Anna Grabowska-Siwiec
University of Bialystok
ORCID: 0000-0003-0788-4171
a.grabowska-siwiec@uwb.edu.pl

Threats to Poland and NATO member states posed by proxy agent networks

Abstract

The article examines the phenomenon of proxy agent networks as an instrument of contemporary intelligence activity, focusing on operational modalities and the associated threats to the security of Poland and NATO member states. The aim is to provide an in-depth analysis of proxy agent networks, with a particular focus on the practices employed by the Russian Federation. The text identifies the consequences of using proxy agents in the context of hybrid and information warfare. It explains why this form of agent network constitutes an effective tool for achieving intelligence objectives, enabling the aggressor to conduct destabilising operations. It also sets out recommendations for state services on how to build societal resilience to this category of intelligence threat.

Key words

agents, proxy, intelligence, counterintelligence, subversion

Introduction

In this article, I employ the term "proxy agent networks" to denote the indirect conduct of intelligence operations, whereby a state sponsor tasks non-state actors or third parties to achieve informational and active effects while maintaining distance and plausible deniability. At first mention, it is useful to note near-synonyms that may appear in the literature – "such as proxy agency, operations using intermediaries (proxy)", or "indirect/outsourced intelligence operations" – but for the sake of terminological consistency, I use only proxy

agent networks throughout. For clarity, I also distinguish this concept from agents of influence, which are primarily oriented towards shaping perceptions, narratives, and decision-making within media, culture, academia, or politics; they may feature within long-term classical intelligence architectures without necessarily operating in a proxy mode. By contrast, proxy agent networks describe a mode of execution (intermediation/outsourcing of risk and cost) that can encompass both influence work and task-oriented operations (reconnaissance, arson, sabotage, etc.).

The word "proxy" derives from English and denotes an agent or a power of attorney. When coupled with the term from the lexicon of security and intelligence services – *agent*, understood (following NATO usage)[1] as a person recruited, trained, directed, and employed to collect and transmit information – the combined notion of the proxy agent emerges[2]. In practice, proxy agent networks enable state services to act by proxy or instead of traditional agent handling (identifying, developing, recruiting, training, and maintaining liaison with assets over a sustained period). The constitutive features of proxy agent networks, to which this article will repeatedly refer, include: (1) indirectness of action, (2) plausible deniability for the sponsor, (3) variegated actors (individuals, loose groups, criminal intermediaries), (4) operational flexibility and scalability across jurisdictions, and (5) transnational reach often facilitated by digital communications.

The etymology of "proxy agent" is commonly linked to the concept of proxy warfare, which has deep historical roots. In the scholarly literature, a proxy war is defined as "an armed conflict in which a third party intervenes indirectly in order to influence the strategic outcome in favour of its preferred faction"[3]. A more specific military definition describes it as "a conflict in which the belligerents employ third parties as an additional means of waging war or as a substitute for the direct use of their own armies"[4]. The concept assumed

1 *Słownik terminów i definicji NATO*, https://wcnjik.wp.mil.pl/u/AAP6PL.pdf [access: 5.08.2025].

2 J.K. Wither, *Outsourcing warfare: Proxy forces in contemporary armed conflicts*, „Security and Defence Quarterly" 2020, vol. 31, no. 4, p. 17.

3 Ibidem.

4 C. A. Kozera et. al., *Game of Proxies – Towards a new model of warfare: Experiences from the CAR, Libya, Mali, Syria, and Ukraine*, „Security and Defence Quarterly" 2020, vol. 31, no. 4, p. 77–97.

particular significance during the Cold War, when the United States and the Soviet Union sought to conduct their rivalry without risking direct military confrontation or nuclear escalation. The USSR supported anti-colonial and revolutionary movements opposed to the West, while the USA backed anti-communist leaders and counter-revolutionaries.

