Addressing the Threats to National Security. Poland's Experience

Eugeniusz CIEŚLAK[1]

[1]*Department, Institute of Security Sciences, Faculty of Social Sciences, Siedlce University of Natural Sciences and Humanities, ul. Żytnia 39, 08-110 Siedlce, Polan d, ORCID 0000-0002-6476-3643*

E-mail: [1]eugeniusz.cieslakl@uph.edu.pl

Abstract

The paper provides an assessment of Poland's efforts to address security threats over the last decade. The analysis is limited to energy security, environment protection, cybersecurity and information threats. Governmental strategies, policies and plans are confronted with the assessments of the Supreme Audit Office, academia and think tanks. The paper identifies common challenges related to development and implementation of the state's response to traditional and emerging threats. It also discusses observed trade-offs and consequences of both actions and hesitance to act.

KEY WORDS: *national security, threats, energy security, environment protection, cybersecurity, information threats, Poland*

1. Introduction

Recent decades have become a period in which threats to national security have changed significantly. In addition to threats in the sphere of cyberspace, information threats have appeared, and climate change has been becoming an existential threat for a number of countries. Traditional security threats have not disappeared, but in combination with the new ones, they have created a qualitatively new situation in the security environment. Such a situation makes efforts to ensure national security more and more difficult. Ensuring state security requires precise identification of threats, determining their impact on state security, and then taking actions to mitigate specific threats. Contrary to popular belief about the priorities of states' actions to counter security threats, the situation seems a bit more complicated. New security threats have been not always treated with due care. Spectacular security events have been needed to discover the potential impact of new threats on the security of the state and its citizens. On the other hand, addressing traditional security threats has often required taking actions that radically affected the social order and have not been favourable to the ruling elites. As a result, addressing threats to national security has been often undertaken with delay and the scope of efforts has been limited by political, economic and social factors. This situation may be exemplified by actions taken by Poland over the past decade in relation to threats to energy security, environmental protection and cyber as well as information threats. The comparative analysis aims to identify the differences of approaches while addressing well known, traditional threats to those related to emerging security threats. The research objective is to analyze and evaluate selected actions taken by Poland to minimize security threats. The analysis has been conducted using a unified research framework for selected security threats, taking into account the stages of threats identification, shaping legal and organizational solutions for countering threats, and implementation of actions addressing the threats. The assessment tries to take into account the effects of actions or lack of them to address specific security threats. The analysis and assessment of Poland's efforts in addressing specific threats to national security has been based on the recent public administration documents regarding the assessment of security threats and ways of addressing them. The assessment confronted the assumptions of governmental conceptual documents such as strategies, and policies with the analysis of the effectiveness of governmental actions carried out by the Supreme Audit Office, recognized academic centres and analytical studies of selected think tanks.

2. Addressing Traditional Threats. Energy Security and Environmental Protection

The discussion of Poland's approach to addressing traditional threats may use the example of actions that has been taken in the field of energy security and environmental protection throughout the recent decade. Poland's strategic ambitions related to energy security and environmental protection were published as a part of the Long-term National Development Strategy Poland 2030 "The Third Wave of Modernity", which was adopted in 2013. The strategy defined energy security as ensuring the optimal amount of energy at the lowest possible prices and the diversification of

[1] Corresponding author.
E-mail address: eugeniusz.cieslakl@uph.edu.pl

sources and routes of energy transmission. It was assumed that actions for energy security would take into account the results of economic efficiency analyzes of specific solutions, which would simultaneously implement both elements of the strategic goal. Due to the scale of obligations and implementation costs, the process of reducing CO2 emissions and air pollutants was of particular importance. The strategy assumed also important to take actions for the efficient use of environmental resources. Optimizing the implementation of this task had become one of the most important premises for the formulation of specific objectives. The basis for selecting a strategy for modernizing and expanding the energy sector was the desire to provide consumers with the optimal amount of energy at the lowest possible prices while reducing the pressure on the environment. The long-term development strategy of Poland assumed that the share of coal and lignite in the overall energy balance of Poland would gradually decrease to approx. 50-60% in 2030. Taking into account the structure of the Polish energy sector at that time, relatively low acquisition costs and large domestic resources of coal and lignite it was planned that they both would remain dominant and would allow for long-term stabilization of Poland's energy security. Coal resources were to ensure security of supply for Poland in the perspective of 30-40 years. It was possible, according to the strategy, to achieve that while maintaining the level of investments in the coal mining sector, and improving the efficiency of production units. Poland planned also for the development of clean coal technologies to reduce the emissions of the energy sector. It was also assumed that in order for coal mining to be profitable, it would be necessary to continuously improve the competitiveness of enterprises in this sector.

