Teka Komisji Prawniczej PAN Oddział w Lublinie, vol. XVII, 2024, no. 2, pp. 349-363
https://doi.org/10.32084/tkp.9050

STATE'S RESILIENCE TO CRITICAL INFRASTRUCTURE THREATS: THE EXAMPLE OF THE RUSSIAN WAR ON UKRAINE

Dr. Piotr Ostrowski

University of Szczecin, Poland
e-mail: piotr.ostrowski@usz.edu.pl; https://orcid.org/0000-0001-7851-4683

Dr. Radosław Zych

University of Szczecin, Poland
e-mail: radoslaw.zych@usz.edu.pl; https://orcid.org/0000-0002-1221-9136

Abstract. The security environment is increasingly complex and uncertain today. This directly impacts the directions of Poland's national security transformation, especially the country's resilience to hybrid threats and war. One such area is threats facing critical infrastructure, facilities of strategic importance as well as services critical to state security and citizens. The article aims to present the way of understanding and building the state's resilience based on the current legislation on the protection of critical infrastructure against hybrid threats and war, based on the example of Russia's armed aggression against Ukraine. The following research question was posed: Does the current legislation defining the tasks of state and private entities responsible for the protection of facilities, equipment, services of so-called critical infrastructure and the adopted system solutions correspond to modern threats? Our study highlights inconsistencies and gaps in the current legislation on the state's resilience to hybrid threats and war.

Keywords: critical infrastructure; threats; security; state's resilience; law.

INTRODUCTION

Security is a core value in the hierarchy of human needs that has always been challenged. Security informs the social life of citizens and their relationship with the state. The modern world is perceived by the international community mainly through the lens of globalization, which rests on three processes: the tightening of bonds between countries, states' diminished impact on the economy, and technological progress [Mierzejewski 2011, 23-24]. One effect of globalization is change, not only in the political arena, but also in the economic, social or cultural spheres. These phenomena greatly contribute to the rise of specific challenges and threats, which are becoming

ISSN 1899-7694
e-ISSN 2719-7379

increasingly diverse, such as terrorism, cyber-terrorism, hybrid operations (below the threshold of war), or direct military engagement. Another type of threat that is less overt in nature is disinformation activities intended to put political, including economic or social pressure on states and other non-state actors, using, among other things, manipulated media. The dissemination of false information and so-called "fake news" is an instrument for waging propaganda and information-psychological war aimed at making society more polarised and interfering with democratic processes. Increasingly, there are differences in the perception of the interests of nation-states and the globalization processes taking place. They are taking various forms as new political and social movements are launched and new ideological postulates are made, such as those challenging the liberalization of international trade or the idea of supranational structures of integration. The international order is revised again and again. Such changes follow mainly from the aspirations of individual states to play a major roles regionally or globally. The superpower motivations of various states are due to differences in their interests, but they are united by a common belief that it is necessary to curb the dominance of the United States of America. In many cases, demands to revise the international order can also be linked to ambitions for territorial expansion.[1] An example of a state that takes various measures to strengthen its position in the world is the Russian Federation. Its neo-imperial policy is being implemented in violation of international law, by infringing on international agreements and treaties and making attempts to destabilize Western integration structures. The greatest threat is the use of coercion in relations with other states and the use of military force. The 2008 military aggression in Georgia, the illegal annexation of Crimea and the seizure of eastern Ukraine in 2014 shook the foundations of the Euro-European security system. Russia's superpower aspirations and further territorial expansion were shown by the use of military force in 2022 in its armed assault on the Ukrainian territory. The full-scale war in Ukraine, which has been going on for more than two years now, poses a direct threat to Poland and other Central and Eastern European countries. The war on Ukraine has exposed Russia's aspiration and goal of reshaping the world order and establishing a new regional order. The methods employed by the Russian army operating in Ukraine testify to violations of international laws – from the UN Charter[2] to the Geneva Convention for the Protection of Victims of War (12 August 1949)[3] and the Additional Protocols to the Geneva Conventions relating to the Protection of Victims of International Armed Conflicts (Protocol I) and the Protection of Victims

[1] See https://www.gov.pl/web/obrona-narodowa/rodowisko-bezpieczenstwa-rp [accessed: 30.05.2024].