The use of proxy agent networks has also been incorporated into the activities of security and intelligence services, particularly foreign intelligence. The term "security service" has not yet been defined in normative terms in Poland; however, in academic discourse, it is commonly understood to refer to services responsible for performing intelligence and counterintelligence tasks. The principal instruments of their activity are operational and reconnaissance measures designed to gather information. Historically, the data collected have served military ends; over time, active measures were added to informational tasks. These include, inter alia, shaping situations advantageous to the state (deception/disinformation), acquiring agents of influence, compromising opponents and targeted killings, as well as sabotage and subversion, and the orchestration of acts with a terrorist character.

Terminological and legal precision. In what follows, I treat "subversion/dywersja", "sabotage", and "terrorism" as legal categories, not colloquial labels. Their use is anchored in the Polish Criminal Code (e.g., the post-2023 wording of Art. 130 on espionage and forms of activity on behalf of a foreign intelligence service; the legal definition of a terrorist offence in Art. 115 §20) and in Directive (EU) 2017/541 on combating terrorism. Accordingly, I employ these terms only where they reflect official qualification by competent authorities, or—where such qualification is pending – use cautious formulations such as "actions of a subversive/sabotage character", explicitly attributing claims to ABW/Prokuratura Krajowa communiqués. This distinction also underlines that not every arson constitutes terrorism, and that legal assessment depends on statutory elements (intent to intimidate a population, coerce public authorities, scale of endangerment, etc.).

Each successive conflict has compelled the security services to expand their areas of operation. The apogee of remit expansion is typically dated to the Cold War, during which – as Tomasz R. Aleksandrowicz observes – "it is difficult to identify any area that would remain outside the sphere of interest

of the security services"[5]. Thus, the functions and tasks of the services are conditioned by the security environment and by the state's interpretation and perception of threats; changes in that environment drive changes in scope and methods. Analysing the tasks and objectives assigned to proxy agent networks allows us to identify them as a contemporary tool (notably in recruitment and digital tasking) employed by the Russian intelligence services. In Poland, the application of proxy agent networks is directly linked to the outbreak of war in Ukraine in February 2022 and to Poland's robust provision of military and international support to the Ukrainian authorities. Actors recruited into such networks pursue strategic aims aligned with those of the Russian state, including, among other objectives, the erosion of support for Ukraine and the reassertion of Russian influence.

Aleksandrowicz also draws attention to the problem of defining the adversary with whom the security services contend. Current hybrid-warfare practices suggest that state intelligence services are appropriating behaviors characteristic of non-state organisations – or masquerading as them – precisely to obscure the identity of the principal. This pattern satisfies the logic of proxy action and further justifies the analytical separation between agents of influence and proxy agent networks as distinct, though sometimes overlapping, categories.

The purpose of this article is to identify and conceptualise proxy agent networks as a contemporary instrument of Russian security and intelligence services, to describe their methods of operation (including digital recruitment, tasking and remuneration), to delineate their targets and effects in Poland and across NATO member states, and to propose avenues for counter-action – from legal-doctrinal clarity and strategic communications to operational counter-intelligence and international cooperation.

5 T.R. Aleksandrowicz, *Służby specjalne w strategicznym zapewnieniu bezpieczeństwa państwa*, [in:] *Strategia bezpieczeństwa narodowego Polski*, ed. J. Gryz, Warszawa 2013, p. 257.

Proxy agent networks in Poland

In 2024, the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego – ABW) published a communiqué characterising subversive (dywersyjne) activities directed against the Republic of Poland[6], as well as against member states of the European Union and NATO, which were initiated and coordinated by Russian special services. It is worth noting here why ABW is the body addressing this category of criminal activity. This follows from the Agency's statutory powers to identify, prevent and combat threats to the state's internal security and constitutional order in the civilian sphere, as well as to identify, prevent and detect the offence of espionage[7]. Espionage is defined in Art. 130 of the Polish Criminal Code[8]. It involves participating in the activities of a foreign intelligence service or acting on its behalf against the Republic of Poland or its partner countries. The 2023 amendment to Art. 130 also enumerates, as categories of activity on behalf of a foreign intelligence service, such conduct as subversion (dywersja), sabotage or offences of a terrorist character (§ 7)[9]. In the military domain, responsibility for prosecuting this kind of activity on behalf of a foreign intelligence service lies with the Military Counterintelligence Service (Służba Kontrwywiadu Wojskowego – SKW).

