattered sources of risk and contribute to the spreading of fear, anxiety and uncertainty in modern societies. International armed conflicts, civil wars, terrorism and extremism, international organised crime, uncontrolled migration, cybercrime, information war, dysfunctionality of states, weakening of norms and institutions of the rule of law are the most important items in a thick catalogue of current threats and security issues. They expect researchers to deepen their reflection, sharpen cognitive inquiry, develop in-depth analysis, and foment methodological innovation.

In 2015 a team of academic teachers, researchers and professionals with a great deal of expertise and practical experience in the field of security was established within the Unit of National Security at the Institute of Political Science and International Relations of the Jagiellonian University in Krakow. It has undertaken research, teaching and popularization activities to deepen theoretical and practical knowledge of mechanisms, rules, institutions and security areas. They are placed in historical and contemporary, as well as prognostic perspectives, referring to internal, national and international security aspects. They seek an interdisciplinary, in-depth, analytical look at the varieties and forms of security present in various dimensions of past and present.

The Jagiellonian Security Review is a new scientific journal that was born out of the need to enrich contemporary security debate in Poland and abroad. Starting from the current scientific activity of the faculty of the Unit of National Security of the Jagiellonian University, it opens the possibility and encourages representatives of academia, research centres and think tanks from Poland and abroad to participate in this debate. It will accompany other important cyclical undertakings of the Unit of National Security: the international (global) Jagiellonian Interdisciplinary Security Conference; domestic Jagiellonian Security Conference; guest lectures of the Unit of National Security.

I invite you to join the debate in the Jagiellonian Security Review for the benefit of the development of Polish security studies and their contribution to international reflection on contemporary security issues.

Artur Gruszczak

Editor in Chief

Marcin Szymański

Analysis – a Human Domain in the Digitized Intelligence Triad

> *„The days are gone where intelligence was a subordinate component of operations. Intelligence now was going to be the leading component"*[1]

Setting the scene

For the past two decades scholars and security practitioners have been emphasizing a liquid nature of the security environment. Dramatic shifts in global security dynamics resulted in several catastrophic events, with the World Trade Center attacks of 2001 being the most illuminating case among them. Deadly terrorist attacks and military responses, quite often resulting in collateral damage, caused thousands of casualties. Catastrophic events and their tragic results have been studied in details by numerous institutions. Among the findings of the post-event explanatory science, "the intelligence failure" became one of the most popular explanations of security actors' inability to anticipate potential threats.

Without a doubt, one can admit that "intelligence" is an iconic word among the constellation of narratives surrounding the contemporary security sphere. The "I" word is widely used by scholars, policy makers, commentators, media outlets, experts and the general public. The question to be asked, however, is whether any solid intellectual investment has been dedicated to explore the meaning of the word. The term is certainly attributed to several disciplines of human activity but for the purpose of further research the focus will be solely concentrated on security-related definitions. Intelligence can be perceived from different perspectives - it may have an informational, analytic, institutional and operational connotations[2]. Sherman Kent, quoted in "Intelligence Power in Peace and War", outlines a triadic definition, which describes intelligence as "a kind of

[1] US Army Lieutenant General Michael Flynn quoted in: R. Shultz, *Military Innovation in War: It Takes a Learning Organization. A case study of Task Force 714 in Iraq,* Tampa 2016, p. 39.
[2] A. Gruszczak, *Europejska wspólnota wywiadowcza: prawo – instytucje – mechanizmy*, Kraków 2014.

knowledge, the type of organization which produces that knowledge, and the activity pursued by such organization"[3].

To narrow the area of interest, this article will give a sense of "intelligence" in the analytical perspective, thus attributing it to the "process" or "activity" leading to the building of "knowledge". Since "the analysis lies at the heart of intelligence"[4], several efforts have been made to define this specific domain. The US Central Intelligence Agency (CIA) has attempted to define the consensual meaning of "intelligence" through the fusion of a few existing definitions. The process, however, resulted far from being easy. The difficulty of finding conceptual coherence is caused mainly by the fact that "formulating a brief definition of so broad a term as intelligence is like making a microscopic portrait of a continent"[5]. After the analysis of four definitions, Martin T. Bimfort – the author of the publication on the CIA web page – arrives at a conclusion that "intelligence" is the process of "collecting and processing of information". Further updates of the CIA conceptual efforts clarify the term as "the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers"[6]. The US National Research Council defines the intelligence analysis as an activity with the goal to "evaluate, integrate, and interpret information in order to provide warning, reduce uncertainty, and identify opportunities"[7]. The military doctrinal lexicon reduces ambiguous wording and brings the patchwork of definitions to one common denominator, which describes "intelligence" as a process of collection, analysis and dissemination of the key information. The "collection – analysis – dissemination" constitutes a triad which is heavily influenced by technology. The collection includes specialized imagery, signal, cyber, "humint"[8] and electronic intelligence domains. Dissemination is supported by an architecture of the command and control networks which are capable to deliver "real-time intelligence" to designated receivers while preventing unauthorized security breaches.

---

[3] Sherman Kent quoted in: M. Herman, *Intelligence Power in Peace and War*, Cambridge 2003, p. 2.
[4] M. Phythian, *Intelligence Analysis Today and Tomorrow*, "Security Challenges", 2009, 5 (1), pp. 67-83.
[5] US Central Intelligence Agency Electronic Library, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm(accessed on 4 October 2016).
[6] US Central Intelligence Agency Electronic Library,https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html(accessed on 4 October 2016).
[7] C. Chauvin, B. Fischhoff, *Intelligence Analysis: Behavioral and Social Scientific Foundations*, Washington, D.C. 2011, p. 4.
[8] Author's note: "humint" – abbreviated name for the branch of the intelligence collection utilizing human sources, human intelligence.

The analysis – even though relying to a large extent on the computing technologies – still represents a sphere dominated by human cognitive capacity. As Mark Phythian claims in his article published in the "Security Challenges": "while technological tools can assist enormously, analysis remains an intellectual process based on the application of human thought and judgement. It is an art assisted by science rather than a science in itself"[9]. It is a human who remains the most unpredictable element of the global security environment, and it must not be anything else but human who is able to navigate through such uncertainties. Predictive approach to the contemporary security environment requires advanced methods – experts describe them as "the high-level cognitive processes producing specific, detailed thought and understanding"[10]. Understanding the dynamics of highly adaptive, complex systems populating global domain requires more than technical perfection of cyber computing. The analytical part of the intelligence triad still remains dominated by critical thinking which is a skill not so far attainable for any available technology.

In this article the author will attempt to emphasize a key role played by a human in "evaluation, integration, and interpretation"[11] of available data - a process earlier defined as the intelligence analysis. The research and its findings are supposed to be exclusively dedicated to the analytical part of the intelligence triad. The author will investigate methods applied to support cognitive process, oriented on turning the raw data into information and knowledge. The opening paragraph of the publication will be dedicated to the evolution of the operational environment and its impact on the intelligence community. Subsequent part of this article will familiarize the reader with methods used by contemporary intelligence institutions in their analytic efforts. Some structural solutions facilitating analytical process will be discussed as well. The author will attempt to confront some of described methods with the challenges posed by modern security environment. The confrontation will be conducted in order to evaluate adequacy of selected solutions. Futuristic reflections referring to the human cognitive function in the intelligence process will summarize the study.

[9] M. Pythian,*op.cit.*
[10] M. W. Hall, G. Citrenbaum, *Intelligence Analysis, How to Think in Complex Environments*, Santa Barbara, Ca. 2010.
[11] The definition of the intelligence analysis comes from: C. Chauvin, B. Fischhoff, *op.cit.*

Defining the context

The opening statement of the European Union's global strategy is probably one of the best points of departure for an attempt to frame the nature of the contemporary security environment: "Our European project, which has brought unprecedented peace, prosperity and democracy, is being questioned. To the east, the European security order has been violated, while terrorism and violence plague North Africa and the Middle East, as well as Europe itself. Economic growth is yet to outpace demography in parts of Africa, security tensions in Asia are mounting, while climate change causes further disruption"[12]. A range of challenges rooted in military, economic, political and social domains are threatening a fragile global balance. Multidimensional and comprehensive character of contemporary security is further enhanced by the presence of technologically supported networks. Inside the bounds of the internet-webbed world, an adjective "global is not just intended in a geographical sense"[13]. Forecasting in such a "system of systems" becomes a complicated endeavor. Segregation of this closely packed universe into functionally connected clusters helps to establish a conceptual framework. Compartmentalization of the strongly networked security environment is not easy. Several agencies use different methods to conduct the functional partition of cyber-interlinked space. NATO for instance adopted the "PMESII domains"[14] to aggregate some of the global dynamics. Political, social, military, infrastructure and information spheres are used to portray the groups of related factors, which are decisive for the status and perspective of the security environment. Authors of the "Global Strategic Trends – Out to 2045" used 13 clusters to conduct "complex mapping process of trends and drivers with particularly strong linkages"[15]. Compartmentalization enabled to conduct a systemic study of the potential future shape of the world's security area.

---

[12] "Shared Vision, Common Action: Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy", p. 7,https://europa.eu/globalstrategy/sites/globalstrategy/files/about/eugs_review_web_0.pdf , (accessed on 21 December 2016).

[13] *Ibidem*.

[14] PMESII: abbreviation for "political, military, economic, social, infrastructure, information" domains which are used by the NATO planners to build system perspective on security challenges. Source: *Allied Command Operations Comprehensive Operations Planning Directive Interim V2.0* (Chapter 4 – Operational Level); p. 4-9.

[15] *Global Strategic Trends - Out to 2045*; published by the UK Ministry of Defense, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/348164/20140821_DCDC_GST_5_Web_Secured.pdf (accessed on 20 December 2016).

Predictive analysis of global security leads to a number of different alternative scenarios. Despite this diversity several key findings seem to dominate speculations about the future. The overarching line of thought bringing numerous conclusions to one common denominator concerns demographic changes. Advances in medical care, economic growth and improving welfare standards have resulted in the world population explosion. Global population is expected to reach 10.4 billion by the year 2045[16]. The effects of the rapid population growth, however, will not be equally distributed throughout the world. Available forecasts highlight the fact that the decline of the population size, which has begun several decades ago, would continue to exert impact on the developed countries. These trends are to be mostly visible across Europe and in Japan. High demand for labor force would be an obvious side effect of the shrinking population in these regions. There is also a range of less emanating threats grown on the basis of the population decline. To name just one of them: the overstretched pension system is supposed to press central budgets and cause social tensions. Concomitantly to these perspectives, less developed regions of the world are expected to be a scene of the reverse tendencies. In accordance with the "Global Strategic Trends", the young adult population is going to grow most rapidly in the sub-Saharan region of Africa. This process is supposed to be accompanied by a rapid urbanization. Ultimately, 70 percent of the global population is expected to live in the cities within the next three decades. Majority of these heavily populated areas are supposed to be located in underdeveloped areas of the southern hemisphere.

Such distribution of human resources will increase social tensions for several reasons. First of all, mishandled and underinvested urban centers will not offer affordable and acceptable living conditions for the masses of their inhabitants. The resulting discontent may produce tensions which in extreme cases could lead to "violent insurgencies"[17]. Secondly, the lack of career prospects will drive large population groups to migrate to more developed countries in search for better opportunities. The migrants will utilize accessible communication technology to maintain close contact with their indigenous groups – this in turn will slow down, and in some cases prevent, their successful integration into society in the host country. The separation, coupled with

[16] *Ibidem*, p. 3.
[17] *Ibidem*, p. XII.

disappointed expectations, will provide another reason for social tensions – this tendency will challenge stability of urban centers in the developed countries. Additionally, the scientific advances, despite of their genuine contribution to the human well-being, will provide radicalized population groups with access to unlimited options of violence. Available technology will enable social groups to communicate globally and covertly – it will also equip individuals and groups with off-the-shelf lethal or dual-purpose sophisticated hardware. According to the "Global Trends 2030", "individuals and small groups will have greater access to lethal and disruptive technologies (particularly precision-strike capabilities, cyber instruments, and bioterror weaponry), enabling them to perpetrate large-scale violence – a capability formerly the monopoly of states"[18].

To conclude: there are numerous indicators supporting the assumption that the majority of the future security threats will be embedded in the large urban populations of the dynamically growing super-cities. Following the assessment of the United Kingdom Ministry of Defense, potential future adversaries of the developed societies "will be found in larger, more complex urban environments, possessing a greater level of information and better access to technology than they do today"[19].

Threat transformations

Contemporary nature of the unconventional threats shows numerous examples to validate above described forecasts. A study of the so-called "Islamic State" provides a good point of departure. This organization is nested primarily in urbanized areas and the use of technology enables it to contact, broadcast, coordinate, recruit and collect funds on the practically global scale. In accordance with a EUROPOL report: "the internet and social media are used for communication and the acquisition of goods (weapons, fake IDs) and services, made relatively safe for terrorists with the availability of secure and inherently encrypted appliances, such as WhatsApp, Skype and Viber. In Facebook, VKA and Twitter they join closed and hidden groups that can be accessed by invitation only,

[18] *Global Trends 2030: Alternative Worlds*, p. III; a publication of the US National Intelligence Council, https://www.dni.gov/files/documents/GlobalTrends_2030.pdf (accessed on 10 December 2016).
[19] *Global Strategic Trends - Out to 2045*, *op.cit*.

and use coded language. (…) The use of encryption and anonymising tools prevent conventional observation by security authorities"[20].

Contemporary interlinked threat systems constantly adapt to the surrounding environment. Michael Hall describes such fibrillating architecture as a complex adaptive system (CAS), which he defines as "a dynamic network of many agents (which may represent cells, species, individuals, firms, nations) acting in parallel, constantly acting and reacting to what the other agents are doing"[21]. Complex systems differ from complicated ones – they create challenges which are characterized by "multiplicity, interdependence and diversity"[22]. The interactions within complex systems are "nonlinear, making the identification of enduring patterns unlikely"[23]. In addition, their adaptive capability enables clandestine affiliation to the urban supra system which provides a perfect sanctuary. This poses a new challenge which Richard Shultz describes as "a complex, clandestine, and networked enemy empowered by information age technology"[24]. Big population centers surround these systems with constant fluidity which is essential to the concealment of their existence. The fluidity of urban areas means that "everything is moving and constantly changing"[25]. The dynamics is not only attributed to the physical sphere of the population center. The phenomenon of constant change also has an impact on the cyber domain. As a result, the clandestine networks can be embedded within "an electronic sanctuary – in which actions can be hidden among innumerable civilian signals that constitute daily cell phone and Internet traffic. It is from this new sanctuary, that the enemy coordinates activities from dispersed networks in order to self- synchronize, pass information, and transfer funds"[26]. Such picture of the operational environment may create an illusory assumption that technology should dominate the world of the predictive intelligence analysis. Nothing could be further from the truth, taking into account that the network connects the people and it serves to support their innovative

[20] *Changes in Modus Operandi of Islamic State Terrorist Attacks*, p. 6, https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-terrorist-attacks (accessed on 1 November 2016).
[21] M. W. Hall, G. Citrenbaum, *op.cit.*, p. 11.
[22] G. Sargut and R. McGrath, *Learning to Live with Complexity*, "Harvard Business Review", September 2011, p. 68, quoted in: R. Shultz, *op.cit.*, p. 32.
[23] R. Shultz, *op.cit.*, p. 32.
[24] *Ibidem*, p. 3.
[25] M. W. Hall, G. Citrenbaum, *op.cit.*, p. 10 .
[26] M. Flynn, R. Juergens, T. Cantrell, *Employing ISR: SOF Best Practices*, "Joint Forces Quarterly", 2008, 50, p. 57.

genius. Statistics and computer-based information management can assist the analyst but with no doubt cannot entirely replace him. To repeat the statement used in the opening section of the article: It is a human who remains the most unpredictable element of the global security environment and it must not be anything else but human who is able to navigate through such uncertainties.

Doctrine – changing templates

"Fluidity", "nonlinear nature", "constant change", "fibrillating systems" are the key words describing the challenges of the contemporary intelligence analysis. Unconventional threats pushed the intelligence community to reject part of wisdom obtained from the standard analytic procedures. Classic military intelligence school was based on a well-defined process of the "Joint Intelligence Preparation of the Operational Environment" (JIPOE)[27]. Operational- and tactical-level analysis, in accordance with the traditional school of thought, included the four-step methodology. Initial activity "defining the operational environment" was designed for the staff to understand geographical limits of the assigned area of responsibility. In the course of the subsequent step: "describing the impact of the operational environment", analysts were to focus on the detailed features of the terrain in order to fully appreciate its potential impact on operations of both friendly and adversary forces. The "system perspective" was introduced in this phase to ensure understanding of the political, economic, military, social, infrastructure and information factors, decisive for the shape of the environment. With military operations gradually shifting toward urban areas, the term "human terrain" was introduced to the intelligence lexicon. This served to emphasize the importance of the social sphere as operational factor. The third phase: "evaluating the adversary", was fully dedicated to thorough studies of the opposite force. The enemy's doctrinal formations were analyzed and their strengths, capabilities and weaknesses were perceived in a comparative perspective with the actor's own potential. The quantitate and qualitative analysis served as the main tool to be used in this phase. The third part of JIPOE was based on the detailed knowledge of the opposing force equipment, structures and doctrines. In the

[27] For a detailed description of the process see: *Joint Publication 2-01.3 "Joint Intelligence Preparation of the Operational Environment", 16 June 2009*, published by US Armed Forces Joint Staff at https://fas.org/irp/doddir/dod/jp2-01-3.pdf (accessed on 1 November 2016).

final step of the process, analysts conducted fusion of the enemy capabilities with the opportunities offered by the geographically designated area of operations. This concluding step, described as "determining adversary courses of action", was supposed to result in a definition of the most likely and most dangerous opposite forces options. Each of the hypothetical courses of action was associated with several indicators which were designed to either confirm or negate the assumed enemy scenario.

Such an approach to the analysis was successfully adopted in the cold war era to the conventional forces confrontation. Currently, however, such "template-based" process is no longer applicable. In a blurry constellation of "nonlinear", "fluid" environment, the process of turning raw data into knowledge requires a non-traditional approach. The evolution of analytical methods was initiated with the advent of the intelligence-driven "war on terror". The initial failure to cripple Al Qaida in Iraq by robust US Special Forces provided the most illuminating example of inadequacy of the conventional military intelligence practice in the fight against unconventional threats. As the retired US General Stanley McChrystal, former commander of the Task Force 714[28], described it, the US Special Forces "were losing to an enemy they should have dominated"[29]. A substantial share of this failure was attributed to the application of inadequate, too orthodox intelligence analysis methods.

Adopting new methods

The nature of unconventional threats required an innovative approach to the intelligence analysis. Indistinct signature of the threat network had to be first identified and then investigated with the ultimate goal to predict its behavior. Predictive intelligence in the unconventional threat environment is based on elaborative studies which are mostly rooted in the system analysis theories. Such perspective requires a two-step approach: firstly, data and assumption-based system model has to be built; secondly, a vision has to be extrapolated into the future in order to anticipate possible developments. The initial modelling phase of the intelligence process is heavily supported by the data collection activity. These efforts need to be strictly prioritized since the number of collecting assets

[28] Author's note: Task Force 714 – US counter terrorism force deployed to Iraq in 2003 with the mission to defeat Al Qaida network.
[29] Retired US Army General Stanley McCrystal quoted in: R. Shultz, *op.cit.*

is usually severely limited. An initial picture of the operational environment is required in order to conduct such prioritization. Early phases of the intelligence analysis include gathering of all available facts relating to the assigned area of interest. Once consolidated, facts are analyzed, grouped and segregated into essential and less important ones. Such routine makes it possible to get a preliminary understanding of the operational environment. The routine also results in identification of information gaps, which in the course of further prioritization become the "intelligence requirements". Analytical efforts are then continued to replace some of the information gaps with assumptions. The contemporary operational environment is fluid. Therefore, the building of any static picture is hardly possible – catalogues of the facts and assumptions are thus required to be constantly verified and updated.

In comparison with the conventional intelligence approach, where the structures, doctrinal formations and equipment of the adversary were to great extent catalogued, the unconventional intelligence struggles with the clandestine networks – each having unique structure and modus operandi. General McChrystal described these webs as "clandestine infrastructure (form), further protected by the clandestine arts (function), to minimize signature"[30]. Such foggy environment makes well-reasoned assumptions particularly useful for a modelling. Initial network models are in most cases built on the assumptions, supported by very few available facts. The analytical procedure requires that any well-reasoned assumption must be verifiable. Assumptions thus become "mini-hypotheses" ready to be tested. Each of them is linked with several variables, which – once observed and measured – can prove or deny the validity of the deduction. This mechanism of verification creates further "intelligence requirements", which are used for the collection tasking[31].

Close coordination between the analysts and collectors is of vital importance, especially at the initial stage of the intelligence picture formation. The efficiently planned and prioritized collection effort serves as a key factor in the system analysis. In accordance with a publication by the Joint Special Operations University, focused collection activities enabled Task Force 714 to "identify central and peripheral figures,

[30] *Ibidem*,p.35.
[31] Autor's own experience, as a battle group commander deployed to the International Security Forces Afghanistan, Regional Command East, Paktika province, 2008.

patterns of behavior, and clusters of nodes of Al Qaida operating system"[32]. The effectively tasked and organized collection system delivers data which is processed into information. The collection must be clearly focused on the "analytically anticipated outcomes"[33]. Such products – depending on their level of the detail and the source of the delivery – are divided into indicators, observables and signatures[34]. The first category of collection deliverables represents "an item of information reflecting the intention or capability of an adversary to adopt or reject a course of action"[35] – it is an incomplete, low probability marker indicating the sheer existence of the adversary. An observable is more concrete, "physical, physiological, emotional property, or absence of one or all of the aforementioned that can be observed or measured directly"[36]. Observables provide the intelligence analysts with a clear, identifiable evidence of the threat presence. They are further divided into "cultural, technical, biometric, functional, and situational ones"[37]. Finally a signature, as "the most finite among the triad"[38] consists of several observables and indicators and enables an advanced hypothesis on the adversary's potential courses of action to be constructed.

