INTERNAL SECURITY IN POLAND AFTER 2015. THREATS AND RESPONSES

Eugeniusz Cieślak, PhD
Baltic Defence College
Faculty member

Zdzisław Śliwa, PhD
Baltic Defence College
Faculty member

Keywords: Poland, internal security, 2015–2020, threats

ABSTRACT

The objective of the article is to provide a preliminary assessment of Poland's response to non-military threats to its internal security. The article discusses threats to Poland's internal security between 2015 and 2020. The scope of analysis is limited to foreign intelligence operations and espionage, extremisms and terrorism, cyber threats, and economic threats, including corruption. Threat assessment focuses on targets for hostile actions, observed patterns and trends, along with consequences to Poland's internal security. Available data on threats to Poland's internal security is consolidated and analysed. The assessment of response to threats discusses its effectiveness and highlights challenges in responding to new threats. The scope of the article is limited to the Internal Security Agency activities and is based on publicly available official governmental documents along with analytical works published in professional periodicals. Based on observed trends, possible future scenarios related to threats to Poland's internal security are presented, and possible responses discussed.

INTRODUCTION

The destabilisation of the security situation in the Euro-Atlantic area by Russia's actions against Ukraine resulted in an immediate increase in threats to Poland's external and internal security. The unfavourable development of the situation required undertaking and intensifying actions aimed at increasing the possibilities of counteracting security threats in the allied, regional and national dimensions. Hybrid threats have become the key threats to Poland's internal security, the catalogue of which is significantly expanding. In recent years, the blurring of the boundary between intelligence threats and hostile cyber, terrorist and economic activities carried out inside the state has become noticeable. The most serious challenges in the field of Poland's security are related to the aggressive policy of the Russian Federation. In recent years, propaganda and disinformation have been the primary instruments of hybrid activities carried out in the information sphere, especially in cyberspace and on social media (Sazonov and Müür, 2017; Śliwa, 2017). As information warfare tools, they are used to weaken Poland's security and weaken its image and position in international relations. The use and deepening of the existing political divisions as well as the exploitation of extremisms perpetuate divisions among Polish citizens, polarise social moods and weaken resilience to external threats. Extremism has been considered as one of the most dynamically developing threats to Poland's internal security after 2015 that may lead to increased violence and even terrorist attacks in the future. The threat of hostile actions by other states and commercial entities for the economic and energy security of Poland is also growing. This applies in recent years to attempts to take over, block, or discredit key investments for the Polish economy. The scale of threats to the cyberspace of the state, its institutions and citizens, is systematically growing and requires comprehensive response.

The aim of the article is to assess the dynamics of changes in the area of threats to Poland's internal security between 2015 and 2020 and their impact on the security of the state and citizens. The article also discusses the actions taken by the state security services to increase Poland's internal security and outlines a forecast for the development of the situation in the coming years. The analysis is limited to four major threats to internal

security posed by foreign secret services and espionage, extremisms and terrorism, cyber threats and economic threats, including corruption. The article thus only focuses on the Internal Security Agency activities and does not discuss the efforts of the Military Counterintelligence Service nor the Central Anti-Corruption Agency. Threat assessment focuses on gauging their scope and targets, magnitude, patterns and trends along with consequences to Poland's internal security. The analysis is limited to the period between 2015 and 2020 and is based on publicly available information provided by the state security authorities and institutions. Responses to each of the threats is then discussed with the aim of assessing their adequacy and effectiveness. Finally, based on historical developments and emerging trends in the security environment, an initial insight on possible future scenarios related to Poland's internal security in coming years is offered. The article references publicly available government documents, analytical studies by think-tanks, and academic research. The discussion presented here is limited to sources not covered by the confidentiality clause.

1. FOREIGN INTELLIGENCE OPERATIONS AND ESPIONAGE

The geostrategic location of Poland along with its membership in NATO and the European Union attracts the attention of foreign intelligence services, including espionage related to security and other functional areas of the state. This area of security is one of the domains of the Ministry of Internal Affairs (MIA), which is responsible for counterintelligence activities. The Ministry has published an overview of foreign services activities between 2015 and 2019, recognising enhanced threats linking it with so-called hybrid tools to impact security. The disappearing boundary between foreign intelligence information-gathering activities and other activities inside Poland is recognised, and it includes the extended use of cyberspace and especially various social media channels. The situation that Poland has been facing in recent years is not new to the region as evidenced by developments in the Baltic states (Winnerstig, 2014) and Ukraine (Mölder, 2016, pp. 101–106). The main targets of foreign espionage and non-information activities in the past five years have been the energy sector, investments, information sphere, and social networks. Among foreign nations that have conducted intelligence operations in Poland after 2015, two have been recognised as particularly interested in influencing the security situation: Russia (through the means of propaganda and disinformation) and China (Serwis Rzeczypospolitej Polskiej, 2020a). The targets of foreign intelligence operations in Poland range from security and military industry to the economy. The adoption of new technologies and operating procedures by foreign intelligence services has necessitated a more focused and deliberate response. Although the threat of foreign intelligence activities in Poland has been growing steadily since 2015, a large amount of information related to counterintelligence was made public only in 2019. After 2015, three persons have been arrested in Poland in connection with espionage for Russia and two persons on charges of spying for China. In October 2016, the Internal Security Agency detained Mateusz Piskorski, a former member of Polish Parliament and a leader of the pro-Russian political party Change. Piskorski has been facing charges of collaborating with Russian civilian intelligence and Chinese intelligence services. He was found to have received financing for pushing a Russian agenda in Poland (Żaryn,

2019). In 2018, an employee of the Ministry of Energy Marek W. was arrested on charges of spying for Russia and then sentenced to jail and prohibited to work in the public administration for ten years. In 2019, a Chinese citizen Wejing W., who was identified as an agent of a civilian intelligence agency, and a Polish national Piotr D. were detained on charges related to espionage (Serwis Rzeczypospolitej Polskiej, 2020b).