In the public domain, only ABW[10], together with the National Public Prosecutor's Office (Prokuratura Krajowa), disseminates information relating to the above-mentioned activities. This is linked to the Agency's competence in both identifying and countering this type of threat. One of the first public

6 *Komunikat dotyczący działalności dywersyjnej FR z dn. 25.10.2024 r.*, https://www.abw.gov.pl/pl/informacje/2569,Komunikat-dotyczacy-dzialalnosci-dywersyjnej--FR.html [access: 18.08.2025].

7 Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, t.j., Dz.U. 2025, poz. 902, art. 5.

8 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, t.j., ibidem, poz. 383, art. 130.

9 S. Hoc, *Szpiegostwo w znowelizowanym Kodeksie karnym*, „Nowa Kodyfikacja Prawa Karnego" 2023, no. 67, p. 119–143; P. Burczaniuk, *Przestępstwo szpiegostwa po nowemu, czyli w świetle nowelizacji Kodeksu karnego z 17 sierpnia 2023 roku*, „Przegląd Bezpieczeństwa Wewnętrznego" 2024, no. 30, p. 49–78.

10 It should be noted that the oldest communication published on the abw.gov.pl website currently dates back to 12.10.2023. It is not possible to read the communications from previous years relating to the activity of this service in the context of sabotage activities carried out for the benefit of foreign intelligence.

statements (since the outbreak of the regular armed conflict in Ukraine in 2022) concerning subversive operations conducted for a foreign intelligence service was the communiqué of 16 March 2023 regarding the actions of 12 persons suspected of cooperating with the Russian special services (it later transpired that the group numbered 16)[11]. The communiqué stated that "the group carried out monitoring of railway routes. Its tasks included, inter alia, identifying, monitoring and documenting consignments of armaments destined for Ukraine. The suspects were also preparing diversionary actions aimed at paralysing deliveries of equipment, weapons and aid for Ukraine"[12]. ABW further indicated that the group had also been tasked with propaganda activities designed to destabilise Polish-Ukrainian relations, to inflame and amplify in Poland sentiments hostile to NATO member states, and to attack the policy of the Government of the Republic of Poland towards Ukraine.

The only available report (more precisely, an infographic) presenting the scope of ABW's activities for the period 2015–2019[13], in identifying intelligence threats to the Republic of Poland, links them to "so-called hybrid warfare". The report underscores that "at present [2019] the boundary is becoming blurred between externally generated intelligence threats and hostile actions carried out within the state". It defines the most serious challenges in the security sphere as those that are associated with the aggressive policy of the Russian Federation. In the last four years [2015–2019], five diplomats of the Russian Federation were expelled from Poland, including four in response to the attempt to poison Sergei Skripal. Five individuals were also detained on espionage charges – three for Russia and two for China." At no point does this report refer to intelligence threats to Poland in the form of subversive or sabotage operations. It follows clearly that the first subversive activities, conducted on behalf of the Russian special services, to be detected and defined by ABW and disclosed publicly were those of the "16-person spy network" in 2023.

The last publicly known information about the activity of spy networks in Poland after the Second World War dates from the 1940s and 1950s. This

11 *ABW rozbiła siatkę szpiegowską*, https://www.gov.pl/web/sluzby-specjalne/abw-rozbila-siatke-szpiegowska [access: 19.08.2025].