A long process of integrating the observables and indicators into the signatures, which serve to build a solid hypothesis, can be conducted with the use of several procedures. Any particular method of the intelligence analysis depends on the specific character of the environment, preferences of the intelligence agency, time, personnel and assets available. Even though some sources mention probability theories, decision analysis and game theory as popular models[39], the system theory has been picked by numerous intelligence actors as the most adequate approach to be utilized in the era ofnetwars. In accordance with the US doctrinal publication: "detailed joint JIPOE by specialists familiar with the underlying principles of networking (which includes substantial pockets of system theory wisdom) is the first step in establishing control over

[32] R. Shultz, *op.cit.*, p.3.
[33] M. W. Hall, G. Citrenbaum, *op.cit.*, p. 37.
[34] *Ibidem*.
[35] *Ibidem*.
[36] *Ibidem*.
[37] *Ibidem*, p. 38.
[38] *Ibidem*, p. 37.
[39] For more details of analytic methods see: Committee on Behavioral and Social Science, *Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences*, http://research.unl.edu/events/docs/Intelligence%20Analysis%20for%20Tomorrow%20NRC%202011.pdf (accessed on 2 December 2016).

the threat network"[40]. The term "system analysis" is defined in Business Dictionary as "a general methodology (not a fixed set of techniques) that applies a 'systems' or 'holistic' perspective by taking all aspects of the situation into account, and by concentrating on the interactions between its different elements"[41]. Such approach has been adopted by numerous analytic institutions to forecast the risks created by the network-based adversary. There are several techniques of the "holistic", "system-oriented" intelligence process. The RAFT method[42], being one of them, maps the environment and builds models. Dale C. Eikmeier describes it as a technique "to illustrate or textually describe the environment" and a tool used "to explain the relationships between relevant actors, their functions and tensions"[43]. At the initial stage of this application, analysts are concentrated on the identification of potential nodes of the system (actors). This activity is prolonged in time, its pace depends on the information availability and the volume of upcoming collection deliverables. The next step – usually subject to a group think – is focused on the relations between the actors. Analysts use available information and assumptions to draw the connections within the system. Links between the nodes are than described on the basis of their function and tension (the latter used to describe the volume of the relationship). Link analyses are believed to be of special importance since, as Hall and Citrenbaum underline, "they are the Achilles' heel of any network, because they can be made transparent, they can be manipulated, and they can be weakened"[44]. Authors of the "Intelligence Analysis" further segregate the links into "technical, human, organizational, thought and functional"[45]categories. Ultimately the system modelling results in a complex graphic product which is usually constructed with the use of a dedicated computer software. The visualization facilitates the perception of the "holistic picture" and supports the discovery of the "new insights and perspectives while improving understanding"[46]. Sound intelligence analysis, conducted in the complex

[40] US Armed Forces, *Commander's Handbook for Attack the Network*, Joint Warfighting Center, Joint Doctrine Support Division, Suffolk, VA, 20 May 2011, p. 34.
[41] Source: Business Dictionary, http://www.businessdictionary.com/definition/systems-analysis-SA.html(accessed on 29 December 2016).
[42] Author's note: abbreviated name of the analytic technique developed by Dale C. Eikmeier. The abbreviation stands for "relations, actors, functions, tensions" – characteristics of the system, being a subject of RAFT method research.
[43] D.C. Eikmeier, *Design for Napoleon's Corporal*, "Small Wars Journal", 27 September 2010, p. 4, http://smallwarsjournal.com/blog/journal/docs-temp/557-eikmeier.pdf (accessed on 29 December 2916).
[44] M. W. Hall, G. Citrenbaum, *Intelligence Analysis*..., p. 125.
[45] *Ibidem*, p. 126.
[46] D.C. Eikmeier, *Design*..., *op.cit.*, p. 4.

environment, requires a thorough understanding of functions and missions of all the networks operating within the assigned area of interest. Once the adequate level of appreciation is achieved, the systems identified in the course of the process are "categorized by their relation to the friendly war effort and objectives"[47]. Color code is usually used to visualize threat, friendly, neutral and malign actors. Sophisticated mapping techniques, often heavily computer-supported, are utilized to produce pictures representing constellations of interrelated, colliding networks. The webs might stand in different relations to each other, they can for instance compete, support, coordinate, collide, they may just co-exist or even stay completely unconnected. The ultimate goal of this broad part of the analysis is "to identify and define all the networks that impact the operational environment, how they interact, and what actions must be taken to influence those networks to achieve the objectives contained in the operations plan"[48]. Such "system engineering", manipulation within lots of interconnected galaxies, requires detailed understanding of the nature of each network.

Grasping the system's dynamics

Mapping does not allow to fully appreciate the capabilities, strengths, limitations, vulnerabilities, internal and external dynamics circulating in each active system. Moreover, mapping provides only limited support to the predictive function of the analytical efforts. Forecasting a future behavior of the system requires more in-depth, micro-scale approach. The study of the center of gravity (COG) enables us to elaborate on a more sophisticated feature of particular systems. The original idea of the "center of mass" originates from the operational art principles laid down by the Prussian general Carl von Clausewitz. The definition of COG was outlined in the 19th-century book "VomKriege"[49] as "the hub of all power and movement, on which everything depends… the point at which all our energies should be directed"[50]. The concept survived the collision with two centuries of the evolution of operational art. Being widely used,

[47] US Armed Forces*, Commander's Handbook*..., p. 35.
[48] *Ibidem*, p. 35.
[49] Author's note: „Vom Kriege" is the original title of „On War" the best selling book written by Carl von Clausewitz in the period of 1816-30. The manuscript was posthumously published by his wife. Being translated and printed in several languages, the book is still highly respected within the military community.
[50] C. von Clausewitz, *On War*, ed. and trans. By M. Howard and P. Paret, Princeton 1976.

nowadays it is defined as "the source of power that provides moral or physical strength, freedom of action, or will to act"[51]. Used as a tool to support system analysis, the COG method identifies critical capabilities, requirements and vulnerabilities of the targeted network. A sequential study of these factors facilitates the framing of a pivotal point – the center of mass of the network. Contemporary analysts conceive the COG as the functional nucleus possessing inherent capability, which is absolutely critical to the whole system. Despite the current provocative tendencies to undermine adequacy of Clausewitzian principles, many of his concepts unquestionably retain their plausibility, even if confronted with unorthodox theories of the netwar era. Regardless of these debates, "it does not matter what Carl von Clausewitz said about the center of gravity in the 19th century. What matters is how we want to use the COG concept in the 21st century"[52]. The old method with some improvements proves to be extremely useful in the network-based environment. Numerous doctrinal publications consider identification of COG as "one of the most important tasks confronting the joint force commander's staff in the operational design process"[53].

The intelligence practice includes several ways to apply the COG analysis method. Specific procedure depends on the organizational culture, preferences and leadership styles of particular analytic institutions. As a RAND study highlights: "in complex operations, there are no routine formulas that planners can always apply to determine a COG"[54]. Dale C . Eikmeier's six steps approach represents one example of the COG identification[55]. This method turns the intellectually challenging process into a patchwork of logically sequenced cognitive activities. The procedure, as described by its author, begins with the identification of the goal which the analyzed system desires to achieve. This initial phase is essential to the whole process, since it shapes perspective on

[51] US Armed Forces, Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms", https://fas.org/irp/doddir/dod/jp1_02.pdf (accessed on 3 November 2016).
[52] D.C. Eikmeier, *Redefining the Center of Gravity*, "Joint Force Quarterly", 2010, 59.
[53] US Armed Forces, Joint Publication 5–0, "Joint Operation Planning", pp. IV–8, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf (accessed on 3 November 2016).
[54] C. M. Schnaubelt, E. V. Larson, M. E. Boyer, *Vulnerability Assessment Method: Pocket Guide, Tool for Center of Gravity Analysis*, Santa Monica, Ca. 2014.
[55] For a more detailed description of the COG analysis method see: Dale C. Eikmeier video lecture at: https://www.youtube.com/watch?v=-RYbtyzfB1w&t=650s (accessed on 3 November 2016); Colonel Dale Eikmeier retired from the U.S. Army in 2008, after 30 years of service as an Air Defense Artilleryman, joint planner and a strategist. His assignments include duty in Europe, Asia and the Pacific and the Middle East. Campaigns include Operations Desert Shield, Desert Storm, Operation Enduring Freedom and Iraqi Freedom. He had faculty positions at the School of Advanced Military Studies, the Army War College, and the Army Command and General Staff College.

subsequent reasoning. Once the desired objective is identified, analysts attempt to list "ways to achieve the ends"[56] – actions which the network needs to perform in order to reach its ultimate objective. The capacity to conduct these actions is therefore reflected in the capabilities of the system (mostly verbs). Subsequently, they are being filtered through the lens of their essentiality to the objective, which the system desires to achieve. The capability which is considered as decisive to accomplish the system's desired end state is designated as "the critical one". In the third step of Eikmeier's method, the analysts are listing "the means required to enable and execute the way or critical capability"[57]. This activity helps to identify these nodes of the system, which provide the defined capabilities. The fourth phase constitutes the pivotal point of the whole COG nomination process. It is based on the confrontation of the critical capability, available means and the desired end state. At this point the analysts attempt to specify, which of the system nodes "inherently possesses the critical capability to achieve the desired end state"[58]. The node selected in this way is defined as the center of gravity of the system. It is the "source of all power", the focal point, without which the network loses the capacity to achieve its desired end state. The remaining two steps of Eikmeier's method are used to select the most critical requirements and vulnerabilities of the network. The COG analysis – in spite of being a relatively aging concept – enables us to fully understand the dynamics of the complex environment, fulfilled with interacting systems. Some of the contemporary analytic techniques utilize elements of the COG approach: "nodal analysis", for instance, exploits the center of gravity concept to identify "the specific functional nodes that empower the network"[59]. Products of the COG analysis are not only useful to create a snapshot vision of the current status of the operational environment – they are even more valuable for a long-term prognosis. The perspective constructed on the basis of the COG identification supports heavily "the speculative – evaluative"[60] category of the intelligence reporting. This particular domain deals with the long-range forecasting and its accuracy is based more on an art, enabling humans to predict reasonably, than on the pure science. As a result, there might be hardly a case

[56] D.C. Eikmeier, *A Logical Method for Center of Gravity Analysis*, "Military Review", 2007, LXXXVII (5), p. 64.
[57] *Ibidem*.
[58] D.C. Eikmeier, *Redefining …*, *op.cit.*,p. 158.
[59] US Armed Forces, *Commander's Handbook…*, *op.cit.*,p. IV-3.
[60] For the categorization of intelligence products by S. Kent, see: M. Herman, *op.cit.*, p. 105.

that two groups of analysts, dealing with the same set of challenges, would come to exactly the same conclusions. The value of the products and their relevance in the confrontation with the future always depends on the level of intellectual and professional potential of the staff.

Human factor – vulnerability of the system

To quote Mark Phythian one more time: the intelligence analysis is a process which to a large extent is based on "the application of human thought and judgement"[61]. It is an art rather than science or – as some prefer to frame it – it is an art supported by science. The driving force behind this particular domain of the intelligence activity is generated by a human intellectual brain horsepower. "Human" constitutes the centerpiece of the process – it is however also human who creates some of its vulnerabilities. The group mindset is typically under some degree of the leverage, exercised by highly suggestive assumptions. Critical, objective thinking is not a common human characteristic. People in general prefer to find confirmations for the satisfying hypothesis rather than to seek a counterargument. Behavioral scientists claim that, typically, groups of human "prematurely converge on one hypothesis (or small set of hypotheses) and then confirm that hypothesis by seeking out supportive data or interpreting existing data in ways favorable to it, rather than seeking data that might disprove it"[62]. Such trend in the human analytic capacity is depicted as a reason for numerous failed assessments. The US intelligence assessment of the Iraqi weapons of mass destruction (WMD) program is probably the best known case. As Mark Phythian describes it: "the problem with analysis over Iraqi WMD was that the original picture contained few dots. In response analysts filled in the gaps with too many of their own dots. These did not exist in the actual, but largely concealed, picture, and so the picture analysts constructed was inaccurate. They constructed a parallel reality on the basis of their own assumptions…"[63] Strong desire of CIA to validate the Iraqi WMD hypothesis, reached at some point a paranoid level. In such a strange mood, CIA restricted access to some information which could make other

[61] M. Phythian,*op.cit.*, pp. 67-83.
[62] Committee on Behavioral and Social Science, *op.cit.*, p. 35.
[63] M. Phythian, *op.cit.*, p. 71.

intelligence institutions formulate challenging assumptions[64]. Competitive and alternative analytical techniques have been developed to limit such intelligence mismanagements. These mechanisms, however, resulted in several by-products characteristic for the intelligence agencies. High professional standards, close group ties, emotional affiliation with the mission amplified by the competitive atmosphere, created a strong feeling of being an elite. Elites tend to create closed, impenetrable communities. Such inclination supports the individual commitment to the organization but it works against one of the most essential principles of the advanced intelligence: data fusion.

With the operational environment becoming more dynamic and fluid, interagency data sharing expanded into an essential part of the intelligence activity. Allowing partners to benefit mutually from their own data base was not a typical practice of the agencies, which preferred the conventional approach. Institutional culture of such organizations has always been dominated by the principles of secrecy and operational security. To quote Mark Phythian again: "the analytic process is inseparable from the organizational environment in which it occurs"[65]. Competitive analysis approach has been imprinted in the US intelligence community since the late 1970s. This particular structural solution has been driven by the desire to seek the most precise and feasible hypothesis concerning military capabilities of the Soviet Union. The compartmentalization of the intelligence community resulted in a competition and rigid separation of the CIA, the Defense Intelligence Agency (DIA), Intelligence and Research Bureau (INR) and other institutions producing intelligence analyses. Such organizational arrangement, according to numerous practitioners, did not produce expected results – on the contrary, it amplified existing biases.

The lack of cooperation within the intelligence community, the deficiency definitely rooted in the human nature, has been numerously quoted as the reason of failure to anticipate terrorist threats. Some of these failures had catastrophic consequences. The most striking example of such deficiency can be drawn from the 9/11 Commission's final report, which uses the "connecting the dots" theory to visualize the failure. The report specifically mentions that "the biggest impediment to all-source

[64] For a more detailed account of these tendencies see: US Senate Select Committee on Intelligence [SSCI], *Report on the US Intelligence Community's Prewar Intelligence Assessments on Iraq*, Washington, DC 2004, pp. 27-28,https://fas.org/irp/congress/2004_rpt/ssci_iraq.pdf (accessed on 3 November 2016).
[65] M. Phythian, *op.cit.*, pp. 67-83.

analysis – to a greater likelihood of connecting the dots – is the human or systemic resistance to sharing information"[66]. Confrontation with highly adaptive, complex and flexible threat networks replaced these patterns with a productive compromise. Compartmentalized intelligence community was too cumbersome to face the challenges – again, the example of the fight against Al Qaida in Iraq brings the most illustrative example. General McChrystal was among the first to outline the need for the intelligence fusion. He declared: "to defeat a networked enemy we had to become a network"[67]. Consequently - after series of the "dry whole"[68] type of operational efforts, the TF 714 introduced a new organizational structure, enabling the intelligence fusion. The Joint Interagency Task Force was created in order to support the counterterrorist effort with the multi-source intelligence analysis. It combined capabilities of the Central Intelligence Agency (CIA), Federal Bureau of Investigations (FBI), National Security Agency (NSA), Defense Intelligence Agency (DIA), National Geospatial-Intelligence Agency (NGA) and others. As a result of this successful fusion, the TF 714 significantly increased the operational tempo. The number of raids consequently expanded from 18 in the year 2004, to 300 raids a month in August 2006[69]. "Rapid intelligence fusion and exploitation became to be the most effective weapon against network based threat"[70]. Since the intelligence sharing has been established as a routine practice ("fusion cells" are nowadays regularly employed as a part of military organizations), the counterterrorist fight turned to be a true "network against network" battle. Such a type of warfare is in accordance with General Stanley McChrystal view the only promising technique to eliminate the unconventional threats.

[66] National Commission on Terrorist Attacks upon the United States, *The 9-11 Commission Report*, p. 417, https://www.9-11commission.gov/report/911Report.pdf (accessed on 3 November 2016).
[67] Retired US Army General Stanley McCrystal quoted in: R. Shultz, *op.cit.*
[68] Author's note: "dry whole" – military slang description of a failed operation.
[69] Source: R. Shultz, *op.cit.*, p.4.
[70] Source: author's conversation with General Stanley McCrystal, while being deployed as the deputy director of Afghan National Security Partnering Center "Army"; International Security Force Afghanistan, 2010.

Facing new challenges

Unorthodox approaches to the analytical process and rejection of the competitive analysis principles have characterized the nature of the functions of intelligence throughout the last one and a half decade. New solutions and techniques have been invented on the basis of the analysis of failures. It means that the intelligence community seems to lag one step behind the dynamics of the change in the security environment. It also means that the community remains in the reactive mode to the revealing events what heavily impacts the accuracy of the predictive intelligence. The vulnerability grows to an alarming size as the methods of violence application quickly evolve. The advent of new formulas in warfare, with the "hybrid warfare" at the top, represents a serious challenge to the analytical community. The strategy, sketched out by General Gerasimov in 2013[71], and then implemented by Russian policy makers one year later in Ukraine, delineates a new approach. The military doctrinal narrative describes the "hybrid warfare" as "the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefitting effects"[72]. Scholars of military science also underline the fact, that the specific nature of the hybrid warfare contains "a range of hostile actions of which military force is only a small part, or measures short of war, that seek to deceive, undermine, subvert, influence and destabilize societies, to coerce or replace sovereign governments"[73]. Such unrestricted type of warfare combines conventional and unconventional approaches. It utilizes kinetic and full range of non-kinetic forms of engagement, with the ultimate goal of exerting influence, rather than defeating an opponent.

With the growing number of options, the human unpredictability increases. Along with this tendency, the speculative-evaluative function of intelligence gets more complicated. Several reasons contribute to such trend. First – the "hybrid warfare" combines strategic and tactical levels: both military and non-military resources to achieve the desired end state. Such organization of the campaign requires strong fusion of

[71] For a detailed account see: C.K. Bartles, *Getting Gerasimov Right*, "Military Review", 2016, 96 (1),pp. 30-39.
[72] Headquarters, Department of the Army, Army Doctrine Publication (ADP) 3-0, "Unified Land Operations", Washington, D.C. 2011, p. 12.
[73] A. Monaghan, *Putin's Way of War: The 'War' in Russia's Hybrid Warfare*, "Parameters", 2015, 45(4).

agencies, working at different levels and for different customers. The engagement of the hybrid adversary is extended in time, and the techniques used to shape the environment for decisive action are extremely difficult to be detected. This is especially true in non-kinetic engagement area – the indicators identified at the tactical level of this specific domain may contribute to the signature of the strategic intent, being executed by psychological warfare or cyber-attacks. This example illustrates the necessity for all-level, all-branch fusion within the intelligence community. The process, although not easy for reasons mentioned in this paper, can be achieved in several ways: "one way to deal with that problem is for the Intelligence Community to evolve into a much larger but distributed and 'virtual community' – one that includes a much broader range of topical experts … Another is for the intelligence community to accept a more supporting role, focusing on collecting secret information on selected problems that matter and leaving the synthesis and more extensive analysis of the world to others"[74].

The need for fusion includes also affiliation of such distant branches as intelligence and counterintelligence. The reason for such recommendation is based on the Gerasimov strategy, which assumes penetration of the targeted state networks long before escalation of the hostilities. Close cooperation of both intelligence branches is required to identify the adversary's intentions in such circumstances. Hunter and Pernik highlighted this tendency: "espionage and network intrusion has preceded conventional military invasion, providing a warning before the conflict escalates to the use of force"[75]. This has been the truth in the cases of Russian campaigns in Georgia and Ukraine. The multi-domain nature of warfare conducted in both these countries also calls for extended "virtual links", reaching beyond the intelligence community. Experts on the economy, politics, social science, behavioral psychology, cyber operations and other areas need to be found in academic, business, media and other non-military branches. In this regard hybrid warfare calls for a truly comprehensive approach to the analysis.

Secondly, the hybrid approach combines conventional and non-conventional means to achieve an end. Facing a full range of challenges, the analysts can no longer rely purely on unorthodox methods, designed to fight terrorists' networks. "Hybrid

[74] G. F. Treverton, C. B.Gabbard, *Assessing the Tradecraft of Intelligence Analysis*, Santa Monica, Ca. 2008, p. 17.

[75] P. Pernik, E. Hunter, "The Challenges of Hybrid Warfare",https://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf(accessed on 2 November 2016).

warfare" calls for "hybrid intelligence", which preferably should combine netwar and the traditional approach techniques. Hard backup, in form of the conventional military capability, even though not being the essential ingredient of the hybrid strategy, still constitutes an essential criterion of its success. The standard military quantitate and qualitative analysis must be then reemphasized. What is most important, however, the analytic staff has to struggle to recognize triggers and modes of employment of hard power. There is no doctrine which could help to read the adversary's intentions in this regard. It is a hardly predictable, human decision-making cycle, which needs to be penetrated in order to formulate the speculative-evaluative conclusions. Decision analysis techniques might be helpful in such forecasting since they "offer systematic procedures for formulating and solving problems that involve choices under uncertainty"[76]. Despite this recommendation, the behavioral and psychological analysis of key individual leaders remains highly important to achieve high standards of precision of the reports.

Finally, the hybrid warfare utilizes to big extent modern, off-the-shelf technologies, with the computer networks being the most popular, non-kinetic enabler. This particular tendency resonated in the NATO doctrinal narrative which described the internet as the medium which "is used to spread or circulate information and opinion, including rumor, with a speed inconceivable a few years ago. The Internet is an unrestricted and unregulated medium, available globally, which an adversary can exploit either to spread his message, as a vehicle to attack friendly systems, or as an open source of intelligence"[77]. The virtual domain is already heavily populated with the agencies utilizing the network to filter out and spread messages. It is an obvious and the most rewarding resource of the open source intelligence (OSINT)– a data bank which makes OSINT the most valuable collection domain. Effective intelligence, applied to reduce the hybrid threat, needs to depend heavily on the technical capability to filter, assess and synthesize information available in the internet. This particular domain is dominated by non-military expertise – outsourcing their particular capabilities provides another potential requirement for enlargement of the analytic "virtual community". The challenge

[76] Committee on Behavioral and Social Science Research, *op.cit.*, p. 39.
[77] NATO Standardization Agency, "Allied Joint Doctrine For Information Operations AJP-3.10", November 2009,pp. 1-4, https://info.publicintelligence.net/NATO-IO.pdf, (accessed on 5 November 2016).

here, however, is to build a compromise between the democratic standards of cyber domain and the level of penetration by intelligence collectors.

Conclusion

The hybrid warfare with no doubt creates a new challenge for the analytic intelligence community. The processes, structures and methods of analysis – so deeply reformed throughout the last decade, need to continue their evolutionary change. Revolutionary developments in warfare have been recognized and appreciated by numerous scholars. The intelligence community cannot ignore these transformations. As the NATO Joint Warfare Center publication highlights, when the Alliance "prepares to develop ways to deter and potentially defeat Russian hybrid threat, innovation will hold the key to success"[78]. The intelligence analytic community – with its key predictive role – needs to stay at the forefront of such an approach. It needs learning organizations, units like the Task Force 714, which provide a perfect example of the institution drawing constructive conclusions from its own failures. The human will occupy a pivotal position in the constellation of these revolutionary changes. It is a leadership role to either stimulate or to suppress the spirit of the initiative. Nothing also seems to indicate that the role of the human as a central node of the analytic process would diminish. As William E. Odom underlines: "emphasis on 'processing' software, often meaning a considerable degree of machine-generated analysis, cannot replace a lot of brain work and labor on the part of analysts, especially in producing the final products"[79]. As the volume of available data increases, the number of the high tech amendments, used to capture and filter OSINT, enormously grows.