Poland has been facing increasing threats from foreign intelligence influence operations. As the hybrid activities that harm Polish security interests are difficult to identify and classify in legal terms, they usually do not end up in courts. Most frequently, foreign citizens suspected of hybrid activities in Poland face administrative actions while the illegal activities of foreign diplomats are addressed by diplomatic procedures. Since 2015, Poland has expelled five Russian diplomats. Four Russian diplomats were expelled from Poland in 2018 as part of the international reaction to the Skripal poisoning (Serwis Rzeczypospolitej Polskiej, 2020a). In March 2019, information collected by the Internal Security Agency led to the expulsion from Poland of the vice-consul of the Consulate General of the Russian Federation in Poznań. The diplomat was declared a persona non grata and was banned from entering Poland and the Schengen area. The Internal Security Agency found the Russian diplomat to have engaged in activities inconsistent with their diplomatic status which could harm Polish-Russian relations (Żaryn, 2019a). In 2018, a Chinese diplomat was expelled from Poland after the conviction of an agent cooperating with the Chinese intelligence in Sweden. According to the Internal Security Agency, the diplomat in question was the senior officer of a Chinese citizen convicted in Sweden. The Chinese diplomat was banned from entering Poland and the European Union (Żaryn, 2019a).

Over the last five years, Poland has ramped up its efforts in addressing hybrid threats. The Internal Security Agency also effectively counteracts hostile hybrid activity by using administrative procedures, such as entry bans, expulsions, denial of permission to stay, negative opinions on applications for citizenship, or withdrawal of permission to stay. The Internal Security Agency has publicised information related to some of the cases. In October 2017, the Russian scholar Dimitrij Karnuakhov, tied to the Russian Institute of Strategic Studies, a Foreign Intelligence Service affiliated think-tank, was expelled from Poland. Karnuakhov was suspected of conducting hostile information activities against Poland.

In late 2017, the Agency assisted in banning three Russian agents posing as researchers from entering the Schengen area. They turned out to be the masterminds behind pro-Russian projects pushed in Poland (Żaryn, 2019b). A telling example of hybrid threats to Poland's security was a case of an attempt to set fire to the office of the Transcarpatian Hungarian Cultural Association in the small town of Uzhhorod in south-western Ukraine. The perpetrators turned out to be Polish citizens who were used to spoiling Hungarian–Ukrainian relations. The Uzhhorod arson attempt was investigated by the Internal Security Agency, which managed to tie the incident to the Polish pro-Kremlin party Change, whose then-leader has been awaiting trial for espionage and cooperation with Russian intelligence services. The case serves as evidence of the complex relationships between the influence of hybrid threats on internal, national and international security in the region. As the spokesman of the Coordinator of Poland's Security Services observed in 2019, 'Narrowing down Russia's hostile activity to spreading lies in the media is a losing battle' (Żaryn, 2019b). In May 2018, two Russian citizens, Yekaterina C. and Anastasia Z., were detained and deported from Poland while three other citizens of the Russian Federation were banned from entering Poland (Deutsche Welle, 2018). According to the Internal Security Agency, all five had made repeated attempts to engage Polish pro-Russian circles in hybrid activities (Żaryn, 2019a). The extent of administrative procedures used to counter hybrid threats is perhaps better illustrated by statistics. Between 2015 and 2019, a total of 28 foreigners were expelled from Poland for activities against the security and interests of the Republic of Poland (Serwis Rzeczypospolitej Polskiej, 2020a).

Protection of classified information plays an essential role in preventing foreign espionage. The Internal Security Agency is responsible for granting Polish citizens and institutions access to NATO, European Union and European Space Agency's classified information. Between 2015 and 2019, approximately 43 thousand individual security clearances and one thousand industrial security clearances were issued. At the same time, 123 persons were denied access to classified information, and the security clearances of almost one hundred persons were revoked. To support the counterintelligence effort, the Internal Security Agency has been increasing its prevention and educational efforts. The statistics available for the period between 2015 and 2019 show 2.6 thousand counterintelligence courses and as many as 58 thousand course participants (Serwis

Rzeczypospolitej Polskiej, 2020a). This aspect is reinforced by other governmental agencies, especially security services, including armed forces within their areas of responsibility. Such complex approach not only supports the efficiency of counterespionage but also contributes to the resilience of the society and awareness of the wide range of threats resulting from the activities of foreign intelligence services in the territory of Poland and beyond.