The long-term development strategy of the country assumed that Poland's participation in the achievement of climate goals would make renewable energy sources one of the most important sources for the power industry. The gross final energy balance assumed reaching the level of 15% from renewable sources in 2020. To achieve this, the implementation of special support tools, such as regulations or fiscal tools, was planned. However; it was emphasized that these tools would have to take into account the primacy of economic efficiency of selected solutions in order to prepare the basis for the future full economic self-sufficiency and competitiveness of the energy sector in Poland. The full cost balance was also to take into account the improvement of the efficiency of renewable distributed energy thanks to the launch of smart grids and the physical proximity of energy generation to the place of its use. The strategy planned also for the synergy of the investments made on the development of the so-called green jobs, especially in the case of distributed energy, bio fuel production, but also environmental infrastructure. The long-term development strategy of Poland took into account the implementation of the nuclear power program as one of the best solutions combining ensuring long-term energy security and stability of electricity supplies along with the implementation of climate and environmental goals. Compared to the coal-based economy, it was assessed that nuclear energy would be an energy source offering additional technological opportunities contributing to lower energy generation costs. Although the investment process was supposed to be long and expensive, the subsequent long-term operations at relatively low operating costs was to make nuclear power the cheapest available source. The costs of nuclear energy was assessed lower to that coal-based already at the cost of CO2 emission allowances above 15Euro per one ton of CO2.

While assessing Poland approach to energy security one has to take into account the synergy of efforts aimed at energy security and environment protection. The long-term development strategy of Poland treated both problems in a balanced way and the protection and improvement of the state of the environment were addresses in a comprehensive way. It was assumed that in 2030 Poland would be a country in which economic growth and social changes would be combined with an improvement in the condition of the environment, considered as a one of the basic conditions for a good quality of life. It was to be possible thanks to the spatial planning system which, from the central to the local levels, was to support the investment decision-making process and, at the same time, to protect particularly valuable natural resources. It was planned that Poland would be a country with assured stable and diversified supplies of fuels and energy, and having adequate strategic reserves. It was assumed to reduce greenhouse gas emissions, e.g. by developing nuclear energy, renewable energy sources and introducing new low- and zero-emission technologies. The necessity of economical and effective management was emphasized, so that energy and natural resources were used rationally. The long-term development strategy of Poland pointed to the growing importance of distributed energy and micro generation, which were to be included in the common smart grid system. Poland was to become a country that effectively reduces greenhouse gas emissions, water and air pollution, eliminates illegal landfills and minimizes the amount of waste going to landfills, and at the same time takes care of preservation of biodiversity and a unique landscape. The vision of Poland in 2030 emphasized the need to effectively identify threats related to the effects of climate change, both those related to the gradual increase in temperature and the increasingly frequent extreme weather phenomena. Poland was supposed to continue the expansion and modernization of the protective infrastructure, adapting to new environmental conditions.

The long-term development strategy of the country formulated a strategic goal of ensuring Poland's energy security and the protection and improvement of the environment. The implementation of this goal was planned through

measures under eight directions of intervention. Activities related to the modernization of infrastructure and energy security were envisaged, including programs encouraging pro-efficiency behavior, diversification of energy sources, including the development of nuclear and distributed energy and fuels and their transmission directions, to ensure Poland's energy security and transformation towards a green economy. In the long-term horizon of the implementation of the strategy, it was assumed that the first block of the first nuclear power plant would be connected to the grid with the prospect of connecting the last block of the second nuclear power plant to the grid around 2030. The strategy also assumed the modernization of electricity and heating networks, increasing energy security by diversifying the directions of obtaining gas and implementing the program of smart grids in the power industry. It was planned to integrate the Polish electricity, gas and fuel markets with regional markets and to strengthen the role of end-users in managing energy consumption.

The strategy assumed that in order to increase the level of environmental protection, improve environmental conditions and reduce the risk associated with climate change, it would be necessary to implement integrated environmental management. The integrated approach was to include the promotion of waste recycling, energy efficiency, efficient use of natural resources, spatial planning with regard to the management of environmentally valuable areas and the protection of water resources. The strategy included a program of adaptation to climate change, minimizing the risks and threats related to the effects of floods and major technological failures. An increase in expenditure on research and development of clean coal technologies and technologies improving the state of the environment was also envisaged throughout the strategy implementation period. The directions of intervention adopted in the long-term development strategy, directly related to the protection and improvement of the natural environment, included the creation of incentives accelerating the development of green economy and increasing the level of environmental protection by protecting water purity, introducing monitoring and protection of biodiversity and counteracting the fragmentation of ecosystems. It was also planned to establish tools for financing biodiversity, including raising the environmental awareness of citizens.

