JAROSŁAW ŁUKASZ KEPLIN

https://doi.org/10.4467/20801335PBW.23.029.18771
https://orcid.org/0000-0003-1865-2261

Building state resilience against hybrid activities

Abstract

Ensuring security in an increasingly complex and uncertain world requires states to address a number of challenges. These include the need to remain cooperative in the international space and the need to pursue their strategic objectives. Often these are followed up by intentional or unintentional threats that can effectively destabilise not only a single state, but also an entire region. Their emergence may be the result of a lack of resilience against hostile actions by state or non-state actors who, in order to achieve their objectives, undertake, among other things, hybrid activities. However, the terms 'state resilience' and 'hybrid activities' are insufficiently precisely formulated in the literature and described in a conceptual rather than a definitional manner. Both national and NATO documents lack universally accepted definitions of these terms. The aim of this article is to present the concept of building state resilience to hybrid activities.

Keywords

hybrid activities, hybrid threats, hybrid warfare, state security, state resilience.

The world in the 21st century is perceived by the international community mainly through the phenomenon of globalisation, shaped by three fundamental processes - tightening international ties, reducing the influence of states on the economy and technological progress[1]. This makes governments and their societies perceive new opportunities related, inter alia, to the free movement of goods and services as well as labour and the development of new technologies. On the one hand, these processes undoubtedly contribute to the economic growth of countries and the expansion of competitiveness between them. On the other hand, globalisation has negative effects, causing e.g. disparities in the level of wealth of societies, a reduction in the role of nation states with an increase in the importance of supranational institutions.

One effect of globalisation is that the nature of threats is changing - they are increasingly taking unusual forms - new forms of terrorism or terror or cyber attacks. Others are less overt in nature and are aimed at exerting pressure, including economic or social pressure, using, among other things, manipulated media as a *proxy*[2]. Through them, attempts are made to influence the economic situation of countries or the mood of society, which can lead to the undermining of such fundamental values as respect for human dignity, freedom and democracy.

Until now, the norms of international law have been created by state governments. Today, specialised non-governmental organisations and experts appointed by international bodies are actively involved. In specific situations, where states fail to comply with the norms of international law, these organisations can introduce sanctions. They thus attempt to influence the political and economic situation of a country and force it to comply with legal norms. In practice, this involves pressure from the commissioning authority concerning the interpretation of the norms, which is beyond its competence. International organisations can therefore influence the actions of states, and the interests of these organisations can be indicated as a higher necessity[3]. In doing so, it should be emphasised that

[1] D.J. Mierzejewski, *Bezpieczeństwo europejskie w warunkach przemian globalizacyjnych* (Eng. European security under the impact of globalisation), Toruń 2011, pp. 23–24.

[2] The term *proxy* refers to an intermediary who pursues an objective on behalf of the actual aggressor or exerts pressure on a designated entity. This allows the initiator of the action to remain anonymous.

[3] An example of an organisation that can significantly influence the behaviour of states is the European Union. The Council, together with the European Parliament and the Commission, can issue regulations and directives which, for the Member States, also become part of national law. As regards complaints and breaches of norms by states, judgements are made by the Court of Justice of the European Union. To a limited extent, the UN Security Council has the right to influence the actions of states. See in more detail: J. Ciechański, *Enklawy transnarodowe w zdecentralizowanym prawie międzynarodowym* (Eng. Transnational enclaves in decentralised international law), in: *Stosunki międzynarodowe. Geneza, struktura, dynamika*, E. Haliżak, R. Kuźniar (eds.), Warszawa 2006, pp. 346–348.

international institutions are - in addition to states - those actors that seek to stabilise and normalise the international situation[4].

Globalisation and the increasing interdependence between different actors in international law often result in unpredictable phenomena, the extent of which is not limited by geographical barriers, political and economic systems. The pressures of globalisation mean that, in the modern world, states are unable to function economically on their own, and their interdependence can give rise to crises or conflicts. Some scholars, including Kenichi Ohmae, view globalisation through the lens of nation states that have partially lost control of their territory, leading to their loss of sovereignty and weakened state structures. Susan Strange, on the other hand, argues that the process of deterritorialisation is an integral part of globalisation, leading to the 'end' of states on the political maps of the world. It demonstrates the erosion of the nation-state's core of authority over its territorial structures[5]. In contrast, David Kilcullen argues that modern nation states are powerful but less flexible - slower to adapt to change than their non-state adversaries[6].

The threats posed by globalisation are creating a new security environment, and the existing conditions and forms of pursuing strategic objectives by state[7] and non-state actors[8] are being transformed. The most relevant non-state actors include non-governmental organisations, transnational corporations with dispersed anonymous ownership, i.e. non-state elements operating in space - global, trans-state

---

[4] I. Popiuk-Rysińska, *Instytucje międzynarodowe* (Eng. International institutions), in: *Stosunki międzynarodowe. Geneza, struktura, dynamika*, E. Haliżak, R. Kuźniar (eds.), Warszawa 2006, p. 353.

[5] See in more detail: Ch. Fjäder, *The nation-state, national security and resilience in the age of globalisation*, "Resilience: International Policies, Practices and Discourses" 2014, vol. 2, no. 2, pp. 114–129. https://doi.org/10.1080/21693293.2014.914771.

[6] D. Kilcullen, *The Accidental Guerrilla*: *Fighting Small Wars in the Midst of Big One*, New York 2009, p. 284.

[7] State actors (states) are categorised as subjects of international law. They are characterised by territory, sovereign power, society, a penal system, and the ability to establish and maintain diplomatic relations with other states. See keyword: state, *Słownik terminów z zakresu bezpieczeństwa narodowego* (Eng. Dictionary of national security terms), issue 6, Warszawa 2008, p. 96.

[8] A non-state actor is defined as an actor relevant to international relations, independent of central government funding and control, operating in a transnational space, lacking territory, society, geographically dispersed and structurally and organisationally complex. Through its actions it can influence the policies of states and economic systems and society. See in more detail: A. Antczak, *Rola aktorów niepaństwowych w kształtowaniu bezpieczeństwa* (Eng. The role of non-state actors in shaping security), "Środkowoeuropejskie Studia Polityczne" 2017, no. 3, pp. 143–145. https://doi.org/10.14746/ssp.2017.3.7; K. Rokiciński, *Ewolucja postrzegania zagrożeń asymetrycznych* (Eng. Evolution of the perception of asymmetric threats), in: *Acti Labores Lucundi. Studia ofiarowane Leopoldowi Ciborowskiemu w siedemdziesiątą rocznicę urodzin*, M. Zieliński, B. Pączek (eds.), Gdynia 2014, p. 196.

or transnational. Undoubtedly, new threats are identified in the geopolitical conditions existing in the 21st century, which are (...) *the result of many phenomena and processes that have remained outside the mainstream of politicians and analysts until recently. These phenomena require a fundamental reorientation not only of the relevant doctrines, the planning of operations, the equipment of the armed forces or the relevant infrastructure, but fundamentally of security-building thinking itself*[9]. It is a truism to say that ensuring state security is a difficult and complex process, and concepts of resilience are often treated as strategies for meeting these challenges. However, the notion that states are responsible for ensuring the security of their borders, the organisation of state structures, the economy and the development of society remains valid.

The aim of this article is to present how state resilience is understood and built in the context of hybrid activities. The achievement of the objective was guided by the following working hypothesis: hybrid actions can significantly affect the state of state security, and building resilience is an effective remedy to this type of threat. Accordingly, a research problem was formulated: how to understand and build state resilience to hybrid activities?

The solution of the indicated research problem required the use of various research methods. The most important ones include: the monographic method, analysis of the literature on the subject, systemic analysis, linguistic interpretation, expert interview [10], inductive and eliminative inference, generalisation and analogy. The application of these methods made it possible to propose a concept for building state resilience to hybrid actions.

Understanding the contemporary security environment

Among the definitions of security created by Polish theoreticians, the position of Ryszard Zięba should be quoted, who believes that security boils down to the existential needs of such entities as individuals, social groups and organisational structures of states. As he explains, (...) *in the most general sense, security can be defined as the certainty of existence and survival, possession and functioning and development of an entity. Certainty is the result not only of the absence of threats, but also arises from the creative activity of the subject in question and is*

[9] G. Ciechanowski, *Wstęp* (Eng. Introduction), in: *Współczesne zagrożenia bezpieczeństwa*, G. Ciechanowski, M. Romańczuk (eds.), Szczecin 2017, pp. 7–8.