12 Ibidem.

13 *Podsumowanie działań ABW*, https://www.gov.pl/web/sluzby-specjalne/podsumowanie-dzialan-abw [access: 19.08.2025].

concerned the network of André Robineau (an official of the French Consulate in Szczecin), who was detained in 1949 and convicted in 1950, together with six other individuals, for activities on behalf of French intelligence. Robineu was pardoned in 1953. Since the entry into force of Art. 130 of the Criminal Code in 1997, there have been no recorded cases of the disclosure of spy networks in Poland[14]. One cannot, however, exclude the existence of a dark figure[15]. The first spy network uncovered in the Third Republic numbered 16 persons, of whom 13, as announced by the National Public Prosecutor's Office in December 2023, were convicted by the Regional Court in Lublin and received aggregate custodial sentences ranging from 1 year and 1 month to 6 years' imprisonment, together with fines. The prosecutor charged the defendants with participation in an organised criminal group under Art. 258 §1 of the Criminal Code and acting for the benefit of a foreign intelligence service against the interests of the Republic of Poland under Art. 130 § 1. The investigation established that the group operated from January 2023 to March 2023 in various locations, including Biała Podlaska, Chełm, Medyka, Przemyśl, Rzeszów, Warsaw, and other localities across the country. The defendants undertook activities, including reconnaissance of critical infrastructure, such as military facilities and seaports. They continuously informed their principals of the results of their intelligence-gathering efforts, for which they received remuneration. The bill of indictment covered a total of 16 individuals belonging to a spy network that was cooperating with Russian special services. The accused were identified as foreign nationals from beyond Poland's eastern border (13 Ukrainian citizens, 2 Belarusian citizens and one Russian – an ice-hockey player). They conducted intelligence as well as propaganda activities against Poland and prepared acts of subversion on the instructions of Russian intelligence. The remaining three individuals were tried in separate proceedings[16].

14 S. Hoc, *Siatki szpiegowskie w kontekście art. 130 kk*, [in:] *Prawo karne na przełomie wieków. Księga jubileuszowa profesora Ryszarda A. Stefańskiego*, eds. M. Rogalski, J. Kosonoga, J.A. Dąbrowski, Warszawa 2025, p. 269.

15 A dark figure is a criminological concept that refers to the number of crimes actually committed that are not included in official crime statistics due to their failure to be disclosed by law enforcement agencies or reported by victims.

16 S. Hoc, *Siatki szpiegowskie*…, p. 283.

In subsequent years, the National Public Prosecutor's Office, in cooperation with the Internal Security Agency and in collaboration with partner countries, identified further subversive operations carried out at the instruction of Russian special services. These include, inter alia:

1. Arson attacks in May 2024 on two construction depots in the Masovian Voivodeship. The operations were commissioned, supervised and financed by an individual linked to the Russian special services – a Colombian national. The suspect received detailed instructions regarding targets and modes of execution via the Telegram messenger. He has already been convicted by a Czech court and sentenced to eight years' imprisonment for the arson of a bus depot in Prague. A Joint Investigation Team was established in the case with the participation of Poland, the Czech Republic, Romania and Lithuania[17];

2. In July 2024, Kristina S. (a Ukrainian national) took part in sending a courier parcel containing explosive materials: nitroglycerin, military electric detonators, an initiation device, a metal vacuum flask with a shaped-charge insert, and powdered aluminium. The device constituted a so-called shaped-charge bomb. The consignment was detected and secured in the warehouses of a courier company in the Łódź Voivodeship. She acted in concert with a Ukrainian national and two Russian citizens. ABW charged the Ukrainian woman with the offence of complicity in bringing about a direct danger of an explosion of explosive materials (sabotage activity)[18];

3. On 6 August 2025, an indictment was filed against three Belarusian nationals and three Polish nationals engaged in organising and carrying out acts of subversion on the territory of Poland. They were accused of setting fire to a building materials warehouse in Gdańsk and attempting to set fire to a company in Marki, near Warsaw. In addition, the group was involved in the illicit trade in weapons, ammunition, explosives and narcotic drugs.

17 *Działał na rzecz obcego wywiadu przeciwko RP. 21 lipca br. Kolumbijczyk usłyszał zarzuty*, https://www.abw.gov.pl/pl/informacje/2662,Dzialal-na-rzecz-obcego-wywiadu-przeciwko -RP-21-lipca-br-Kolumbijczyk-uslyszal-z.html [access: 21.08.2025].

18 *Akt oskarżenia w sprawie planowania działań sabotażowych*, https://www.abw.gov.pl/pl/informacje/2665,Akt-oskarzenia-w-sprawie-planowania-dzialan-sabotazowych.html [access: 21.08.2025].