The long-term development strategy of Poland provided for the development and implementation of a strategic plan of adaptation to climate change, including detailed criteria used to define priority investments in the area of the adaptation to climate change, assessment of the current impact and the impact of future climate changes on particularly sensitive sectors and areas. One of the elements of this plan were multi-variant assessments of the risk of natural disasters and appropriate adaptation actions with their estimated costs. Adapting to climate change was to be supported by introducing public policy instruments that would integrate activities in individual sectors of water management, agriculture, forestry, transport, health, construction, spatial management, maritime economy, tourism, energy to increase climate protection. It was assumed that the negative effects of floods would be limited by minimizing the flood risk, implementing an integrated catchment management system and restoring natural water retention. The strategy called also for the implementation of small water retention programs in areas particularly exposed to floods and drought. The threat assessments, objectives and actions envisaged in the long-term development strategy of Poland in relation to energy security and environmental protection were further refined in the medium-term development strategy of the country and the sector strategies. The Strategy "Energy Security and Environment. The Perspective until 2020" was adopted on April 15, 2014. It was one of nine integrated development strategies, created on the basis of the Act of December 6, 2006 on the principles of development policy. The document detailed the provisions of the Mid-Term National Development Strategy 2020 in the field of energy and the environment protection and constituted guidelines for the Polish energy policy. The main objective of the "Energy Security and Environment" Strategy was to ensure a high quality of life for the present and future generations, taking into account environmental protection, and to create conditions for the sustainable development of the modern energy sector, capable of ensuring Poland's energy security as well as a competitive and effective economy. The specific objectives of this strategy included: sustainable management of environmental resources, providing the national economy with a secure and competitive energy supply and improvement of the environment. Moreover; the document also indicated horizontal issues that would span beyond the indicated time perspective.

An assessment of the effectiveness of actions taken in Poland before 2020 in relation to energy security and environmental protection seems a relatively simple task. The strategic documents include tangible indicators for monitoring the implementation of the objectives and statistical data on changes in their values in subsequent years are available. However; a more detailed analysis combined with an assessment of the causes and consequences of the implementation of specific actions in the field of energy security and environmental protection seems more difficult. No doubt, that a number of the objectives related to ensuring Poland's energy security included in the strategic documents have been achieved. The security of supply of energy resources has improved and a risk of using energy supplies by adversary international actors as a political blackmail decreased. The energy efficiency of Poland's economy has increased, which resulted in lower consumption of energy and water by the industry. While assessing Poland efforts to improve its energy security, one has to see also areas where progress did not meet expectations. A

decade ago, basing Poland's long-term energy security on coal and lignite seemed to be a low-risk strategy. It was considered a way to buy time for the development of renewable energy and nuclear energy. Climate changes, which accelerated the decarbonization process, put the rationality of such an approach into question. Any further dependence of the economy on energy obtained from coal seems nowadays both too expensive and not prospective. Sustainment of energy production from coal and lignite has not required significant investments. It has provided Poland a significant margin of energy independence from the import of energy resources and has not increased the direct costs for society. Such an approach postponed the necessity of unpopular decisions related to the restructuring of the mining industry and bearing relatively high costs of replacing coal heating devices with more environmentally friendly ones by individual energy consumers. While unpopular decisions were avoided it did not come without a cost. The strategic decisions on coal-dependant energy sector has slowed down the development of renewable energy sources in Poland. In 2016, the so-called wind farms act was adopted, which, by forcing the distance of wind turbines from residential buildings, in practice prevented the development of obtaining electricity in this way in Poland's land areas. Construction of offshore wind farms, which will not be burdensome for society, is not expected until 2025. The inhibition of investments in this renewable energy source put into question the achievement of 15% of the demand for renewable energy in 2020, despite the dynamic development of photovoltaic solar energy systems in recent years.

The high costs of investing in nuclear energy and the negligence of successive economy and energy ministers postpone the prospect of launching nuclear power plants in Poland before 2030. While the project for Poland's energy policy 2040 hopes for 2033, it does not seem realistic. The Supreme Audit Office estimated in 2018 that the delays in nuclear power generation in Poland would amount to at least five years. During this time, it will be necessary to buy CO2 emission allowances to generate energy in coal power plants, which will cost from PLN 1.6 to 2.5 billion per year. The growing costs of coal extraction in Poland have led to increased imports of this raw material from abroad, including Russia. Thus, an environmental burden is combined with social and geopolitical implications. Additionally, the increase in the costs of CO2 emissions raised the price of electricity generation from coal in Poland. As a consequence, in recent years, social problems related to the increase in prices of energy obtained from coal have become apparent, both for individual consumers and for the industry and services sector. The use of coal to heat residential buildings by individual users contributes to the maintenance of an unacceptable level of air pollution in Poland, which generates indirect social costs in the form of health hazards. It seems more and more urgent to restructure the coal sector and close unprofitable mines and move away from coal as a fuel for heating residential buildings by individual consumers. In 2018, the European Commission estimated that forty one thousand coal miners would lose their jobs in Poland's Silesia region alone by 2030. Looking at Poland's addressing energy security problems related to coal one can see serious challenges during the coming decade. Poland will have to make up for the lost time and achieve EU standards in the field of energy security and decarbonization faster and at a more perceptible cost to the society than it would have been faced if the activities had been planned and executed over a longer period.