Notwithstanding these trends, nothing seems to indicate that technology would serve in any foreseeable future as an equalizer for a human cognitive capacity. Numerous prognoses predict that machine warfare will saturate the future battlefield with unmanned systems. Despite this tendency, the human, with its inherent strategic brilliance, will most likely continue to be the central node of the decision-making system.

[78] J. R. Davis Jr., *Continued Evolution Of Hybrid Threats The Russian Hybrid Threat Construct and the Need for Innovation*, "Three Swords Magazine", 2015, 28.
[79] W. E. Odom, *Intelligence Analysis*, "Intelligence and National Security", 2008, 23(3), pp. 316–332.

There is a very little evidence that any computer-based system will be capable to predict human behavior which determines the strategy. To conclude: even though tremendous amounts of resources are spent on hardware and software upgrades, the investment in quality of the human analytic capacity will remain an indispensable and the most cost-effective venture for any institution aspiring for a respected position among the intelligence community. Hopefully, the intelligence analysis methods will continue to evolve into a fascinating human cognitive branch bringing intellect into service of global and regional security.

Streszczenie

Anglojęzyczny termin "intelligence" zyskał wręcz ikoniczne znacznie w czasie burzliwego okresu zwanego „wojną z terrorem". W zależności od perspektywy i kontekstu, słowo „intelligence" może mieć różne konotacje. W narracji doktrynalnej jest ono kojarzone z informacją, analizą, instytucją, czy też operacją. Rozpatrywany w ujęciu procesu, termin ten określa cykl zdobywania, przetwarzania i dystrybuowania istotnych informacji. Najważniejszym ogniwem powyższej sekwencji jest analiza. Jako „serce procesu" stanowi ona przedmiot polemik praktyków i naukowców. Oś tych dyskusji nadzwyczaj często penetruje obszar wpływu cyfryzacji na skuteczność czynności analitycznych. Wnioskując z dostępnych publikacji ocenić należy, że predyktywna funkcja analiz wywiadowczych wciąż pozostaje domeną zdominowaną przez umysł ludzki. Człowiek jest najbardziej nieprzewidywalnym elementem globalnego środowiska bezpieczeństwa – z tego właśnie względu funkcja prognoz, w tym pełnym chaosu obszarze, musi pozostać ludzką domeną.

W artykule autor opisuje kluczową rolę czynnika ludzkiego w procesie ewaluacji, integracji i interpretacji zasobów informacyjnych. Publikacja zawiera opisy metod, które stosuje się dla wsparcia kognitywnej funkcji procesu konwersji danych w informacje i wiedzę. Część wstępna artykułu poświęcona jest charakterystyce współczesnego środowiska bezpieczeństwa. Autor opisuje wpływ, jaki współczesna specyfika wywiera na kulturę organizacyjną środowisk analitycznych. Następnie przedstawione zostały wybrane metody, stosowane w procesie analizy danych. Rozwinięcie tego paragrafu stanowi opis rozwiązań strukturalnych, które umożliwiają praktyczne stosowanie opisanych metod. W dalszej części publikacji autor podjął próbę konfrontacji części z przedstawionych rozwiązań z wyzwaniami, jakie stawia przed środowiskiem analitycznym współczesne otoczenie. Artykuł zamyka kilka refleksji, poświęconych kierunkom ewolucji organizacji i metod analiz wywiadowczych.

Słowa kluczowe: wywiad • analiza • bezpieczeństwo narodowe • analiza wywiadowcza

Abstract

"Intelligence" is an iconic word in the "War on Terror" era. It can be perceived from different perspectives: it may have an informational, analytic, institutional and operational connotations. Analysis, being "at the heart of intelligence" has drawn attention of numerous scholars and practitioners. As the world becomes increasingly digitized, the predictive role of analysis still remains dominated by human cognitive skills. It is human who remains the most unpredictable element of the global security environment, and it must be nothing else but human who is able to navigate through such uncertainties.

In this article the author attempts to emphasize the key role played by human in evaluation, integration, and interpretation of available data - a process defined as the intelligence analysis. The research and its findings are exclusively dedicated to the analytic part of the intelligence triad. The author examines methods applied to support cognitive processes, seeking to convert raw data into information and knowledge. The opening part of this paper is dedicated to the evolution of the operational environment and its impact on the intelligence community. Subsequent part of the article familiarizes the reader with the methods used by contemporary intelligence institutions in their analytical efforts. Several structural solutions facilitating analytic process are discussed. The author attempts to confront some of the described methods with challenges posed by the modern security environment. This confrontation seeks to evaluate adequacy of selected solutions. Future-oriented reflections referring to the human cognitive functions in the intelligence analysis process are included in the conclusions.

Keywords: intelligence • intelligence analysis • national security • analysis

Artur Gruszczak

NATO wobec zagrożeń wewnętrznych bezpieczeństwa obszaru transatlantyckiego w pierwszych latach zimnej wojny

Wprowadzenie

Głównym motywem instytucjonalizacji współpracy państw Zachodu po II wojnie światowej był nie tylko narastający lęk przed zagrożeniami militarnymi ze strony Związku Radzieckiego, ale także rosnące wpływy partii i ugrupowań komunistycznych, aktywnie wspieranych przez Międzynarodówkę Komunistyczną (Komintern).

Państwa założycielskie NATO zadeklarowały w Traktacie Waszyngtońskim, iż będą „ochraniać wolność, wspólne dziedzictwo i cywilizację swych narodów, oparte na zasadach demokracji, wolności jednostki i rządów prawa”[1]. Strategia NATO w czasie zimnej wojny w powszechnym rozumieniu polegała na stałym rozwoju zdolności do powstrzymywania zagrożeń dla bezpieczeństwa i stabilności obszaru północnoatlantyckiego dzięki mechanizmom zbiorowej samoobrony oraz systematycznemu wzmacnianiu czynników odstraszania. Naturalnym „adresatem” polityki i strategii NATO były państwa bloku wschodniego, zaś podstawową płaszczyzną interakcji, na której realizowane były cele i zadania Aliantów była Europa podzielona „żelazną kurtyną”.

W kontekście zimnowojennej rywalizacji z blokiem wschodnim, ochrona podstaw ustrojowo-ideologicznych Zachodu rozumiana była jako powstrzymywanie i zwalczanie sił komunistycznych prowadzących aktywną, choć często ukrytą, działalność polityczną w krajach członkowskich NATO, a także jako walka z sowiecką infiltracją systemów politycznych państw Zachodu. Jednym z podstawowych celów polityki sowieckiej było nie tylko systematyczne podważanie legitymacji demokratycznego kapitalizmu, jako wzorca ustrojowego świata zachodniego, ale także dążenie do rozbicia spójności Zachodu oraz zakwestionowanie skuteczności i zdolności do działania głównych instytucji

[1] *Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r.*, „Dziennik Ustaw”, 2000, nr 87, poz. 970.

wspólnoty euroatlantyckiej, w szczególności NATO. W kontekście „wielkiej strategii" (grand strategy) przyjętej przez Sojusz Północnoatlantycki pod wpływem Stanów Zjednoczonych, kwestia zagrożeń ładu publicznego i bezpieczeństwa wewnętrznego wydawała się zagadnieniem drugoplanowym i takie przekonanie utwierdzane było przez dziesięciolecia epoki zimnowojennej przez funkcjonariuszy NATO, przywódców państw członkowskich oraz badaczy.

Niniejszy artykuł ma na celu zbadanie strategicznych, politycznych i organizacyjnych uwarunkowań i form współdziałania służb wywiadowczych oraz sił specjalnych[2] państw członkowskich NATO w obliczu zagrożeń bezpieczeństwa wewnętrznego wynikających z definiującej zimną wojnę ostrej konfrontacji między Wschodem a Zachodem. Opiera się na założeniu, iż tworzony od końca lat 40. XX wieku pod egidą Stanów Zjednoczonych system bezpieczeństwa euroatlantyckiego obejmował w pierwszym okresie funkcjonowania środki i metody zarówno strategicznego odstraszania w wymiarze militarnym, jak też powstrzymywania i przeciwdziałania wpływom aktorów społecznych i politycznych o lewicowej i prosowieckiej orientacji aktywnych na zachodzie Europy. Ten drugi wymiar bezpieczeństwa Zachodu angażował służby odpowiedzialne za bezpieczeństwo wewnętrzne i utrzymanie ładu publicznego. Lęk przed wzrostem wpływów komunistycznych i infiltracją lewicy przez agentów Moskwy skłonił Stany Zjednoczone i ich europejskich sojuszników do tworzenia sieci tajnych służb, włączonej na początku lat 50. do struktury instytucjonalnej Organizacji Paktu Północnoatlantyckiego. Utworzenie tajnych komórek planowania i działań operacyjnych podległych Sojuszniczemu Dowództwu NATO w Europie służyło niedopuszczeniu do pojawienia się na Zachodzie sowieckiej „piątej kolumny" dostrzeganej w lewicowych ruchach i partiach politycznych.

Posługując się metodą historyczną, autor niniejszego tekstu wskazuje na instytucjonalne podejście do organizacji w ramach NATO służb odpowiedzialnych za wykrywanie i zwalczanie wewnętrznych zagrożeń dla strategicznych interesów bezpieczeństwa Sojuszu. Prezentując dwa studia przypadku, dotyczące organizacji pod egidą Stanów Zjednoczonych służb wywiadowczych w Niemczech i Włoszech, a więc

[2] W niniejszym tekście stosuję wymiennie termin „siły specjalne" oraz „wojska specjalne" na określenie wyodrębnionych militarnych formacji (oddziałów i pododdziałów) wyspecjalizowanych w prowadzeniu szczególnie trudnych i ryzykownych operacji o charakterze obronnym, zaczepnym, rozpoznawczym i antyterrorystycznym.

głównych wrogów koalicji antyfaszystowskiej podczas II wojny światowej, autor zwraca uwagę na ograniczenia współpracy i słabości instytucjonalnej koordynacji operacji *Stay-Behind* prowadzonych przez służby specjalne państw zachodniej Europy pod nadzorem NATO.

Bezpieczeństwo wewnętrzne w strategii NATO

Tworzenie sieci tajnych służb[3] państw Zachodu było jednym z ważniejszych epizodów historii Europy po zakończeniu II wojny światowej. Te działania, podjęte u zarania zimnej wojny, w okresie kształtowania się wyraźnych podziałów geopolitycznych i strategiczno-militarnych w powojennej Europie, stanowiły element instytucjonalizacji polityczno-wojskowej i ekonomicznej współpracy Zachodu. Zagrożenie ze strony stalinowskiego Związku Radzieckiego i wspieranych przez Sowietów sił komunistycznych w Europie było na tyle poważne, że skłoniło zachodnich sojuszników do podjęcia szerokiej choć ściśle tajnej współpracy służb wywiadowczych i wojsk specjalnych. Innym problemem była niestabilna sytuacja w byłych państwach faszystowskich, w szczególności Włoszech i zachodnich Niemczech, a w związku z tym obawy o powodzenie demokratyzacji i defaszyzacji/denazyfikacji pod kuratelą zwycięskich mocarstw. Pomni doświadczeń okresu po I wojnie światowej, demokratyczni przywódcy państw zachodnich obawiali się odrodzenia nastrojów rewanżystowskich, aktywności skrajnej prawicy i środowisk neofaszystowskich.

Pierwotna, przyjęta na początku lat pięćdziesiątych XX w., strategia NATO skupiała się na wzmocnieniu zdolności odstraszania, zwłaszcza nuklearnego, oraz kolektywnej obronie obszaru północnoatlantyckiego przed agresją sił konwencjonalnych państw bloku wschodniego. Już w pierwszych oficjalnych (choć ściśle tajnych) dokumentach Sojuszu zwracano uwagę na konieczność zapewnienia bezpieczeństwa ludności, zasobów i zasad ustrojowych w państwach członkowskich. W dokumencie Komitetu Wojskowego NATO z 1950 r. zatytułowanym „Strategiczne zalecenia w

[3] W niniejszym tekście stosuję termin „tajne służby" na określenie formacji cywilnych i wojskowych prowadzących działania operacyjno-rozpoznawcze o charakterze niejawnym, realizujące zadania określone przez najwyższych przedstawicieli władzy wykonawczej w państwie i zazwyczaj wyłączone spod nadzoru parlamentarnego.

sprawie regionalnego planowania północnoatlantyckiego"[4] podkreślono, że jednym z zagrożeń bezpieczeństwa obszaru północnego Atlantyku są sprzeczne z interesami Aliantów wywrotowe i sabotażowe działania Sowietów na całym świecie, zmierzające do ustanowienia na całym świecie komunistycznych reżimów poprzez doprowadzenie do upadku bastionów władzy demokratycznej[5]. W pierwotnej „Koncepcji strategicznej obrony obszaru północnoatlantyckiego" z 1 grudnia 1949 r. zakładano „współpracę, w miarę możliwości, w planowaniu wojny psychologicznej i innych operacji specjalnych"[6]. Przeświadczenie o integralnym związku między militarnym/nuklearnym odstraszaniem a wzmacnianiem demokracji i/lub stabilności ustrojowej przewijało się w kolejnych dokumentach strategicznych przyjętych w latach 50. W dokumencie MC 48 z 1954 r. podkreślono, że elementem przewagi strategicznej Sojuszu jest monolityczny system polityczny, oparty na zasadach wolności i demokracji[7].

W koncepcji strategicznej MC 14/2 z 23 maja 1957 r. w rozdziale III dotyczącym innych, tj. pozamilitarnych, zagrożeń bezpieczeństwa NATO znalazło się następujące założenie: „(...) Sowieci mogą uznać, że jedynym sposobem skutecznego osiągnięcia ich celów będzie rozpoczęcie operacji o ograniczonych celach, takich jak infiltracje, wtargnięcia lub wrogie działania na lokalną skalę na obszarze NATO, wspierane przez nich skrycie lub otwarcie (...)"[8]. W związku z tym jednym z celów zawartych w koncepcji strategicznej jest zastosowanie przez państwa członkowskie odpowiednich środków służących „zachowaniu porządku na froncie wewnętrznym"[9]. W punkcie 26. dokumentu MC 14/2 doprecyzowano rozumienie strategicznych wyzwań stojących przed Sojuszem Północnoatlantyckim w sferze bezpieczeństwa wewnętrznego: „NATO musi być również przygotowane do natychmiastowej reakcji z odpowiednią siłą – a tym samym utrzymywania właściwych środków - na jakiekolwiek inne firmy agresji na terytorium

[4] *Strategic Guidance for North Atlantic Regional Planning, M.C. 14, 28 March 1950*, w: *NATO Strategy Documents 1949-1969*, NATO Historical Office, Brussels 1997, s. 85-105
[5] *Intelligence Guidance for North Atlantic Regional Planning*, aneks do dokumentu MC 14, w: *NATO Strategy Documents 1949-1969...*, *op.cit.*, s. 102.
[6] *Koncepcja strategiczna obrony obszaru północnoatlantyckiego DC 6/1 1 grudnia 1949 r.*, w: R. Kupiecki, *Siła i solidarność. Strategia NATO 1949-1989*, Warszawa 2009, s. 400.
[7] *The Most Effective Pattern of NATO Military Strength for the Next Few Years, M.C. 48 (FINAL), 22 November 1954*, w: *NATO Strategy Documents 1949-1969...*, *op.cit.*, s. 235.
[8] *Ogólna Strategiczna Koncepcja Obrony Obszaru Północnoatlantyckiego MC 14/2*, w: R. Kupiecki, *op.cit.*, s. 363-64.
[9] *Ibidem*, s. 365.

NATO, takie jak infiltracja, wtargnięcie lub lokalne wrogie działania, bez konieczności sięgania po broń nuklearną"[10].

Koncepcja strategiczna z 1957 r. została dopasowana do nowej sytuacji strategicznej związanej z postępami Sowietów w dziedzinie technologii rakietowych i budowy pocisków balistycznych dalekiego zasięgu. Szybki postęp technologii wojskowych i wprowadzanie nowoczesnych typów broni przez obydwa bloki wojskowe: NATO i Układ Warszawski, a także wzrost aktywności lewicy, w tym lewicowych związków zawodowych oraz partii komunistycznych, w niektórych krajach Europy Zachodniej (Francja, Włochy)[11] zwracały uwagę planistów Paktu na kwestie związane z ładem publicznym i stabilnością ustrojową Zachodu[12]. Dlatego zasady planowania obronnego ujęte w dokumencie MC 14/2 oprócz przedsięwzięć militarnych uwzględniały aspekty polityczne, informacyjne, psychologiczne i ekonomiczne rywalizacji Wschód-Zachód.

W przyjętym przez Komitet Wojskowy 14 kwietnia 1958 r. dokumencie MC 78 zawarto definicje terminów związanych z zagrożeniem ładu i stabilności wewnętrznej na obszarze północnoatlantyckim. Zdefiniowano takie formy aktywności przeciwników Paktu, jak wrogie działania, wtargnięcia i infiltracje. Zaostrzająca się od początku lat sześćdziesiątych walka wywiadów, agresywne plany KGB wobec Zachodu i niezdecydowana postawa USA, widoczna w szczególności w okresie kryzysu berlińskiego 1958-1962, wzbudzały rosnące zaniepokojenie co do zdolności wspólnoty transatlantyckiej do przeciwdziałania wzmożonej aktywności bloku wschodniego[13].

Jeden z amerykańskich analityków, cytowany przez Roberta Kupieckiego, sformułował następujące zalecenie: „Powinniśmy zabiegać o zachowanie i wzmocnienie cywilizacji, która mając korzenie w obszarze śródziemnomorsko-północnoatlantyckim, ma charakter uniwersalny. Ta cywilizacja jest zagrożona z zewnątrz przez światową anarchię oraz przez wewnętrzną pokusę niespójności, dlatego też państwa tego obszaru muszą blisko współpracować, także wojskowo. To stanowi główny powód istnienia NATO i

[10] *Overall Strategic Concept for the Defense of the North Atlantic Treaty Organization Area MC 14/2*, w: *NATO Strategy Documents 1949-1969...*, *op.cit.*, s. 294.
[11] Zob. M.-P. Rey, *The Western European Communist Parties in the Cold War, 1957-68*, w: W. Loth (red.), *Europe, Cold War and Coexistence, 1953-1965*, London and Portland, OR 2004, s. 203-05.
[12] M. Trachtenberg, *A Constructed Peace. The Making of European Settlement 1945-1963*, Princeton, NJ 1999, s. 201-202.
[13] Zob. V.M. Zubok, *Spy vs. Spy: The KGB vs. the CIA, 1960-1962*, „CWIHP Bulletin", 1994, nr 4, s. 22-25.

Sojusz jako całość jest funkcjonalnym tworem dla osiągnięcia tego celu”[14]. Taki pogląd znalazł potwierdzenie w kolejnej koncepcji strategicznej, MC 14/3, przyjętej w grudniu 1967 r. Uznano w niej, że jednym z elementów wiarygodnego odstraszania jest gotowość stawienia czoła jakiejkolwiek formie, potencjalnej czy faktycznej, agresji, w tym tajnym operacjom prowadzonym przez państwa Układu Warszawskiego.

Zagrożenie ze strony bloku wschodniego wiązało się m.in. z prowadzoną przez nich działalnością wywrotową, włączając w to rozprzestrzenianie ideologii komunistycznej oraz eksport uzbrojenia i surowców. NATO zakładało, że „Sowieci mogą prowadzić tajne akcje dla inspirowania niepokojów, zagrożeń i dywersji, aby w ten sposób stworzyć dogodne warunki do ich późniejszego wykorzystania”[15]. Zagrożenie bezpieczeństwa wewnętrznego postrzegane było również w kontekście gotowości Sowietów do użycia środków militarnych w wymiarze „ograniczonej agresji”. W dokumencie MC 14/3 zaznaczono jednak, że bardziej prawdopodobne od ograniczonej agresji przy użyciu wojsk państw Układu Warszawskiego jest skorzystanie z „innych sił lub lokalnych grup rewolucyjnych wspieranych przez komunistów”[16]. W związku z tak pojmowanymi źródłami zagrożeń na państwa członkowskie NATO nałożono obowiązek „gromadzenia i przekazywania informacji wywiadowczych oraz pełnienia roli sił bezpieczeństwa przeciwstawiających się działaniom w ramach tajnych operacji przeciwko państwom NATO”[17].

W latach siedemdziesiątych – w okresie odprężenia i negocjacji rozbrojeniowych między Wschodem i Zachodem – i osiemdziesiątych: czasie ostrej konfrontacji ideologicznej, konfliktów regionalnych i intensywnego wyścigu zbrojeń, strategiczne wytyczne przyjęte w dokumentach Paktu w latach pięćdziesiątych i sześćdziesiątych nie straciły na ważności i aktualności, podtrzymując przekonanie o konieczności skutecznych działań „na froncie wewnętrznym”.

[14] J.W. Holmes, *The Advantages of Diversity in NATO*, w: K.H. Cerny, H.W. Briefs (red.), *NATO in Quest of Cohesion*, New York 1965, s. 300, cyt. za: R. Kupiecki, *op.cit.*, s. 96.
[15] *Ogólna Koncepcja Strategiczna Obrony Obszaru Północnoatlantyckiego MC 14/3*, w: R. Kupiecki, *op.cit.*, s. 382.
[16] *Ibidem*, s. 383.
[17] *Ibide*m, s. 387.

Operacja „Gladio"

31 maja 1972 r. w lesie opodal włoskiej wioski Peteano nastąpił wybuch bomby umieszczonej we Fiacie 500, która spowodowała śmierć trzech karabinierów i poważne rany czwartego[18]. Anonimowy telefon poinformował policję, że odpowiedzialność za zamach wzięła organizacja o nazwie *Brigate Rosse* („Czerwone Brygady"), która znana była policji od 1971 r. jako jedna z lewackich grup stosujących przemoc jako narzędzie walki politycznej. W wyniku operacji sił policyjnych aresztowano blisko 200 przedstawicieli organizacji lewicowych, głównie członków Komunistycznej Partii Włoch (PCI)[19]. W 1984 r. sędzia Felice Casson podjął śledztwo w sprawie zamachu bombowego w Peteano oraz związku między tym wydarzeniem a odkryciem w 1972 r. nielegalnego składu broni na przedmieściach Triestu. Wyniki śledztwa były dużym zaskoczeniem. Pierwotny raport w sprawie Peteano został sfałszowany, do zamachu użyto materiału wybuchowego C-4 stosowanego wówczas przez armię amerykańską oraz oddziały wchodzące w skład sił NATO, zaś sam zamach został zorganizowany przez skrajnie prawicową grupę *Ordino Nuovo* współpracującą z włoskim wywiadem wojskowym SID (*Servizio Informazioni Difesa*), przemianowanym w 1977 r. na Służbę Informacji i Bezpieczeństwa Wojskowego SISMI (*Servizio per le Informazioni e la Sicurezza Militare*). W 1990 r. sędzia Casson odkrył w archiwach SISMI dokumenty zawierające informacje o działaniach tajnych służb koordynowanych przez NATO w ramach operacji pod kryptonimem „Gladio" (Miecz). W sierpniu 1990 r. premier rządu włoskiego Giulio Andreotti przedstawił specjalnej komisji włoskiego parlamentu raport potwierdzający rewelacje sędziego Cassona[20].