[2] Journal of Laws of 1947, No. 23, item 90.

[3] Journal of Laws of 1956, No. 38, item 171.

of Non-International Armed Conflicts (Protocol II), drawn up in Geneva on 8 June 1977.[4] Attacks and bombings on key critical infrastructure and services that are essential to the functioning of civilians, damaging city power systems, the destruction of transport networks, communications, medical care facilities, food production and distribution channels, all demonstrate the tremendous effort Ukraine must undertake to defend itself.

A country's defence capabilities imply its ability to conduct effective defence activities, protect its citizens, and the entirety of national heritage [Wojnarowski 2014, 69]. According to Jan Wojnarowski, state defence capabilities are a totality of measures undertaken and is the focus of the entire state apparatus, public administration and the state economy [Idem 2005, 5]. It can be assumed that state defence is related to the activities undertaken by the entire state aimed at countering military and non-military threats, using all its instruments, tools and resources.

State defence is closely linked to state resilience. Resilience, which is the maintenance and development of capabilities in the civilian and military spheres serving to considerably hamper hostile actions, is regarded as one of the preconditions for state security [Rey 2022]. Resilience is built in response to diverse regional threats, including hybrid and increasingly global threats. Every state is obliged to build up its resilience [ibid.].

In the literature on the subject we find many publications on state resilience [Fjäder 2014,114-29; Pospisil and Kühn 2016, 1-16; Nowak 2022, 29-50; Keplin 2023, 13-38] built in response to threats caused not only by armed conflicts but also by other natural or technological factors caused by human error. The subject of this paper aligns with the research on state policies to tackle security threats. Over the past few years, this area of research has been the object of constant interest for researchers in Poland and abroad.

This paper seeks to present the way of understanding and building state resilience based on the current legislation on the protection of critical infrastructure against hybrid threats and war, using the example of Russia's armed aggression in Ukraine. The following research problem was conceived: Do the current legislation defining the tasks of state and private entities responsible for the protection of facilities, devices, services of so-called "critical infrastructure" and the adopted system solutions correspond to modern threats? To address the research problem, we used various research methods, such as the qualitative method, document research method, system analysis, inductive and eliminative reasoning.

[4] Journal of Laws of 1992, No. 41, item 175.

1. NORMS GOVERNING THE PROTECTION OF CRITICAL INFRASTRUCTURE AND FACILITIES OF STRATEGIC IMPORTANCE

Today, issues related to critical infrastructure are presented in the context of its protection. The uninterrupted operation of critical infrastructure ensures a required standard and continuity of distribution of services, for which the state is responsible. The protection of critical infrastructure is an obligation arising from legal norms, which means that its owners, administrators of facilities, installations and devices are under a legal obligation to protect them against various hazards. The concepts of critical infrastructure and its protection are defined in the Crisis Management Act.[5] According to Article 3(2), "critical infrastructure comprises systems and their components consisting of functionally related objects, including built structures, equipment, installations, services of key importance to the security of the state and its citizens and assurance of the proper functioning of public administration bodies, institutions and entrepreneurs. Critical infrastructure encompasses: (a) systems that supply energy, energy resources and fuels, (b) communication systems, (c) information and, communication technology networks, (d) financial systems, (e) food supply, (f) water supply, (g) health care, (h) transportation, (i) rescue systems, (j) systems ensuring the continuity of public administration, (k) production, storage, storage and use of chemical and radioactive substances, including pipelines for dangerous substances." Defined in this way, the concept of critical infrastructure and the catalogue of its component systems shows the great importance of their proper functioning for the security of the state and its citizens.

Now, the statutory concept of critical infrastructure protection, as defined in Article 3(3) of the 2007 Act, is understood as all activities aimed at ensuring the functionality, continuity of operations and integrity of critical infrastructure in order to prevent hazards, risks or vulnerabilities, and to mitigate and neutralize their effects, as well as to rapidly restore such infrastructure in the event of failures, attacks and other occurrences disrupting its proper functioning.