Poland will remain subject to foreign intelligence operations in the future. Most likely Russian intelligence services will remain active in both espionage and influence operations. They may also inspire and support malicious hybrid activities against Poland's security interests at home territory and abroad. Experts also highlight the increasing scope and intensity of Chinese intelligence operations in Poland. This evolving threat will require deliberate approach integrating legal, conceptual, and organisational efforts. The Chairman of the Parliamentary Commission for Secret Services has observed that the Polish legal definition of espionage is outdated and not entirely relevant to current security threats (Lesiecki, 2019). The definition needs to be updated to address, among other issues, the role of agents of influence and clarify the relevant parts of the criminal code. Strategic communication is viewed as crucial to Poland's counterintelligence efforts (Raubo, 2020). A number of specialists call for a more robust public communication to increase social awareness of the threats of foreign espionage and influence operations. It may also help to build trust in Polish counterintelligence services and demystify some aspects of their operations (Maciążek, 2019).

2. TERRORISM AND EXTREMISM

Poland has not suffered any large-scale terrorist attack in recent years; however, the country could be targeted by radical, extremist, or even internal radicals. Nevertheless, as Poland does not exist in a vacuum, there 'has been a significant evolution of the terrorist threat in the region, and Poland's membership in the European Union (E.U.) and NATO, as well as the participation of Polish troops in international peace operations, are considered a factor that may increase the risk of terrorist attacks in Poland or against Polish citizens abroad' (U.N. Security Council Counter-Terrorism Committee, 2019). This relates to not only direct attacks but also to Poland's status as the East border of the EU and Schengen area causing interest in using the territory of the country for direct activities and transfer routes in connection with illegal drug trade, human trafficking, arms trade, smuggling, or money laundering. The actual list of possible illegal activities is much longer and all of these could lead to terrorist-type attacks as a revenge to disrupt security system and services. Another factor to consider is the active participation of Poland's armed forces and security services, mainly police, in operations abroad in conflict zones. As their involvement in these areas (such as Afghanistan and Iraq) is directly connected to the activities of terrorist organisations, Poland could be a target for revenge actions. Next, foreign terrorist fighters could try and establish networks inside the country as a staging ground for actions inside Poland or abroad.

Between 2015 and 2019, six people were convicted in Poland for terrorism-related activities. Most of the cases were tied to jihadist terrorism. In 2016, the Internal Security Agency arrested Mourad T., who was involved in organising the Paris bomb attacks in November 2015. Mourad T. was one of the most influential people in the leadership structures of the so-called Islamic State. In 2018, the Moroccan citizen Abdeljalil A.E.K. was sentenced to 8 years in prison. The information gathered by the Polish counterintelligence in relation to his arrest was pivotal to thwarting terrorist attacks in two European countries. In March 2019, Mourad T. was sentenced to 3 years and 8 months in prison (Serwis Rzeczypospolitej Polskiej, 2020b). The Agency also prevented a terrorist attack by Mikołaj B., who was arrested in May 2019 in Warsaw. Mikołaj B. was preparing

to carry out a terrorist attack in a public place as part of his revenge on the opponents to the Islamic religion. In September 2019, a 27-year old Polish citizen was sentenced to four years in prison for participating in a terrorist organisation operating in Syria. In December 2019, the Internal Security Agency detained Maksym S., a radical Islamist who was planning an attack in the town of Puławy. To keep the terrorist threat under control, the Internal Security Agency has been monitoring the situation to prevent uncontrolled returns of foreign fighters to Poland. Those efforts are directed at both Polish citizens and foreigners attempting to travel to other countries via Poland. According to the Agency, there is no indication of the potential terrorist threat from radicals, including Islamic fanatics, decreasing in the near future.

The last five years have seen an evolving threat of right-wing extremist and radical movements using neo-Nazi narratives and posing a direct threat to some ethnic and religious minorities and social groups in Poland. The increasing prevalence of this trend calls for decisive actions against such groups to prevent them from closing ranks with political sympathisers. Rising extremism may cause risks to both the internal security of Poland as well as its reputation abroad. As the right-wing extremists cooperate closely with their counterparts abroad, it makes sense to use administrative measures to limit such cooperation. The Internal Security Agency has publicised information about its activities that aimed at reducing a threat of right-wing extremism. Recently, Anton T., a Swedish citizen and a member of a neo-Nazi organisation who came to Poland for paramilitary training, was expelled from Poland with immediate effect by the decision of the Minister of Internal Affairs and Administration. According to the Internal Security Agency, the man posed a serious, real, and present danger to security and public order in Poland. The man was a member of the neo-Nazi Nordic Resistance Movement, which is seeking to create a National Socialist North European Republic through revolutionary means. Another activist with ties to neo-Nazi circles, a Russian man called Konstantin B., was declared a persona non grata in November 2019 for his continued contacts with the representatives of the Polish extreme right. Konstantin B. planned to use the Polish neo-Nazi circles for illegal activities. In September 2020, Internal Security Agency officers detained a German citizen suspected of participating in an organised crime group operating in Poland and other countries. The detainee, Jurgen K., was active on social media presenting radical anti-system views

and supporting extreme right-wing organisations. During the search of the place of work and residence of the detained man, 1.2 kg of TNT along with ammunition and a tear grenade were found (Infosecurity 24, 2020). The Internal Security Agency has made efficient use of various mechanisms for neutralising terrorist and extremist threats over the past five years. At the request of the Agency, 39 people whose presence in Poland was associated with the threat of terrorism were deemed undesirable in Polish territory and 14 were expelled or obligated to return to their home countries (Serwis Rzeczypospolitej Polskiej, 2020b).