Reakcje polityków, dziennikarzy, opinii publicznej oraz instytucji państwowych w państwach członkowskich NATO uruchomiły proces „wywabiania białych plam" w zimnowojennej historii Paktu. Parlamentarne komisje śledcze powołane w niektórych krajach zachodnioeuropejskich (Włochy, Belgia, Luksemburg, Szwajcaria), wypowiedzi i relacje funkcjonariuszy służb specjalnych uczestniczących w operacji „Gladio", a także

[18] R. Faligot, R. Kauffer, *Służby specjalne. Historia wywiadu i kontrwywiadu na świecie*, Warszawa 1998, s. 455.
[19] Ph.P. Willan, *Puppetmasters. The Political Use of Terrorism in Italy*, London 1991, s. 153.
[20] M. Coglitore, *Operazione Gladio*, http://www.intermarx.com/ossto/operazione.html (dostęp 12.04.2017).

dociekliwość dziennikarzy umożliwiły ujawnienie wielu skrywanych do tego czasu informacji rzucających światło na nieznane obszary współpracy transatlantyckiej[21].

Operacja „Gladio" miała swój początek we Włoszech – kraju pogrążonym w kryzysie społeczno-politycznym i gospodarczym, niosącym brzemię faszystowskiej przeszłości, kraju, w którym główną siłą polityczną pod koniec lat czterdziestych XX w. stała się Włoska Partia Komunistyczna (PCI). Celem Stanów Zjednoczonych i NATO było niedopuszczenie do „politycznego wstrząsu", jakim byłby udział PCI – samodzielnie czy nawet w koalicji – w rządzeniu państwem[22]. Amerykańskie władze tworzyły struktury wywiadowcze na terenie Włoch już od 1943 r., po odsunięciu Mussoliniego od władzy i wypowiedzeniu wojny III Rzeszy przez rząd marszałka Badoglia. Alianci korzystali z działających agentów włoskiego wywiadu wojskowego, zacieśniając kontrolę nad nimi, a następnie pozwalając na częściową samodzielność. Po zwycięstwie w wyborach parlamentarnych w 1948 r. popieranej przez Amerykanów i wspieranej finansowo przez CIA Demokracji Chrześcijańskiej[23], rząd Alcidego de Gasperiego za zgodą Stanów Zjednoczonych utworzył wojskową służbę wywiadowczą SIFAR (*Servizio Informazioni*

[21] Najpełniejszą, monograficzną, będącą rezultatem kilkuletnich badań, choć kontrowersyjną jeśli chodzi o wykorzystane źródła, pracą dotyczącą operacji „Gladio" jest książka Daniele'a Gansera, *NATO's Secret Armies. Operation Gladio and Terrorism in Western Europe*, Abingdon and New York 2005. Na początku lat dziewięćdziesiątych XX w., po ujawnieniu "tajnych armii NATO", ukazały się liczne publikacje książkowe: publicystyczne, biograficzne i analityczne poświęcone współpracy służb specjalnych państw NATO w ramach operacji „Gladio". Do pierwszej kategorii, publicystycznej, należy zaliczyć: L.A. Müller, *Gladio – das Erbe des Kalten Krieges. Der Nato-Geheimbund und sein deutscher Vorläufer*, Hamburg 1991; J. Willems (red.), *Gladio*, Brussels 1991; H. Gijsels, *Network Gladio*, Leuven 1991; P. Moroni, M. *Coglitore,* S. Scarso (red.), *La Notte dei Gladiatori. Omissioni e silenze della Repubblica*, Padova 1992; G. Fasanella, C. Sestieri con G. Pellegrino, *Segreto di Stato. La verità da Gladio al caso Moro*, Torino 2000. Spośród nielicznych publikacji pióra bezpośrednich aktorów zaangażowanych w realizację działań w ramach tajnych operacji NATO warto wymienić książki generała Gerrarda Serravallego, w latach 1971-1974 szefa włoskich jednostek „Gladio" w ramach służby wywiadu wojskowego SID (G. Serravalle, *Gladio*, Roma 1991) i generała Paola Inzerilliego, dowódcy włoskich jednostek Gladio w latach 1974-76, szefa sztabu włoskiego wywiadu wojskowego SISMI w latach 1989-91 (P. Inzerilli, *Gladio. La verità negata*, Bologna 1995). Inzerilli w 2009 r. opublikował apologetyczną relację z operacji „Gladio" we Włoszech i działań *stay-behind* w Europie (P. Inzerilli, *La vittoria dei gladiatori. Da Malga Porzus all'assoluzione di Rebibbia*, Brescia 2009). Wśród opracowań analitycznych, choć bez należytego aparatu naukowego,należy zwrócić uwagę na: Ph.P. Willan, *Puppetmasters. The Political Use of Terrorism inItaly*, London 1991; J.-F. Brozzu-Gentile, *L'Affaire Gladio. Les réseaux secrets américains au coeur du terrorisme en Europe*, Paris 1994; E. Bettini, *Gladio. La repubblica parallela*, Roma 1996; R. Cottrell, *Gladio, NATO's Dagger at the Heart of Europe. The Pentagon-Nazi-Mafia Terror Axis*, San Diego 2012. Cennym źródłem informacji jest także trzyczęściowy film dokumentalny zrealizowany przez Allana Francovicha dla programu Timeline w BBC2 i emitowany w czerwcu 1992 r. Film dostępny na YouTube: http://www.youtube.com/view_play_list?p=01BDBF4FF8112D87&search_query=francovich (dostęp: 14.10.2016).

[22] L. Nuti, *The Italian 'Stay-Behind'Network – The Origins of Operation 'Gladio'*, „Journal of Strategic Studies", 2007, 30 (6), s. 958-62.

[23] Zob. K. Mistry, *Approaches to Understanding the Inaugural CIA Covert Operation in Italy: Exploding Useful Myths*, „Intelligence and National Security", 2011, 26 (2-3), s. 246-268.

Forze Armate). Po powstaniu NATO, służba ta została włączona do koordynowanych przez sojusz operacji *stay-behind*[24]. Na przełomie lat 40. i 50. XX w. SIFAR za przyzwoleniem CIA rekrutował do sieci swych współpracowników osoby związane z nielegalnymi skrajnie prawicowymi organizacjami, takimi jak *Ordine Nuovo* czy *Propaganda Due* (P2). W 1951 r. ówczesny szef SIFAR gen. Umberto Broccoli wyszedł z inicjatywą utworzenia we współpracy z innymi włoskimi służbami wywiadowczymi sieci tajnych organizacji wywiadowczych i bojowych zdolnych do działania na tyłach wroga (*stay-behind*) w warunkach okupacyjnych. Ustalono utworzenie sieci 200 agentów, a na początek przeszkolenie kilku oficerów włoskiej armii przez bytyjski SIS. W 1953 r. na Sardynii zbudowano specjalny ośrodek szkoleniowy sabotażystów. Pod koniec 1956 r. struktura organizacyjna operacji „Gladio" była gotowa. W tym czasie zawarto tajne porozumienie włosko-amerykańskie dotyczące organizacji i działalności włoskich tajnych działań *stay-behind*[25].

Skutkiem operacji „Gladio" był brak jakiejkolwiek kontroli parlamentarnej i – nierzadko – rządowej nad służbami specjalnymi uczestniczącymi w tajnych operacjach. W ramach przygotowań do działań na wypadek zagrożenia komunistyczną dywersją albo możliwością przejęcia władzy przez komunistów zgromadzono znaczne ilości broni, amunicji i sprzętu wojskowego, w tym nawet moździerze kal. 60 mm. We Włoszech zidentyfikowano 139 tajnych składów broni[26]. Z ujawnionych przez komisje parlamentarne raportów oraz szczątkowych informacji pochodzących od polityków i funkcjonariuszy służb specjalnych wynika nie tyle niewiedza najwyższych przedstawicieli władz państwowych, ile zgoda na oddanie w ręce tajnych służb pełni kompetencji w zakresie prowadzonych pod egidą NATO operacji służących zapewnieniu bezpieczeństwa wewnętrznego w obliczu zagrożenia komunistycznego.

Budowa struktur *stay-behind* w Niemczech

Sytuacja w zajętych po II wojnie światowej przez zachodnie mocarstwa częściach Niemiec budziła poważne zaniepokojenie władz okupacyjnych. W szczególności

[24] M. Faini, *The US Government and the Italian coup manqué of 1964: the unintended consequences of intelligence hierarchies*, „Intelligence and National Security", 2016, 31 (7), s. 1011.
[25] L. Nuti, *op.cit.*, s. 963-64.
[26] D. Ganser, *The ghost of Machiavelli: An approach to operation Gladio and terrorism in cold war Italy*, „Crime, Law & Social Change", 2006, 45 (2), s. 121.

Amerykanie nie kryli obaw zarówno przed odrodzeniem nazizmu, jak też – przede wszystkim – infiltracji sowieckiej agentury oraz – jak to było po I wojnie światowej – wzrostu popularności ideologii marksistowskiej oraz ruchów rewolucyjnych w społeczeństwie. W obliczu powojennego chaosu w Niemczech, a także słabości działań rozpoznawczych w oparciu o źródła otwarte i lokalnych, często przypadkowych informatorów[27], władze amerykańskie uznały za niebędne utworzenie i kierowanie pod kontrolą Centralnej Agencji Wywiadowczej (Central Intelligence Agency – CIA) i Służby Kontrwywiadu Armii Stanów Zjednoczonych (Army Counterintelligence Corps) sieci agentów posiadających dobre rozeznanie w środowiskach lewicowych, w szczególności w kręgach komunistów, a także posiadających umiejętności techniczne, na przykład obsługi urządzeń i systemów telekomunikacyjnych czy szyfrowania. Proces rekrutacji odbywał się bez odpowiedniego rozpoznania, Amerykanie często nie mieli odpowiedniej wiedzy o niemieckich kandydatach, albo też przymykali oczy na nieścisłości lub braki w dokumentacji ukrywające nazistowską przeszłość kandydatów[28].

Ujawnione dokumenty CIA i niemieckiej Federalnej Służby Wywiadowczej (BND), do których dotarli dwaj niemieccy dziennikarze Erich Schmidt-Eenboom i Ulrich Stoll i zrelacjonowali ich zawartość w książce *Die Partisanen der NATO*[29], a także niemiecki historyk Michael Wala[30], potwierdziły udział wielu byłych funkcjonariuszy III Rzeszy w organizowanych przez amerykański wywiad i kontrwywiad operacjach *stay-behind*[31]. Do tego czasu najwięcej uwagi poświęcano tzw. Organizacji Gehlena — zorganizowanej i kierowanej przez byłego generała Wehrmachtu Reinharda Gehlena nieformalnej sieci tajnych agentów rekrutujących się z dawnych hitlerowskich formacji: SS, Gestapo i Służby

[27] Zob. D. Alvarez, *American Clandestine Intelligence in Early Postwar Europe*, „Journal of Intelligence History", 2004, 4 (1), s. 16.
[28] *Introduction*, w: R. Breitman, N. J. W. Goda, T. Naftali, R. Wolfe (red.), *U.S. Intelligence and the Nazis*, Cambridge 2005, s. 7. Szerzej o wykorzystywaniu funkcjonariuszy Trzeciej Rzeszy przez służby wywiadowczej USA piszą Richard Breitman and Norman J.W. Goda w: *Hitler's shadow Nazi war criminals, U.S. intelligence, and the Cold War*, Washington, DC 2010, http://www.archives.gov/iwg/reports/hitlers-shadow.pdf (dostęp: 17.10.2016); także: Ch. Simpson, *Blowback. America's Recruitment of Nazis, and Its Destructive Impact on Our Domestic and Foreign Policy*, New York 2014.
[29] E. Schmidt-Eenboom, U. Stoll, *Die Partisanen der NATO: Stay-Behind-Organisationen in Deutschland 1946–1991*, Berlin 2015.
[30] M. Wala, *Stay-behind operations, former members of SS and Wehrmacht, and American intelligence services in early Cold War Germany*, „Journal of Intelligence History", 2016, 15 (2), s. 71-79.
[31]Zob. *Forging an Intelligence Partnership: CIA and the Origins of the BND, 1945-49*, w: K.C. Raffner (red.), *Forging an Intelligence Partnership: CIA and the Origins of the BND, 1945-49. A Documentary History*, vol. 1, Washington, D.C. 1999. Także: T. Naftali, *Berlin to Baghdad: The Pitfalls of Hiring Enemy Intelligence*, „Foreign Affairs", 2004, 83 (3).

Bezpieczeństwa Rzeszy[32]. Ujawnione dokumenty wskazały na inne organizacje przygotowane do działań o charakterze *stay-behind*.

Generał Gehlen, stojąc od 1942 r. na czele wydziału wschodniego (*Fremde Heere Ost)* służby wywiadowczej Wermachtu, posiadał szeroką wiedzę na temat organizacji i funkcjonowania totalitarnego aparatu Związku Sowieckiego. Tuż przed klęską III Rzeszy, w przekonaniu o przyszłym konflikcie między USA a ZSRR oraz amerykańskich potrzebach rozpoznawczo-wywiadowczych na okupowanym terytorium Niemiec, generał Gehlen zreorganizował podległe mu jednostki wywiadu wojskowego, a po dwóch tygodniach od kapitulacji III Rzeszy poddał się Amerykanom[33]. W trakcie przysłuchań w obozie jenieckim amerykańscy oficerowie zorientowali się w szerokich zasobach wiedzy Gehlena o sytuacji w Niemczech i w ZSRR, po czym zaproponowali mu współpracę. W lipcu 1946 r. Reinhard Gehlen i jego byli współpracownicy, tworzący nieformalną Organizację Gehlena, rozpoczęli działalność w ramach Grupy Ewaluacyjnej pracującej na potrzeby Zarządu Wywiadu Armii Stanów Zjednoczonych. Analizy wywiadowcze dostarczane przez Organizację Gehlena rezydującą w Pullach spotkały się z dużym uznaniem władz amerykańskich. W tym czasie Organizacja Gehlena dysponowała siecią około 3 tys. tajnych informatorów działających w 37 rezydenturach ulokowanych na terytorium Niemiec (uznawanym w granicach sprzed 1937 r., a więc obejmujących tereny zachodnich i północnych ziem PRL i utworzonej wkrótce NRD). Ogromna ilość informacji dostarczanych przez informatorów pozwalała na przygotowanie 200 raportów miesięcznie[34]. Szczególnie cenne okazało się rozpoznanie wywiadowcze w oparciu o działania agenturalne i nasłuch radiokomunikacyjny podczas blokady Berlina w 1948 r.[35]

W lipcu 1949 r. Organizacja Gehlena została podporządkowana Centralnej Agencji Wywiadowczej. Po zjednoczeniu zachodnich stref okupacyjnych i utworzeniu

---

[32] Zob. H. Höhne, H. Zolling, *The General Was A Spy.The Truth About General Gehlen and His Spy Ring*, Toronto – New York – London 1972, s. 232-234. Odpowiedzią na tę książkę, powstałą na podstawie serii artykułów opublikowanych przez obydwu autorów na łamach tygodnika *Der Spiegel* wiosną 1971 r., było wydanie drukiem wspomnień gen. Gehlena: R. Gehlen, *Der Dienst. Erinnerungen 1942-1971*, Mainz – Wiesbaden 1971. Por. R. Kilarski, *Organizacja wywiadowcza R. Gehlena*, Warszawa 1978; T. Kopyś, *Początki wywiadu zachodnioniemieckiego oraz jego aktywność w Polsce w latach pięćdziesiątych i sześćdziesiątych XX w.*, „Aparat Represji w Polsce Ludowej 1944-1989", 2011, nr 1 (8-9), s. 153-75.

[33] J. Wegener, *Shaping Germany's Post-War Intelligence Service: The Gehlen Organization, the U.S. Army, and Central Intelligence, 1945–1949*, „Journal of Intelligence History", 2007, 7 (1), s. 46-47; T. Naftali, *Reinhard Gehlen and the United States*,w: R. Breitman, N. J. W. Goda, T. Naftali, R. Wolfe (red.), *U.S. Intelligence and the Nazis*, Cambridge 2005, s. 379-81.

[34] J. Wegener, *op.cit.*, s. 48.

[35] H.-H. Crome, *The "Organisation Gehlen" as Pre-History of the Bundesnachrichtendienst*, „Journal of Intelligence History", 2007, 7 (1), 34.

Republiki Federalnej Niemiec Gehlen skontaktował się z czołowymi funkcjonariuszami rządu kanclerza Konrada Adenauera, w szczególności podsekretarzem stanu a później szefem urzędu kanclerskiego Hansem Globkem[36], przekonując ich o profesjonaliźmie jego organizacji i lojalności wobec władz federalnych[37]. W 1956 r. Organizacja Gehlena została przekształtcona w Federalną Służbę Wywiadowczą (BND), działającą w ustrojowych ramach Republiki Fedralnej Niemiec[38].

Organizacja Gehlena dysponowała rozbudowaną strukturą rozpoznawczo-analityczną funkcjonującą na potrzeby i pod kuratelą najpierw amerykańskiego wywiadu i kontrwywiadu wojskowego, a od 1949 r. wywiadu zagranicznego (CIA). W gronie kilku tysięcy członków sieci stworzonej przez Reinharda Gehlena znaleźli się członkowie organizacji o charakterze bojowym, przygotowanych do prowadzenia działań psychologicznych i przeciwdywersyjnych, charakterystycznych dla operacji *stay-behind*. Organizowane i finansowane przez CIA, miały tworzyć sieć komunikacji i informacji w celu rozpoznawczym, a także stawić zbrojny opór w razie działań komunistycznych dywersantów lub sowieckiej inwazji wojskowej. Największą z tych grup o paramilitarnym charakterze była Służba Techniczna: działająca w ramach Związku Młodzieży Niemieckiej, antykomunistyczna organizacja młodzieżowa założona z inicjatywy Franka Wisnera - ówczesnego szefa Biura Koordynacji Polityki nadzorującego z ramienia CIA operacje *stay-behind*. Inną strukturą była sieć KIBITZ – stworzona w 1950 r. przez placówkę CIA w Karlsruhe i kierowana przez byłego oficera SS Waltera Koppa[39]. W założeniu, w razie działań komunistycznych wrogów siatka KIBITZ była odpowiedzialna za gromadzenie informacji oraz uaktywnienie i obsługę ukrytych radiostacji. Po ujawnieniu przez prasę istnienia KIBITZ i przynależności do niej byłych oficerów SS, w tym członków zbrojnych oddziałów Waffen SS odpowiedzialnych za zbrodnie wojenne, siatka została rozwiązana w połowie 1953 r.[40].

[36] Hans Globke był prawnikiem, urzędnikiem Ministerstwa Spraw Wewnętrznych III Rzeszy, autorem ustaw dyskryminujących mniejszości rasowe, przede wszystkim ustaw norymberskich z 1935 r., a także głównym radcą prawnym w kierowanym przez hitlerowskiego zbrodniarza Adolfa Eichmanna Urzędzie do spraw Żydów. Zob. R. Wistrich, *Who's Who in Nazi Germany*, London – New York 2002.
[37] T. Naftali, *Reinhard Gehlen...*, *op.cit.*, s. 396-97.
[38]Zob. R. Gehlen, *op.cit.*, s. 138-140; H. Höhne, H. Zolling, *op.cit.*, s. 232-234.
[39] M. Wala, *op.cit.*, s. 72.
[40] T. Naftali, *New Information on Cold War CIA Stay-Behind Operations in Germany and on the Adolf Eichamnn Case*, s. 2, https://fas.org/sgp/eprint/naftali.pdf (dostęp: 16.10.2016).

Od 1956 r., po przekształceniu Organizacji Gehlena w Federalną Służbę Wywiadowczą (BND)[41] i oficjalnym włączeniu przedstawiciela Niemiec Zachodnich do natowskiego Tajnego Komitetu Planowania, niemieckie służby stały się cennym partnerem amerykańskiej CIA oraz brytyjskich SIS i SAS w szkoleniu, planowaniu i wsparciu logistycznym operacji *stay-behind* w Europie[42].

Organizacja tajnych operacji NATO

Tajny raport Służby Wywiadowczej Sił Zbrojnych Republiki Włoskiej (SIFAR) z 1 czerwca 1959 r. (jeden z najważniejszych dokumentów odkrytych przez sędziego Felice Cassona w 1990 r.) zatytułowany «„Siły specjalne" SIFAR i operacja „Gladio"»[43], nie tylko zawierał szczegółowe informacje o zakresie, charakterze, organizacji i realizacji operacji pod kryptonimem „Gladio", ale także wiązał te działania z organami struktury wojskowej NATO, przede wszystkim z Naczelnym Dowództwem Sojuszniczych Sił w Europie (SHAPE) oraz Naczelnym Dowódcą Sił Sojuszniczych w Europie (SACEUR). W ramach SHAPE działał Tajny Komitet Planowania (*Clandestine Planning Committee* - CPC), pełniąc funkcje koordynacji i planowania strategicznego, a ponadto funkcjonował Tajny Komitet Sojuszniczy (*Allied Clandestine Committee* – ACC), w którym państwa członkowskie reprezentowane były przez szefów służb specjalnych odpowiedzialnych za przygotowanie i prowadzenie operacji *stay-behind*.