[10] Interviews were counducted between 2015 and 2022 with representatives of the Government Security Center, Doctrine and Training Centre of the Polish Armed Forces and Polish Naval Academy.

variable over time, i.e. it is in the nature of a social process[11]. A general definition of the term 'security' can be found in the Dictionary of national security terms, where it is explained as (...) *a state that provides a sense of certainty, and guarantees for its preservation, and a chance for improvement. One of the basic human needs. It is a situation characterised by the absence of risk of losing something that a person particularly values, for example: health, work, respect, feelings, material goods*[12]. When explaining the nature of the security phenomenon, it is important to bear in mind its relationship to the phenomenon of risk[13]. Achieving the desired state of security requires the entity to be active beforehand, allowing it the freedom to pursue its own interests in the environment in which it operates, which will consequently ensure the development and survival of the entity. In order for an entity to experience security, it must therefore eliminate the risk of threats by addressing challenges and opportunities in the security environment.

It is worth noting that during the Cold War, European security was seen through the lens of military threats. After the collapse of the bipolar world system, the conceptual scope of the term 'security' expanded. A representative of the Copenhagen School, Barry Buzan, made an important contribution to the formation of the perception of security. He accepted that security problems should be considered in a broader scope than just the political-military one[14].

Analysing developments since the 1990s, it is impossible not to notice that the concept of security is constantly being redefined. New areas of security are now emerging, e.g. cyber security, critical infrastructure, energy security, economic security, social security, maritime security, humanitarian security, social security and many others, and the scope of the meaning of these terms continues to expand. A trend has therefore emerged whereby a state security threat is understood as anything that can disrupt the functioning of the state and its society in any way. Therefore, it is nowadays believed, as Marian Kopczewski points out, that the subject of security is all individuals who have their own interests and express

---

[11] *Bezpieczeństwo międzynarodowe po zimnej wojnie* (Eng. International security after the Cold War), R. Zięba (sci. ed.), Warszawa 2008, p. 16.

[12] Keyword: security, *Słownik terminów z zakresu bezpieczeństwa narodowego*, issue 6, Warszawa 2008, p. 14.

[13] R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje – struktury – funkcjonowanie* (Eng. Institutionalisation of European security. Concepts - structures - functioning), Warszawa 2004, p. 28.

[14] After: A. Sekściński, *Bezpieczeństwo wewnętrzne w ujęciu teoretycznym. Geneza i współczesne rozumienie w naukach politycznych* (Eng. Internal security in theoretical terms. Origins and contemporary understanding in political science), "Kwartalnik Naukowy OAP UW e-Politikon" 2013, no. 6, pp. 47–48.

ambitions to pursue them[15]. The reasons for adopting this position include the need for the security discourse to take into account, in addition to the interdependence between actors of international law, the norms of war, arms control and the importance of non-governmental actors in particular[16]. The modern dimension of security is not only about survival, territorial integrity, state sovereignty, but also about ensuring an adequate quality of life for the population, an adequate economic level for the state and protecting the environment[17]. Threats cannot be treated selectively. It is necessary to diagnose the changes taking place in the international space also in a long-term perspective.

As of 24 February 2022, the world is focused on events in Ukraine, but just as important remains the problem of the political situation in Belarus, which is also a determinant of Poland's security and the formation of relations with the Russian Federation (RF). Security considerations cannot overlook the state of Turkish-Russian relations or the tensions in relations between the European Union (EU) and its member states. The ambitions of states regarding the Arctic and the possibility of its military exploitation are also not insignificant, and in the new global order taking shape, the future of US-China relations. The pursuit of strategic goals in the international arena determines the multifaceted game of maintaining the status quo in terms of preserving defence capabilities and skilfully adapting to challenges[18]. Awareness of the existence of threats and the need to look after one's own national interests determine the course of action taken by states in the international arena. As a result, some states are adapting to the changing strategic environment, while others are attempting to reduce vulnerability.

[15] M. Kopczewski, *Bezpieczeństwo wewnętrzne państwa – wybrane elementy* (Eng. Internal security of the state - selected elements), "Doctrina. Studia społeczno-polityczne" 2013, no. 10, p. 107.

[16] E. Cziomer, M. Lasoń, *Podstawowe pojęcia i zakres bezpieczeństwa międzynarodowego i energetycznego* (Eng. Basic concepts and scope of international and energy security), in: *Międzynarodowe bezpieczeństwo energetyczne w XXI wieku*, E. Cziomer (ed.), Kraków 2008, p. 16.

[17] M. Lasoń, *Bezpieczeństwo w stosunkach międzynarodowych* (Eng. Security in international relations), in: *Bezpieczeństwo międzynarodowe w XXI wieku. Wybrane problemy*, E. Cziomer (sci. ed.), Kraków 2010, pp. 10–11.

[18] J. Raubo, *GlobState III, czyli zrozumieć świat i wykorzystać wiedzę do budowania sił zbrojnych* (Eng. GlobState III, or understanding the world and using knowledge to build forces), Defence24, 13 XII 2020, https://defence24.pl/sily-zbrojne/globstate-iii-czyli-zrozumiec-swiat-i-wykorzystac-wiedze-do-budowania-sil-zbrojnych-komenatrz [accessed: 7 VII 2022].

The problem in defining state resilience and hybrid activities

The issue of building states' resilience to hybrid activities has been discussed repeatedly at successive NATO summits[19]. A 2021 communiqué in Brussels stated that hybrid attacks and cyberattacks on Alliance countries could trigger Article 5 of the North Atlantic Treaty[20]. The *National Security Strategy of the Republic of Poland* 2020 devotes an entire subsection to the problem of state resilience and universal defence. Section 2.2 makes it clear that it is necessary to (...) *build the resilience of the state to threats, including those of a hybrid nature, ensure the universal nature of civil defence and civil protection*[21]. In the aforementioned document, the concept of hybrid threats was mentioned five times, but neither its definition nor an explanation of what is included in them appeared. The word 'resilience' was used as many as eleven times to refer to taking action (...) *to increase the resilience of the state and society to contemporary threats*[22]. Increasing the resilience of the state is understood as (...) *creating a system of universal defence, based on the effort of the whole nation, and building an understanding of the development of the resilience and defence capabilities of the Republic of Poland*[23]. This is to include: building a system of universal defence, resilience to hybrid threats, developing the capacity of the health system and public administration structures, as well as in preventing and responding to terrorist threats, combating organised crime, including criminal activities in cyberspace[24]. Hereafter, the term 'resilience' is used to refer to enhancing economic security, including financial security, by taking measures that improve resilience to international financial crises, especially those that serve to strengthen the stability of the public finance system. These actions also refer to diplomatic, legal and administrative activities that increase a country's resilience to the risk of energy supplies being used as an instrument

[19] In Newport in Wales in 2014, in Warsaw in 2016, in Brussels in 2018 and in London in 2019.

[20] See in more detail: W. Lorenz, *Szczyt NATO w Brukseli – przełomowy moment dla Sojuszu* (Eng. NATO summit in Brussels - a breakthrough moment for the Alliance), PISM, 15 VI 2021, https://www.pism.pl/publikacje/Szczyt_NATO_w_Brukseli__przelomowy_moment_dla_Sojuszu [accessed: 10 VII 2022]. See also: R. Opas, *Użyją art. 5? Stoltenberg nie wyklucza* (Eng. Will they use Article 5? Stoltenberg does not rule out), Wiadomości WP, 11 X 2022, https://wiadomosci.wp.pl/uzyja-art-5-stoltenberg-nie-wyklucza-6821910367021888a [accessed: 11 X 2022].

[21] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020* (Eng. National Security Strategy of the Republic of Poland 2020), https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, p. 15 [accessed: 15 X 2022].

[22] Ibid, p. 10.

[23] Ibid, p. 15.