It is worth mentioning that Poland has developed a comprehensive approach for addressing terrorist and extremist threats in recent years. Countering terrorist propaganda has been included as one of the priorities of the Internal Security Agency. As online terrorist propaganda can intimidate societies by publicising brutal acts of violence against innocent people and aims at recruiting more jihadists, there was a need for an adequate response. Two aspects of countering terrorist propaganda have included regulation of the content of internet media and holding responsible those who engage in such propaganda activities. In 2017, based on evidence collected by the Internal Security Agency, Dawid D. was convicted of propaganda activities for a terrorist organisation. In 2018, the Internal Security Agency blocked the official media channels of the so-called Islamic State in the state's internet domains (Serwis Rzeczypospolitej Polskiej, 2020b).

To increase societal resilience to terrorist threats, Poland created the Terrorism Prevention Centre of Excellence in 2018. The Centre has been consolidating efforts of national state security agencies and extending international connections toward common goals of reducing terrorist threats. The Centre has been focusing on counteracting extremist and terrorist threats through ensuring an early response to the first symptoms of radicalisation in the society. The Centre has specialised in terrorism prevention in the broad sense, the key element of which is the dissemination of knowledge of the possibility of preventing adverse security events. For this purpose, the Centre has organised profiled training for officers and employees of secret services, as well as public administrative bodies and other entities. The Terrorism Prevention Centre has sought to become a centre of excellence that brings together the knowledge and experience of domestic and foreign secret services, public institutions, as well as

the achievements of scientific research centres in the field of terrorism prevention. It intends to develop a broad preventive mechanism based on the cooperation of all public administrative bodies and the private sector, placing citizens in the centre of the process of shaping security culture in Poland. To achieve such objectives, the Centre develops training programmes and conducts training in the field of terrorism prevention. A significant part of the Centre's activities are social campaigns that raise awareness of terrorist threats and build security culture within the society. The Centre also prepares profiled recommendations in the field of terrorism prevention and develops training materials and guides. It has also been involved in the organisation of meetings, workshops, and seminars both at the national level and in cooperation with domestic and foreign experts.

Although the Centre is a relatively new institution, it has successfully combined national and foreign experience and expanded its capacities and staff. As at September 2020, the Centre has been involved in 17 state-wide projects, cooperating with 40 partners, organising 300 meetings and providing training to 3,841 persons within a broader system of prevention to terrorism and extremism (Terrorism Prevention Centre of Excellence, 2020).

The terrorist threat will remain an important issue for Poland's internal security for years to come. Although there have been no terrorist attacks in Poland in recent years, jihadist terrorist networks have operated there, planning and supporting attacks in other countries. There is a growing concern of rising extremism, typically extreme and nationalist right wing and neo-Nazi affiliated networks that call for violence against ethnic and social minorities. Such networks may increase cooperation with similar organisations from abroad and shift from non-lethal violence to more coordinated attacks with firearms and explosives. They will be susceptible to external influence and might be used as a tool in hybrid activities in Poland and abroad. Most likely, at least some of the extremist networks will also engage in criminal activities. The potential for lone wolves as perpetrators of terrorist attacks and hate crimes must also be taken into account when discussing future developments related to Poland's internal security (Raubo, 2020).

3. THREATS TO THE SECURITY OF POLAND'S CYBERSPACE

Similar to other states, Poland is becoming more and more dependent on cyberspace-enabled services. Social and economic development is increasingly dependent on quick and unhindered access to information. The efficiency and stability of ICT systems are crucial not only for the internal security of the state but also have an impact on virtually every area of state and civil activity. The period between 2015 and 2020 saw an evolution of cyber threats that had a direct impact on Poland's internal security. The Internal Security Agency's CSIRT GOV team reacted to more than one hundred thousand computer incidents between 2015 and 2019. One-third of those incidents turned out to be cyber threats. The number of computer incidents has steadily increased after 2015. Whereas in 2015 CSIRT GOV dealt with 16,123 cases of suspected computer incidents, the number of such cases rose to 31,865 in 2018 and 226,914 in 2019 (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, 2019). Most of the cases turned out to be false positives and the numbers of confirmed computer incidents were 8,914 in 2015, 6,236 in 2018, and 12,405 in 2019. Advanced persistent groups campaigns have constituted a growing portion of the threats to Poland's cyberspace after 2015. Most of the malicious traffic against the governmental administration networks in 2019 originated from the Russian cyberspace. Communication to malicious internet addresses along with active scanning of the governmental administration networks made up almost 80% alerts issued by the early warning systems. Government institutions (32.81%), critical infrastructure (31.21%), and the Ministries (19.01%) were most frequently subjected to active scanning in 2019. State security services and military accounted for only 5.27% of active scanning cases in 2019 (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego 2017, 2018, 2019).

The urgency of actions to assure Poland's cybersecurity was recognised as early as in 2015. The Supreme Audit Office reports published at the time pointed at critical deficiencies in defining the legal and conceptual framework for actions, deficient financing and insufficient coordination (Najwyższa Izba Kontroli, 2015). The security of state administration infrastructure used for public services was determined to be inadequate

by the Supreme Audit Office in 2016 (Najwyższa Izba Kontroli, 2016). Similar audits of the local government administration infrastructure in 2018 revealed shortcomings in data protection systems (Najwyższa Izba Kontroli, 2019). The situation called for a coordinated and comprehensive approach to the security of Poland's cyberspace. In 2018, the Act on the National Cybersecurity System was finally adopted after lengthy preparations, and in 2019, the Strategy for the Protection of the Cyberspace of the Republic of Poland for 2019–2024 was published (Ministerstwo Cyfryzacji, 2019). A decade after initial governmental efforts related to cyberspace security, a coherent legal and conceptual framework for action has been finally developed. While not all issues have been resolved, a solid basis for further works has been established (Cieślak, 2020).