It transpires from this definition that critical infrastructure is of crucial importance to the state as a territorial community and an organization that encompasses the general public residing in its territory. Therefore, the legislator has imposed a legal duty of protection as specified in Article 6(5), in such a way that "the owners, as well as independent or dependent possessors of facilities, installations or devices of critical infrastructure are obliged to protect them, in particular by preparing and implementing, according

[5] Act of 26 April 2007 on Crisis Management, Journal of Laws of 2023, item 122 [henceforth: 2007 Act].

to anticipated risks, plans for the protection of critical infrastructure, and maintaining their own reserve systems to ensure the security of this infrastructure and sustain its infrastructure, until it is fully restored." This means that managers of facilities, installations and devices are obliged by the law to protect critical infrastructure. If its functioning is disrupted, state institutions may lose their capability, in part or in whole, to perform their basic administrative and service functions, and to exercise effective control over their entire territory. The statutory regulations are supplemented by the National Programme for the Protection of Critical Infrastructure,[6] intended to improve critical infrastructure security. Among other things, the programme defines the goals, requirements, and standards to ensure the efficient functioning of critical infrastructure. It also includes detailed criteria that make it possible to determine which facilities, equipment and services are part of critical infrastructure systems.

National regulations and system solutions regarding the protection of areas, facilities, devices, installations and services have many underpinnings in statutory regulations that variously classify facilities under special protection and specify different organisation, responsibilities and competences necessary to protect them. This legal dualism impedes the unification of the system of protection of critical infrastructure facilities or, more broadly, facilities of strategic importance for state security. The first Polish regulations legislated a decade earlier than the Crisis Management Act, concerning the mandatory protection of areas, facilities and devices are found in the Act of 22 August 1997 on the Protection of Persons and Property.[7] The types of respective facilities are mentioned in Article 5(2), including in particular: 1) state defence facilities, 2) facilities serving to protect the economic interest of the state, 3) public security facilities, 4) facilities serving to protect other important interests of the state, 5) facilities, including construction structures, devices, installations, services included in the unified list of facilities, installations, equipment and services included in critical infrastructure.

According to the wording of Article 5(1) the legislator specified that the areas, facilities, devices and transports important for the defence system, the state's economic interest, public security and other important interests of the

---

[6] Resolution No. 2010/2015 of the Council of Ministers of 2 November 2015 on the adoption of the National Programme for the Protection of Critical Infrastructure, taking into account Resolution No. 116/2020 of the Council of Ministers of 13 August 2020 amending the Resolution on the adoption of the National Programme for the Protection of Critical Infrastructure and Resolution No. 38/2023 of 21 March 2023 amending the Resolution on the adoption of the National Programme for the Protection of Critical Infrastructure, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [accessed: 03.06.2024].

[7] Act of 22 August 1997 on the Protection of Persons and Property, Journal of Laws of 2021, item 1995.

state mentioned in this law are subject to mandatory protection of specialized armed protective formations or an adequate technical security system.

Another group of facilities under special and mandatory protection are marine and port facilities and installations. Legal regulations in this area of the state's responsibility are found in the Act of 4 September 2008 on the Protection of shipping and seaports.[8] The Act specifies the rules of ship and seaport protection, including the protection of the life and health of the personnel of seaports, port facilities or ships, in accordance with the requirements set forth in international regulations governing the safety of life at sea and the protection of ships and port facilities. This act, adopted at the time by the Polish Parliament, transposed within the scope of its regulation Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security.[9] Considering the growing risks of sabotage, terrorist and diversion, the act was amended to expand the range of the state's obligations to enhance the protection of port facilities, marine devices and installations. Security rules have also been defined concerning: 1) the Baltic Pipe, an inter-system gas pipeline linking the transmission systems of Poland and Denmark, together with the infrastructure necessary for its operation in the sea territories of the Republic of Poland; 2) facilities, equipment and installations that are part of the infrastructure providing access to ports of primary importance to the national economy; 3) all kinds of structures and equipment used in the exclusive economic zone of artificial islands and intended for the exploration or exploitation of resources, as well as other projects for the economic exploration and exploitation of the exclusive economic zone, in particular for energy purposes, including offshore wind farms in the meaning of Article 3 item 3 of the Act of 17 December 2020 on Promoting Energy Production in Offshore Wind Farms,[10] and sets of devices for power derivation in the meaning of Article 3 item 13 of the Promotion Act, as well as submarine electricity and fibre optic networks or pipelines, and related infrastructure; 4) the liquefied natural gas regasification terminal in Świnoujście.