[24] Ibid, pp. 15–20.

of political pressure from other countries[25]. The issue of building the resilience of state structures to the effects of hybrid action is a frequent element of public debate, also undertaken by the National Security Bureau[26]. The need to build resilience to military, non-military and hybrid threats is also emphasised by the Government Centre for Security[27]. It states that in a situation of deteriorating security in the region, the resilience of a state to emerging threats is one of the basic conditions for ensuring its protection[28]. Therefore, state resilience to hybrid threats has an important place in national and international debates and security strategies. However, there is still a lack of terms for 'state resilience' and 'hybrid activities' that are widely recognised and used in NATO and EU documents as well as in national documents. The definitions formulated so far are ambiguous, often conceptual and leave room for interpretation, which is not conducive to scientific cognition. The way in which these concepts are perceived depends on the perception of the interpreter as a specific subject who, on the basis of his or her knowledge, formulates a theory that is the result of interpretative activities related to the problem being addressed. According to the rules of definition construction, the definition should specify the sense, meaning of the defined word or expression, be precise, unambiguous and logical[29].

---

[25] Ibid, pp. 33–34.

[26] P. Soloch, P. Pietrzak, *Szczyt NATO w Warszawie: uwarunkowania, rezultaty, wnioski dla Polski* (Eng. NATO summit in Warsaw: conditions, results, conclusions for Poland), "Bezpieczeństwo Narodowe" 2016, no. 37–40, p. 31.

[27] M. Kubiak, *Zarządzanie kryzysowe a bezpieczeństwo narodowe w dobie zagrożeń hybrydowych* (Eng. Crisis management and national security in the age of hybrid threats), "Biuletyn Kwartalny Rządowego Centrum Bezpieczeństwa" 2018, no. 24, p. 4. The RCB's analytical bulletins are available at: https://www.gov.pl/web/rcb/biuletyn-analityczny-rzadowego-centrum-bezpieczenstwa (editor's note); *Budowanie odporności państw członkowskich sojuszu – implementacja wytycznych NATO* (Eng. Building the resilience of alliance member states - implementation of NATO guidelines), Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/budowanie-odpornosci-panstw-czlonkowskich-sojuszu-implementacja-wytycznych-nato/ [accessed: 20 XII 2018]; *Odporność na zagrożenia tematem seminarium RCB* (Eng. Resilience to threats the topic of the RCB seminar), Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/odpornosc-na-zagrozenia-tematem-seminarium-rcb/ [accessed: 20 XII 2018]; A. Zasadzińska-Baraniewska, *Zarządzanie kryzysowe wobec nowego typu zagrożeń – spotkanie eksperckie w Rządowym Centrum Bezpieczeństwa* (Eng. Crisis management in the face of a new type of threat - expert meeting at the Government Centre for Security), "Biuletyn Kwartalny Rządowego Centrum Bezpieczeństwa" 2017, no. 19, p. 4.

[28] *Odporne NATO* (Eng. Resilient NATO), Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/odporne-nato/ [accessed: 20 XII 2020].

[29] M. Bartoszewicz, *Definicje legalne w świetle zasady określoności prawa* (Eng. Legal definitions in the light of the principle of legal certainty), in: *Dookoła Wojtek… Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Preisnerowi*, R. Balicki, M. Jabłoński (eds.), Wrocław 2018, pp. 355–356.

Given the lack of formal definitions in the field of state resilience and in order to make the subject matter more precise, it is worth introducing a design definition that can serve to clarify the problem under study.

At the outset, it should be noted that the concept of resistance also functions in other fields of knowledge, such as engineering science and medicine. In mechanical engineering, it refers to the understanding of the behaviour and susceptibility of materials to deformation under the influence of various external forces applied. In this context, it is a measure of the resistance of a given material to the actions of a force so that it can withstand without breaking or permanently changing shape. The measure of resistance in such a situation is therefore the time it takes for the material to return to its original shape after the cessation of the acting force[30]. In medical science, the issue of immunity is dealt with by immunology. In this science, immunity refers to (...) *the processes by which the human organism maintains the equilibrium of the internal environment in the event of exposure to a foreign substance with antigenic properties of external or internal origin*[31]. In turn, the *PWN Dictionary of Polish Language* defines the word 'resilient' in two ways as (...) *not susceptible to physical or moral influences and as* (...) *not subject to infection by pathogenic microorganisms*[32]. According to an *English-Polish dictionary*, 'resilient' means (...) *resilient, able to recover quickly (e.g. from ilness)*, and 'to be resilient' means: *to resist, to resist, to hold back*[33].

With regard to state resilience, the wording of the cited definitions can be understood as follows:

– "insensitive" - resistant to influence, not subject to influence, able to maintain the status quo;
– "resisting" - able to overcome threats.

By analogy with definitions adopted from engineering and medical sciences as well as dictionaries, the author formulated a definition of state resilience as the ability to resist the offensive actions of the aggressor(s) or the ability to adapt to new conditions while maintaining the prospect of existing security, while

[30] *Wytrzymałość materiałów – rodzaje, co to jest?* (Eng. Strength of materials - types, what is it?), EBMIA, 30 VIII 2021, https://www.ebmia.pl/wiedza/porady/obrobka-porady/wytrzymalosc-materialow-rodzaje/ [accessed: 23 VII 2022].

[31] Keyword: immunology, https://mediweb.pl/slownik-nauk-i-specjalnosci-lekarskich [accessed: 20 VIII 2022].

[32] Keyword: resilience, *Słownik języka polskiego PWN* (Eng. PWN Dictionary of the Polish Language), https://sjp.pwn.pl/slowniki/odporno%C5%9B%C4%87.html [accessed: 20 VIII 2022].

[33] Keyword: resilient, in: *Oxford Wordpower. Słownik angielsko-polski z indeksem polsko-angielskim*, Oxford University Press 2002, p. 643.

guaranteeing survival and unwavering development[34]. From this definition, state resilience is understood as the ability to resist and respond to and manage crisis situations. It is therefore also the ability to adapt to a new situation. State resilience understood in this way consists of capabilities in the civilian and military spheres. This confirms that building a state's resilience is the refinement of its capabilities in the face of new threats. These capacities mean, among other things, dealing effectively with the actions of an aggressor and being able to maintain the confidence of one's own society in the state authorities and the international community in a threatening situation[35]. The problem with such a definition of state resilience remains how to measure or assess state resilience and with which tools this should be done. Without developing a system of indicators and measures, a reliable assessment of the actual state is impossible. Their proper selection makes it possible to know how and on what scale the analysed threat or phenomenon causes changes in the security environment. Therefore, each indicator and measure should be conditioned by the purposefulness of its introduction. It is necessary to establish why they are being introduced, what is intended to be measured, what is expected from the measure and indicator, while indicating how it will be measured or estimated and the source of the data. This leads to the development and adoption of a methodology. Only then can it be determined where resilience needs to be improved.

With regard to acquiring resilience to hybrid actions, it is necessary to understand them - what they are or are not - and to relate them to areas of state functioning. It should be noted that the use of the term 'hybrid actions' can be grasped in at least three dimensions: **epistemological** - as a way of scientific cognition, **ontological** - pointing to the essence of their being, time and space, and **objective** (scopic) - what they are[36].

---

[34] The author has formulated this definition on the basis of: J. Mokrzycki, C. Pawlak, *Budowanie odporności państwa gwarancją jego bezpieczeństwa* (Eng. Building the resilience of the state as a guarantee of its security), in: *Kształtowanie przestrzeni bezpieczeństwa państwa*, G. Ciechanowski, K. Ligęza, A. Rurak (sci. eds.), Gdynia 2019, p. 38. The definition is also elaborated in the document: *Koncepcja Kompleksowego Wzmacniania Odporności RP* (Eng. Concept for Comprehensive Resilience Strengthening of the Republic of Poland), prepared by the Government Centre for Security. After: G. Matyasik, *Jak wygląda polska odporność?* (Eng. What does Polish resilience look like?), INFOSECURITY24, 4 IV 2023, https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/jak-wyglada-polska-odpornosc [accessed: 10 IX 2023].

[35] *Commitment to enhance resilience*, North Atlantic Treaty Organization, 8 VII 2016, https://www.nato.int/cps/en/natohq/official_texts_133180.htm [accessed: 21 VIII 2022].

[36] A similar division was made by Bogdan Zdrodowski in his cognitive approach to security. See in more detail: B. Zdrodowski, *Istota bezpieczeństwa* (Eng. The essence of security), in: *Wybrane problemy bezpieczeństwa wewnętrznego państwa*, A. Misiuk (ed.), vol. 34, Warszawa 2014, p. 34.