Poland's actions to protect and improve the condition of the environment in the last decade should be assessed as partially effective. Expenditures on environmental protection remain at a stable level ensuring the implementation by the state of tasks in this area. Despite the economic growth, Poland Domestic Material Consumption per capita does not show a visible upward trend and resource productivity in Poland's economy improves. However; both of those positive trends should be seen in comparison with the numerical indicators for Poland and the European Union. Domestic Material Consumption per capita, amounting to 18.488 tons in 2019, is clearly higher than 14.136 tons for the 27 Member States of the European Union. At the same time resource productivity in Poland was only 56.3% of the average for EU27. Significant progress has been made in improving water purity and reducing water use. The most serious of unresolved environmental problems in Poland relates to air quality. The use of coal as primary energy commodity in the economy has a negative impact on air quality in Poland. Its share in the structure of consumption of primary energy carriers in Poland in 2016 was 39.8%. The share of energy consumption from coal and biomass in households per capita was 46% in total. In 2016, this source was responsible for 45% of the emissions of pollutants into the air in Poland. Despite the observed reduction in the emission of dust precursors (especially sulfur dioxide) and the measures taken to reduce the concentrations of particulate matter in the air, high concentrations of PM10 and PM2.5 remain the most important air quality problem in Poland. These excessive concentrations take place both in relation to the daily (PM10) and annual (PM10 and PM2.5) standards and concern mainly urban and agglomeration areas. In the southern part of Poland it is also a problem for many non-urban areas. Concentrations of PM10 above EU accepted levels usually occur in winter and are mainly related to dust emissions from individual heating of buildings and from transport. Other causes of high concentrations of PM10 include emissions from industrial plants, heating plants, power plants and unfavorable weather conditions such as including long-term inversion situations, wind silences. In the case of some Polish towns, their location, e.g. in mountain valleys or river valleys, has a significant impact on the level of air pollution with PM10, which makes it difficult to disperse the pollutants. Important in terms of health effects, air pollutants in Poland are compounds from the group of polycyclic aromatic hydrocarbons, which are included in the

PM10 suspended dust. The air quality assessment for 2017 in terms of benzo(a)pyrene (BaP) showed that out of forty-six zones subject to assessment, only three did not exceed the applicable EU standards, and in forty-three zones, daily and annual EU BaP concentration levels were exceeded. Such a large number of zones with exceeding the standards is mainly related to the structure of fuel consumption in households. As the source of such air pollution is the incomplete combustion of fuels, the highest concentrations of benzo(a)pyrene and other polycyclic aromatic hydrocarbons occur in the autumn and winter season in densely built-up areas where houses or apartments are individually heated with coal or wood. The scale of the problem is evidenced by the fact that as much as 88% of benzo (a) pyrene emissions into the atmosphere in Poland come from individual farms.

Among the European Union countries, air pollution standards are most often violated in Poland. Poland has one of the highest levels of particulate matter pollution. Among almost three thousand cities from around the world included in the World Health Organization database, according to data for the years 2012-2015, forty five Polish cities were in the top 100 most polluted European countries in terms of PM10. Taking into account the air pollution PM10, PM2.5 and B(a)P, Poland is one of the EU countries with the worst air quality. The data of the European Environment Agency report from 2017 show, inter alia, that in 2015, out of 28 EU countries, the most frequent excessive levels of daily concentrations of PM10 (nationwide) occurred in Bulgaria, and then in Poland. In turn, in the case of PM2.5 and benzo(a)pyrene, the annual concentration of these substances in 2015 placed Poland in the first place among the most polluted European Union countries. Poland is the European record holder in benzo(a)pyrene emissions. There are some places in Poland where the WHO standards for B(a)P concentration are exceeded forty times. The Chairman of the Supreme Audit Office stated in 2019 that this is a consequence of the problem of poverty. In Poland, benzo(a) pyrene in the air comes mainly from garbage burnt in domestic stoves. The vast majority of it is released into the atmosphere as a result of individual heating of buildings. Annually, about forty six thousand people die in Poland due to air pollution. Research conducted at the Silesian Center for Lung Diseases has shown that 6% more people die from general diseases and 8% more from heart diseases during the smog alarm, i.e. when the concentrations of PM 10, PM 2,5 and B(a)P are significantly exceeded. According to the data of the European Environment Agency, PM2.5 alone contributed to the premature death of over forty-three thousand people in Poland in 2016.