Tajny Komitet Planowania (CPC) został utworzony w lipcu 1951 r. z rozkazu Naczelnego Dowódcy Sojuszniczych Sił NATO w Europie na bazie Tajnego Komitetu Unii Zachodniej, elementu tworzonej na podstawie Paktu Brukselskiego z 17 marca 1948 r. struktury organizacyjnej Unii Zachodniej[44]. Po przejęciu zadań związanych z bezpieczeństwem i obroną państw-stron Paktu Brukselskiego przez NATO, Tajny Komitet Unii Zachodniej został związany z dowództwem wojskowym Sojuszu i

[41] Zob. R. Gehlen, *op.cit.*, s. 138-140; H. Höhne, H. Zolling, *op.cit.*, s. 232-234.
[42] D. Ganser, *NATO's Secret Armies*, s. 200-204.
[43] *Servizio Informazioni delle Forze Armate. Ufficio R – Sezione SAD: Le forzespeciali del SIFAR e l'operazione GLADIO. Roma, 1 Giugno 1959*, http://se2.isn.ch/serviceengine/FileContent?serviceID=PHP&fileid=F0397478-D85B-B79E-5ED6-1BD9FDD9D0CF&lng=it (dostęp: 12.05.2016). Tłumaczenie na j. angielski dostępne w: D. Ganser, *The ghost of Machiavelli...*, *op.cit.*, s. 138-47.
[44] G. Arboit, *Quelles «Armées Secrètes» de l'OTAN?*, „Rapport de recherche", nr 18, Centre Français de Recherche sur le Renseignement (CF2R), Paris, Mai 2016, s. 20.

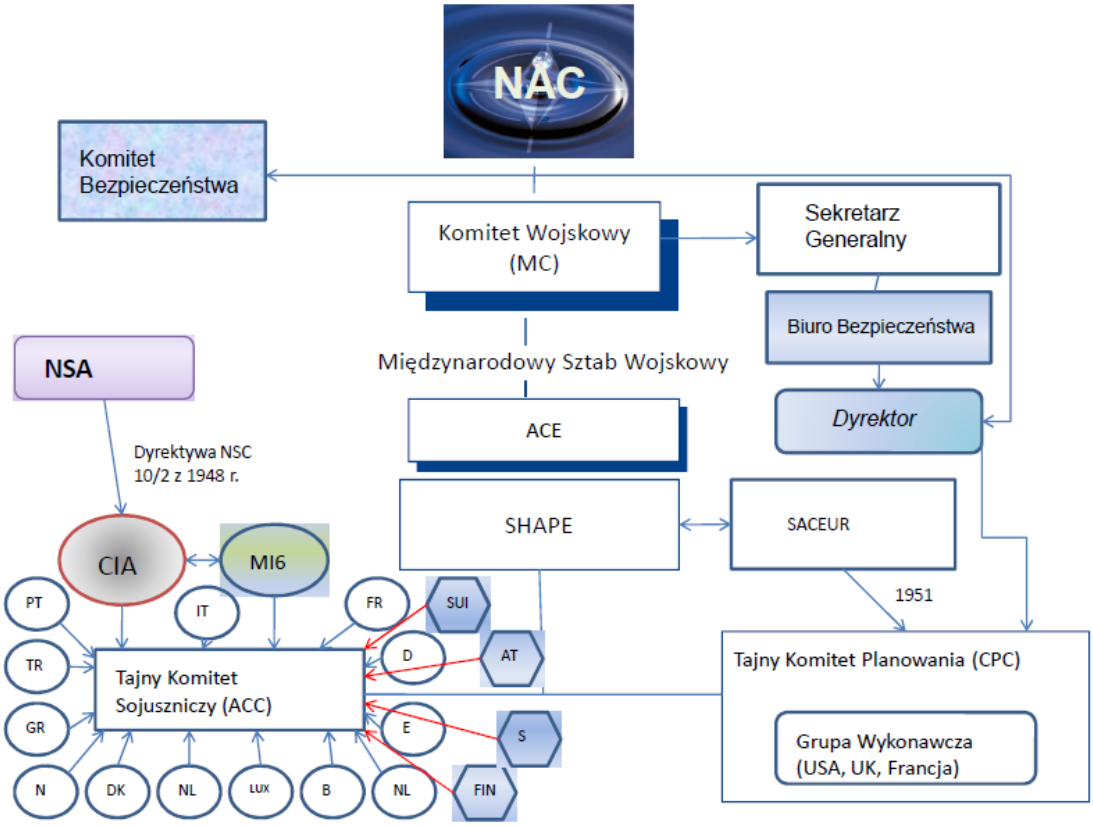
ulokowany w Paryżu[45]. Tajny Komitet Planowania był łącznikiem między Sojuszniczym Dowództwem Sił NATO w Europie a kierownictwem służb specjalnych państw członkowskich, odpowiadał za właściwą koordynację tych kontaktów oraz odpowiednie i skuteczne wdrażanie decyzji podjętych przez SHAPE. W praktyce, wskutek nieformalnej zgody członków NATO na obsadzenie stanowiska SACEUR przez czterogwiazdkowego generała armii Stanów Zjednoczonych (pierwszym Naczelnym Dowódcą Sił Sojuszniczych w Europie był gen. Dwight Eisenhower), działalność CPC została zdominowana przez Stany Zjednoczone, wspomagane przez Wielką Brytanię i Francję. Te trzy mocarstwa tworzyły tzw. Grupę Wykonawczą w ramach CPC. Tajny Komitet Planowania zbierał się zazwyczaj dwa razy w roku w Paryżu. Po wystąpieniu Francji z NATO i przeniesieniu w 1967 r. organów Paktu do Brukseli, CPC obradował raz lub dwa razy do roku w Kwaterze Głównej NATO. Prócz tego dowódcy tajnych służb spotykali się co najmniej raz w roku w jednej ze stolic państw uczestniczących w działaniach *stay-behind*[46].

Tajny Komitet Sojuszniczy (ACC – w 1974 r. zmienił swą nazwę na Sojuszniczy Komitet Koordynacyjny)[47] został zawiązany jako luźna struktura współdziałania tajnych służb państw Zachodu jeszcze w 1947 r. we Włoszech. Według niektórych autorów, do Traktatu Waszyngtońskiego powołującego do życia Organizację Paktu Północnoatlantyckiego, dołączono tajny protokół zobowiązujący państwa-sygnatariuszy traktatu do powołania narodowych tajnych organów bezpieczeństwa, których celem było przeciwdziałanie i zwalczanie dywersji oraz innych form zagrożeń ze strony sił komunistycznych[48]. Koordynacją współpracy aliantów miała zająć się powołana w tym czasie (20 maja 1949 r.) Agencja Bezpieczeństwa Sił Zbrojnych USA (przekształcona w 1952 r. w Narodową Agencję Bezpieczeństwa – NSA)[49]. ACC miał luźną strukturę organizacyjną o charakterze koordynacyjno-łącznikowym, w którym państwa uczestniczące w działaniach *stay-behind* reprezentowane były przez wysokich oficerów

[45] D. Ganser, *NATO's Secret Armies, op.cit.*, s. 28.
[46] D. Ganser, *The ghost of Machiavelli...*, *op.cit.*, s. 124.
[47] Ch. Cogan, *'Stay-Behind' in France: Much AdoAbout Nothing?*, „Journal of Strategic Studies", 2007, 30 (6), s. 948-49.
[48] A. Rowse, *Gladio: The Secret US War to subvert Italian Democracy*, „Covert Action Quarterly", 1994, 49, s. 3.
[49] J.T. Richelson, *The U.S. Intelligence Community*, 4th ed., Boulder and London 1999, s. 30-31. Autor ten podkreśla, że utworzenie tych instytucji wywiadowczych objęte było ścisłą tajemnicą i dopiero w 1957 r. administracja USA oficjalnie potwierdziła istnienie NSA.

służb wywiadowczych. W ściśle tajnych spotkaniach, organizowanych co kilka miesięcy w stolicach państw zaangażowanych w operacje *stay-behind*, regularnie uczestniczyli przedstawiciele USA, Wielkiej Brytanii, Francji, RFN i krajów Beneluksu, pozostałe państwa zaś zapraszane były przez Amerykanów tylko wówczas, gdy planowane lub prowadzone działania tych państw bezpośrednio dotyczyły[50].

Wykres 1. Struktura instytucjonalna sieci współpracy tajnych służb w ramach NATO.



Źródło: opracowanie własne.

W wymiarze szkoleniowym i taktyczno-technicznym, podstawą współpracy była instrukcja ramowa wydana przez CPC w listopadzie 1952 r. Określała trzy podstawowe obszary operacji *stay-behind*: 1) rozpoznanie wywiadowcze; 2) infiltracja i eksfiltracja; 3) operacje psychologiczne[51]. Odpowiedzialność za organizację i prowadzenie szkoleń spoczęła na Jednostkach Specjalnych Sił Lądowych USA (*US Special Forces*, tzw. Zielone

[50] L. Nuti, *op.cit.*, s. 972; L. Risso, *Propaganda and Intelligence in the Cold War. The NATO Information Service*, London – New York 2014, s. 68.
[51] G. Arboit, *op.cit.*, s. 22.

Berety), powołanych w 1952 r. jako 10. Grupa Sił Specjalnych (10 SFGA). W listopadzie 1953 r. 10. SFGA przerzuciła część spośród 2300 komandosów do Republiki Federalnej Niemiec, zakładając w bawarskiej miejscowości Bad Tölz, w opuszczonych pomieszczeniach byłej SS-Junkerschule, tajną bazę i ośrodek szkoleniowy, będący w kolejnych dekadach miejscem kontaktów funkcjonariuszy sił specjalnych, przygotowywania planów wspólnych szkoleń oraz nieformalnych uzgodnień operacyjnych. Amerykańskie „Zielone Berety" wspomagane były przez brytyjskie siły specjalne SAS (*Special Air Service*), które następnie przejęły pełną odpowiedzialność za przygotowanie jednostek specjalnych i koordynację tajnych operacji w wybranych krajach Zachodu: Belgii, Holandii, Francji, Portugalii.

Kluczową rolę w organizowaniu tajnych operacji za pośrednictwem ACC odgrywała Centralna Agencja Wywiadowcza USA (CIA), zwłaszcza po objęciu w lutym 1953 r. stanowiska jej dyrektora przez Allena Dullesa. CIA miała zasadniczy udział w tworzeniu „tajnej armii NATO". W czerwcu 1948 r. Narodowa Rada Bezpieczeństwa Stanów Zjednoczonych wydała instrukcję nr NSC 10/2 upoważniającą Centralną Agencję Wywiadowczą do planowania i prowadzenia tajnych operacji skierowanych przeciwko wrogim organizacjom i państwom lub służących wspieraniu sojuszniczych rządów. „Tajne operacje" obejmowały takie działania, jak propaganda, wojna gospodarcza, bezpośrednie działania prewencyjne, działania wywrotowe we wrogich państwach, w tym pomoc dla podziemnego ruchu oporu, grup partyzanckich oraz oddziałów wyzwoleńczych na uchodźstwie a także wspieranie lokalnych antykomunistycznych ruchów w krajach zagrożonych ekspansją komunizmu. Instrukcja zakazywała prowadzenia przez CIA operacji w konfliktach zbrojnych, wojskowych działań wywiadowczych i kontrwywiadowczych, jak również działań pod przykryciem oraz dezinformacji dla celów operacji wojskowych[52]. Komórką CIA odpowiedzialną za planowanie i prowadzenie tajnych operacji było Biuro Projektów Specjalnych, przemianowane 28 października 1948 r. na Biuro Koordynacji Polityki (Office of Policy Coordination - OPC)[53]. Pierwszy

[52] *National Security Council Directive on Office of Special Projects NSC 10/2,Washington, June 18, 1948*, w: M. Warner (red.), *CIA Cold War Records: The CIA under Harry Truman*, Washington, D.C. 1994, s. 213-216. Por. W.J. Dougherty, *Executive Secrets: Covert Action and Presidency*, Lexington 2004, s. 122-24; T.K. Adams, *U.S. Special Operations Forces in Action: The Challenge of Unconventional Warfare*, London and Portland 1998, s. 44-45.

[53] J. Prados, *Presidents' Secret Wars: CIA and Pentagon Covert Operations from World War II through the Persian Gulf*, Chicago 1986, s. 32; G. Arboit, *op.cit.*, s. 15.

dyrektor OPC, porucznik Frank Wisner, był faktycznie organizatorem i „architektem" siatki służb specjalnych w ramach operacji *stay-behind*[54].

Istotną rolę w koordynowaniu, monitorowaniu i utrzymywaniu bieżącej współpracy tajnych służb odgrywało Biuro Bezpieczeństwa NATO, organ działający od chwili utworzenia struktury organizacyjnej Paktu, podporządkowany Sekretarzowi Generalnemu i pełniący wobec niego funkcje doradcze. Dyrektor Biura Bezpieczeństwa przewodniczył jednocześnie Komitetowi Bezpieczeństwa NATO, organowi odpowiedzialnemu za koordynację wspólnych działań w obliczu zagrożeń dla obszaru północnoatlantyckiego ze strony takich zjawisk, jak terroryzm, szpiegostwo, działalność wywrotowa i aktywność grup komunistycznych.

Ta robocza struktura tylko z pozoru była funkcjonalna i pozwalała na skuteczną realizację celów z zakresu bezpieczeństwa wewnętrznego. Podstawowym dylematem, odzwierciedlającym głębszy problem relacji transatlantyckich, a więc kontestowanie przez europejskich aliantów dominacji Stanów Zjednoczonych w Sojuszu, było wypracowanie kompromisowej formuły planowania i zarządzania tajnymi operacjami w sposób satysfakcjonujący zarówno USA, jak też europejskich członków NATO. Zdominowanie operacji *stay-behind* przez amerykańskie instytucje bezpieczeństwa: CIA, NSA i USAF (Siły Zbrojne Stanów Zjednoczonych) wywoływało niechęć ze strony niektórych państw. Dodatkową komplikacją był fakt, że w sieci jednostek specjalnych włączonych do operacji znajdowały się także te z państw nienależących do NATO: Szwajcarii, Austrii, Szwecji i Finlandii[55]. Dobrą ilustracją złożonych relacji między SHAPE a ACC było memorandum przedstawiciela USA w Komitecie Wojskowym NATO gen. Leona Johnsona ze stycznia 1957 r. w reakcji na wypowiedź głównodowodzącego sił NATO w Europie generała Laurisa Norstada na temat niewystarczającego wsparcia wywiadowczego dla SHAPE ze strony państw członkowskich. SACEUR, powołując się na statut (*charter*) Tajnego Komitetu Planowania (CPC)[56], wskazywał, że nie ma przeciwwskazań do wzmożonego przekazywania informacji wywiadowczych przez CPC w stanach nagłych. Jednak generał Johnson nie zgodził się z sugestią SACEUR i

[54] D. Ganser, *NATO's Secret Armies, op.cit.*, s. 55; R. Faligot, R. Kauffer, *op.cit.*, s. 462.
[55]Zob. L. Nuti, O. Riste, *Introduction – Strategy of 'Stay-Behind'*, „Journal of Strategic Studies", 2007, 30 (6), s. 933.
[56] Statut CPC nie został do tej pory odtajniony.

zanegował konieczność rozszerzenia kompetencji CPC w zakresie tajnych operacji wywiadowczych[57].

Problemy koordynacji tajnych grup roboczych oraz jednostek państw włączonych w tworzenie gotowości do prowadzenia operacji *stay-behind* uwidoczniły się na początku lat sześćdziesiątych. Współpraca w wykrywaniu i przeciwdziałaniu działań wywrotowych skupiała się na rozpoznaniu wywiadowczym i siłą rzeczy zeszła na poziom kontaktów dwustronnych, w których głównym interlokutorem pozostawała CIA. Niemniej po fiasku przygotowanego przez tę agencję desantu w Zatoce Świń w celu obalenia rządu Fidela Castro na Kubie w kwietniu 1961 r., na CIA spadła lawina krytyki, która skutkowała ograniczeniem środków na tajne operacje. Ówczesny dyrektor Centralnej Agencji Wywiadowczej Richard Helms ogłosił zakończenie tajnych działań w zachodniej Europie. Równocześnie w Naczelnym Dowództwie Sojuszniczych Sił w Europie (SHAPE) pojawiły się wątpliwości jeśli chodzi o zdolność adaptacji sieci *stay-behind* do nowych elementów doktrynalnych i operacyjnych, takich jak działania kontrinsurekcyjne czy operacje wojsk specjalnych. Koordynacja sieci skupiła się w trójstronnej grupie wykonawczej, zaś spotkania ACC i CPC odbywały się raz na dwa lata[58].

Ostatnie posiedzenie ACC, pod kierownictwem generała Raymonda van Calstera, szefa belgijskiej Generalnej Służby Wywiadowczej SGR (*Service General de Renseignement*), miało miejsce w Brukseli w dniach 23-24 października 1990 r.[59] Operacje s*tay-behind* dobiegły końca, Sojusz Północnoatlantycki przygotowywał się do sprostania nowym wyzwaniom na progu epoki pozimnowojennej.

Uwagi końcowe

Prowokacje, operacje terrorystyczne i tajne akcje podejmowane w państwach członkowskich Paktu przez siły specjalne włączone do operacji *stay-behind* osłabiły wpływy komunistycznej lewicy na Zachodzie, ale jednocześnie wzbudziły wiele wątpliwości co do legitymacji takich działań oraz rzeczywistych korzyści dla stabilizacji Sojuszu. Polityczne usankcjonowanie przemocy stosowanej w tajnych operacjach sił

[57] *Memorandum for the Joint Chiefs of Staffs on Clandestine Intelligence*, http://www.php.isn.ethz.ch/collections/colltopic.cfm?lng=en&id=20216&navinfo=15301 (dostęp: 14.05.2016).
[58] G. Arboit, *op.cit.*, s. 28.
[59] *Belgian Parliamentary Commission Enquiry into Gladio*, „Statewatch Bulletin", 1992, 2 (1), s. 2-3.

specjalnych NATO, kompromitujące wyczyny (akty terroru, antyrządowe konspiracje, propaganda antydemokratyczna) organizacji wciągniętych do współpracy ze służbami specjalnymi oraz kompletna nieprzejrzystość działań *stay-behind* stały w zasadniczej sprzeczności z proklamowanymi w preambule do Traktatu Waszyngtońskiego zasadami demokracji i praworządności.

Koniec zimnej wojny, rozwiązanie Układu Warszawskiego i ZSRR oraz rozpad bloku wschodniego odsunęły na daleki plan dywagacje dotyczące reperkusji działań typu *Stay-behind*. Jednak katalog zagrożeń „nowego typu" wprowadzony do koncepcji strategicznej NATO przyjętej w listopadzie 1991 r. w Rzymie uwydatniał konieczność wypracowania nowej formuły odpowiedzi na „miękkie" zagrożenia. Po 11 września 2001 r. zagrożenie terrorystyczne uruchomiło różnorodne formy działania zarówno na płaszczyźnie polityki wewnętrznej państw członkowskich, jak też w relacjach transatlantyckich i w strukturach sojuszu północnoatlantyckiego.

Streszczenie

Niniejszy artykuł ma na celu zbadanie strategicznych, politycznych i organizacyjnych uwarunkowań i form współdziałania służb wywiadowczych oraz sił specjalnych państw członkowskich NATO w obliczu zagrożeń bezpieczeństwa wewnętrznego wynikających z definiującej zimną wojnę ostrej konfrontacji między Wschodem a Zachodem. Lęk przed wzrostem wpływów komunistycznych i infiltracją lewicy przez agentów Moskwy skłonił Stany Zjednoczone i ich europejskich sojuszników do tworzenia sieci tajnych służb, włączonej na początku lat 50. do struktury instytucjonalnej Sojuszu Północnoatlantyckiego. Utworzenie tajnych komórek planowania i działań operacyjnych podległych Sojuszniczemu Dowództwu NATO w Europie służyło niedopuszczeniu do pojawienia się na Zachodzie sowieckiej „piątej kolumny" dostrzeganej w lewicowych ruchach i partiach politycznych.

Autor niniejszego tekstu wskazuje na instytucjonalne podejście do organizacji w ramach NATO służb odpowiedzialnych za wykrywanie i zwalczanie wewnętrznych zagrożeń dla strategicznych interesów bezpieczeństwa Sojuszu. Prezentując dwa studia przypadku, dotyczące organizacji pod egidą Stanów Zjednoczonych służb wywiadowczych w Niemczech i Włoszech, autor zwraca uwagę na ograniczenia współpracy i słabości instytucjonalnej koordynacji operacji *stay-behind* prowadzonych przez służby specjalne państw zachodniej Europy pod nadzorem NATO.

Słowa kluczowe: NATO • bezpieczeństwo europejskie • stay-behind • tajne operacje

Abstract

This article aims to explore the strategic, political and organizational determinants and forms of interaction between the intelligence services and the special services of NATO member states in the face of internal security threats resulting from the confrontation between the East and the West during the Cold War. The fear of the growing Communist influence and infiltration of the left by Soviet agents prompted the United States and its European allies to create a network of secret services incorporated in the early 1950s into the institutional structure of the North Atlantic alliance. The creation of secret planning and operational units subordinated to NATO's Allied Command Europe served to prevent the emergence of a "fifth column" in the West, epitomized by left-wing movements and political parties.

The author of this article points to the institutional approach to NATO services responsible for detecting and combating internal threats to the strategic security interests of the Alliance. By presenting two case studies concerning the creation under the aegis of the United States of intelligence service in Germany and Italy, the author draws attention to the limitations of cooperation and weaknesses of institutional coordination of stay-behind operations conducted by the secret services of Western European countries under NATO's supervision.

Keywords: NATO • European security • stay-behind • clandestine operations

Łukasz Dawid Dąbrowski

Antyterrorystyczne kompetencje służb państwowych odpowiedzialnych za obronność, bezpieczeństwo i porządek publiczny w obszarze świadczenia usług telekomunikacyjnych i internetowych

Uwagi wstępne

Polska nie należy obecnie do państw bezpośrednio zagrożonych działaniami terrorystycznymi[1], niemniej „żadne państwo nie może mieć jednak pewności co do własnego bezpieczeństwa"[2]. W zglobalizowanym świecie ataki terrorystyczne mogą przejawiać się w różnych formach, w tym przy wykorzystaniu łączności telekomunikacyjnej. Możliwość wykorzystywania sieci telekomunikacyjnych, a właściwie usług świadczonych za ich pośrednictwem, w tym usług internetowych, do różnych celów terrorystycznych jest nader oczywista[3]. Współcześnie dostrzega się konieczność zwalczania nie tylko przestępstw o charakterze terrorystycznym, ale także zapobiegania czynom „na przedpolu" terroryzmu, stwarzającym warunki dla prowadzenia działalności terrorystycznej oraz ułatwiającym realizację zamachów[4]. W związku z możliwością aktywności terrorystycznej służbom państwowym odpowiedzialnym za obronność, bezpieczeństwo i porządek publiczny przyznano szereg uprawnień w szczególności w zakresie dostępu do danych telekomunikacyjnych i danych internetowych.