The entities responsible for ship and port security are not only port managers, but also ministers, heads of central offices, provincial governors, directors of maritime offices listed in Article 4 of the Act. On the other hand, the entities responsible for the prevention, reduction or removal of a direct threat including terrorist threats to the listed facilities according to Article 27 of the Act are: the Internal Security Agency, the Polish Armed Forces, the Police, and the Border Guard.

---

[8] Act of 4 September 2008 on the Protection of Ships and Seaports, Journal of Laws of 2024, item 597.

[9] OJ L 310/28, 25.11.2005.

[10] Journal of Laws of 2024, item 182.

Legal regulations on the protection of critical infrastructure also apply to services that are key to state security. Responsibilities concerning the security of this sensitive infrastructure are regulated in the Act of 5 July 2018 on the National Cyber Security System. The inclusion of this legislation in the national legal order implements the EU Directive on ensuring a high common level of security of information networks and systems within the territory of the European Union.[11] The system is intended to ensure cybersecurity at the national level by ensuring the uninterrupted provision of both key and digital services, and an appropriate level of security for the ICT systems used to provide these services. Supervised by the Ministry of Digitization, the system includes operators of key services (such as the energy, transportation, health and banking sectors), digital service providers. The statutory regulations on the cybersecurity policy were further developed by the Resolution of the Council of Ministers No. 125 of 22 October 2019, adopting the Cyber Security Strategy of the Republic of Poland 2019-2024.[12] The strategy extends the activities undertaken by the government administration and aimed at raising the level of cybersecurity. It defines strategic goals and relevant policy and regulatory measures aimed at achieving a high level of cybersecurity – that is, above all, the resilience of the information systems of key service operators, critical infrastructure operators, digital service providers, and the resilience of public administration to cyberthreats.

Another piece of legislation comprehensively regulating the duty to defend the State is the Homeland Defence Act.[13] By providing a special regulation in a crucial area represented by the constitutional duty to defend the state, this law, among other things, specifies the competence of authorities in cases when a request is made to recognise a facility as particularly important for the security or defence of the state (Articles 614 and 617). Tasks relating to the protection of objects of special importance for the security or defence of the state are found in section 20, "Militarization and protection of objects of special importance for the security or defence of the state."

Another area of protection that is important for state security and defence is the 2020 Strategic Reserves Act.[14] According to Article 3, Strategic reserves shall be created to counteract threats to state security and defence, security, public order and health, and the occurrence of a natural disaster or crisis a situation, for the purposes of supporting the performance of tasks in the area of state security and defence, restoration of critical infrastructure,

---

[11] This Act, within the scope of its regulation, implements Directive 2016/1148 of the European Parliament and of the Council (EU) of 6 July 2016 on measures for a high common level of security of networks and information systems within the Union, OJ L 194/1, 19.7.2016.

[12] "Monitor Polski" of 2019, item 1037.

[13] Act of 11 March 2022 on the Defence of Fatherland, Journal of Laws of 2024, item 248.

[14] Act of 17 December 2020 on Strategic Reserves, Journal of Laws of 2023, item 294.

mitigation of disruptions in the continuity of supplies serving the functioning of the economy and meeting the basic needs of citizens, saving their lives and health, realisation of the national interests of the Republic of Poland in the field of national security, fulfilling its international obligations, as well as providing assistance and support to entities of public international law.

Another matter regulating critical infrastructure security is the 2002 Aviation Act.[15] This legislation not only regulates the sphere of legal relations in the field of civil aviation (Article 1(1)), but also matters relating to protection against destruction of or damage to aviation airport devices, ground or onboard devices, disruption of their operation or serious damage to the persons operating such devices when this causes a significant disruption to air traffic or the operation of an airport or a threat to the safety of civil aviation (Article 2(20)). The act also defines physical protection of aircraft. The above security areas are part of critical infrastructure.