Cybersecurity has remained one of the key areas for the Internal Security Agency in recent years. The operations of CSIRT GOV have focused on the protection of the state's administration cyberspace. The CSIRT GOV Computer Security Incident Response Team, led by the Head of the Internal Security Agency, acts as the national level CSIRT responsible for coordinating the process of responding to computer incidents occurring in the national cybersecurity system (Polska, 2018). It is tasked with the detection and prevention of threats to the cyber security of ICT systems of public administrative bodies. The CSIRT GOV also protects the system of ICT networks covered by a uniform list of facilities, installations, devices, and services included in the critical infrastructure, as well as ICT systems, owners, and holders of critical infrastructure facilities, installations or devices, defined in legal regulations on crisis management. As the number of threats and security incidents has been increasing in recent years, each incident has been addressed as a risk of violating the security of the state and citizens.

In order to ensure a more efficient response to any threats to Poland's cybersecurity, CSIRT GOV has been expanding its early warning systems and participation in international cybersecurity networks. The ARAKIS 3.0 GOV early warning system provides data on both external threats and vulnerabilities of the state's administration information and computer networks. It has been extensively used for testing vulnerabilities. In 2019, CSIRT GOV audited 35 information and computer systems of ten government administrative institutions, revealing 13,035 vulnerabilities. Corrective actions have subsequently been undertaken. Important

political events, such as elections to the European Parliament and Poland's Parliament, along with official national holidays and anniversaries, have been considered as high-risk events in terms of cybersecurity. Due attention is paid to the monitoring and mitigation of cyber threats related to such occasions. Polish CSIRT teams have systematically participated in multinational exercises, such as NATO-CMX, Cyber Coalition, and Locked Shields to prepare better for the protection of the state's cyberspace (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego 2019).

The security of Poland's cyberspace will remain crucial for the state's internal security. As the dependence on network-enabled services is ever-increasing, the need for a comprehensive approach to the cybersecurity system becomes more and more urgent. Poland will have to increase its efforts to improve the protection of the critical infrastructure assets (Rządowe Centrum Bezpieczeństwa, 2020). Better private-public partnership solutions in the field of cybersecurity have been sought for, and significant efforts are directed at improving Poland's independence in the digital domain through the development of cryptographic tools and national expert cyber centres. The need for a secure cyberspace becomes even more evident as it is used more and more frequently for hostile information operations and hybrid activities.

4. THREATS TO ECONOMIC SECURITY

The National Security Strategy of the Republic of Poland published in May 2020 recognised the urgency of strengthening economic security being faced by globalisation processes and growing competition on foreign markets. This is directly linked with internal security, national defence potential but also with state and societal resilience in the face of modern threats. Special attention has been given to the financial sector, which is vulnerable to speculative attacks on the Polish currency or capital drain. As this sector is significantly affected by external trends, there is a need to close ranks with international supervisory institutions and internal law enforcement agencies. Financial stability is an essential factor motivating the use of the Polish banking system for money laundering, as it has been in the case of the ING Bank Śląski, a subsidiary of the ING BSK, which was used to launder Ukrainian and Russian money within a so-called 'mirror trading' system. Another bank, Bank Spółdzielczy in Skierniewice, was the subject of a prosecutors' investigation connected to money laundering and drug trade; deposits valued at 1.3 bn PLN were seized (Wilkowicz, 2020). Those are not only cases, and their impact is important from the perspective of trust in the national banking system and overall security, as financial issues are of great importance for every citizen. From another vital perspective, the financial sector is closely connected to the position of a country in the international arena. Therefore, reasonable and purposeful government interference in economic matters is an essential factor for the security in this sector after 2015.

Another factor affecting the internal security of Poland is the safety of the supply of natural resources. Oil and natural gas have been traditionally exploited by Russia as an international policy tool to pressure selected nations. This is done directly by establishing different prices for different nations, specifically those recognised as hostile or friendly. After decades of a Russian monopoly in supplying oil and natural gas to Poland, a common perception of threats resulting from such a situation has developed. Poland is clearly aware of such threats, demonstrated by the investment in a strategically important Liquid Natural Gas Terminal in Świnoujście to ensure the stability of supplies for the population and state enterprises. The termination of gas supplies to Ukraine by Gazprom in the recent past

has demonstrated the effect of such a tool on economic and personal security. In parallel, Warsaw is actively trying to stop the Nord Stream 2 gas pipeline project, calling it a direct threat to energy security and not only for Poland but for Eastern Europe in general. The decision of the Office of Competition and Consumer Protection in October 2020 to impose a penalty on Gazprom (29bn PLN) and five companies participating in the project (234mln PLN) was a clear message and an act of protecting national economic interests (U.N. Security Council Counter-Terrorism Committee, 2019). This aspect is linked with gas prices and continuity of supplies as increasing prices on the internal market could cause dissatisfaction among natural gas users in Poland, especially among the poorer part of society and strategic companies using this type of natural resources for production processes. At the same time, the Internal Security Agency has been focusing its efforts on protecting the Liquid Natural Gas Terminal project in Świnoujście against hostile economic and information actions.