W niniejszym artykule przez służby państwowe odpowiedzialne za obronność, bezpieczeństwo i porządek publiczny rozumie się: Policję[5], Straż Graniczną[6], Krajową

[1] Institute for Economics & Peace, *Global Terrorism Index 2016*, s. 95, http://visionofhumanity.org/app/uploads/2017/02/Global-Terrorism-Index-2016.pdf, (dostęp: 29.04.2017).
[2] D. Szwacz, *Zagrożenia terrorystyczne w Polsce – Oceny i przeciwdziałanie*, „THINK. Studenckie Naukowe Czasopismo Internetowe Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie", 2016, nr 1 (25), s. 16.
[3] Zob. B. Hoffman, *Oblicza terroryzmu*, Warszawa 2001, s. 171 i n.
[4] K. Wiak, *Kryminalizacja finansowania terroryzmu w polskim prawie karnym*, „Palestra", 2010, nr 7-8, s. 57-58.
[5] *Ustawa z dnia 6 kwietnia 1990 r. o Policji*, „Dziennik Ustaw" (dalej jako „Dz. U.") z 2016 r., poz. 1782, 1948 i 1955 oraz z 2017 r., poz. 60 i 244.
[6] *Ustawa z dnia 12 października 1990 r. o Straży Granicznej*, „Dz. U." z 2016 r., poz. 1643, 1948 i 1955 oraz z 2017 r., poz. 60 i 244.

Administrację Skarbową[7], Żandarmerię Wojskową i wojskowe organy porządkowe[8], Agencję Bezpieczeństwa Wewnętrznego oraz Agencję Wywiadu[9], Służbę Kontrwywiadu Wojskowego oraz Służbę Wywiadu Wojskowego[10], a także Centralne Biuro Antykorupcyjne[11].

Głównym celem artykułu jest przedstawienie zakresu czynności, jakie mogą być podejmowane przez te służby by zapobiegać i zwalczać działania terrorystyczne podejmowane przy wykorzystaniu usług telekomunikacyjnych. Ponieważ znaczna część z tych uprawnień ingeruje w prywatność obywateli (abonentów), konieczne stało się również syntetyczne ujęcie mechanizmów kontrolnych podejmowanych działań. Szeroki zakres kompetencji służb państwowych jest szczególnie widoczny w porównaniu z uprawnieniami sądów i prokuratur, którymi organy te dysponują na etapie postępowań sądowych. W porównaniu tym uwidoczniona zostaje również dysproporcja praw i gwarancji, jakimi dysponują osoby kontrolowane na etapie postępowania operacyjnego, a którymi dysponują na etapie postępowania sądowego.

Główną metodą zastosowaną w opracowaniu jest metoda dogmatyczna. Przedmiotem analizy prawniczej są postanowienia ustaw kompetencyjnych służb państwowych odpowiedzialnych za obronność, bezpieczeństwo i porządek publiczny, a także niektóre uregulowania prawne zawarte w ustawie z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (k.p.k)[12] oraz w ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych[13]. Przedstawienie podobieństw kompetencji przyznanych poszczególnym służbom, a także różnic w zakresie dysproporcji praw i gwarancji, jakimi dysponują osoby kontrolowane na etapie postępowania operacyjnego i sądowego umożliwia metoda prawnoporównawcza. Przedstawienie uprawnień służb państwowych dokonane na przykładzie ustawy o Policji, ma również mutatis mutandis zastosowanie w

[7] *Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej*, „Dz. U." z 2016 r., poz. 1947 i 2255 oraz z 2017 r., poz. 88 i 244.
[8] *Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych*, „Dz. U." z 2016 r., poz. 1483 i 1948 oraz z 2017 r., poz. 244.
[9] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, „Dz. U." z 2016 r., poz. 1897, 1948 i 1955 oraz z 2017 r., poz. 60.
[10] *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*, „Dz. U." z 2014 r., poz. 253, z późn. zm.
[11] *Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym*, „Dz. U." z 2016 r., poz. 1310, 1948, 1955 i 2255 oraz z 2017 r., poz. 60 i 244.
[12] *Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego*, „Dz. U." z 1997 r., nr 89 poz. 555, ze zm.
[13] *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*, „Dz. U." z 2016 r., poz. 904, ze zm.

przypadku pozostałych podmiotów uprawnionych. Do określenia zakresu danych telekomunikacyjnych i internetowych, do których mają dostęp uprawnione służby, konieczne było przedstawienie uregulowań zawartych w ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[14] (dalej: Pt.) oraz w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[15].

Dane telekomunikacyjne

Na podstawie uregulowań ustaw kompetencyjnych poszczególnych służb państwowych możliwe jest przeprowadzanie niejawnej kontroli operacyjnej, która polega m.in. na „uzyskiwaniu i utrwalaniu treści rozmów i korespondencji, w tym prowadzonej za pomocą środków komunikacji elektronicznej"[16], a także „uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych"[17].

W zakresie działalności telekomunikacyjnej uprawnione podmioty mają więc możliwość dostępu i utrwalania przekazów telekomunikacyjnych nadawanych lub odbieranych przez abonentów, a także przez telekomunikacyjne urządzenie końcowe, co oznacza uprawnienie do kontroli korespondencji telekomunikacyjnej. Kontrola korespondencji dotyczy nie tylko informacji z rozmów telefonicznych prowadzonych w sieci ruchomej lub stacjonarnej, ale także innych przesyłanych informacji: SMS lub innego rodzaju tekstów, faksów, obrazów, filmów, a także informacji zawartej w poczcie głosowej i poczcie elektronicznej[18]. Wszystkie te informacje są bowiem przesyłane za

[14] *Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne*, „Dz. U." z 2004 r., nr 171, poz. 1088 ze zm.
[15] *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną,* „Dz. U." z 2013 r., poz. 1422 oraz z 2015 r., poz. 1844.
[16] Art. 19 ust. 6 pkt 1 i 3 ustawy o Policji, art. 9 e ust. 7 pkt 1 i 3 ustawy o Straży Granicznej, art. 118 ust. 4 pkt 1 i 3 ustawy o Krajowej Administracji Skarbowej, art. 31 ust. 7 pkt 1 i 3 ustawy o Żandarmerii Wojskowej, art. 27 ust. 6 pkt 1 i 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego, art. 17 ust. 5 pkt 1 i 3 ustawy o Centralnym Biurze Antykorupcyjnym, art. 31 ust 4 pkt 1 i 3 ustawy o Służbie Kontrwywiadu Wojskowego.
[17] Art. 19 ust. 6 pkt 4 ustawy o Policji, art. 9 e ust. 7 pkt 4 ustawy o Straży Granicznej, art. 118 ust. 4 pkt 4 ustawy o Krajowej Administracji Skarbowej, art. 31 ust. 7 pkt 4 ustawy o Żandarmerii Wojskowej, art. 27 ust. 6 pkt 4 ustawy o Agencji Bezpieczeństwa Wewnętrznego, art. 17 ust. 5 pkt 4 ustawy o Centralnym Biurze Antykorupcyjnym, art. 31 ust 4 pkt 4 ustawy o Służbie Kontrwywiadu Wojskowego.
[18] Usługa poczty elektronicznej nie jest usługą telekomunikacyjną. Jej zasadniczym elementem są: udostępnienie indywidualnego konta pocztowego, zapewnienie możliwości odbierania poczty elektronicznej kierowanej na konto pocztowe, wysyłania poczty elektronicznej z konta pocztowego oraz przechowywania poczty elektronicznej, natomiast usługa przekazywania poczty elektronicznej jest usługą

pomocą sieci telekomunikacyjnej[19]. W oparciu o istniejące uregulowania możliwy jest również „podsłuch elektroniczny przy użyciu tzw. pluskiew, zminiaturyzowanych aparatów podsłuchowych. Dotyczy to więc nie tylko podsłuchu telefonicznego, lecz także każdej innej formy kontroli rozmów, także tych prowadzonych poza siecią telekomunikacyjną"[20]. Możliwy jest również „*podsłuch* transmisji w sieciach komputerowych za pomocą specjalnego oprogramowania"[21]. Dotyczy to więc wszelkich rozmów „bez względu na to jak i gdzie są prowadzone (w domu, w parku, na ulicy, w biurze itd.)"[22]. W ramach tych uregulowań dopuszczalne jest przejmowanie danych komputerowych za pomocą transmisji teleinformatycznych czy analizy fal elektromagnetycznych oraz fal akustycznych emitowanych przez drukarki[23].

Kontrolując treść korespondencji telekomunikacyjnej podmioty uprawnione mają również dostęp do tak zwanych danych towarzyszących, czyli informacji związanych z przekazami telekomunikacyjnymi oraz związane ze świadczoną usługą telekomunikacyjną[24] i danymi osobowymi[25], a także danych o próbach uzyskania połączenia między zakończeniami sieci, w tym danych o nieudanych próbach połączeń[26].

Określone w ustawie o Policji i pozostałych ustawach resortowych uprawnienie do uzyskiwania i utrwalania treści rozmów prowadzonych za pomocą komunikacji elektronicznej to tak zwany podsłuch operacyjny, który należy odróżnić od podsłuchu procesowego przewidzianego w uregulowaniach k.p.k. Podsłuch procesowy można

telekomunikacyjną. (Uzasadnienie ustawy o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw wraz z projektami aktów wykonawczych. Sejm RP VI kadencji – druk nr 1448 z 30 października 2008 r., s. 40-41).

[19] B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Policji. Komentarz*, Warszawa 2015, s 105.

[20] Por. B. Hołyst, *Podsłuchiwanie i inwigilacja użytkowników mediów elektronicznych w kontekście bezpieczeństwa informacyjnego*, „Prokuratura i Prawo", 2015, nr 3, s. 5-31.

[21] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, Warszawa 2010, s. 58.

[22] T. Grzegorczyk, *Kodeks postępowania karnego. Komentarz*, Warszawa 2005, s. 601.

[23] A. Sakowicz, *Kodeks postępowania karnego. Komentarz*, Warszawa 2016, s. 585. Zob. też: *Rozporządzenie Ministra Sprawiedliwości z 24.6.2003 r. w sprawie sposobu technicznego przygotowania sieci służących do przekazywania informacji, do kontroli przekazów informacji oraz sposobu dokonywania, rejestracji, przechowywania, odtwarzania i niszczenia zapisów z kontrolowanych przekazów*, „Dz. U." z 2003 r., nr 110, poz. 1052).

[24] Dane transmisyjne oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne. Dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej lub w ramach usług telekomunikacyjnych wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych. (Art. 159 ust. 1 pkt 3 i 4 Pt.).

[25] Dotyczące w szczególności: nazwisk i imion, imion rodziców, miejsca i daty urodzenia, adresu miejsca zamieszkania i/lub adresu korespondencyjnego, numeru ewidencyjnego PESEL, nazwy, serii i numeru dokumentów potwierdzających tożsamość. (Art. 161 ust. 2 Pt.).

[26] Art 159. ust. 1 pkt 5 Pt.

stosować po formalnym wszczęciu postępowania przygotowawczego, podsłuch operacyjny może mieć miejsce w każdym czasie[27].

Kontrola i utrwalanie treści rozmów telefonicznych prowadzone na podstawie k.p.k. na rzecz sądu i prokuratury są dopuszczalne tylko wtedy, gdy toczące się postępowanie lub uzasadniona obawa popełnienia nowego przestępstwa dotyczy jedynie najpoważniejszych przestępstw. Podsłuch procesowy, zgodnie z art. 237 § 4 k.p.k., dopuszczalny jest w stosunku do „osoby podejrzanej, oskarżonego oraz pokrzywdzonego lub innej osoby, z którą może się kontaktować oskarżony albo która może mieć związek ze sprawcą lub z grożącym przestępstwem". Uregulowania art. 239 § 1 k.p.k. dopuszczają odroczenie „ogłoszenia postanowienia o kontroli i utrwalaniu rozmów telefonicznych osobie, której ono dotyczy, na czas niezbędny ze względu na dobro sprawy". Z tym, że ogłoszenie takiego postanowienia „wpostępowaniu przygotowawczym może być odroczone nie później niż do czasu zakończenia tego postępowania" (art. 239 § 2 k.p.k.). Osobie, której dotyczy postanowienie „o kontroli i utrwalaniu rozmów telefonicznych przysługuje zażalenie, w którym może domagać się zbadania zasadności oraz legalności kontroli i utrwalania rozmów telefonicznych" (art. 240 k.p.k.)[28].

Z kolei zgodę na stosowanie podsłuchu operacyjnego na podstawie ustawy o Policji wydaje sąd okręgowy właściwy miejscowo ze względu na siedzibę składającego wniosek organu Policji. Ponieważ kontrola operacyjna prowadzona jest niejawnie, podsłuchiwana osoba może nigdy nie dowiedzieć się o stosowanym wobec niej środku. Nie przewidziano również żadnego środka zaskarżenia lub kontroli właściwości zastosowanego podsłuchu. W tym kontekście szczególne rozwiązanie wprowadzono na mocy art. 9 ustawy antyterrorystycznej, zgodnie z którym cudzoziemiec podejrzany o działalność terrorystyczną może być podsłuchiwany bez zgody sądu i prokuratury[29]. Uregulowanie ustawy wyposaża szefa ABW w możliwość działania „poza kontrolą, w tym poza kontrolą następczą sądu"[30]. Zauważyć należy, że na mocy art. 57 § 2 ustawy z dnia

[27] Por. P. Kosmaty, *Przechwytywanie przekazów telekomunikacyjnych w świetle Konwencji o pomocy prawnej w sprawach karnych pomiędzy Państwami Członkowskimi Unii Europejskiej*, „Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego", 2011, vol. IX, s. 138.
[28] Zażalenie na postanowienie prokuratora rozpoznaje sąd (art. 240 k.p.k. *in fine).*
[29] M. Górka, *Wolność czy bezpieczeństwo? Przyczynek do rozważań na przykładzie ustawy o działaniach antyterrorystycznych z dnia 10 czerwca 2016 roku*, „e-Politikon", 2016, nr XIX, s. 64.
[30] P. K. Marszałek, *Polskie ustawodawstwo antyterrorystyczne a prawa człowieka*, „Studia Lubuskie", 2016, Tom XII, s. 139.

28 stycznia 2016 r. Prawo o prokuraturze[31] podmioty określone w ustawie[32] upoważnione zostały do kontroli czynności operacyjno-rozpoznawczych prowadzonych przez służby państwowe. Kontrola ta „jest sprawowana w szczególności przez badanie faktycznych podstaw tych czynności oraz ich legalności, prawidłowości i efektywności"[33]. Nadzoru tego nie może jednak traktować jako instrumentu alternatywnego dla weryfikacji dokonywanej przez sąd, którego rolą powinna być „ocena materiałów przedstawionych przez służby pod kątem absolutnej konieczności zastosowania środków specjalnych wkraczających w obszar praw i wolności obywatelskich"[34]. Niemniej jednak rola prokuratora wydaje się znacząca, jako organu odpowiedzialnego za zgodne z prawem podejmowanie działań operacyjnych[35]. Dodatkowo w przypadku kontroli operacyjnej na organach ją stosujących nie ciąży obowiązek informacyjny, co często prowadzić może do sytuacji, w której osoba, wobec której stosowany jest taki środek nie wie, że „nastąpiła ingerencja w jej podstawowe i gwarantowane konstytucyjnie prawa"[36].

Kolejnym uprawnieniem o skutku odwrotnym do kontroli korespondencji telekomunikacyjnej jest możliwość stosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze. Policja[37], Straż Graniczna[38], Żandarmeria Wojskowa[39], Agencja Bezpieczeństwa Wewnętrznego[40], Służba Kontrwywiadu Wojskowego[41] oraz Biuro Ochrony Rządu[42] uprawnione zostały do blokowania nadawania, odbioru lub transmisji informacji niezależnie od ich rodzaju[43]. Zastosowanie urządzeń blokujących jest dopuszczalne w razie zagrożenia bezpieczeństwa publicznego

[31] *Ustawa z dnia 28 stycznia 2016 r. - Prawo o prokuraturze*, „Dz. U." z 2016 r., poz. 177, 1579, 2103, 2149 i 2261 oraz z 2017 r., poz. 38.
[32] Prokurator Generalny, Prokurator Krajowy lub upoważniony przez nich prokurator.
[33] Zob. § 2 *Rozporządzenia Ministra Sprawiedliwości w sprawie sposobu realizacji czynności prokuratora w ramach kontroli nad czynnościami operacyjno-rozpoznawczymi z dnia 13 lutego 2017 r.*, „Dz. U." z 2017 r., poz. 292.
[34] T. Kuć, *Analiza funkcjonalności systemu kontroli i nadzoru nad służbami specjalnymi w Polsce*, „Przegląd Bezpieczeństwa Wewnętrznego", 2017, nr 16 (9), s. 208.
[35] E. Gruza, M. A. Kędzierski, *Zakres kompetencji organów policyjnych uprawnionych do wnioskowania okontrolę operacyjną*, „Przegląd Bezpieczeństwa Wewnętrznego", 2016, nr 14 (8), s. 39.
[36] M. Tomkiewicz, *Stosowanie kontroli operacyjnej w toku postępowania karnego*, „Rocznik Nauk Prawnych", 2016, nr 4, s. 132.
[37] Art. 18c ust. 1 ustawy o Policji.
[38] Art. 10e ust. 1 ustawy o Straży Granicznej.
[39] Art. 30a ust. 1 ustawy o Żandarmerii Wojskowej.
[40] Art. 26a ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego.
[41] Art. 29a ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego
[42] Art. 7a ust. 1 ustawy z dnia 16 marca 2001 r. o Biurze Ochrony Rządu, „Dz. U." z 2016 r., poz. 552, 904, 960, 1250.
[43] S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2013, s. 1049.

lub zakłócenia porządku publicznego, w szczególności w trakcie zgromadzeń lub imprez masowych o różnym charakterze (kulturalnym, sportowym lub religijnym). Zastosowanie takich urządzeń uniemożliwia komunikację na całym terytorium, w którego zasięgu znajduje się dane urządzenie blokujące. Podobną możliwość działania przewiduje Pt., które w art. 180 ust. 1, nakłada na przedsiębiorców telekomunikacyjnych obowiązek blokowania połączeń lub przekazów informacji na żądanie uprawnionych podmiotów lub umożliwienia tym podmiotom dokonania samodzielnej blokady. Zakres czynności blokujących obejmuje wszelkie przekazy telekomunikacyjne, w tym „usługi przekazywania krótkich wiadomości tekstowych lub multimedialnych oraz przekazy informacji, co oznacza, że możliwe jest zablokowanie wszelkich informacji przekazywanych w sieci telekomunikacyjnej"[44]. W odróżnieniu od stosowania urządzeń zakłócających, blokada na podstawie Pt. dotyczy określonych numerów lub użytkowników, a nawet poszczególnych usług, z których korzysta dany abonent. Uniemożliwia więc wymianę informacji pomiędzy określonymi osobami lub urządzeniami, lub poprzez blokadę określonej usługi (na przykład transmisji danych) może wymusić skorzystanie z innej (na przykład połączenia głosowego).

Kolejne uprawnienie służb państwowych jest również korelatem obowiązków ciążących na przedsiębiorcach telekomunikacyjnych, na których nałożono obowiązek przechowywania i udostępniania danych (retencji danych[45]) telekomunikacyjnych. W ramach tego obowiązku[46] podmiotom uprawnionym przyznano prawo dostępu do gromadzonych przez przedsiębiorców danych. Prawo to przysługuje również sądom i prokuraturze uprawnionym do uzyskiwania wykazu połączeń telekomunikacyjnych czyli tak zwanych bilingów (art. 218 k.p.k.). W ramach retencji danych podmioty uprawnione, w tym sądy i prokuratura, nie mają dostępu do treści rozmów telefonicznych. Po pierwsze, kwestie podsłuchu telefonicznego regulują inne przepisy (art. 237 k.p.k., art. 179 Pt. i na przykład art. 19 ustawy o Policji), a po drugie w ramach retencji danych nie

[44] *Ibidem*.
[45] Retencja danych dotyczy danych niezbędnych do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie, do którego kierowane jest połączenie; Dodatkowo określenia: daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia, lokalizacji telekomunikacyjnego urządzenia końcowego. Obowiązek retencji danych nie dotyczy treści przekazu telekomunikacyjnego.
[46] Szerzej M. Rogalski, *The period of retention of telecommunications data which must be disclosed at the request of the court or the prosecutor in connection with pending criminal proceedings*, "Ius Novum", 2014, nr 2, s. 95-105.

dochodzi do rejestracji i przechowywania treści korespondencji telekomunikacyjnej.

Uregulowanie art. 218 k.p.k. nie wskazuje podmiotów, których bilingi podlegają kontroli. W pierwszej kolejności dotyczyć to będzie podejrzanego (oskarżonego) oraz niekiedy również pokrzywdzonego. Dopuszczalna staje się kontrola każdej osoby, która ma lub może mieć związek z przestępstwem lub jego sprawcą. W konsekwencji „kontrola może dotyczyć osób, które nie mają nic wspólnego z przestępstwem, a tylko kontaktują się ze sprawcą, ale w przedmiocie i zakresie, który nie ma żadnego związku z przestępstwem"[47]. O dokonanej kontroli informuje się abonenta telefonu lub nadawcę, którego wykaz połączeń lub innych przekazów informacji został wydany. „Odroczenie dokonania takiej informacji może nastąpić jedynie w uzasadnionych przypadkach"[48]. Na marginesie zaznaczyć należy, że w postępowaniu cywilnym brak analogicznych uregulowań, co oznacza, że dowód z wykazu połączeń telefonicznych może zostać przeprowadzony tylko wtedy, gdy strona uprawniona do otrzymania takiego dokumentu od operatora przedłoży go sądowi[49].

Służbom państwowym przyznano także pewne uprawnienia odnoszące się do infrastruktury telekomunikacyjnej. Ustawa o działaniach antyterrorystycznych przewiduje uprawnienie do żądania od przedsiębiorców telekomunikacyjnych montażu „tymczasowych instalacji radiokomunikacyjnych, w szczególności stacji bazowych ruchomej sieci telekomunikacyjnej"[50]. Uregulowanie to ma na celu „zapewnienie łączności, w szczególności z numerami alarmowymi, w związku z wydarzeniami, głównie imprezami masowymi lub zgromadzeniami, podczas których może wystąpić zdarzenie o charakterze terrorystycznym albo zagrożenie bezpieczeństwa i porządku publicznego"[51]. Obowiązek ten jest realizowany na „żądanie ministra właściwego do spraw informatyzacji lub organu odpowiedzialnego za bezpieczeństwo i porządek publiczny"[52].