The critical infrastructure protection zone also includes railway areas. The 2003 Railway Transport Law,[16] specifies rules for the management of railway infrastructure (Article 1). The act defines terms such as, among others, a railway with defensive significance, a railway of state importance, whose maintenance and operation is justified by state defence, including the needs of the Polish Armed Forces and allied troops in times of the State's increased defence readiness, as well as in wartime, intended to be covered by technical protection (Article 4, points 2a, 2b).

The network of key services, which are telecommunications services, is another zone of critical infrastructure protection. The 2004 Telecommunications Law[17] imposes tasks and obligations on telecommunications entrepreneurs for the benefit of defence, state security and public safety and order, in the field of telecommunications. Pursuant to Article 179(2), a telecommunications entrepreneur is obliged to perform tasks and duties in the preparation and maintenance of designated elements of telecommunications networks for the provision of telecommunications for the direction of the national security management system, including state defence, carried out under the terms specified in plans, decisions or agreements concluded between telecommunications entrepreneurs and authorized entities.

Another area of responsibility related to the protection of critical infrastructure and defence issues is the legal regulations under the 2003 act on spatial planning and development.[18] According to Article 1(2), "planning and spatial development shall take into account, among others, the needs of state

[15] Act of 3 July 2002, the Aviation Law, Journal of Laws of 2023, item 2110.
[16] Act of 28 March 2003, the Railway Transport Law, Journal of Laws of 2024, item 697.
[17] Act of 16 July 2004, the Telecommunications Law, Journal of Laws of 2014, item 243.
[18] Act of 27 March 2003 on Spatial Planning and Development, Journal of Laws of 2023, item 977.

defence and security, the need to ensure an adequate quantity and quality of water for the population, and the need to prevent serious failures and limit their impact on human health and the environment. It is the responsibility of state and local government bodies to implement tasks related to state defence and the protection of elements of essential infrastructure for the population.

Another legal act regulating special protection of facilities important for state defence or security is the Decree of the Council of Ministers of 21 April 2022 on facilities particularly important for state security or defence and their special protection.[19] The decree specifies the types of facilities of special importance for state defence or security by assigning them to one of two the categories, the procedure for recognizing facilities as particularly important for state defence or security and for their loss of such character, and activities necessary to prepare special protection of facilities (§§ 2, 3, 8).

The above presentation of the most important legislation in force in the national legal system demonstrates the multidimensionality and multifaceted nature of critical infrastructure protection. This is reflected in the definition of the concepts of critical infrastructure and other important facilities, areas and equipment subject to special protection. Critical infrastructure protection is regulated by many normative acts, which does not favour a unified system allowing essential facilities that are important for state and citizens' security to be protected.

2. RESILIENCE OF NATIONAL CRITICAL INFRASTRUCTURE: THE EXAMPLE OF THE WAR IN UKRAINE

The state's duty to protect the security, rights and freedoms of its citizens is safeguarded by the Constitution of the Republic of Poland.[20] It gives prominence to the security of the state, which is an overriding formula covering both the external and internal spheres of its citizens. From Article 5 of the Constitution stems a norm that constitutes the obligation of Polish State to safeguard the independence and inviolability of its territory, ensure human and civil rights and freedoms, as well as the security of its citizens, protect the national heritage and the natural environment in keeping with the principle of sustainable development. From this norm transpires the obligation of the state to take measures to ensure effective protection of these values. This was accurately expressed by Wojciech Lis: "The obligation to realize the values set forth in Article 5 of the Constitution of the Republic of Poland is absolute, that is, the state cannot evade it. Such an obligation is

[19] Journal of Laws of 2022, item 880.

[20] Constitution of the Republic of Poland of 2 April 1997, Journal of Laws No. 78, item 483 as amended.

first and foremost actualized in a situation of emergency" [Lis 2015, 127]. This opinion implies that the state should be the guarantor of its citizens' security. One of the segments that ensures a smoothly functioning state is critical infrastructure. It is characterized by the streamlined operation of systems and their interrelated facilities, devices, installations, services that are essential for the security of the state and its citizens. The usability of critical infrastructure is intended to ensure the smooth operation of public administration bodies, institutions, and businesses. Disruptions of its functioning can make the State and its institutions lose, in whole or in part, the ability to exercise its constitutional prerogatives and exercise effective control over its entire territory.