The scale of actions necessary to solve the problems related to air pollution in Poland is huge. These actions would have to directly affect a significant part of the society and in the next few years force the involvement of significant financial resources by private persons, local governments and government administration. While this has been a serious problem before, the financial implications of Covid-19 call into question the viability of such a scenario in the near future. Achieving a quick improvement in air quality could only be possible after introducing a fundamental change in the method of heating households and limiting the possibility of using solid fuels in the municipal-living sector. To this end, the Supreme Audit Office proposed to immediately eliminate the possibility of using solid fuels in newly constructed buildings within the range of heating or gas networks, and in the medium-term perspective (five to ten years), to introduce an obligation to connect existing buildings to heating or gas networks in the event of the existence of such technical possibilities. The problem in the implementation of the above postulate is the social costs associated with the replacement of heating systems, and then their use by the poorest part of society. In the opinion of the Supreme Audit Office, the problem of smog must be solved together with the problem of poverty of many Polish families. And this task does not seem an easy one in any country.

3. Addressing Emerging Threats. Cybersecurity and Information Threats

Facing emerging threats of a qualitatively new nature constitutes a greater challenge than addressing traditional threats. In the initial period after the emergence of new threats, there is no full awareness of their potential impact on national security. Some of the consequences are delayed in time. The common recognized patterns of actions needed for effective addressing new threats are also missing. In such a situation, the state is doomed to act by trial and error, and it takes time to accumulate international experience that might be adopted. In the case of Poland, the above mechanisms revealed themselves in addressing threats to cyberspace security and information threats. A requirement for comprehensive approach to cyber threats was formally acknowledged in Poland in 2008. In November of that year "The Government program for the protection of the cyberspace of the Republic of Poland for the years 2008-2011" was adopted. In the following years, a number of conceptual documents was developed to guide governmental efforts in the field of cyberspace protection, including, among others, further projects of governmental cyberspace protection programs, policies and state cybersecurity strategies for the coming years. However; for almost a decade no consistent legal framework for the national cyberspace protection system was developed in Poland. The lack of basic legally binding obligations that would define the general principles of the cyberspace protection system, the roles, tasks and responsibilities of the state and private stakeholders harmed the efforts. Since there were no coherent legal regulations at the strategic level of the state, the individual ministries and state institutions were not able to provide a coherent and systemic approach to ensuring the security of the state's cyberspace. Works on

the preparation of the government proposal for a legal act on the national cybersecurity system were lengthy. As Gapiński observed in 2016, the delays resulted, among others, from the need to regulate the issues of public-private cooperation and defining the financing for the protection of the state's cyberspace. Legislative activities were also delayed by the lack of a single decision-making center that would be able to effectively coordinate the activities of other public institutions. Finally, in August 2018, the act on the national cybersecurity system was approved. It implemented the European Union' directive on security of network and information systems (NIS Directive) into the Polish legal system. This legal act defined regulations enabling the creation of an effective ICT security system at the national level. The current guidance for the governmental administration efforts in the field of cybersecurity were included in "The Cybersecurity Strategy of the Republic of Poland for 2019-2024" adopted in October 2019. The strategy provides a detailed guidance for implementation of the legal act on the national cybersecurity system. It defines actions that will increase the level Poland's of resistance to cyber incidents as well as the level of information security in the public, military and private sectors. The strategy includes objectives related to the cybersecurity of the Republic of Poland, such as the development of the national cybersecurity system. An in-depth cooperation and a greater coordination of law enforcement activities have been planned to increase effectiveness of the fight against cybercrime in Poland. The strategy provides also for a closer cooperation between the governmental administration and the territorial self-government authorities. The strategy aims at increasing the level of resilience of ICT networks and systems in public administration and the private sector. It calls for the adoption of national cybersecurity standards to regulate the organizational and technical requirements across the state's cyberspace and its users. The standards will be applied also to cloud computing and mobile applications. The strategy devotes a lot of attention to developing public awareness of good practices in the cyberspace and vigilance of cyber threats.