Poland's state security services have become increasingly aware of hostile economic and financial actions that may directly influence the state's internal security. In 2015, the Russian fertiliser tycoon Acron was trying to take over Polish chemicals giant Grupa Azot, which was seen as an aggressive step to monopolise the market in this specific field. In reaction, the Polish government implemented a law permitting the state control of selected national companies of strategic value. The list of such companies is evolving and includes Emitel S.A., Grupa Azoty S.A., KGHM Polska Miedź S.A, Polski Koncern Naftowy Orlen S.A, PKP Energetyka S.A., and Tauron Polska Energia S.A (Ostrowski, 2020). The government is currently working on a new law requiring foreign investors to have state approval to buy shares in a company equal or exceeding 10% share capital or concerning buying a significant block of shares (e.g. 20%, 40%).

Investors from the European Union/European Economic Area will not be subject to restrictions if they have been registered there at least two years to avoid hostile takeovers. Hostile takeover attempts are not exclusively linked with Russian capital, as, for example, KGHM falls within the area of interest of the U.S. Freeport-McMoRan Copper & Gold, Australian Rio Tinto, or Chinese investors. Next, foreign companies have taken significant interest in food production companies, which is an important factor that could influence the food prices in Poland and affect food security

along with the protection of natural environment. It might affect the basic needs of the population with a strong influence on societal stability. The trend to take over Polish companies is growing, and it is linked to the Covid-19 crisis and weakness of the currency and the continuing expansion of big and rich players. There are direct risks connected to this factor, as taxes from national enterprises support the Polish economy, while in the case of companies funded by foreign capital, the funds are transferred abroad.

The economic sphere has always been attractive for crime-related activities, especially tax violations and corruption among participants on both ends – givers and receivers. The crime-supporting factor in Poland is that it has been benefiting from significant economic growth during the last decades using national resources along with significant funds coming from the EU. Investments into infrastructure are creating opportunities at all levels and stages of their implementation. The Poland Corruption Report published in January 2018 highlighted that corruption was a problem for businesses operating in Poland (GAN Risk & Compliance Portal, 2018). The public procurement, justice, and land administration sectors carry exceptionally high risks. Political corruption constitutes a challenge to fair business as politicians use their positions to gain benefits, and practices of nepotism and cronyism are widespread. Poland's Criminal Code offences include active and passive bribery, bribery of foreign officials, extortion, and money laundering. The public procurement sector was especially linked with this negative trend by a diversion of public funds and favouritism in decisions of government officials, tailor-made specifications for particular companies, unclear selection or evaluation criteria, collusive bidding, and conflicts of interest (GAN Risk & Compliance Portal, 2018). However, the Corruption Perceptions Index (CPI) indicates that Poland has made progress in this area: the Transparency International CPI 2019 ranked Poland 41st with 58 points (the scale: highly corrupted 0 points, minimal corruption 100 points). This is a result of a decisive approach toward fighting this negative aspect of the economy having an impact on nations and other factors as Foreign Direct Investments.

The Internal Security Agency can also boast considerable successes in combating economic crimes. According to one study, the Internal Security Agency has revealed attempts at tax fraud for over PLN 3 billion

and conducts, under the supervision of various units of the prosecutor's office, an average of 140 proceedings concerning tax offences each year. Some 1.5 thousand persons received accusations of committing tax crimes, and the value of the secured property of suspects in tax depletion cases is over PLN 260 million (60 mln Euro) (Serwis Rzeczypospolitej Polskiej, 2020a). The negative trend is, however, that corruption cases are more common in the public sector compared to private or public/private sectors. In 2018, of a total of 1,229 cases, 895 were in the public sector (73%), and the trend continued in 2019 as among 1,366 corruption cases as many as 948 (70%) were related to the public sector (Internal Security Agency, 2020). The main areas of corruption were infrastructure, construction, and real estate. The trend is reinforced by the employment of random people in the public sector not able to manage and control respective enterprises. It is often linked with nepotism and returning favours to trusted persons but not exactly qualified ones.

The economy-related threats and risks are highly interconnected, as many of them have an impact on security from the national level down to single individual personal security. Therefore, there is a need to see all of them in context, not forgetting that the country is a part of broader international systems as an outcome of globalisation and a variety of agreement. As mentioned, the banking system, natural resources supplies, and others are under pressure from external competitors or hostile nations/organisations reinforced by internal risks line crimes, corruption, nepotism or politically driven economic system. The Internal Security Agency will continue to play an important role in addressing external economic threats to Poland's security.

CONCLUSIONS

The internal security of Poland has been subject to a number of external threats in recent years. Russian aggressive actions have destabilised the security situation in the Euro-Atlantic area and increased the scope and magnitude of threats to Poland's external and internal security. Poland has been facing a growing threat of foreign espionage, intelligence, and influence operations. While most of them are attributed to the Russian Federation, the intensity of Chinese secret services actions in Poland raises more and more concerns. Terrorism and extremism have not resulted in a high number of casualties or losses in recent years, and the overall terrorist threat has remained relatively low. However, terrorism and lone wolf attacks motivated by extremist narratives and ideas may pose a threat to Poland's internal security in coming years.