The strategic areas outlined in the previous section have necessitated the introduction of legal protective and defensive mechanisms. Protective and defensive undertakings are designed to create proper conditions for the continuity of the national economy if state security were in peril and in the event of war. State resilience is closely linked to defence. In recent years and especially after Russia's assault on Ukraine, the term 'resilience' has appeared frequently in public debates, expert discussions, being also a topic of public interest. Resilience – the maintenance and development of capabilities in the civilian and military spheres that will efficiently counter threats – is one of the basic conditions for state security. Today, if we look at the war in Ukraine, we see the need for building resilience within society to develop immunity against various types of threats. On the national level, references to state resilience are found in Poland's National Security Strategy, approved by the President of Poland on 12 May 2020.[21] This provision is no longer binding as its legal basis was repealed in 2022.[22] The introduction to this document, in the paragraph describing the security environment, there are references to the need to enhance the resilience of the state and society. Emphasis is laid on increasing the state's resilience to threats by creating a system of universal defence, based on the efforts of the entire nation, and building understanding for the development of Poland's resilience and defence capabilities.

Elements related to Poland's resilience to various kinds of risks are addressed in the National Crisis Management Plan and its amendment adopted by the Council of Ministers on 3 March 2022.

From the presented analysis of the legal tools serving the protection of critical infrastructure and the adopted state resilience solutions, it is clear

[21] "Monitor Polski" of 2020, item 413.

[22] The Order of the President of the Republic of Poland of 12 May 2020 on the Approval of the National Security Strategy of the Republic of Poland was repealed by the Act of 11 March 2022 on Homeland Defence.

that at the national level there are various operational systems designed to neutralize risks, but they are often not integrated with one another in terms of their scope and personnel involved. The existing legal regulations come from various sources and affect a multi-faceted obligation to protect critical infrastructure and other facilities of special importance for state defence and security.

Nevertheless, the problem of critical infrastructure protection in Poland calls for a revision of the existing approach to protecting the state and society from threats below the threshold of war and from war itself. The armed aggression in Ukraine has verified the assumptions not only of modern war doctrines, but also of approaches to the protection of civilians. Russian troops are following a scorched-earth tactics, destroying everything they encounter along the way. In addition to this, the aggressor is conducting coordinated, massive air strikes targeting civilian critical infrastructure. Power plants, hospitals, transformer stations, heat and power stations and waterworks have become targets of attacks using remotely controlled rockets and drones. Public transport and food production have been paralysed, and sewage treatment plants have stopped operating. These operations are directly targeting the civilian population, which is struggling with shortages of food, health care, housing, social provisions and other vital goods necessary for survival. At the same time, diversion, sabotage and terrorist actions are being conducted. This painful Ukrainian experience compels us to see what kind of state resilience capacity Poland has in confrontation with armed and hybrid actions conducted by Russia in Ukraine. The public sphere is full of information about the state of Poland's defence preparations for Russia's potential military. Military and civilian experts dealing with issues of contemporary threats and the security environment of Poland present their opinions and assessments of hybrid (sub-threshold) threats and the resilience capabilities of our country. The 10th National Forum for Critical Infrastructure Protection was held in Warsaw on 5 October 2023, during which a report titled "Poland learning from the conclusions and experiences drawn from the analysis of a state's resilience to hybrid (sub-threshold) threats and war" was presented.[23] The report was prepared by the Government Security Centre in cooperation with the Centre's external experts the Centre for Eastern Studies and the Polish Institute of International Affairs. The purpose of the report was to identify challenges and problems in the sphere of civilian operations and to present conclusions and findings relating to Poland's system for enhancing its resilience [Raubo 2023]. This study presents, on the one hand, the identified challenges on the Ukrainian side caused by Russia's armed aggression, and on the other hand, based on

[23] See https://www.gov.pl/web/rcb/x-krajowe-forum-ochrony-infrastruktury-krytycznej-za-nami [accessed:04.06.2024].

the Ukrainian experience, conclusions and proposals for actions to increase Poland's resilience.