From the research conducted so far in the field of threats with hybrid characteristics and hybrid actions, it appears that these concepts gained prominence after the bloodless annexation of Crimea by the Russian Federation, resulting from the inability of states and NATO to recognise the situation in the security environment[37]. The lack of precise definitions defining this type of threat generates confusion and causes public dispute in such an important area as state security, which is among the most highly valued and protected values. The problem of the imprecise formulation of definitions of hybrid operations and threats with hybrid characteristics has also been recognised by many military researchers and theorists, who consider the use of these terms to be useless and sometimes even dangerous. They point out that definitions in the area of hybridity, especially those published after 2014, refer directly to RF actions rather than to the phenomenon understood holistically[38].

The definitions presented so far are general enough to cover a wide variety of phenomena and create the potential for different catch-all interpretations, thus blurring the traditional distinction between peacetime and war and conflict[39].

[37] The events in Ukraine in 2014, and in particular the annexation of Crimea, have been identified by numerous researchers and security experts as hybrid war or hybrid threats. In addition to these two popular terms, other less common terms such as hybrid action, hybrid conflict, hybrid attack, fourth-generation conflict and grey area action have emerged as one of many attempts to explain the hybridity of contemporary conflicts. See: A. Rácz, *Russia's Hybrid War in Ukraine Breaking the Enemy's Ability to Resist*, Helsinki 2016, p. 40; S. Bolzen, *"Die NATO muss auf grüne Männchen vorbereitet sein"*, Die Welt, 17 VIII 2014, http://www.welt.de/politik/ausland/article131296429/Die-Nato-muss-auf-gruene-Maennchen-vorbereitet-sein.html/ [accessed: 27 I 2015]; C. Pawlak, J. Keplin, *Aneksja Krymu w kontekście działań hybrydowych* (Eng. Annexation of Crimea in the context of hybrid activities), "Kwartalnik Bellona" 2016, no. 3, pp. 23–24; J. Keplin, *Działania hybrydowe jako niewidzialne zagrożenia* (Eng. Hybrid activities as invisible threats), in: *Wojna Federacji Rosyjskiej z Zachodem* (Eng. The war between the Russian Federation and the West), M. Banasik (ed.), Warszawa 2022, pp. 167–168; T. Usewicz, J. Keplin, *Hybrid Actions and Their Effect on EU MaritimeSecurity*, "Journal on Baltic Security" 2023, vol. 9, no. 1, pp. 32–68. https://doi.org/10.57767/jobs_2023_001; J. Keplin, *Działania hybrydowe na Morzu Bałtyckim. Zarys problemu dla bezpieczeństwa Rzeczypospolitej Polskiej* (Eng. Hybrid activities in the Baltic Sea. Outline of the problem for the security of the Republic of Poland), "De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2022, vol. 8, no. 2, pp. 54–68. https://doi.org/10.34739/dsd.2022.02.04.

[38] See: P. Ochmann, J. Wojas, *Wojna hybrydowa jako przykład umiędzynarodowionego konfliktu wewnętrznego* (Eng. Hybrid warfare as an example of internationalised internal conflict), "Studia Prawa Publicznego" 2018, no. 2, pp. 101–102. https://pressto.amu.edu.pl/index.php/spp/article/view/21068/20355 [accessed: 1 XII 2022]; A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna* (Eng. Hybridity of modern warfare - a critical analysis), in: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (eds.), Warszawa 2011, p. 17.

[39] E. Reichborn-Kjennerud, P. Cullen, *What is Hybrid Warfare?*, Norwegian Institute of International Affairs, 2016, https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf, pp. 1–2 [accessed: 1 XII 2022].

In such a situation, hybrid threats can be everything to everyone. Therefore, the state and its structures must be aware of contemporary threats and be prepared for a variety of challenges, not just one type of threat.

Analysis of the problem indicates that the aggressor takes action in advance, and that the preparation time can last from several to even several years. This allows them to refine the strategic objective and intermediate objectives, as well as to forecast the desired outcomes and adopt an initial strategy. In the first instance, the aggressor will focus on identifying and analysing the target in terms of:

- vulnerabilities and weaknesses of the state in different areas of its functioning,
- strengths as constraints or impediments to achieving the goal (membership in alliances, economic, social situation and others)[40].

Activities will include the synchronised use of multiple tools[41] adapted to the vulnerability of the areas. It should be added that information operations will be a means of greatly facilitating success. This position coincides with the views of Carl von Clausewitz, according to whom the achievement of strategic objectives can be achieved by means other than war. He mentions politics as an important tool[42]. An aggressor, using policy elements, can pursue its objectives covertly or overtly. Therefore, any effective strategy should take into account the complexity of the environment, identify ways to achieve victory and avoid oversimplifying the problem. Any omission of essential elements by the attacked party results in the aggressor gaining a situational advantage. It is therefore important to constantly monitor threats both internally and externally. Their analysis is a key step to identify potential risks, as it allows an understanding of the aggressor's motivations. Furthermore, considering its intentions, potential interests, needs, methods of action, as well as its willingness to achieve its main or intermediate objectives, is the most important element of effective state security management. It is also important to determine the actual capabilities and resources of the aggressor, whether they are sufficient to achieve the objective. Thus, the continuous monitoring of threats allows for a rapid response and the adaptation of adequate tools to the identified danger, allows for an effective response to the changing situation, which in turn contributes to the preservation of state stability and sovereignty.

---

[40] J. Keplin, *Analityczny model działań hybrydowych narzędziem wspomagającym bezpieczeństwo państwa* (Eng. Analytical model of hybrid activities a tool to support state security), in: *Współczesne zagrożenia bezpieczeństwa*, G. Ciechanowski, M. Romańczuk (eds.), Szczecin 2017, pp. 127–138.

[41] Such as, for example, diplomatic, economic, information, sanctions, embargoes and others.

[42] See in more detail: M. Mazur-Bubak, *Wybrane teorie leżące u podstaw współczesnego paradygmatu wojny* (Eng. Selected theories underlying the contemporary paradigm of war), "Internetowy Magazyn Filozoficzny Hybris" 2015, no. 30, pp. 82–83, https://dspace.uni.lodz.pl/xmlui/handle/11089/20342 [accessed: 20 XI 2022].

It should be added that sustainable socio-economic development requires an adequate level of security, i.e. the ability to ensure the unthreatened exploitation of opportunities (potential) in building an efficient economy as the basis for creating wealth for the state and its society[43]. Today's hybrid threats can be generated by both state[44] and non-state actors[45]. As Ryszard Zięba explains, (...) *contemporary threats and dangerous phenomena are a reflection of the changes that are constantly taking place in the lives of nations and states, and are the result of actions taken by states and non-state actors to secure their own interests*[46]. This means that the world order is changing and the prevailing rules are being modified. Competition for energy resources and a growing demand for food, water, as well as new technologies, is becoming noticeable.

Non-state actors, such as non-government organisations (NGOs), multinational and transnational corporations and, in a particular situation, individuals, can influence state policies, economic systems and society, and their lobbying activities can shape international law that serves their interests. In addition, engaging NGOs as proxies allows the aggressor to avoid responsibility and conceal illegal activities. In such a case, proving aggression proves very difficult. Krzysztof Liedel believes that in the coming decades, states will base their security on the provisions of international laws, and their effectiveness will depend on their interpretation in the international arena[47]. This creates the need to modify views on state security, its threats and guarantees. These threats are, for example, hostile informational or economic actions aimed at influencing society, or economic and technological dependence or dependence on other states or corporations for the supply of raw materials, thereby influencing the policies of the targeted state. The security environment of a state can therefore be destabilised as a result

[43] H. Świeboda, *Prognozowanie zagrożeń bezpieczeństwa narodowego Rzeczypospolitej Polskiej* (Eng. Forecasting threats to the national security of the Republic of Poland), Warszawa 2017, p. 8.

[44] The most common threats posed by state actors are revisionist aspirations, the initiation or fuelling of internal conflicts, the application of political and economic pressures, the pursuit of another state's dependence on energy resources, information and disinformation activities, which can be carried out, among others, in cyberspace.

[45] Threats from non-state actors most often include the actions of terrorist groups (e.g. jihad), the actions of organised crime groups, organised drug and arms trafficking, hostile actions of corporations seeking to influence state policy.