The investigation revealed the mechanisms by which subversive actions were commissioned and executed on the instructions of foreign services, as well as the routes used to smuggle illicit materials from Ukraine into EU member states[19];

4. On 12 May 2025, the National Public Prosecutor's Office announced that the fire at the shopping centre on ul. Marywilska 44 in Warsaw on 12 May 2024 had been the result of arson commissioned by the intelligence service of the Russian Federation. The evidentiary material gathered in the case allowed charges to be brought against two Ukrainian citizens who acted in concert with the perpetrators of the arson. The group's objective was to carry out arson attacks on large-format facilities within EU member states. This group is also responsible, inter alia, for the arson of an IKEA store on 9 May 2024 in Vilnius[20].

Communiqués issued by ABW and the National Public Prosecutor's Office reveal the systematic activity of foreign special services – primarily Russian and Belarusian – using proxy agents against Poland and its allies. The activities include:

– Arson attacks on civilian and industrial facilities;

– Dispatch of consignments containing explosive materials transported by courier companies;

– Propaganda operations aimed at polarising society;

– Classical espionage against defence-significant facilities (so-called external reconnaissance, conducted chiefly on behalf of the Belarusian special services);

– Operations targeting Russian and Belarusian opposition figures.

The majority of perpetrators – particularly of subversive acts – are young people originating from Belarus and Ukraine; they are most commonly financially motivated and recruited via internet messengers (Telegram).

19 *Akt oskarżenia w sprawie działań dywersyjnych na rzecz obcego wywiadu*, https://www.abw.gov.pl/pl/informacje/2666,Akt-oskarzenia-w-sprawie-dzialan-dywersyjnych-na-rzecz-obcego-wywiadu.html [access: 21.08.2025].

20 *Zarzuty w związku z pożarem hali przy ul. Marywilskiej 44*, https://www.gov.pl/web/prokuratura-krajowa/zarzuty-m44 [access: 21.08.2025].

Proxy agent networks targeting NATO member states

Subversive operations conducted by proxy agents on the instructions of Russian intelligence are taking place not only on the territory of Poland but are also directed against other NATO member states. In April 2024, two individuals (German citizens of Russian origin) were detained in Germany for preparing, at the behest of Russian intelligence, attacks on military installations, arms factories, industrial facilities and transport infrastructure used to supply Ukraine. The planned actions took the form of arson and the detonation of explosive devices, and one of the intended targets comprised installations of the United States Armed Forces in Bavaria, where Ukrainian soldiers[21] are being trained. In Lithuania, Latvia, Estonia and the United Kingdom, saboteurs inspired by Russia have primarily attacked so-called soft civilian targets (e.g., industrial halls, shops, warehouses)[22]. In May 2022, persons preparing an attack on the Lielvārde military air base were detained in Latvia[23].

As indicated above, once selected and tasked, a given individual may carry out similar activities across several countries. Such was the case, inter alia, with the Colombian national who operated in the Czech Republic and Poland, while the perpetrators of the fire at the shopping centre on ul. Marywilska 44 in Warsaw are also responsible for the arson of an IKEA store on 9 May 2024 in Vilnius.

Characteristic features of the intelligence use of proxy networks

When characterising proxy agent networks in the context of special services' activities, attention should be paid to features such as the utilisation of non-state actors or individuals motivated ideologically and/or financially to achieve intelligence objectives without the direct involvement of official intelligence structures. The term "proxy agent network" may also refer to systems and mechanisms whereby intelligence services employ intermediaries to collect

21 F. Bryjka, *Rosyjskie działania dywersyjne wobec państw NATO*, „Biuletyn PISM" 2024, no. 112.
22 Ibidem.
23 Ibidem.

information, conduct operations or perform tasks that, for various reasons, they cannot or do not wish to undertake directly through official structures.