As regards critical infrastructure protection, the report contained, among other things, conclusions and proposals to: 1) implement a training and exercise programme for critical infrastructure protection, 2) build backup internet communications including those for unofficial communication, 3) prepare critical infrastructure operators to respond to incidents caused by drones by counteracting threats from unmanned systems to the security of critical infrastructure, 4) safeguard the availability of goods and services in case of supply chains are disrupted, 5) integrate the critical infrastructure protection system with the territorial protection system through its militarization – giving organizational-mobilization assignments and employee mobilization assignments to critical infrastructure personnel and employees of specialized armed protection formations or internal security services [Raubo 2023].

The deliberations also highlighted the need to implement new legislation on cybersecurity protection in the form of: 1) a new act implementing the provisions of the CER Directive[24] and executive regulations; the implementation will consist in amending the Crisis Management Act and establishing a body (or bodies) in charge of enforcing the CER Directive; 2) the implementation of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).[25]

These are directives that Poland must incorporate into the Polish legal system. The report also addresses other areas connected with state resilience. The paper presents only selected aspects associated with the protection of critical infrastructure. The document, which was inspired by the war in Ukraine, shows challenging it is for state and local government bodies to build systemic solutions for state resilience, starting by revising the background of the existing legislation, and then introducing new regulations, based on which new holistic solutions for building state resilience will be created. The report notes the legal gaps and lack of regulation of national law in the implementation of EU directives in the field of cyberthreats, among others, based on Ukraine's present war experience. This war teaches that the equipment and installations of key services and critical

[24] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333/164, 27.12.2022

[25] OJ L 333/80, 27.12.2022. See https://www.gov.pl/web/rcb/x-krajowe-forum-ochrony-infrastruktury-krytycznej-za-nami [accessed:04.06.2024].

infrastructure facilities must be kept fully operational at all cost. An important point raised by the report is the intensification of training and exercise related to critical infrastructure protection. Through exercises, employees and management staff consolidate their knowledge of procedures and substantially contribute to the improved ability to protect critical infrastructure by preventing threats and responding appropriately.

On the basis of the presented analysis of the current legislation and the conclusions presented in the report of the Government Security Centre, we can propose that a coherent supra-ministerial civilian and military solutions be developed to integrate the system of the State's resilience to modern threats.

CONCLUSIONS

The military assault on Ukraine has not only changed the security architecture of Central and Eastern Europe, but also completely changed the approach to state defence and resilience to modern threats. The war experience shows a poignant but very instructive lesson in dealing with the Russian army following scorched earth tactics. One of the tactical goals of the aggressor is to totally paralyse Ukraine, disabling its defence forces, destroy key critical infrastructure and command centres, information flow, and cause shockwaves across the nation. Since the beginning of the armed invasion, Poland has been paying more attention to the protection of its critical infrastructure. Legal regulations on critical infrastructure did not appear until 2007 – in the Crisis Management Act, but issues related to the protection of areas, facilities, devices and transport had appeared much earlier (in 1997), when the Act on the Protection of Persons and Property came into force. Also, solutions for the protection of category 1 and 2 facilities were regulated in 2003 in a decree of the Council of Ministers categorising objects of special importance for state defence and security and their special protection (currently the 2022 decree is in force) (CM Decree, 2022). The 2008 act, which is a *lex specialis* for the protection of maritime infrastructure and port facilities and devices, should also not be ignored. The characterization of the current legal acts presented in the section above reveals a range of legal sources regulating matters concerning the protection of facilities of special importance to state security. They apply different methodology in defining criteria of threats, measures for the protection of facilities and devices, various procedures and requirements for agreeing on security plans, as well as ways in which private or state entities can provide protection. Such a diversity of regulations does not favour a unified and holistic approach to protection, and consequently greater organized state resilience to threats to facilities, devices, services essential to the functioning of the state. In practice, this legal chaos is conducive to a diverse approach to

the idea of protection. The current legal state makes it difficult to respond flexibly and quickly to emergencies or other threats requiring a response. A similar diversity of regulations and concepts is visible in the system of state defence management. This state of affairs is described by Julian Maj, who points out that the discourse on the system of state defence management lacks a clear conceptual and legal base [Maj 2013], which impedes the use of terms that can be used equally or understood similarly by most participants of the debate. This applies mainly to concepts such as national defence, defence capabilities, state defence readiness, etc. Since these concepts are mentioned in the Polish Constitution and other normative acts, their meaning must be made unequivocal so that deliberations can be held on the same factual basis [ibid.].