While looking for factors that decreased the effectiveness of Poland's efforts to assure its cyberspace security one may point at mistakes that were made in relation to the unity of effort, financing and developing manpower. The low effectiveness of the governmental efforts related to the protection of Poland's cyberspace was to some extent caused by the lack of continuity of efforts. Several consecutive reorganizations of the ministries responsible for the cyberspace protection can be considered as a factor that caused significant delays and contributed to the fragmentation of efforts in this area. Just during the last decade the responsibility of being the leading ministry for the security of cyberspace was being transferred between interior, interior and administration, and digital affairs ministries. There was also an open disagreement on the nature of cyber threats, which were viewed as primary military or civilian by respective ministries. The restructuring of the government was usually accompanied by a temporary organizational chaos, which resulted in the interruption of regulatory and organizational work. Security of Poland's cyberspace also lacked due attention for a long time. In 2015, the Supreme Audit Office assessed that Poland's security was perceived in a conventional manner and that cybersecurity problems were not in the center of the attention of the top management of the governmental administration, in particular the Prime Minister. The governmental administration did not understand the technological changes and was not aware of raising cyber threats. As the Supreme Audit Office observed, the lack of awareness of cyber threats and their consequences for the state's security paralyzed the activities of the governmental administration in the field of the cyberspace security before 2014. The organizational cultures of the governmental administration institutions that were involved in the creation of Poland's cyberspace protection system made them wait for the EU regulations instead of taking active measures in this respect. The unsatisfactory level of the awareness about the cyber threats has been also a result of uncoordinated activities for the collection of data on computer incidents. In 2014 the Supreme Audit Office argued that there was not a system of collecting and recording information about the computer incidents in Poland, and there were no legal obligations to report incidents by the most important users and administrators of the cyberspace. As a consequence, the governmental administration did not even have a general knowledge about the scale and categories of the computer incidents in the Polish cyberspace. The situation has not improved significantly since then. The assessment of threats to Poland's cyberspace carried out by the governmental administration institutions is basically limited to threats to the administration's ICT, while a comprehensive monitoring of the situation in the state's cyberspace is still not available. A coherent approach to raising awareness about cyber threats was missing for a quite long time even if education had been crucial to the governmental administration efforts for assuring the Poland's cyberspace security. Despite the common recognition of the importance of the education for the cybersecurity, its potential was not been fully utilized by the governmental administration during early years of the recent decade. Educational and training activities carried out until 2014 by the Police, the Scientific and Academic Computer Network, the Government Security Center and the Internal Security Agency were bottom-up initiatives and were not coordinated as part of the government's system of training and educational activities.

The assessment of the government efforts for assuring the security of Poland's cyberspace, needs addressing an issue of human resources, taking into account both their availability and professionalism. The governmental administration has now to compete on the labor market with the private sector, which also needs a significant number

of cybersecurity specialists. The problems with acquiring the most valuable specialized personnel result, among others, from the unattractive financial conditions of employment in the governmental administration and the state institutions. Rigid rules for remuneration of employees in the public sector that prevent the use of separate payment schemes for employees with special skills have hitherto meant that non-wage incentives for cybersecurity specialists might be used. Financing training, participation in exercises and international cooperation for the cybersecurity specialists proved temporarily effective as incentives. Nevertheless, in the end many employees ended up in the commercial companies after several years of work in the governmental administration and state institutions, during which they gained knowledge, qualifications and professional contacts. Polish cybersecurity experts estimate that the situation related to the availability of qualified personnel for the needs of Poland's cyberspace security will not improve significantly in coming years. This assessment is consistent with the audit results of the Supreme Audit Office published in 2019. In the post-audit statement, the Minister of Digital Affairs indicated that the main reason for the difficulties in employing the IT specialists by the territorial self-government administration was a result of insufficient financial resources. The deficiencies of the specialists in the field of cybersecurity are also felt throughout the Polish economy. In the absence of competitiveness of the governmental administration in terms of employment conditions, it seems unlikely that it could effectively compete with the commercial sector companies for the specialists necessary to ensure a high level of security of Poland's cyberspace.