Hybrid threats have become one of the critical threats to Poland's internal security and are considered to be tied closely to the actions of adversary governments. The recent years have seen a blurring of the boundaries between intelligence threats and hostile cyber, terrorist, and economic activities carried out inside Poland and outside of its borders. Propaganda and disinformation inspired by Russia have become the primary instruments of hybrid activities carried out in cyberspace. They weaken Poland's security and its position in international relations. At the same time, hybrid activities exploit political divisions and extremisms among Polish citizens, undermining the internal security of the state and its resilience to external threats.

The trends that have been observed in recent years suggest that the scope and magnitude of cyber threats to Poland's security will grow significantly in the coming years. Actions of foreign states, along with criminals, will pose a threat to Poland's public administration, industry, and banking, as well as individual citizens. Furthermore, the cyberspace may be used for hybrid activities and hostile information operations. The protection of Poland's cyberspace will remain crucial for the state's internal security in the coming years. A comprehensive approach combining public and private efforts will focus on the improvement of the protection of the critical infrastructure assets. Actions aimed at Poland's independence

in the digital domain will be given priority. That, in turn, will translate into more robust efforts related to the development of cryptographic tools and building national cyber expertise.

Protection of Polish economic interests against external hostile activities will remain one of the primary tasks of the Internal Security Agency in the future. The economy has a direct impact on internal security both at the national level and for the security of any individual citizen. With the globalisation of the economy, the frequency of potential external state and commercial actors' interference with the Polish economy may increase, and their intentions may not always be clear. The protection of vital national investments against hostile takeovers, corruption, and hybrid activities will be given priority as such investments improved Poland's security. The actions of the Internal Security Agency will be coordinated with other state's security agencies, as well as the Central Bureau for Anticorruption and the Police.

REMARK

The views presented by the authors are their own opinions and do not represent the official position of the Baltic Defence College.

Contacts:

Eugeniusz Cieślak, PhD
Baltic Defence College
E-mail: Eugeniusz.cieslak@baltdefcol.org

Zdzisław Śliwa, PhD
Baltic Defence College
E-mail: Zdzislaw.sliwa@baltdefcol.org

REFERENCES AND SOURCES

Cieślak E., (2020). Adressing the threats to national security. Poland's experience. In: Bekesiene S. and Hoskova-Mayerova S., *Challenges to national defence in contemporary geopolitical situation. CNDCG' 2020 Proceedings of the 2nd International Scientific Conference. Vilnius, Lithuania*. Vilnius: LKA

Deutsche Welle., (2018). *Poland busts Russian 'hybrid warfare' ring.* [Viewed 8 September 2020]. Available from: https://www.dw.com/en/poland-busts-russian-hybrid-warfare-ring/a-43831566

Forsal., (2019). *Raport ABW: Najpoważniejsze wyzwania w sferze bezpieczeństwa wiążą się z agresywną polityką Rosji*, 6 grudnia. [Viewed 15 September 2020]. Available from: https://forsal.pl/artykuly/1443411,abw-najpowazniejsze-wyzwania-w-sferze-bezpieczenstwa-wiaza-sie-z-agresywna-polityka-rosji.html

GAN Risk & Compliance Portal (2018), *Poland Corruption Report*. [Viewed 4 October 2020]. Available from: https://www.ganintegrity.com/portal/country-profiles/poland/

Infosecurity 24., (2020). ABW zatrzymała obywatela Niemiec podejrzewanego o udział w grupie o charakterze terrorystycznym. *Inforsecurity24.pl*, 1.10. [Viewed 8 October 2020]. Available from: https://www.infosecurity24.pl/abw-zatrzymala-obywatela-niemiec-podejrzewanego-o-udzial-w-grupie-o-charakterze-terrorystycznym

Lesiecki R., (2019). Polska definicja szpiegostwa do zmiany. Szef speckomisji dla *InfoSecurity24.pl*, 16.01. [Viewed 8 October 2020]. Available from: https://www.infosecurity24.pl/polska-definicja-szpiegostwa-do-zmiany-szef-speckomisji-dla-infosecurity24pl

Maciążek P., (2019). *Gdzie się podziały jawne raporty ABW?*, 03.12 [Viewed 8 October 2020]. Available from: https://osluzbach.pl/2019/03/12/maciazek-gdzie-sie-podzialy-jawne-raporty-abw/

Ministerstwo Cyfryzacji., (2019). *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*. [Viewed 26 September 2020]. Available from: http://prawo.sejm.gov.pl/isap.nsf/ DocDetails.xsp?id=WMP20190001037

Mölder, H. (2016). The War of Narratives – Putin's Challenge to International Security Governance in Ukraine. *Estonian Journal of Military Studies*, VI (2)

Najwyższa Izba Kontroli., (2015). *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP. Informacja o wynikach Kontroli. KPB-4101-002-00/2014 Nr ewid. 42/2015/p/14/043/KPB*. [State authorities'

fulfillment of tasks related to protection of the Republic of Poland's cyberspace. The information of the control results]. [Viewed 26 September 2020]. Available from: https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf

Najwyższa Izba Kontroli., (2016). *Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych*, KPB.410.004.05.2015, Nr ewid. 42/2016/p/15/042/KPB. [Ensuring the operational security of IT systems used to carry out public tasks]. [Viewed 26 September 2020]. Available from: https://www.nik.gov.pl/plik/id,10771,vp,13104.pdf

Najwyższa Izba Kontroli., (2019). *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*, [Information security management in local self-government administration entities]. [Viewed 26 September 2020]. Available from: https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/pobierz,kap~p_18_006_20180726124543153260914 3~01,typ,kk.pdf

Internal Security Agency, (2020), *Obszary przestępczości korupcyjnej w Polsce w latach 2018–2019*, Internal Security Agency, Warsaw.