[47] M. Rogalski, *Udostępnianie danych telekomunikacyjnych sądom i prokuraturom*, „Prokuratura i Prawo", 2015, nr 12, s. 59-73.
[48] Zob. M. Czerwińska, P. Czarnecki, *Katalog dowodów w postępowaniu karnym*, Warszawa 2014.
[49] A. Marciniak, K. Piasecki (red.), *Kodeks postępowania cywilnego. Tom I. Komentarz. Art. 1–366*, Warszawa 2016, komentarz do art. 308 k.p.c.
[50] Art. 13 ust. 1 ustawy o działaniach antyterrorystycznych.
[51] *Ibidem*.
[52] M. Piotrak, *Rola i zadania szefa Agencji Bezpieczeństwa Wewnętrznego w zarządzaniu kryzysowym i ochronie infrastruktury krytycznej*, „Przegląd Bezpieczeństwa Wewnętrznego", 2016, nr 8 (15), s. 78.

Dane internetowe

Pojęcie „danych internetowych" wprowadzone zostało w ustawie z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw[53]. Przez dane internetowe rozumie się dane wymienione w art. 18 ust. 1–5 ustawy o świadczeniu usług drogą elektroniczną. Policja[54] oraz inne podmioty uprawnione[55] upoważnione zostały do dostępu do tych danych, które można podzielić na trzy grupy: 1) internetowe, 2) eksploatacyjne oraz 3) inne dane. Do danych internetowych zalicza się nazwisko i imiona usługobiorcy, numer ewidencyjny PESEL lub numer dokumentu potwierdzającego tożsamość, adres zameldowania na pobyt stały, adres do korespondencji, dane służące do weryfikacji podpisu elektronicznego usługobiorcy, adresy elektroniczne usługobiorcy[56]. Z kolei dane eksploatacyjne określono w ustawie jako „oznaczenia identyfikujące usługobiorcę, oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca, informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną, informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną"[57]. Inne dane to dane określone w art. 18 ust. 2 ustawy jako "dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia" oraz określone w art. 18 ust. 4 ustawy jako „inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną".

Dane te w pewnym zakresie pokrywają się z danymi telekomunikacyjnymi. Dotyczy to w szczególności danych dotyczących użytkownika i danych eksploatacyjnych w zakresie rozpoczęcia i zakończenia korzystania z usługi. W pozostałym jednak zakresie wykraczają znacznie poza dotychczasowe uregulowania, posługując się dodatkowo zwrotami niedookreślonymi pozwalającymi na szeroką interpretację ich postanowień. Tworzą jednocześnie katalog otwarty danych internetowych. Ustawa w art. 18 ust. 2 i 4 posługuje się klauzulą prowadzącą w konsekwencji do rozszerzającej interpretacji

[53] *Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw*, „Dz. U." z 2016 r., poz. 147.
[54] Art. 20c ust. 1 pkt 3 ustawy o Policji.
[55] Art. 106 ust. 1 ustawy o Straży Granicznej, art. 114 ust. 1 pkt 3 ustawy o Krajowej Administracji Skarbowej, art. 30 ust. 1 pkt 3 ustawy o Żandarmerii Wojskowej, art. 28 ust. 1 pkt 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego, art. 18 ust. 1 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym, art. 32 ust. 1 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego.
[56] Art 18 ust. 1 ustawy o świadczeniu usług drogą elektroniczną.
[57] Art. 18 ust. 5 ustawy o świadczeniu usług drogą elektroniczną.

katalogu danych internetowych. Prowadzić to może „m.in. do przyjęcia, że dane takie to także informacje o aktywności użytkownika w Internecie czyli odwiedzanych przez niego stronach internetowych, o aktywności na forach dyskusyjnych lub portalach społecznościowych”[58].

Wchodzące w skład danych eksploatacyjnych informacje o rozpoczęciu, zakończeniu i zakresie świadczonej usługi mogą być uzyskiwane w konsekwencji dostępu do danych o ruchu w sieci telekomunikacyjnej, a więc danych o „połączeniach pomiędzy urządzeniami komputerowymi, ich adresy IP, daty i czas trwania połączenia, rodzaj połączeń. Uzyskiwanie takich informacji wiąże się z możliwością uzyskania informacji o skorzystaniu przez usługobiorcę z usługi świadczonej drogą elektroniczną. W tzw. logach systemowych serwerów zapisywane są dane o ruchu, adresy przeglądanych stron internetowych, zapisy wysyłanych wiadomości SMS czy poczty elektronicznej. Informacji o odwiedzanych stronach i korzystaniu z usług dostarczają również pliki *cookies*”[59]. Tak „szeroki zakres informacji będzie pozwalał na szerokie i precyzyjne odtworzenie różnych aspektów życia prywatnego znajdujących odzwierciedlenie m.in.: w rodzajach odwiedzanych stron internetowych oraz przekazywanych informacjach w ramach korzystania z usług świadczonych drogą elektroniczną”[60], w tym „informacji związanych z intymną sferą życia danej osoby (np. zdjęć i danych o preferencjach seksualnych)”[61].

Z punktu widzenia aktywności internetowej, istotne znaczenie ma uprawnienie do tak zwanej blokady dostępności stron internetowych. Możliwość stosowania blokady wprowadzono do ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (art. 32c) na mocy ustawy o działaniach antyterrorystycznych. Blokowanie możliwe jest na mocy postanowienia Sądu Okręgowego w Warszawie. Zgodnie z uzasadnieniem projektu ustawy rozwiązanie to ma zapobiegać, przeciwdziałać i pomagać w wykrywaniu przestępstw o charakterze terrorystycznym. Organizacje terrorystyczne

[58] *Opinia Biura Studia i Analiz Sądu Najwyższego w sprawie poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw*, s. 8, http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=154 (dostęp: 27.04.2017).

[59] K. Klafkowska-Waśniowska, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, w: D. Lubasz, M. Namysłowska (red.), *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, Warszawa 2011, s. 215.

[60] *Uwagi Helsińskiej Fundacji Praw Człowieka do poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy nr 154)*, s. 8, http://www.hfhr.pl/wp-content/uploads/2015/12/HFPC_opinia_ustawa_o_policji_30122015.pdf , (dostęp: 27.04.2017).

[61] M. Domagała, *Prawnokarna ochrona prywatności użytkowników Internetu*, „Państwo i Prawo”, 2010, nr 3, s. 75-86.

„wykorzystują bowiem Internet do promowania swojej ideologii, zamieszczania instruktarzu w zakresie sposobu przeprowadzania zamachów terrorystycznych oraz komunikowania się ze swoimi zwolennikami”[62].

Kolejne uprawnienie przyznane służbom państwowym jest pośrednio związane z aktywnością telekomunikacyjną i internetową. Dotyczy bowiem możliwości uzyskiwania i utrwalania danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych. Uprawnienie to stanowi rodzaj niejawnego przeszukania, które dotychczas odbywało się na podstawie art 236a k.p.k., to jest wymagało zachowania odpowiednich gwarancji procesowych osobie poddanej tego typu czynnościom. Aktualne uregulowania prawne powodują, „że osoba, której przeszukano w ten sposób np. komputer, może się o tym nigdy nie dowiedzieć”[63]. Tymczasem obowiązki informacyjne odgrywają szczególną rolę w procesie kontrolnym podejmowanych przez służby państwowe działań. Kontrolę nad uzyskiwanymi przez te organy danymi telekomunikacyjnymi i internetowymi powierzono sądom okręgowym właściwym dla siedziby organu danej służby państwowej, któremu udostępniono te dane. Odmiennie jednak od kontroli, jaka przewidziana jest w przypadku kontroli treści przekazów telekomunikacyjnych (podsłuch), kontrola danych telekomunikacyjnych i internetowych jest kontrolą następczą. Kontrola następcza polega na przekazywaniu przez dany organ w okresach półrocznych sprawozdania obejmującego „liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych lub internetowych oraz rodzaj tych danych i kwalifikacje prawne czynów, w związku z którymi wystąpiono o dane telekomunikacyjne lub internetowe, albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych”[64]. W ramach prowadzenia kontroli sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie organom tych danych.

Jak wynika z powyższych uregulowań w kontroli następczej sąd ma jedynie

---

[62] *Uzasadnienie do Rządowego projektu ustawy o działaniach antyterrorystycznych oraz o zmianie niektórych innych ustaw, Druk nr 516*, s. 41, http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=516 (dostęp: 27.04.2017).

[63] *Uwagi Helsińskiej Fundacji Praw Człowieka*..., *op. cit.*, s. 10.

[64] Art. 20ca ust. 2 ustawy o Policji, art. 10ba ust. 2 ustawy o Straży Granicznej, art. 116 ust. 2 ustawy o Krajowej Administracji Skarbowej, art. 28a ust. 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 30b ust. 1 ustawy o Żandarmerii Wojskowej, art. 18a ust. 2 ustawy o Centralnym Biurze Antykorupcyjnym, art. 32a ust. 2 ustawy o Służbie Kontrwywiadu Wojskowego.

możliwość oceny złożonego przez daną służbę sprawozdania. Nie bada więc treści zgromadzonych danych, a w konsekwencji czy uzyskanie tych danych było niezbędne. Przyjęte rozwiązanie kontrolne nie spełnia więc wymogów wynikających z wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., w którym wskazano wymóg wprowadzenia niezależnej kontroli każdego przypadku uzyskiwania danych telekomunikacyjnych poprzez niezwłoczną ocenę zasadności ich uzyskania. Co prawda Trybunał dostrzega możliwość stosowania kontroli uprzedniej, między innymi gdy „chodzić może o dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma konieczności pilnego działania służb”[65]. Jednak obecny model kontroli nie jest wystarczający. Na uwagę zasługuje stanowisko Generalnego Inspektora Ochrony Danych Osobowych, zgodnie z którym „kontrola następcza powinna być traktowana jako wyjątek i stosowana jedynie w sprawach niecierpiących zwłoki. W każdym przypadku niezależny organ powinien ocenić czy pozyskanie danych jest w konkretnej sytuacji rzeczywiście niezbędne i należycie uzasadnione oraz czy cel, w którym dane są udostępniane nie mógłby zostać zrealizowany przy użyciu innych, mniej ingerujących w prywatność jednostki środków”[66].

Następczej kontroli sądowej nie podlegają jednak wszystkie dane uzyskiwane w celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego, bądź wsparcia działań poszukiwawczych lub ratowniczych. W związku z tymi czynnościami organy uprawnione mogą bowiem uzyskiwać dane z elektronicznego wykazu abonentów (art. 179 ust. 9 Pt.), dane osobowe abonentów (art. 161 Pt.), a „w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika”[67]. Dodatkowo, „w przypadku stacjonarnej publicznej sieci telekomunikacyjnej” dane te obejmują również informacje o „nazwie miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi”[68]. Do

[65] Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. akt K 23/11, s. 177.
[66] *Opinia Generalnego Inspektora Ochrony Danych Osobowych z dnia 30 grudnia 2015 r. do projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk nr 154)*, s. 4, http://www.giodo.gov.pl/1520254/id_art/8994/j/pl/, (dostęp: 29.04.2017).
[67] Art. 20cb ust. 1 pkt 3 ustawy o Policji, art. 10bb ust. 1 pkt 3 ustawy o Krajowej Administracji Skarbowej, art. 30c ust. 1 pkt 3 ustawy o Żandarmerii Wojskowej, art. 28b ust. 1 pkt 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego, art. 18b ust. 1 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym, art. 32b ust. 1 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego.
[68] Art. 20cb ust. 1 pkt 4 ustawy o Policji, art. 10bb ust. 1 pkt 4 ustawy o Krajowej Administracji Skarbowej, art. 30c ust. 1 pkt 4 ustawy o Żandarmerii Wojskowej, art. 28b ust. 1 pkt 4 ustawy o Agencji

przetwarzania tych danych nie jest wymagana zgoda osoby której dotyczą, brak również konieczności informowania o fakcie ich przetwarzania. Dodatkowo systematyka ustawy o Policji wskazuje, że kontroli tej nie podlegają również dane telekomunikacyjne i internetowe uzyskane w celu poszukiwania osób zaginionych[69].

Uwagi końcowe

Do kompetencji przyznanych służbom państwowym w zakresie zapobiegania i zwalczania działań terrorystycznych w obszarze telekomunikacji zalicza się w szczególności: dostęp i możliwość utrwalania przekazów telekomunikacyjnych i danych towarzyszących, blokowanie ruchu telekomunikacyjnego, dostęp do przechowywanych przez przedsiębiorców telekomunikacyjnych danych objętych obowiązkiem retencji, a także nakładanie na nich obowiązku stawiania tymczasowych instalacji radiokomunikacyjnych oraz dostęp do informacji o aktywności w Internecie. Dane telekomunikacyjne i internetowe można uzyskiwać przede wszystkim „w celu zapobiegania lub wykrywania przestępstw, ale również w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych"[70]. Wszystkie powyższe dane mogą być przetwarzane bez wiedzy i zgody osoby, której dotyczą. Ustawa o działaniach antyterrorystycznych[71], zawiera wykaz czynności zbieżnych z zakresem czynności operacyjnych stosowanych przez podmioty uprawnione na mocy ustaw kompetencyjnych. Główna różnica polega na tym, że środki stosowane w oparciu o ustawę antyterrorystyczną mogą być nałożone przez Szefa ABW jedynie wobec osoby niebędącej obywatelem polskim[72].

Celem podejmowanych przez podmioty uprawnione działań jest głównie kontrola korespondencji (podsłuch), dążenie do ujawnienia treści wiadomości lub uzyskanie wiedzy o samym ruchu informacji, a więc monitorowanie ruchu telekomunikacyjnego[73].

Bezpieczeństwa Wewnętrznego, art. 18b ust. 1 pkt 4 ustawy o Centralnym Biurze Antykorupcyjnym, art. 32b ust. 1 pkt 4 ustawy o Służbie Kontrwywiadu Wojskowego.

[69] *Opinia Biura Studia i Analiz Sądu Najwyższego w sprawie poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw*, s. 6, http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=154, (dostęp: 29.04.2017).

[70] Art. 20c ust. 1 ustawy o Policji.

[71] „Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych", *Dz. U.* z 2016 r., poz. 904, ze zm.

[72] Art. 9 ust. 1 ustawy o działaniach antyterrorystycznych.

[73] Por. J. A. Krasucki, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2015, s. 1389.

Dostęp do danych internetowych znacznie wykracza poza ogólnie pojęty monitoring lub kontrolę korespondencji, umożliwiając dogłębną ingerencją w prywatność osoby kontrolowanej. Przyjęte rozwiązania z pewnością mogą przyczynić się do przeciwdziałania i zwalczania szerokiego wachlarza przestępczości, w tym przestępczości terrorystycznej. Prowadzą jednak do poważnych ograniczeń w zakresie korzystania przez jednostkę z praw i wolności konstytucyjnych, w szczególności z prawa do prywatności, tajemnicy korespondencji oraz zasady autonomii informacyjnej[74].

Dodatkowo ustawa o Policji, a co za tym idzie także pozostałe ustawy kompetencyjne, nie wprowadzają „mechanizmów mających na celu zagwarantowanie osobie, wobec której zastosowano środki kontroli operacyjnej, możliwości zakwestionowania chociażby ex post ich legalności na drodze sądowej"[75]. Nie przewidziano też zewnętrznej kontroli następczej[76]. Dodatkowo, przyjęte założenie „wykonywania obowiązków sprawozdawczych, z zachowaniem wymogów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, uniemożliwia osobom zainteresowanym dostępu do informacji czy doszło do ingerencji w ich konstytucyjne prawa i wolności, co prowadzi do pozbawienie danej osoby skutecznej ochrony podstawowych praw i wolności konstytucyjnych"[77]. Na konieczność informowania osób objętych kontrolą operacyjną wskazywano wielokrotnie w orzeczeniach Trybunału Konstytucyjnego[78]. Obowiązek informacyjny ma szczególne znaczenie zwłaszcza w odniesieniu do danych internetowych. Prawo jednostki do poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji z pewnością nie ma charakteru absolutnego[79]. Niemniej jednak, charakter materii, z jaką wiąże się stosowanie podsłuchu telefonicznego lub możliwość dostępu do informacji dotyczących aktywności w

[74] Zob. A. Karwowski, *Prawo do prywatności a uprawnienia służb specjalnych do wykonywania czynności operacyjnych*, w: J. Jaskiernia (red.), *Europejski system ochrony praw człowieka. Aksjologia-instytucje-efektywność*, Toruń 2015, s. 489 i n.

[75] *Opinia Naczelnej Rady Adwokackiej do poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy nr 154)*, s. 5, http://www.adwokatura.pl/z-zycia-nra/opinia-nra-do-projektu-nowelizacji-ustawy-o-policji/ , (dostęp: 29.04.2017).

[76] J. Podkowik, *Niezależna kontrola udostępniania danych telekomunikacyjnych*, „Przegląd Legislacyjny", 2015, nr 2 (92), s. 26.

[77] *Stanowisko Ośrodka Badań Studiów i Legislacji Krajowej Rady Radców Prawnych z dnia 30 grudnia 2015 r. dotyczące poselskiego projektu ustawy o zmianie ustawy o policji oraz niektórych innych ustaw (druk nr 154)*, s. 5-6, http://bibliotekakirp.pl/items/show/514, (dostęp: 29.04.2017).

[78] Wyrok z dnia 12 grudnia 2005 r., sygn akt K 32/04, w postanowieniu sygnalizacyjnym z dnia 25 stycznia 2006 r., sygn akt S 2/06, a także w wyroku z dnia 30 lipca 2014 r., sygn akt K 23/11.

[79] W. Jasiński, *Dowodowe czynności wykrywcze a ingerencja w prawo do prywatności - standardy strasburskie*, „Europejski Przegląd Sądowy", 2015, nr 1, s. 17-25.

Internecie, zobowiązuje do niezwykłej ostrożności i rygorystycznego przestrzegania określonych przez ustawę granic ich legalności[80]. Jednakże to, czy służby uprawnione nie nadużywają przysługujących im uprawnień w wielu przypadkach nie będzie podlegało kontroli, ani sądowej ocenie działań aparatu państwa.

Streszczenie

W związku z możliwą aktywnością terrorystyczną poprzez wykorzystanie łączności telekomunikacyjnej, służbom państwowym odpowiedzialnym za obronność, bezpieczeństwo i porządek publiczny przyznano szereg uprawnień, w szczególności w zakresie dostępu do danych telekomunikacyjnych i danych internetowych. Celem podejmowanych przez służby państwowe działań jest głównie kontrola korespondencji (podsłuch), dążenie do ujawnienia treści wiadomości lub uzyskanie wiedzy o samym ruchu informacji, a więc monitorowanie ruchu telekomunikacyjnego, ale także dostęp do danych internetowych. Przyjęte rozwiązania z pewnością mogą przyczynić się do przeciwdziałania i zwalczania przestępczości terrorystycznej. Prowadzą jednak do poważnych ograniczeń w zakresie korzystania przez jednostkę z praw i wolności konstytucyjnych. Wobec powyższego po środki te powinno się sięgać niezwykle ostrożnie i rygorystycznie przestrzegać określonych przez ustawę granic ich legalności.

Słowa kluczowe: dane telekomunikacyjne • dane internetowe • kontrola korespondencji • podsłuch • podmioty uprawnione

Summary

Considering the potential use of telecommunications services by terrorists, state security services have been granted with a number of rights regarding access to telecommunications and internet data. The main objective of these units is to control communications (wiretapping), reveal the content of the messages or gain knowledge of the traffic information, monitoring telecommunications traffic, but also access to Internet data. The solutions can certainly contribute to the prevention and fight against terrorist crime. However, at the same time these measures could violate constitutional rights and freedoms. Therefore, should be applied extremely carefully and should adhere strictly to the law regulations.

Keywords: telecommunication data • Internet data • control communications • wiretapping • authorized entities

[80] Por. P. Hofmański, *Kodeks postępowania karnego. Komentarz do art. 1 - 296*, Tom I, Warszawa 2011, s. 1285.

Piotr Bajor

A strategic challenge - The influence of historical policy on the current shape of the Polish-Ukrainian relations

Historical issues have been one of the most important elements influencing the relations between Poland and Ukraine after the collapse of the Soviet Union. Over the course of many years, the governments of both countries have been highlighting the necessity of implementing the process of reconciliation and many statements have been made in this regard. The latest events in the Polish-Ukrainian relations have indicated, however, that historical issues are still essential for mutual understanding and, as a consequence, the relations between Poland and Ukraine have significantly worsened. Therefore, in this article some key documents that became the reason of tensions in bilateral relations will be analyzed.

In the course of time, the Polish-Ukrainian relations have been defined in terms of strategic partnership. The governments of both countries kept stressing how special the relations between Poland and Ukraine werefor a constructive cooperation in bilateral relations, as well as at a widerinternationallevel. Within the next couple of years many documents have been adopted which related to the tragic pages of history of their relations and have been directed toward mutual reconciliation[1].

Based on the analysis of the current processes undergoing in the Polish–Ukrainian relationship, one can put forward a hypothesis that reconciliation advocated in the mentioned documents addressed mainly political elites and authorities, and has not led to any broader changes in the Polish and Ukrainian societies. What is more, the historical policy of Ukraine due to the actions taken by the Ukrainian Institute of National Remembrance (UINR) after the "Revolution of Dignity" has raised concerns about its

[1] Such matters have been recently analyzed by many researchers and experts, and the results of the research are presented in such publications as: T. Horbowski, P. Kosiewski (eds.),*Pamięć i pytania o tożsamość. Polska-Ukraina*, Warszawa 2013; T. A. Olszański, *Miejsce UPA w wielkiej wojnie ojczyźnianej. Dylematy polityki historycznej Ukrainy*, Punkt Widzenia OSW, Nr 35, Warszawa, June 2013; J. Konieczna-Sałamatin, *Polacy i Ukraińcy – wzajemne postrzeganie w trudnych czasach*, in T. Horbowski, P. Kosiewski (eds.), *Polityka bezpieczeństwa. Polska-Ukraina*, Warszawa 2015.

approach toward the nationalist groups, part of which – from the Polish perspective – are perceived as responsible for the Volhynian massacre.

Resolutions of the Polish Parliament on genocide

In the aftermath of controversial Ukraine's actions, a vigorous debate opened in Poland regarding the commemoration of innocent victims killed by Ukrainian nationalists. Some politicians from rulling party insisted that the Volhynian tragedy should be considered as genocide against the Polish nation[2]. The attempts to include such wording in a resolution on the Volhynian case had been made in the Polish Parliament before the "Revolution of Dignity" began in Kiev. In 2013, such a proposal was submitted by some deputies to the Sejm (the lower chamber) as well as by senators (members of the upper house). However, the resolution that was eventually adopted at that time included the following wording – "ethnic cleansing with the characteristic of genocide"[3]. In 2016, following the victory of the Law and Justice party in the parliamentary elections in October 2015, a significant change occurred in the approach of the parliamentary majority and the government, which got strongly committed to include the term "genocide" as appropriate for the classification of the Volhynian tragedy.