Inadequate financing has been the most serious factor that decreased the effectiveness of the government efforts for ensuring the security of Poland's cyberspace. During the initial period of works on the governmental plans to protect the state's cyberspace a "no additional costs" approach was adopted. It meant that the governmental administration was supposed to assure the cybersecurity without any additional external financing. Consequently, no additional financial resources were allocated to carry out tasks in this respect. In the audit report published on June 23, 2015, the Supreme Audit Office concluded that the lack of identification of funding sources and the lack of allocation of financial resources have practically paralyzed the actions of the governmental administration in the field of protecting cyberspace. According to the Supreme Audit Office, the lack of adequate funding for cyber security tasks will pose a significant threat to the state infrastructure and will limit the state's capability to respond effectively to events occurring in cyberspace, which may have significant consequences, including financial ones. The issue of financing the state's cybersecurity was raised in consecutive strategy and policy documents adopted by Polish government. The "Cybersecurity Strategy of the Republic of Poland for 2017-2022" indicated the obligation of the institutions implementing public tasks to include cybersecurity expenditures in their financial plans. The strategy did not provide any meaningful estimation of the size and structure of the costs of implementing the cybersecurity strategy of the Republic of Poland for 2017-2022. It called for the establishment of a multi-annual financing plan for the construction of the cybersecurity system and the implementation of specific projects within it. The strategy for 2019-2024 contains relatively general declarations about financing the security of Poland's cyberspace. The strategy requires that the institutions performing public tasks include expenditure on cybersecurity in their financial plans. The current strategy does not provide detailed information about the costs of implementing the cybersecurity strategy. The strategy indicates two basic sources of financing activities. These are to be financial resources included in the financial plans of the institutions involved in the implementation of the cybersecurity strategy for 2019-2024, as well as financial resources from the National Center for Research and Development and European Union funds.

The emergence of information threats is a relatively new phenomenon if taking into account a time-scale of a possible state's response. For a long time information threats were considered in Poland as a part of a broader spectrum of cyber threats. The national security strategy of 2014 contained several notions of information security and threats, but it meant mainly protection of classified information and technical security of ITC systems. Broadly discussed Russian information operations to influence the U.S. presidential elections served as an eye-opener to the Polish government. This situation changed recently and the new security strategy addresses information threats in a more comprehensive way. The document adopted in May 2020 calls for ensuring the safe and secure functioning of the state and citizens in the information space. The strategy envisages building a strategic-level capacity to protect Poland's information space. Strategic level efforts will include system approach to counter threats of disinformation. The information space has been defined through the lens of interconnected of virtual, physical and cognitive domains. To be able to address information threats in an effective manner Poland plans to create a unified system of strategic communication of the state. The strategic communication systems mission is to forecast, plan and implement coherent communication activities, using a wide range of communication channels and media, and use tools of detection and influence in various areas of national security. Polish government stresses the importance of active measures to counter disinformation by building capacities and establishing cooperation procedures with news and social media, involving citizens and Non-Governmental Organizations. The newest edition of the national security strategy strives also to raise public awareness of the threats of information manipulation through information security education. One may also see efforts to improve legislation and provide a coherent conceptual framework for Poland's actions to address information threats. Information threats will be addressed in a novel to the act on crisis management as a part of wider

legislation efforts to build societal resilience in Poland against hybrid threats. Respective proposals were presented to the parliamentary commission for internal affairs in June 2020.

Recent years saw the establishment of a specialized team within the governmental administration that would deal directly with information threats. The working team for hybrid threats constitutes a part of the Government Crisis Management Team, a consultative and advisory body established at the Council of Ministers. Disinformation is one of the subjects of the work of this working team. The team has been tasked with an early identification of hybrid, including information threats and supporting the coordination of activities in this area. The team was established in September 2018, and its tasks include monitoring hybrid threats and assessing the risk of emergencies as a result of hybrid activities. It prepares proposals for responding to hybrid threats, and coordinates the activities of government administration, state institutions and services. The need to establish such a team was one of the conclusions of the CMX16 and CMX17 exercises of the NATO Crisis Response System. The need for urgent action in this area also resulted from the needs of Poland's national allied obligations and membership in the European Union. The team activities are partly classified. Publicly available information show that it has been involved in addressing hybrid threats in the context of protection of key state investments, ensuring the security of the organization and the course of election processes, monitoring and analysis of foreign media activity in relation to the situation in the Republic of Poland and in the field of Polish issues. The team contributes also to information and education activities aimed at increasing social resilience to hybrid threats. It takes part in activities aimed at counteracting hybrid threats undertaken in cooperation with the NATO and the EU.

Information threats are on the raise and there is no doubt that they need an adequate response. The phenomenon of disinformation in the digital environment and the use of digital media to influence society has been widely discussed in the scientific community and among practitioners in this field in Poland. It should be noted that there are many different views on the diagnosis of the current situation in Poland, despite the relatively high degree of agreement for the views on the general assumptions of information operations. It should be assumed that in the coming years, along with gaining the necessary experience and growing awareness of the impact of information threats on national security, the effectiveness of the actions taken by Poland will increase. Similar to the solutions adopted to ensure the cyberspace security, addressing information threats will require a transparent legal and conceptual framework, continuity and unity of efforts, and adequate financing and shaping of personnel resources.