Ostrowski S., (2020). Ochrona polskich spółek przed przejęciami. Jak nowe prawo ma działać w praktyce?. *Forsal.pl* 2 June. [Viewed 8 October 2020]. Available from: https://forsal.pl/artykuly/1480601,ochrona-polskich-spolek-przed-przejeciami-jak-nowe-prawo-ma-dzialac-w-praktyce.html

Poland., (2020). *National Security Strategy of the Republic of Poland*. [Viewed 22 September 2020]. Available from: https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

Polska. *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*. Warszawa. Kancelaria Sejmu. [Viewed 26 September 2020]. Available from: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/ WDU20180001560/U/D20181560Lj.pdf

Raubo J., (2020). Pracowity rok polskich służb specjalnych [OPINIA], 6 stycznia. [Viewed 8 October 2020]. Available from: https://www.infosecurity24.pl/pracowity-rok-polskich-sluzb-specjalnych-opinia

Rządowe Centrum Bezpieczeństwa, (2020). *Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity. Uchwała nr 210/2015 Rady Ministrów z dnia 2 listopada 2015 r. w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej z uwzględnieniem Uchwały nr 116/2020 Rady Ministrów z dnia 13 sierpnia 2020 r. zmieniającej uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej*. [Viewed 10 October 2020]. Available from: https://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-2020-tekst-jednolity.pdf

Sazonov V. and Müür K., (2017), Introduction: Russian Hybrid and Information Warfare, in Sazonov V. et al (eds) *Russian Information Operations Against Ukrainian Armed Forces and Ukrainian Countermeasures (2014–2015),* ENDC Occasional Papers No 6/2017, pp. 9–12

Serwis Rzeczypospolitej Polskiej, 2020. *Podsumowanie działań ABW.* [Viewed 26 September 2020]. Available from: https://www.gov.pl/web/sluzby-specjalne/podsumowanie-dzialan-abw

Serwis Rzeczypospolitej Polskiej, 2020. *Silny kontrwywiad, silne gwarancje bezpieczeństwa.* [Viewed 21 September 2020]. Available from: https://www.gov.pl/web/sluzby-specjalne/silny-kontrwywiad-silne-gwarancje

Śliwa Z., (2017), "Hybrid Warfare" – The Military Security Domain's Considerations in Sazonov V. et al (eds) *Russian Information Operations Against Ukrainian Armed Forces and Ukrainian Countermeasures (2014–2015),* ENDC Occasional Papers No 6/2017, pp.13-27

Terrorism Prevention Centre of Excellence., (2020). *Centrum Prewencji Terrorystycznej to jednostka Agencji Bezpieczeństwa Wewnętrznego zajmująca się w szeroko pojętą profilaktyką antyterrorystyczną.* [Viewed 26 September 2020]. Available from: https://tpcoe.gov.pl/cpt/o-nas/1659,Centrum-Prewencji-Terrorystycznej-to-jednostka-Agencji-Bezpieczenstwa-Wewnetrzne.html

UN Security Council Counter – Terrorism Committee, 2019. *CTC conducts its first assessment visit to Poland.* [Viewed 28 September 2020]. Available from: https://www.un.org/sc/ctc/news/2019/12/17/ctc-conducts-first-assessment-visit-poland/

UOKiK, (2020). *Nord Stream 2 - maximum penalties imposed by UOKiK President.* [Viewed 25 September 2020]. Available from: https://www.uokik.gov.pl/news.php?news_id=16818

Wilkowicz Ł. (2020). 'Polska nie jest już bezpieczną przystanią. Chodzi o pranie pieniędzy' [online]. *Dziennik.pl.* 22 September. [Viewed 3 October 2020]. Available from: https://gospodarka.dziennik.pl/news/artykuly/7829060,polska-bezpieczna-przystan-pranie-pieniedzy-banki-knf-aml.html

Winnerstig, M. (2014). *Tools of destabilisation: Russian soft power and non-military influence in the Baltic States.* FOI-R-2990-SE. [Viewed 5 October 2020]. Available from: https://www.stratcomcoe.org/mike-winnerstig-ed-tools-destabilization-russian-soft-power-and-non-military-influence-baltic-states

Żaryn S., (2019). NATO 2020 Defined. Poland's Internal Security Service is critical to hunting down spies. *Defense News* December 2. [Viewed 8 October 2020]. Available from: https://www.defensenews.com/opinion/

commentary/2019/12/02/polands-internal-security-service-is-critical-to-hunting-down-spies/

Żaryn S., (2019). *Russia's hybrid warfare toolkit has more to offer than propaganda*, August 09. [Viewed 3 October 2020]. Available from: https://www.defensenews.com/opinion/commentary/2019/08/09/russias-hybrid-warfare-toolkit-has-more-to-offer-than-propaganda/

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV)., (2020). *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku*. [Viewed 5 October 2020]. Available from: https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/969,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2019-roku.html

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV)., (2019). *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku*. [Viewed 5 October 2020]. Available from: https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/964,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2018-roku.html

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV)., (2017). *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 roku*. [Viewed 5 October 2020]. Available from: https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/957,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2016-roku.html