On July 7, 2016, the Senate of the Republic of Poland adopted a resolution on "paying tribute to the victims of genocide committed by Ukrainian nationalists on the citizens of the Republic of Poland in 1939-1945". In the first part of the document senators made reference to the tragic historical events. They pointed to the 73rd anniversary of the culmination of the crime waves that were committed against the Polish citizens by the Organization of Ukrainian Nationalists, Ukrainian Insurgent Army, and SS Galizien division. It was emphasized that as a result of this act of genocide during the Second World War more than one hundred thousand Poles, Jews, Armenians, Czechs,

[2] *Michał Dworczyk o ludobójstwie na Wołyniu: "Dobre relacje z Ukrainą mogą być budowane tylko w oparciu o prawdę"*, https://wpolityce.pl/polityka/281440-michal-dworczyk-o-ludobojstwie-na-wolyniu-dobre-relacje-z-ukraina-moga-byc-budowane-tylko-w-oparciu-o-prawde; *PiS do Ukraińców: nie upamiętniamy ludzi, którzy mają na rękach krew niewinnych*, http://www.tvn24.pl/wiadomosci-z-kraju,3/list-politykow-pis-do-ukraincow-w-zwiazku-z-73-rocznica-wolynia,654243.html (accessed on 12 October 2016).

[3] *Sejm zdecydował. Rzeź wołyńska "czystką etniczną o znamionach ludobójstwa". 10 posłów PO złamało dyscyplinę*, http://www.rp.pl/artykul/1028773-Sejm-zdecydowal--Rzez-wolynska--czystka-etniczna-o-znamionach-ludobojstwa---10-poslow-PO-zlamalo-dyscypline.html (accessed on 12 October 2016).

and members of other national minorities died. Senators highlighted that an accurate number of victims is still unknown to this day[4].

The Senate also stressed that amongst the victims there was also a lot of Ukrainians who had been helping the Poles. Therefore, senators expressed their "respect and appreciation" to them for showing such support while risking their own lives. They also called upon the President of the Republic of Poland to award those people. The Senate also showed its highest appreciation to the self-protective formations that made their attempts to defend the victims[5].

Further in the document, the Polish Senate paid tribute to all Polish citizens who were "viciously murdered by the Ukrainian nationalists". It was added that the victims to this day were not properly commemorated and many of them were not given a chance for a decent burial. It was also highlighted that the massacres were not properly classified since according to the historical truth they constituted genocide. Therefore, the Senate called upon the Sejm to name July 11th the "National Day of Remembrance of Victims of Genocide committed against the Polish citizens by Ukrainian nationalists". Senators showed their respect also for East Borderland communities as well as all those who over decades "have been demanding the truth about a genocide and care about the remembrance of the victims"[6].

The matter of commemorating the victims of the Volhynian conflict in the first half of 2016 was also put on the Sejm's agenda. On July 22, 2016, deputies adopted a resolution with the same title as that adopted by senators. Both acts partially corresponded each other. The Sejm also indicated that, as a result of genocide committed by Ukrainian nationalists in 1939-1945, more than one hundred thousand people were murdered, although an exact number of victims is still unknown to this day. Similarly to the Senate, Sejm emphasized that such structures as the Organization of Ukrainian Nationalists, Ukrainian Insurgent Army, SS Galizien division, as well as other formations collaborating with the Nazis were responsible for this tragedy. Both acts are also very similar in their parts relating to the lack of commemoration of the victims and a decent

[4] *Uchwała Senatu Rzeczypospolitej Polskiej z dnia 7 lipca 2016 r. w sprawie oddania hołdu ofiarom ludobójstwa dokonanego przez nacjonalistów ukraińskich na obywatelach II Rzeczypospolitej w latach 1939–1945*, "Monitor Polski", http://www.monitorpolski.gov.pl/MP/2016/638/1 (accessed on 12 October 2016).
[5] *Ibidem*.
[6] *Ibidem*.

burial, lack of recognition of self-protective formations, no respect for the Ukrainian people helping the victims and the need of honoring them with national awards, as well as lack of acknowledgment for all those people who have for years been demanding to expose the truth about those tragic events[7].

The Sejm's resolution included additional elements that were not mentioned in the document adopted by the Senate. Deputies highlighted that the former voivodships of the Republic of Poland were strongly affected during wartime as two biggest totalitarianisms of the 20th century met their match on their territories. It was pointed out that the steps taken by both occupants created some favorable conditions to awaken ethnic and religious hatred. It also was emphasized that the initiatives taken by the Polish Underground State in order to reach an agreement with the Ukrainian organizations did not bring about any satisfactory results. Moreover, it was stressed that the facts concerning the retaliatory actions taken by the Polish side, during which civilian population living in the Ukrainian villages faced death, should not be omitted[8].

The Sejm also agreed with the recommendation proposed by senators and decided to designate July 11th the National Day of Remembrance of Victims of Genocide committed by Ukrainian nationalists against the citizens of Poland. The Sejm also insisted to establish a crime scene, create a full list of victims, and provide a decent burial. The Polish MPs at the same time called for the continuation of reconciliation and dialogue with Ukraine at the political and religious levels. The Sejm also exhorted the historians from both countries to develop further cooperation, increasing the access to the source materials in the national archives as well as to strengthen cooperation between the governments of the Republic of Poland and Ukraine in the "most important matters for both countries' future relationship". It also was highlighted that only historical truth could pave the way to reconciliation and mutual forgiveness[9].

[7] *Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 22 lipca 2016 r. w sprawie oddania hołdu ofiarom ludobójstwa dokonanego przez nacjonalistów ukraińskich na obywatelach II Rzeczypospolitej Polskiej w latach 1943–1945*, "Monitor Polski", http://www.monitorpolski.gov.pl/MP/2016/726/1 (accessed on 12 October 2016).
[8] *Ibidem*.
[9] *Ibidem*.

Joint Declaration of the President of the Republic of Poland and the President of Ukraine

The above described resolutions adopted by the Polish parliament caused a sharp criticism and vehement reactions in Ukraine. In the follow-up comments, it was emphasized that the Polish MPs politicized the matter of reconciliation, showed a one-sided opinion and the Ukrainian side should react to these actions of the Polish Sejm and Senate. It is worth mentioning in the context of such vehement discussions a very significant visit that Polish president Andrzej Duda paid in Kiev on the occasion of the 25th anniversary of Ukraine's independence. During Duda's meeting with his Ukrainian counterpart, both leaders emphasized the need of continuing historical dialogue at the level of historians and research institutions, as well as taking the representatives of civil society into wider consideration in this process[10].

During the visit, the presidents of Poland and Ukraine signed a special declaration that included the analysis of the existing shape of the Polish-Ukrainian relations as well as priorities for the future. The document also referred to the symbolic fact that Poland had been the first state in the world that officially acknowledged Ukraine's independence in 1991. Also, some remarkable achievements of the past 25 years in the Polish-Ukrainian relations were mentioned. It was declared that a further development of the strategic relationship between both countries is an "historical no-alternative choice". It also was emphasized that the deepening of collaboration between Poland and Ukraine has good prospects, a significant potential, and lies in the deepest interest of both countries and their nations[11].

Resolution of the Supreme Council of Ukraine

It should be emphasized that the purpose of Duda's visit in Kiev was also to reduce the tension in the Polish-Ukrainian relations. In the following weeks a lively discussion

[10] *Andrzej Duda w Kijowie z okazji 25. rocznicy niepodległości Ukrainy*, http://www.prezydent.pl/aktualnosci/wizyty-zagraniczne/art,101,prezydent-na-uroczystosciach-z-okazji-25-rocznicy-uchwalenia-aktu-niepodleglosci-ukrainy.html (accessed on 12 October 2016).
[11] *Wspólna deklaracja Prezydenta RP i Prezydenta Ukrainy*, http://www.prezydent.pl/aktualnosci/wizyty-zagraniczne/art,102,spotkanie-prezydenta-rp-i-prezydenta-ukrainy.html (accessed on 12 October 2016).

ensued in Ukraine on a possible response from the Supreme Council of Ukraine to the documents adopted by the Polish Parliament. A proposal of the respective resolution was eventually submitted on September 8, 2016 by deputies of several parties, as part of political consensus regarding this matter[12].

The draft of the resolution was a subject of deliberations of the parliamentary Committee on International Affairs. It was stressed, as a justification, that in July 2016 the Polish Sejm and Senate adopted two documents on commemoration of the victims of genocide that was committed by Ukrainian nationalists. Further, in the draft document itsadvocates analyzed some specific wordings of the Polish resolutions referring to the Ukrainian side being responsible for the Volhynian tragedy. It was highlighted that the resolutions could negatively influence the Polish-Ukrainian relations. At the same time, the Ukrainian MPs indicated that the Supreme Council, as an important forum of bilateral cooperation, should take up its position in regard to those documents. It was indicated, therefore, that the aim of adopting the proposed resolution would be to express Ukraine's opinion in this matter. Moreover, the Polish parliamentarians were called upon to restrain from further politicization of the tragic chapters of the shared history[13].

After the discussion, the Committee on International Affairs suggested the Supreme Council to adopt the proposed document. In the Committee's position, it was indicated that the Supreme Council's reaction is necessary since the resolutions of the Polish parliament contain a distorted, legally and politically incorrect opinion of the tragic Polish-Ukrainian history. An opinion was expressed that the actions taken by the Polish deputies and senators squandered the political and diplomatic work of both countries, directed toward mutual reconciliation and understanding[14].

Before the voting on the resolution, a vehement discussion took place in the Ukrainian parliament. Deputies criticized the documents adopted by the Polish

[12] The draft to the parliament was submitted by the following MPs: Iho rHryniv (Petro Poroshenko Bloc), Maksym Burbak (People's Front), Oleh Bereziuk (Self Reliance), Yulia Tymoshenko (Batkivshchyna), Oksana Syroid (Self Reliance), Borys Tarasiuk (Batkivshchyna), Ivan Krulko (Batkivshchyna), Iryna Podolyak (Self Reliance), Oleh Liashko (Oleh Liashko Radical Party). See: *Проект Постанови про Заяву Верховної Ради України "У зв'язку з ухваленням Сенатом і Сеймом Республіки Польща постанов від 7 липня 2016 року та 22 липня 2016 року що до Волинської трагедії"*, http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=59978 (accessed on 12 October 2016).
[13] *Висновок комітету*, http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=59978 (accessed on 12 October 2016).
[14] *Ibidem*.

parliamentarians and underlined the necessity to adequately respond to it[15]. Eventually, 247 deputies from different parliamentary fractions, as well as non-attached MPs, voted in favor of adopting the resolution. A detailed list of the distribution of votes amongst the respective parliamentary fractions is presented below.

Table 1. Fractions voting in the Supreme Council in regard to responding to the act of the Polish parliament

Name of the fraction/group	In favor	Against	Abstention	Non-voting	Not present
Petro Poroshenko Bloc	99	0	2	22	20
People's Front	61	0	0	13	6
Non-attached	25	0	2	6	13
Opposition Bloc	0	0	0	29	14
Self-Reliance	23	0	0	0	3
Revival Party	1	0	0	5	17
Batkivshchyna	15	0	0	0	6
Oleh Lyashko Radical Party	19	0	0	0	2
People's Will	4	0	0	9	6

Source: *Поіменне голосування про проект Постанови про Заяву Верховної Ради України "У зв'язку з ухваленням Сенатом і Сеймом Республіки Польща постанов від 7 липня 2016 року та 22 липня 2016 року що до Волинської трагедії" (№5095 в редакції Комітету) - заосновута в цілому*", http://w1.c1.rada.gov.ua/pls/radan_gs09/ns_golos?g_id=8479 (accessed on 12 October 2016).

In the first part of the adopted document the Supreme Council indicated that it reacted to the documents of both houses of the Polish parliament with regret as well as deep disappointment. It was stressed that the political and legal analysis of the tragic events of the shared history included in those resolutions was incorrect. The Ukrainian

[15] *Стенограма пленарного засідання 08 вересня 2016. Засідання п'яте. Сесійний зал Верховної Ради України*, http://rada.gov.ua/meeting/stenogr/show/6293.html (accessed on 12 October 2016).

parliament highlighted the fact that both countries share the same examples of the joint struggle for freedom, as well as conflicts which caused much bloodshed. The deputies emphasized that commemoration of all victims should be respected appropriately on the territories of both countries. The Supreme Council also stressed that in the past years much effort was made on both sides for reconciliation and commemoration of those Polish and Ukrainian people who were innocently killed during World War II. The deputies also added that this commemoration was expressed in several documents adopted by both countries, intended for mutual forgiveness and reconciliation[16].

Therefore, it was stated that the Sejm's decision to declare July 11th the "day of remembrance of victims of genocide that was committed by Ukrainian nationalists against the citizens of Poland" should be considered as politicization of the tragic events of a common history. It was also added that the decision made by the Polish parliament was accompanied by chauvinistic rhetoric and anti-Ukrainian actions related to destruction of Ukrainian memorials, attacks against participants of religious ceremonies, as well as the ban on some cultural events[17].

The Supreme Council of Ukraine declared that the acts of the Sejm and Senate undermine political and diplomatic efforts of both countries and nations directed toward mutual forgiveness, understanding and honoring the innocent victims. Therefore, the Ukrainian parliament condemned the biased resolutions of the Sejm and Senate, directed to undermine positive results of cooperation that had been achieved as part of the constructive dialogue of both countries. The Supreme Council concluded that one-sided political opinions on the historical events can bring about a huge risk of creating conflicts between Poland and Ukraine and also may breed further radicalization of both societies. In this regard, the Supreme Council of Ukraine stated that the grounds for reconciliation and compromise between two nations can only be established by the mutual recognition of historical facts. It was highlighted that personal responsibility needs to be attributed for war crimes and crimes against humanity[18].

The Ukrainian parliament also urged historians of both countries to pursue a true dialogue aimed to explain all unknown facts and historical circumstances based on

[16] *Заява Верховної Ради України "У зв'язку з ухваленням Сенатом і Сеймом Республіки Польща постанов від 7 липня 2016 рокута 22 липня 2016 року що до Волинської трагедії"*, http://iportal.rada.gov.ua/news/Novyny/134295.html (accessed on 12 October 2016).
[17] *Ibidem*.
[18] *Ibidem*.

reliable archival materials. The Ukrainian deputies also indicated that it is necessary to have a possibility of interpretation of historical events by both sides. They pointed out that the politicians of both countries should restrain from instrumentalizing history and using it to gain some temporary political advantages.

In the final part of the document, the Ukrainian parliamentarians made an appeal to both nations and Polish politicians to continue the strategic Polish-Ukrainian partnership and avoid exposing it to the manipulations of sensitive historical issues by different political powers. They also called upon Polish politicians to stop politicizing the tragic chapters of the shared history and focus on the building of constructive relations in order to "strengthen the partnership in democratic Europe based on European values"[19].

Declaration of memory and solidarity by the Sejm of the Republic of Poland and the Supreme Council of Ukraine

The act of the Supreme Council was the next element that exacerbated the discussion on historical issues in the Polish-Ukrainian relations. Another factor that had an influence on its shape was the Polish movie „Volhynia" directed by Wojciech Smarzowski and released in the Polish theaters in October 2016. Some Ukrainian politicians and commentators described it as a partial story showing only those episodes of the difficult chapters in shared history which were convenient for Poland[20]. At the same time, diplomatic talks were held with the purpose of breaking a standoff and tension in bilateral relations. They ended with an agreement that a respective document relating to historical issues would be adopted by both parliaments. Therefore, on October 20, 2016, the Sejm of Poland and the Supreme Council of Ukraine adopted a joint „Declaration of Remembrance and Solidarity"[21].

---

[19] *Ibidem*.

[20] See: P. Lang, *Co Ukraińcy piszą o "Wołyniu"?*, http://jagiellonski24.pl/2016/10/14/co-ukraincy-pisza-o-wolyniu/ (accessed on 12 October 2016).

[21] P. Bajor, *Deklaracja Pamięci i Solidarności,* Komentarz Zakładu Bezpieczeństwa Narodowego UJ, nr 9 (18) 2016, http://www.zbn.inp.uj.edu.pl/komentarze?p_p_id=56_INSTANCE_lXg4&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&groupId=92718966&articleId=134744737 (accessed on 26 October 2016).

The document consists of two parts. The first one relates to historical matters, the second one to political aspects. A reference to the tragic historical events during World War II was made in the declaration. Both parliaments deplored the aggressors and stressed how weakly the international community reacted at that time tothe escalation of totalitarian attitudes and practices as well as chauvinistic postures before World War II which had led to the outbreak of war and, as a consequence, to occupation in the whole region of Eastern and Central Europe[22].

It was also indicated in the document that it is necessary to intensify objective studies conducted by the historians and start a „sincere and friendly" cooperation between the experts and the researchers. It was also highlighted that it is crucial to restrain some forces whose activity is harmful and provoke mutual conflicts in Poland and Ukraine[23].

Concluding remarks

The joint parliamentary declaration was the last element in the historical discussion between Poland and Ukraine in 2016. It can be considered as a sign of political will on both sides to break the stalemate which lasted for long in relation to tragic episodes of history of both countries. The adoption of the resolution contributed to the loosening of tensions in the Polish-Ukrainian relations. To verify the research hypothesis formulated in the beginning of this article, it must be said that the tragic episodes of history are still one of the most important factors influencing the Polish–Ukrainian relations and the ongoing process of reconciliation is still far from making it real. Therefore, within the next couple of years, both governments should take further actions directed to tighten bilateralrelations and follow the course of strategic cooperation which is mutually beneficial for both countries.

[22] *Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 20 października 2016 r. Deklaracja Pamięci i Solidarności Sejmu Rzeczypospolitej Polskiej oraz Rady Najwyższej Ukrainy*, http://orka.sejm.gov.pl/proc8.nsf/uchwaly/946_u.htm (accessed on 21 October 2016).
[23] *Ibidem*.

Streszczenie

W prezentowanym artykule omówione zostały najważniejsze kwestie historyczne, które w ostatniej perspektywie miały wpływ na uwarunkowania i kształt stosunków polsko-ukraińskich. Przedstawiona została analiza uchwał parlamentów Polski i Ukrainy oraz wspólnego dokumentu przyjętego przez obie izby oraz ich wpływ na bieżące relacje pomiędzy Polską a Ukrainą.

Słowa kluczowe: stosunki polsko-ukraińskie • partnerstwo strategiczne • polityka historyczna • pojednanie

Summary

In this article the most important historical issues which have influenced the developments and the shape of the Polish-Ukrainian relations have been discussed. Also, the analysis of the resolutions of the Polish and Ukrainian parliaments has been offered, as well as a joint document adopted by both houses has been examined as to its content and the way it hasinfluenced the current relations between Poland and Ukraine.

Keywords: Polish-Ukrainian relations • strategic partnerhip • historical policy • reconciliation

Autorzy

Piotr Bajor - doktor nauk humanistycznych, adiunkt w Zakładzie Bezpieczeństwa Narodowego Instytutu Nauk Politycznych i Stosunków Międzynarodowych Uniwersytetu Jagiellońskiego; publicysta w branżowych pismach specjalistycznych.

Łukasz Dawid Dąbrowski – doktor nauk prawnych, wykładowca Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, adwokat, członek Komisji Legislacyjnej Naczelnej Rady Adwokackiej, autor publikacji z zakresu międzynarodowego prawa karnego, międzynarodowej ochrony praw człowieka i prawa telekomunikacyjnego.

Artur Gruszczak – doktor habilitowany nauk społecznych, profesor nadzwyczajny Uniwersytetu Jagiellońskiego, kierownik Zakładu Bezpieczeństwa Narodowego Instytutu Nauk Politycznych i Stosunków Międzynarodowych Uniwersytetu Jagiellońskiego, autor monografii i artykułów dotyczących bezpieczeństwa europejskiego, współpracy wywiadowczej i policyjnej w Unii Europejskiej.

Marcin Szymański – magister bezpieczeństwa narodowego, asystent w Zakładzie Bezpieczeństwa Narodowego Instytutu Nauk Politycznych i Stosunków Międzynarodowych Uniwersytetu Jagiellońskiego; oficer Wojsk Specjalnych. Zainteresowania naukowe obejmują: przemoc w stosunkach międzynarodowych; inżynieria społeczna i jej zastosowania w procesie osiągania celów strategicznych; Comprehensive Approach: strategie reagowania kryzysowego Sojuszu Północnoatlantyckiego.

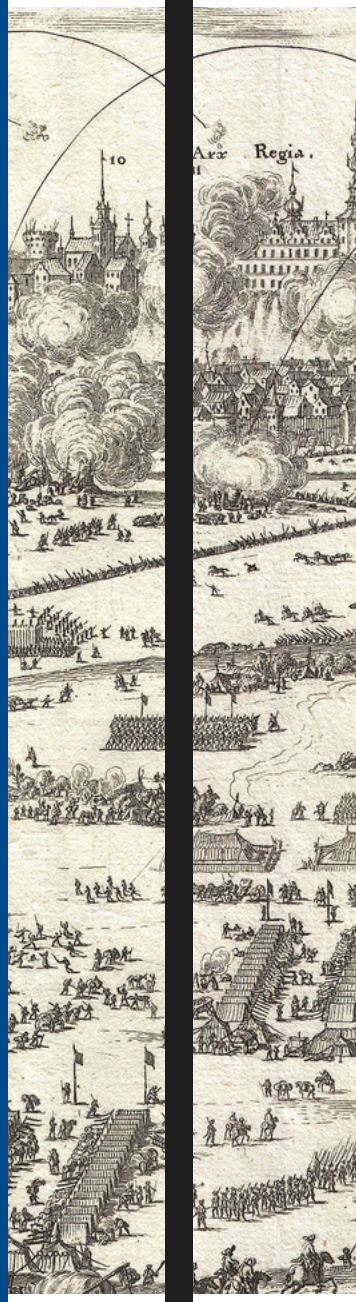
Authors

Piotr Bajor – PhD in Political Science, Assistant Professor at the Faculty of International and Political Studies, Jagiellonian University in Kraków. He is also an journalist and columnist for various magazines in Poland.

Łukasz Dawid Dąbrowski – PhD in Law, Lecturer at the Cardinal Stefan Wyszyński University in Warsaw, attorney-at-law, member of the Legislative Council of the Polish Bar Council, author of publications in the field of international criminal law, international human rights law and telecommunication law.

Artur Gruszczak – PhD in Political Science, Associate Professor at the Faculty of International and Political Studies, Jagiellonian University in Kraków, Chair of National Security. He has written extensively on European security, intelligence and police cooperation in the European Union.

Marcin Szymański – MA in National Security, Assistant Professor at the Faculty of International and Political Studies, Jagiellonian University in Kraków; senior officer in the Polish Special Operations Command. His interests and research include such topics as: violence in international relations; social engineering; comprehensive approach to contemporary crises, including NATO's crisis response.



#JPB

www.przeglad.uj.edu.pl
jpb@uj.edu.pl