4. Conclusions

The analysis on how Poland has addressed the threats to its national security allows identification of specific patterns of actions. Identification of threats and assessment of their impact on national security has usually been a long-term process subjected to a number of intertwined conditions, primarily of a political nature. Development of the legal and organizational frameworks to address specific threats to national security took time and often took place by trial and error, and the preliminary solutions were not always optimized for a specific threat. In addressing threats to national security, Poland has sometimes faced problems with the development and implementation of long-term strategies and policies, as well as with their stable and sufficient financing. The assessment of Poland's efforts related to assuring energy security and environment protection revealed broad spectrum of factors that influenced both shaping the state's strategy and its implementation. Concerns about possible social costs of planned investments resulted in half measures that only partially addressed the treats. Emerging threats needed longer time to be acknowledged and faced problems created by a lack of coherent conceptual framework to guide to governments actions. As recent experience suggests, while addressing emerging threats to national security, Poland may react with a certain delay and the initial actions may not be fully adequate to the nature of these threats and their potential effects on national security. In short term, Poland's actions to address security threats may be also influenced by ad hoc political decisions related to the priorities of the state's policy, which may hinder the coherence of actions aimed at addressing security threats in a long term perspective.

Ensuring an acceptable level of national security by Poland has required coherent, long-term efforts that minimized adverse effects of security threats. The analysis of Poland's experience in addressing threats to its national security suggests that a broad spectrum of intertwined factors influenced first the identification of security threats and their impact on state's security, then development of legal and organizational frameworks for addressing threats and finally the implementation of strategies and policies. Based on the assessment of recent experience, some predictions may be made on how Poland will address emerging security threats to national security and how effective those efforts may be. Most likely, addressing traditional threats will face the dilemma of priority and costs. It means that efforts for assuring energy security and environment protection may take longer than previously planned and unpopular decisions may be avoided because of political motivations. As Covid 19 revealed addressing emerging threats is doomed to trial and error approach. Poland will probably be cautious not to overreact to emerging threats, which in turn may slow down the reaction and reduce its initial effectiveness.

References

1. **Cieślak E.** Ocena wybranych działań administracji państwowej na rzecz bezpieczeństwa cybernetycznego, in: J. Kisielnicki et al. (ed.) Rola i zadania administracji publicznej w zarządzaniu bezpieczeństwem w Polsce Rzeszów Wydział Zarządzania Politechniki Rzeszowskiej, 2017, pp. 119-133
2. **Główny Inspektorat Ochrony Środowiska.** Stan środowiska w Polsce. Raport 2018, 2019, pp. 91-101
3. **InfoSecurity 24**. Poselskie dyskusje nad nowelą ustawy o zarządzaniu kryzysowym, 3 czerwca 2020, no pagination, https://infosecurity24.pl/poselskie-dyskusje-nad-nowela-ustawy-o-zarzadzaniu-kryzysowym
4. **Jarosz I. et al.** System bezpieczeństwa cyberprzestrzeni RP. NASK. Warszawa 2015, p. 175-179
5. **Kancelaria Sejmu.** Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, p. 2/43
6. **Kubiak M., Topolewski S.** (eds.), Bezpieczeństwo informacyjne w XXI wieku. Wydawnictwo UPH. Siedle 2016, pp. 159-176
7. **Ministerstwo Cyfryzacji.** Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, 2019, p. 7
8. **Ministerstwo Energii.** Polityka energetyczna Polski do 2040 r. Strategia rozwoju sektora paliwowo-energetycznego (PEP2040). projekt. wersja 2.1 08.11.2019, 2019, p. 52-56
9. **Najwyższa Izba Kontroli.** Czyste powietrze za sto lat?, 2019, no pagination, https://www.nik.gov.pl/aktualnosci/czyste-powietrze-za-100-lat.html
10. **Najwyższa Izba Kontroli.** Inwestycje w moce wytwórcze energii elektrycznej w latach 2012-2018, 2018, p. 8-11
11. **Najwyższa Izba Kontroli.** Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP, 2015, pp. 40-46, 68-69
12. **Najwyższa Izba Kontroli.** Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego, 2019, p. 40
13. **Prezydent RP.** Strategia bezpieczeństwa narodowego RP, 2014
14. **Prezydent RP.** Strategia bezpieczeństwa narodowego RP, 2020, pp. 21-22
15. **Rada Ministrów.** Bezpieczeństwo Energetyczne i Środowisko - perspektywa do 2020 r. Strategia sektorowa, 2014, p.
16. **Rada Ministrów.** Długookresowa strategia rozwoju kraju. Trzecia fala nowoczesności 2030, 2013, pp. 103-107
17. **Rada Ministrów.** Strategia na rzecz odpowiedzialnego rozwoju do roku 2020 (z perspektywą do 2030r), 2017, pp. 320-352
18. **Wrzosek M. (ed.).** Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes. NASK. Warszawa 2019, pp. 7-10