[46] R. Zięba, *Współczesne wyzwania i zagrożenia dla bezpieczeństwa międzynarodowego* (Eng. Contemporary challenges and threats to international security), "Stosunki Międzynarodowe – International Relations" 2016, vol. 52, no. 3, p. 9. https://doi.org/10.7366/020909613201601.

[47] K. Liedel, *Zagrożenia hybrydowe. Jak zmienia się środowisko bezpieczeństwa RP?* (Eng. Hybrid threats. How is the Polish security environment changing?), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, special edition: *Hybrid warfare*, p. 52.

of the use of a variety of coordinated forms of influence by an aggressor, with varying degrees of intensity and in different areas of state functioning. The range of threats and their transformation can be expected to widen, making them more difficult to identify and respond to. According to Thomas Schuman, the most common way of influencing the state is through blackmail, intimidation of politicians and the media, so that they themselves destabilise and dismantle their country[48]. In the absence of a universal guarantee of state security and the relatively easy pursuit of aggressive policies by various actors, it is typical to use soft measures of influence. Firstly, informational activities are gaining great importance, which, with the use of modern technologies, are one of the more effective tools. The area of information and communication systems, which is the space in which hybrid actions are carried out, is extremely important. Attacks in cyberspace do not necessarily have a destructive effect on IT systems used in critical infrastructure or banks, but they can cause situational discomfort and raise concerns[49]. Secondly, the aim may be to steal and disclose information relevant to state security. Thirdly, the action may involve the introduction of false information into the information space, as well as the use of false security certificates for the purpose of not only material gain but also intimidation[50]. It should be added that part of the risks in the IT area are due to the lack of an acceptable level of security of data stored

[48] "T. Schuman" was the pseudonym of former KGB agent Yuri Bezmenov, an employee of the Novosti Press Agency in New Delhi, where he was responsible for conducting propaganda for the Soviet regime. He was a specialist in disinformation techniques, overt and covert propaganda, and ideological diversion (Russian: активные мероприятия). In 1970, after his hostile attitude towards the USSR was detected, he fled to the USA. He provided the Americans with a wealth of significant information on techniques for ideological subversion and ways to destabilise by disrupting single areas (e.g. diplomatic, economic) by taking control of key sectors related to these areas, up to and including bringing the entire state into crisis. He shared his reflections in a book. See in more detail: T. Schuman (Yuri Bezmenov), *Love Letter to America*, Los Angeles 1984, pp. 17–19.

[49] Activities in cyberspace concern attacks carried out not only by certain state and non-state actors, but also by hackers often acting for emotional reasons and out of a desire to impress. They make up a significant proportion of attackers. Activities in cyberspace may also involve the theft of sensitive data and hacking into bank accounts and can be classified as common crimes. See in more detail: K. Rokiciński, *Wybrane aspekty zagrożeń asymetrycznych na morzu w funkcji wykorzystania sił morskich* (Eng. Selected aspects of asymmetric threats at sea as a function of the use of naval forces), "Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, y. 46, no. 1, p. 165.

[50] Dutch company DigiNotar was attacked by internet criminals. More than 500 SSL certificates were stolen from DigiNotar, including those issued to the CIA and Mossad. As a result, the company declared bankruptcy. Australian hosting provider Distribute.it. and English internet provider Cloud Nine experienced similar activity. See in more detail: A. Jadczak, *Zaatakowana przez hakerów DigiNotar ogłosiła upadłość* (Eng. DigiNotar, attacked by hackers, has declared bankruptcy), Computer World, 23 IX 2011, https://www.computerworld.pl/news/Zaatakowana-przez-hakerow-DigiNotar-oglosila-upadlosc,375383.html [accessed: 4 I 2019].

in IT systems used to carry out important public tasks[51]. Marian Cieślarczyk stresses that (...) *currently a significant part of society has not kept up with the development of modern technologies* (...) *and is not able to foresee the consequences associated with their use, which entails great risks*[52].

It is also important to pay attention to states that are trying to rebuild their power position and aim to create a multipolar world. There is nothing new in undertaking hybrid activities, but globalisation, modern technology or digitalisation have greatly increased their effectiveness and their ability to influence selected targets. It should be emphasised that hybrid activities are not regular diplomatic actions, economic agreements, and certainly not conflict and war between states. Hybrid actions can instead exist between the latter two states. They are used as a cheaper alternative to classic armed conflict, lasting much longer at a perceptibly lower cost. In hybrid actions, the threats posed by them are recognised earlier than the aggressor as the perpetrator. The aggressor, by adopting different targets and ways of using proxies[53], makes its activities difficult to detect.

In attempting to explain hybrid activities, it is important to remember that they are not limited to military action. The aggressor by its operations wants to influence the politics of the state, its society and its economy under conditions of peace, countering or responding to these threats will therefore be different from those involving military force. It can be hypothesised that any use of tools[54] under conditions of peaceful functioning of the state is understood as a deliberate action by a state or non-state actor, which will result in an expected response in the affected area, e.g. a change in state policy or public behaviour, the reception of information in accordance with the will of the initiator of such actions. In reality, hybrid activities are difficult to recognise and pose a real threat.

Following the accepted line of reasoning, hybrid activities can be defined as follows:

---

[51] *NIK o bezpieczeństwie danych* (Eng. NIK on data security), Najwyższa Izba Kontroli, 16 V 2016, https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-danych.html [accessed: 18 XI 2018].

[52] M. Cieślarczyk, *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i odporności państwa* (Eng. Theoretical and methodological basis for the study of state security and resilience problems), Siedlce 2009, p. 14.

[53] What is important is the use of *proxies*, e.g. NGOs and transnational corporations, to achieve the goal, so that the actual aggressor goes undetected and the blame for aggressive actions can be assigned to another actor.

[54] In relations between subjects of international law, these tools include politics, contracting, the use of other subjects of international law (*proxies*), information activities, disinformation, attempts to depend on energy resources or other goods, among others.

> (…) these are activities aimed at achieving political and strategic objectives by the aggressor with the possibility of maintaining existing economic and/or diplomatic relations. These actions are carried out by state and/or non-state actors in a planned and coordinated manner, combining various means of pressure and dependency on the aggressor. They may be conducted in political, economic, military and social environments, including national, ethnic and religious minorities, while varying in time, space (geographical area) and intensity and using proxies. These activities are carried out under conditions of normal state functioning[55].

State resilience against hybrid activities

Today, the state is considered to be the guarantor of the general welfare of its citizens. It achieves this goal through, among other things, the implementation of policies on social benefits, social security, access to education, law enforcement, public security, protection of critical infrastructure and other important areas. This approach to the state's role in providing security therefore points to a complex socio-political and socio-economic framework that state institutions should take into account. With regard to state resilience, this introduces into the discourse both tangible[56] and intangible criteria[57] that are difficult to measure. Furthermore, it forces the exact type of state resilience in need of improvement and refinement, as no state is resilient in all areas of security[58]. It is therefore important to establish what

[55] *Koncepcja udziału Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom hybrydowym* (Eng. Concept of participation of the Polish Armed Forces in countering hybrid threats), Centrum Doktryn i Szkolenia, Bydgoszcz 2017, p. 8. The definition presented here is the result of the work on this concept. The author of this article was the head of the project team for the development of this concept.

[56] For example, military potential, energy resources, water, metal ores, etc.

[57] For example, a state's will to act and determination to achieve strategic goals, states' aspirations, ideologies, strategies, alliance sustainability, information, society's ability to neutralise threats, etc.

[58] The priority is to identify those areas of state security that are most vulnerable to contemporary threats - e.g. environmental, from terrorism and sabotage, to technical systems failures, in maintaining energy supply chains and others.

the purpose of these activities is and against what this resilience is to be built[59]. This requires a choice of priorities and therefore entails the use of adequate resources[60].

With regard to hybrid activities, it is crucial to understand that these activities target multiple domains of state security, so resilience must be considered with the specifics of these domains in mind. These threats are complex, characterised by high dynamics of change, which makes their detection difficult. This requires the preparation of new solutions to support the early warning system[61]. Lech Wojciech Zacher points out that awareness of the occurrence of potential threats, crises and disasters is important, without which there is no possibility of supporting global security[62]. Jack Williams[63] believes similarly, and adds that any relevant information should be analysed in order to make an informed assessment of what might happen in the future. In his view, threat assessments are always predictable, and describing a forecasted event is not the result of analysing the intelligence at hand, but of applying several analytical techniques to combine vast amounts of information in a complex system[64].