Therefore, the current regulations require a comprehensive, holistic and unified approach to the development of a national model for the protection of critical infrastructure facilities and other facilities that are critical for state security.

It is necessary to take measures to improve the management of facility protection by putting together a range of fragmented regulations applied concurrently. This requires compact and interdisciplinary organisational and legal solutions in this area, aimed at creating an integrated system of national security management. The crucial link within this model must be a body coordinating work at the governmental level. The experience of the war in Ukraine shows how important it is to establish a central coordinating body for the protection of critical infrastructure. The Ukrainian war experience makes us aware that keeping operational the equipment and installations of key services and critical infrastructure facilities must be a top priority. An extremely important element of the protection of critical infrastructure and other facilities, equipment and installations that are critical for state security is the organisational ability to prevent, prepare for and respond to threats on the part of the managers and staff of these facilities. In this context, it is of utmost importance to intensify training and exercise programmes for the protection of critical infrastructure.

To sum up, the way to increase the State's resilience stipulated in the Polish National Security Strategy of 2020, which was in effect until recently, is not reflected either in the Act on Homeland Defence or in other acts such as the Crisis Management Act or other acts on emergencies. Such solutions should, sooner or later, find their way into a new draft law on civil protection and civil defence.

REFERENCES

Fjäder, Christian. 2014. "The nation-state, national security and resilience in the age of globalisation." *Resilience. International Policies, Practices and Discourses* 2(2):114-29. https://doi.org/10.1080/21693293.2014.914771

Keplin, Jarosław Ł. 2023. "Budowanie odporności państwa na działania hybrydowe." *Przegląd Bezpieczeństwa Wewnętrznego* 29(15):13-38. https://doi.org/10.4467/20801335PBW.23.018.18760

Lis, Wojciech. 2015. *Bezpieczeństwo wewnętrzne i porządek publiczny jako sfera działania administracji publicznej*. Lublin: Wydawnictwo KUL.

Maj, Julian. 2013. "Wybrane aspekty organizacji systemu kierowania obronnością RP i dowodzenia SZ na czas W." In *Minister Obrony Narodowej i Naczelny Dowódca Sił Zbrojnych w Systemie Kierowania Bezpieczeństwem Narodowym RP Wybrane problemy*, edited by Waldemar Kitler, 141-57. Warszawa: AON.

Mierzejewski, Donat J. 2011. *Bezpieczeństwo europejskie w warunkach przemian globalizacyjnych*. Toruń: Adam Marszałek.

Nowak, Tomasz. 2022. "Budowa odporności na obecne i przyszłe zagrożenia o charakterze hybrydowym. Rekomendacje dla Polski." *Roczniki Nauk Społecznych* 14(50):29-50. https://doi.org/10.18290/rns22504.10

Pospisil, Jan, and Florian P. Kühn. 2016. "The resilient state: New regulatory modes in international approaches to state building?" *Third World Quarterly* 37:1-16. https://doi.org/10.1080/01436597.2015.1086637

Raubo, Jacek M. 2023. "Dlaczego Polska nie odrabia ukraińskiej lekcji o odporności?" https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/dlaczego-polska-nie-odrabia-ukrainskiej-lekcji-o-odpornosci-komentarz [accessed: 05.06.2024].

Rey, Robert. 2022. "Społeczeństwo odporne na zagrożenia." https://www.gov.pl/web/rcb/spoleczenstwo-odporne-na-zagrożenia [accessed: 31.05.2024].

Wojnarowski, Jan. 2014. "Dekompozycja Systemu obronnego państwa w systemie bezpieczeństwa narodowego." *Zeszyty Naukowe AON* 4(97). file:///C:/Users/Piotr/Downloads/Decomposition_systemu_obronny_pa%C5%84s%20(1).pdf [accessed: 30.05.2005].

Wojnarowski, Jan. 2005. *System obronności państwa*. Warszawa: AON.