On the basis of a critical analysis of the literature on the subject, the author concludes that one of the actions that can significantly support the building of a state's resilience to hybrid activities is to strive for effective recognition and identification

---

[59] The concept of building a state's resilience to hybrid action was developed, among others, as part of the project Countering Hybrid Warfare implemented as part of the Multinational Capability Development Campaign, in which the author participated. The project had two editions - in 2015-2016 and 2017-2018 - and the work resulted in, among other things, a paper: *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare*, https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf [accessed: 7 X 2022].

[60] Ch. Fjäder, *The nation-state*…, p. 122.

[61] P. Cullen, *Hybrid threats as a new 'wicked problem' for early warning*, Hybrid CoE, 4 VI 2018, https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-8-hybrid-threats-as-a-new-wicked-problem-for-early-warning/ [accessed: 12 X 2018].

[62] L.W. Zacher, *Trwały rozwój – utopia czy realna możliwość?* (Eng. Sustainable development - utopia or a real possibility?), "Problemy Ekorozwoju – Problems of Sustainable Development" 2008, vol. 3, no. 2, p. 66.

[63] Professor Jack F. Williams' interests include risk in the energy industry. He was a director and leader at Binder Dijker Otte & Co. (BDO) Consulting, where he served as a financial advisor, accountant and fraud detection expert. In addition, he was a consultant to the US federal government and the private sector in the areas of threat analysis, risk assessment, infrastructure protection. Among other things, he currently teaches at St. John's University School of Law Bankruptcy Policy Institute.

[64] J.F. Williams, *Critical Energy Infrastructure Protection Policy Research Series: Al-Qaida threats and strategies: the religious justification for targeting the international energy economy*, The Canadian Centre of Intelligence and Security Studies at Carleton University, March 2008, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.612.473&rep=rep1&type=pdf, p. 18 [accessed: 17 XI 2018].

of threats, those existing but undetected, as well as future threats that will result from political decisions taken and from changes in the security environment. It is impossible not to agree with Krzysztof Ligęza, who points out that it is impossible to recognise all threats, as some of them appear unexpectedly, both in terms of time and place. He adds that the essence of security is to think ahead about the type of threats and to be adequately prepared to minimise the consequences should they occur[65].

These arguments demonstrate that properly developed methods and tools can support the process of developing viable scenarios to prepare for potential events. This is in line with Zacher's thesis that (...) *the most important aim of thinking about the future is not so much to discover it, but to prepare ourselves for the various options we may face when confronted with an unknown fate*[66]. Halina Świeboda points out that anticipatory thinking is part of the process of designing future actions[67]. Therefore, each properly prepared scenario is a source of knowledge and contributes to the creation of an appropriate forecasting system with an early warning system concept, which should result in the development of a strategy to counteract unfavourable phenomena. It is advisable to develop an analytical tool that takes into account trends and phenomena in the security environment. This requires a systemic perception of the object and subject of research, taking into account factors arising from globalisation and the internal conditions of the state. Identifying threats, forecasting the internal situation of a state, as well as international relations, involves a set of assertions and assumptions that explain them, and these should be used when preparing such an analytical tool[68].

It should also be noted that in the 21st century there is a greater vulnerability of society to the risks associated with the development of civilisation, political, economic, social and informational tensions. The problem is how to educate a society, which is often unaware of threats, to become resilient to them. Therefore, it is also the task of the modern state to prepare society for the emergence of potential

[65] K. Ligęza, E. Iwanina-Szopińska, *Zabezpieczenie logistyczne ludności poszkodowanej w sytuacjach kryzysowych w aspekcie zapewnienia bezpieczeństwa* (Eng. Logistics security for affected populations in emergency situations), in: *Paradygmaty badań nad bezpieczeństwem. Zarządzanie kryzysowe w teorii i praktyce*, M. Kopczewski, I. Grzelczak-Miłoś, M. Walachowska (sci. eds.), Poznań 2013, pp. 353–364.

[66] L.W. Zacher, *Problemy i metody przewidywania przyszłości (przegląd tendencji w literaturze)* (Eng. Problems and methods of predicting the future (review of trends in the literature)), in: *Czy warto myśleć o przyszłości?*, Warszawa 1996, p. 28.

[67] H. Świeboda, *Prognozowanie zagrożeń bezpieczeństwa*…, p. 11.

[68] M. Sułek, *Prognozowanie i symulacje międzynarodowe* (Eng. International forecasting and simulation), Warszawa 2010, p. 13.

changes or negative events in the area of security. It is important to diagnose the level of a community's ability to respond to specific threats, both at the level of the population as a whole and at the level of social groups and individuals. In this case, the way in which the state will descript these negative events and how it will present their impact on society and the current situation in the state is important. Appropriate communication of information will contribute to the acquisition of resilience in terms of potential dangers as a result of increased awareness of them, thereby gaining the ability to adapt when unexpected threats arise. A resilient society has the ability to cope and is able to smoothly return to proper functioning[69].

The two approaches outlined - understood as the need to develop tools to recognise and identify risks and to build public awareness - determine the way in which state policy is designed and strategies to achieve goals in different areas of state functioning. As a result, the state acquires the ability to deal with shocks and crises. Consequently, it is necessary to develop diplomacy that can support efforts to create common ground in pursuing similar goals in the international space and, consequently, ensuring world peace[70]. Building and strengthening trust from other states is particularly important to create sustainable state resilience in the international space, especially against hybrid activities. In international relations it is important to be aware of the consequences of decisions taken. Every political decision, and above all the introduction of new norms of international law, brings specific consequences in areas of state functioning, as well as causing interactions between actors of international law. In a particular situation, the existence of a particular entity may be threatened, prompting it to make immediate and extraordinary use of tools with which to safeguard its interests. These approaches should have a direct bearing on the development of concepts, strategies and doctrines. Their substantive quality, the way in which the problem is framed, and the accuracy of the assessments adopted will influence the building of state resilience.

[69] K. Górska-Rożej, *Kształtowanie odporności na zagrożenia w społecznościach lokalnych* (Eng. Building resilience in local communities), "Przegląd Policyjny" 2018, no. 1, p. 57. https://doi.org/10.5604/01.3001.0013.6643.

[70] J. Pospisil, F.P. Kühn, *The Resilient State: New Regulatory Modes in International Approaches to State Building?*, "Third World Quarterly" 2016, vol. 37, no. 1, pp. 5–7. https://doi.org/10.1080/01436597.2015.1086637.

Summary

The expert opinions presented confirm that states and their societies are now more vulnerable to new forms of threats than they were a few decades earlier. This is mainly due to the development of new technologies, in particular the infrastructure that facilitates access to and exchange of information. The new cyber space, also referred to as the fifth dimension of warfare, provides a convenient environment for cybercrimes and cyberattacks that can threaten state and public security.

In the new geopolitical circumstances, subliminal aggression is becoming apparent, in which adversaries deliberately keep their actions below the threshold of war. Their aim is to achieve accepted objectives while generating difficulties in obtaining a decision-making consensus in international security organisations and services and institutions responsible for security in the state. In addition, the repeated violations of the norms of international law, the territorial borders of sovereign states and human rights require the intervention of international organisations and other states, which often fail. It is also a significant problem that states find it increasingly difficult to achieve their strategic objectives, which many times conflict with or differ from the objectives of other actors or remain unknown. This approach to building resilience to hybrid action results in reduced cooperation between states and non-state actors, and therefore difficulty in maintaining the existing global order. Therefore, building resilience to hybrid activities requires a good understanding of the causes of gaps and vulnerabilities in areas of state functioning that can be exploited by a potential aggressor. It should be recalled that threats do not generate themselves - the right conditions must exist for them to arise. There must always be a cause in the form of an aggressor's intentional action, its own inadequacies and a favourable environment.

It is also important to understand that for hybrid activities to be effective, the triad must exist: **the intentionality of the aggressor's actions - the vulnerabilities of the attacked - the capabilities of the aggressor**. This demonstrates that the threats resulting from hybrid action are variable, making it difficult for the attacked to recognise and respond to them, which takes time. This requires greater attention and focus at the strategic-political level. It is therefore necessary to implement appropriate legal regulations and security rules in response to specific threats. This should take into account technological advances, as well as cooperation between the private sector and state institutions, research centres and NGOs. It can be assumed that building the resilience of the state also means expanding knowledge of contemporary threats.

Given the uncertainty and complexity of global interdependencies, state resilience should be seen as a deliberate activity of the state - aimed at identifying

the factors that cause threats and focused on building efficient state structures that have the ability to also establish relationships with non-state actors operating inside and outside the country. Only such activities will guarantee the state's ability to protect itself from contemporary threats or reduce the risk of their occurrence.

Bibliography

Antczak A., *Rola aktorów niepaństwowych w kształtowaniu bezpieczeństwa* (Eng. The role of non-state actors in shaping security), "Środkowoeuropejskie Studia Polityczne" 2017, no. 3, pp. 143–158. https://doi.org/10.14746/ssp.2017.3.7.

Bartoszewicz M., *Definicje legalne w świetle zasady określoności prawa* (Eng. Legal definitions in the light of the principle of legal certainty), in: *Dookoła Wojtek… Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Preisnerowi*, R. Balicki, M. Jabłoński (eds.), Wrocław 2018, pp. 355–364.

Bezpieczeństwo międzynarodowe po zimnej wojnie (Eng. International security after the Cold War), R. Zięba (sci. ed.), Warszawa 2008.

Ciechanowski G., *Wstęp* (Eng. Introduction), in: *Współczesne zagrożenia bezpieczeństwa*, G. Ciechanowski, M. Romańczuk (eds.), Szczecin 2017, pp. 7–8.

Ciechański J., *Enklawy transnarodowe w zdecentralizowanym prawie międzynarodowym* (Eng. Transnational enclaves in decentralised international law), in: *Stosunki międzynarodowe. Geneza, struktura, dynamika*, E. Haliżak, R. Kuźniar (eds.), Warszawa 2006, pp. 346–348.

Cieślarczyk M., *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i odporności państwa* (Eng. Theoretical and methodological basis for the study of state security and resilience problems), Siedlce 2009.

Cziomer E., Lasoń M., *Podstawowe pojęcia i zakres bezpieczeństwa międzynarodowego i energetycznego* (Eng. Basic concepts and scope of international and energy security), in: *Międzynarodowe bezpieczeństwo energetyczne w XXI wieku*, E. Cziomer (ed.), Kraków 2008, pp. 13–28.

Fjäder Ch., *The nation-state, national security and resilience in the age of globalisations*, "Resilience: International Policies, Practices and Discourses" 2014, vol. 2, no. 2, pp. 114–129. https://doi.org/10.1080/21693293.2014.914771.

Górska-Rożej K., *Kształtowanie odporności na zagrożenia w społecznościach lokalnych* (Eng. Building resilience in local communities), "Przegląd Policyjny" 2018, no. 1, pp. 54–65. https://doi.org/10.5604/01.3001.0013.6643.

Gruszczak A., *Hybrydowość współczesnych wojen – analiza krytyczna* (Eng. Hybridity of modern warfare - a critical analysis), in: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (eds.), Warszawa 2011, pp. 9–17.

Keplin J., *Analityczny model działań hybrydowych narzędziem wspomagającym bezpieczeństwo państwa* (Eng. Analytical model of hybrid operations a tool to support state security), in: *Współczesne zagrożenia bezpieczeństwa*, G. Ciechanowski, M. Romańczuk (eds.), Szczecin 2017, pp. 127–138.

Keplin J., *Działania hybrydowe jako niewidzialne zagrożenia* (Eng. Hybrid activities as invisible threats), in: *Wojna Federacji Rosyjskiej z Zachodem*, M. Banasik (ed.), Warszawa 2022, pp. 163–186.

Keplin J., *Działania hybrydowe na Morzu Bałtyckim. Zarys problemu dla bezpieczeństwa Rzeczypospolitej Polskiej* (Eng. Hybrid activities in the Baltic Sea. Outline of the problem for the security of the Republic of Poland), "De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2022, vol. 8, no. 2, pp. 54–68. https://doi.org/10.34739/dsd.2022.02.04.

Kilcullen D., *The Accidental Guerrilla*: *Fighting Small Wars in the Midst of Big One*, New York 2009.

Kopczewski M., *Bezpieczeństwo wewnętrzne państwa – wybrane elementy* (Eng. Internal security of the state - selected elements), "Doctrina. Studia społeczno-polityczne" 2013, no. 10, pp. 103–122.

Kubiak M., *Zarządzanie kryzysowe a bezpieczeństwo narodowe w dobie zagrożeń hybrydowych* (Eng. Crisis management and national security in the age of hybrid threats), "Biuletyn Kwartalny Biura Analiz i Reagowania RCB" 2018, no. 24, pp. 3–5.

Lasoń M., *Bezpieczeństwo w stosunkach międzynarodowych* (Eng. Security in international relations), in: *Bezpieczeństwo międzynarodowe w XXI wieku. Wybrane problemy*, E. Cziomer (sci. ed.), Kraków 2010, pp. 9–32.

Liedel K., *Zagrożenia hybrydowe. Jak zmienia się środowisko bezpieczeństwa RP?* (Eng. Hybrid threats. How is the Polish security environment changing?), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, special edition: *Hybrid warfare*, pp. 51–58.

Ligęza K., Iwanina-Szopińska E., *Zabezpieczenie logistyczne ludności poszkodowanej w sytuacjach kryzysowych w aspekcie zapewnienia bezpieczeństwa* (Eng. Logistics security for affected populations in emergency situations), in: *Paradygmaty badań nad bezpieczeństwem. Zarządzanie kryzysowe w teorii i praktyce*, M. Kopczewski, I. Grzelczak-Miłoś, M. Walachowska (sci. eds.), Poznań 2013, pp. 353–364.

Mazur-Bubak M., *Wybrane teorie leżące u podstaw współczesnego paradygmatu wojny* (Eng. Selected theories underlying the contemporary paradigm of war), "Internetowy Magazyn Filozoficzny Hybris" 2015, no. 30, pp. 74–93.

Mierzejewski D.J., *Bezpieczeństwo europejskie w warunkach przemian globalizacyjnych* (Eng. European security under the impact of globalisation), Toruń 2011.

Mokrzycki J., Pawlak C., *Budowanie odporności państwa gwarancją jego bezpieczeństwa* (Eng. Building the resilience of the state as a guarantee of its security), in: *Kształtowanie przestrzeni bezpieczeństwa państwa*, G. Ciechanowski, K. Ligęza, A. Rurak (sci. eds.), Gdynia 2019, pp. 35–46.

Ochmann P., Wojas J., *Wojna hybrydowa jako przykład umiędzynarodowionego konfliktu wewnętrznego* (Eng. Hybrid warfare as an example of internationalised internal conflict), "Studia Prawa Publicznego" 2018, no. 2, pp. 101–121. https://doi.org/10.14746/spp.2018.2.22.5.

Pawlak C., Keplin J., *Aneksja Krymu w kontekście działań hybrydowych* (Eng. Annexation of Crimea in the context of hybrid activities), "Kwartalnik Bellona" 2016, no. 3, pp. 23–32.

Popiuk-Rysińska I., *Instytucje międzynarodowe* (Eng. International institutions), in: *Stosunki międzynarodowe. Geneza, struktura, dynamika*, E. Haliżak, R. Kuźniar (eds.), Warszawa 2006, pp. 353–375.

Pospisil J., *The Resilient State: New Regulatory Modes in International Approaches to State Building*?, "Third World Quarterly" 2016, vol. 37, no. 1, pp. 1–16. https://doi.org/10.1080/01436597.2015.1086637.

Rácz A., *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*, Helsinki 2016.

Rokiciński K., *Ewolucja postrzegania zagrożeń asymetrycznych* (Eng. Evolution of the perception of asymmetric threats), in: *Acti Labores Lucundi. Studia ofiarowane Leopoldowi Ciborowskiemu w siedemdziesiątą rocznicę urodzin*, M. Zieliński, B. Pączek (eds.), Gdynia 2014.

Rokiciński K., *Wybrane aspekty zagrożeń asymetrycznych na morzu w funkcji wykorzystania sił morskich* (Eng. Selected aspects of asymmetric threats at sea as a function of the use of naval forces), "Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, y. 46, no. 1, pp. 151–171.

Schuman T., *Love Letter to America*, Los Angeles 1984.

Sekściński A., *Bezpieczeństwo wewnętrzne w ujęciu teoretycznym. Geneza i współczesne rozumienie w naukach politycznych* (Eng. Internal security in theoretical terms. Origins and contemporary understanding in political science), "Kwartalnik Naukowy OAP UW e-Politikon" 2013, no. 6, pp. 42–79.

Słownik angielsko-polski (Eng. English-Polish dictionary), Oxford 2002.

Słownik terminów z zakresu bezpieczeństwa narodowego (Eng. Dictionary of national security terms), issue 6, Warszawa 2008.

Soloch P., Pietrzak P., *Szczyt NATO w Warszawie: uwarunkowania, rezultaty, wnioski dla Polski* (Eng. NATO summit in Warsaw: conditions, results, conclusions for Poland), "Bezpieczeństwo Narodowe" 2016, no. 37–40, pp. 13–31.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (Eng. National Security Strategy of the Republic of Poland), Warszawa 2022, p. 10.

Sułek M., *Prognozowanie i symulacje międzynarodowe* (Eng. International forecasting and simulation), Warszawa 2010.

Świeboda H., *Prognozowanie zagrożeń bezpieczeństwa narodowego Rzeczypospolitej Polskiej* (Eng. Forecasting threats to the national security of the Republic of Poland), Warszawa 2017.

Usewicz T., Keplin J., *Hybrid Actions and Their Effect on EU MaritimeSecurity*, "Journal on Baltic Security" 2023, vol. 9, no. 1, pp. 32–68. https://doi.org/10.57767/jobs_2023_001.

Zacher L.W., *Problemy i metody przewidywania przyszłości (przegląd tendencji w literaturze)* (Eng. Problems and methods of predicting the future (review of trends in the literature)), in: *Czy warto myśleć o przyszłości?*, Warszawa 1996, pp. 1–105.

Zacher L.W., *Trwały rozwój – utopia czy realna możliwość?* (Eng. Sustainable development - utopia or a real possibility?), "Problemy Ekorozwoju – Problems of Sustainable Development" 2008, vol. 3, no. 2, pp. 63–68.

Zasadzińska-Baraniewska A., *Zarządzanie kryzysowe wobec nowego typu zagrożeń – spotkanie eksperckie w Rządowym Centrum Bezpieczeństwa* (Eng. Crisis management in the face of a new type of threat - expert meeting at the Government Centre for Security), "Biuletyn Kwartalny Biura Analiz i Reagowania RCB" 2017, no. 19, pp. 3–5.

Zdrodowski B., *Istota bezpieczeństwa* (Eng. The essence of security), in: *Wybrane problemy bezpieczeństwa wewnętrznego państwa*, A. Misiuk (ed.), vol. 34, Warszawa 2014, pp. 32–50.

Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje – struktury – funkcjonowanie* (Eng. Institutionalisation of European security. Concepts - structures - functioning), Warszawa 2004.

Zięba R., *Współczesne wyzwania i zagrożenia dla bezpieczeństwa międzynarodowego* (Eng. Contemporary challenges and threats to international security), "Stosunki Międzynarodowe – International Relations" 2016, vol. 52, no. 3, pp. 9–31. https://doi.org/10.7366/020909613201601.

Internet sources

Bolzen S., *"Die NATO muss auf grüne Männchen vorbereitet sein"*, Die Welt, 17 VIII 2014, http://www.welt.de/politik/ausland/article131296429/Die-Nato-muss-auf-gruene-Maennchen-vorbereitet-sein.html/ [accessed: 27 I 2015].

Budowanie odporności państw członkowskich sojuszu – implementacja wytycznych NATO (Eng. Building the resilience of alliance member states - implementation of NATO guidelines), Rządowe Centrum Bezpieczeństwa, 21 XII 2017, https://rcb.gov.pl/budowanie-odpornosci-panstw-czlonkowskich-sojuszu-implementacja-wytycznych-nato/ [accessed: 20 XII 2018].

Commitment to enhance resilience, North Atlantic Treaty Organization, 8 VII 2016, https://www.nato.int/cps/en/natohq/official_texts_133180.htm [accessed: 21 VIII 2022].

Cullen P., *Hybrid threats as a new 'wicked problem' for early warning*, Hybrid CoE, 4 VI 2018, https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-8-hybrid-threats-as-a-new-wicked-problem-for-early-warning/ [accessed: 12 X 2018].

https://mediweb.pl/slownik-nauk-i-specjalnosci-lekarskich [accessed: 20 VIII 2022].

Jadczak A., *Zaatakowana przez hakerów DigiNotar ogłosiła upadłość* (Eng. DigiNotar, attacked by hackers, has declared bankruptcy), Computer World, 23 IX 2011, https://www.computerworld.pl/news/Zaatakowana-przez-hakerow-DigiNotar-oglosila-upadlosc,375383.html [accessed: 4 I 2019].

Lorenz W., *Szczyt NATO w Brukseli – przełomowy moment dla Sojuszu* (Eng. NATO summit in Brussels - a breakthrough moment for the Alliance), PISM, 15 VI 2021, https://www.pism.pl/publikacje/Szczyt_NATO_w_Brukseli__przelomowy_moment_dla_Sojuszu [accessed: 10 VII 2022].

Matyasik G., *Jak wygląda polska odporność?* (Eng. What does Polish resilience look like?), INFOSECURITY24, 4 IV 2023, https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/jak-wyglada-polska-odpornosc [accessed: 10 IX 2023].

MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare, https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf [accessed: 7 X 2022].

NIK o bezpieczeństwie danych (Eng. NIK on data security), Najwyższa Izba Kontroli, 16 V 2016, https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-danych.html [accessed: 18 XI 2018].

Odporne NATO (Eng. Resilient NATO), Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/odporne-nato/ [accessed: 20 XII 2020].

Odporność na zagrożenia tematem seminarium RCB (Eng. Resilience to threats was the topic of an RCB seminar), Rządowe Centrum Bezpieczeństwa, 13 III 2017, https://rcb.gov.pl/odpornosc-na-zagrozenia-tematem-seminarium-rcb/ [accessed: 20 XII 2018].

Opas R., *Użyją art. 5? Stoltenberg nie wyklucza* (Eng. Will they use Article 5? Stoltenberg does not rule out), Wiadomości WP, 11 X 2022, https://wiadomosci.wp.pl/uzyja-art-5-stoltenberg-nie-wyklucza-6821910367021888a [accessed: 11 X 2022].

Raubo J., *GlobState III, czyli zrozumieć świat i wykorzystać wiedzę do budowania sił zbrojnych* (Eng. GlobState III, or understanding the world and using knowledge to build forces), Defence24, 13 XII 2020, https://defence24.pl/sily-zbrojne/globstate-iii-czyli-zrozumiec-swiat-i-wykorzystac-wiedze-do-budowania-sil-zbrojnych-komenatrz [accessed: 7 VII 2022].

Reichborn-Kjennerud, E., Cullen P., *What is Hybrid Warfare?*, Norwegian Institute of International Affairs, 2016, https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf [accessed: 1 XII 2022].

Słownik języka polskiego PWN (Eng. PWN Dictionary of the Polish language), https://sjp.pwn.pl/slowniki/odporno%C5%9B%C4%87.html [accessed: 20 VIII 2022].

Williams J.W., *Critical Energy Infrastructure Protection Policy Research Series: Al-Qaida threats and strategies: the religious justification for targeting the international energy economy*, The Canadian Centre of Intelligence and Security Studies at Carleton University, March 2008, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.612.473&rep=rep1&type=pdf, [accessed: 17 XI 2018].

Wytrzymałość materiałów – rodzaje, co to jest? (Eng. Strength of materials - types, what is it?), EBMIA, 30 VIII 2021, https://www.ebmia.pl/wiedza/porady/obrobka-porady/wytrzymalosc-materialow-rodzaje/ [accessed: 23 VII 2022].

Lt Cdr (ret) Jarosław Łukasz Keplin, PhD

Doctor in the field of social sciences in the discipline of security sciences, Assistant Professor at the Department of Internal Security of the Department of National Security at the Pomeranian University in Słupsk. He served, among others, in the Submarine Squadron, 3rd Flotilla of Ships, worked in the Centre for Doctrine and Training of the Armed Forces. He has participated in missions abroad. His research interests include national and international security issues, problems of threat identification and analysis, and forms of influence of states and non-state actors on state security.