The characteristic features of proxy networks include:

1) Structural features:

a) Indirect mode of operation – the principal (here understood as the commissioning party) acts through intermediaries, allowing it to retain distance from the operations conducted,

b) Diversity of actors – proxy networks may encompass a wide range of non-state entities, individuals or groups who may or may not be in some form of mutual dependency,

c) Operational flexibility – proxies enable action in the "grey zone" between peace and war, exploiting information activities, cyber operations, clandestine actions by the special services or ordinary criminal conduct;

2) Functional features:

a) Plausible deniability – although contemporary proxy operations often do not conceal the sponsor's involvement, they still afford a degree of deniability in the event of failure,

b) Cost-effectiveness – employing proxies is significantly cheaper than directly engaging regular armed forces or official intelligence structures by recruiting so-called classical agents,

c) Risk minimisation – proxies allow the sponsor to avoid the negative political consequences associated with direct involvement;

3. Strategic features:

a) Long-term horizon – the use of proxy networks frequently presupposes long-term strategic relationships. Actions taken today may yield the desired effect for the sponsor in a decade or more'

b) Multidimensionality – contemporary proxy networks encompass not only military aspects but also technical, cyber and informational dimensions (disinformation, propaganda),

c) Adaptability – proxy agents can be rapidly adjusted to the sponsor's changing operational and strategic requirements.

Attention should also be drawn to the targets of proxy attacks in Poland, which have primarily been civilian facilities, including warehouses and large retail outlets, with arson as the principal method employed. Hostile activity is increasingly taking on the characteristics of terrorist conduct.

Conclusion and Recommendations

As is unambiguously evident from official ABW and National Public Prosecutor's Office communiqués, an intensification of subversive activity carried out by proxy networks in Poland has been observed since 2023. The ABW communiqué of 25 October 2024 is the first to provide a synthetic summary of such operations on behalf of a foreign intelligence service and marks a watershed in ABW's official public communications. For the first time, it directly employed the term "subversive activities" in the context of Russian special services, thereby introducing a new category of threats into the public discourse on the state's internal security. The communiqué presents a comprehensive analysis of Russian subversive operations, highlighting their systematic and coordinated nature. It discloses details of operational methodology, including the use of internet messengers for recruitment and handling, payments to contractors in cryptocurrencies, and the recruitment of individuals from countries such as Ukraine and Belarus[24].

The strategic objectives of Russian subversive activity were also identified: to intimidate citizens of Poland and of Western states and to discourage support for Ukraine and its people. An important aspect is the drive to foment chaos, a sense of insecurity, distrust of state authorities, social unrest and internal destabilisation. The long-term consequences of such actions may also include a crisis of democratic values, deep societal polarisation, and the entrenchment of anti-immigrant and extreme nationalist attitudes.

It is noteworthy that neither ABW nor the National Public Prosecutor's Office uses the term "proxy network" in their communiqués. This may be linked to an avoidance of terminology reserved for operational practice and associated with classified operational guidelines. In many countries, the terms "agent" and "agent network" are professional designations drawn from the operational vocabulary of the special services.

The publication of the communiqué also signifies ABW's formal recognition of a new dimension of Russian hybrid activities directed against

24 The use of the term "coming from former USSR countries" by the Internal Security Agency is noteworthy, which, in the author's opinion, is a measure aimed at not directly pointing to Ukrainian citizens so as not to incite social antagonisms between Ukrainians and Poles.

Poland – subversive and sabotage operations with a terrorist character. In the Author's assessment, these do not replace traditional intelligence operations, such as the cultivation of durable agents of influence, work under non-official cover, diplomatic cover or the exploitation of walk-ins. The aforementioned classical intelligence activities may proceed in parallel with newer tools such as proxy networks. Cyberspace and the widespread use of social media have been integrated into intelligence operations as inexpensive and practical tools, enabling the recruitment and effective deployment of proxy agents in areas such as subversion, sabotage, and terrorist activity.

In building resilience to proxy-network operations, the activity of state institutions – including services responsible for counterintelligence tasks – is of cardinal importance. Beyond the October 2024 communiqué, there is a lack of information materials from ABW promoted through widely accessible channels commonly used by the public, such as social media (e.g., TikTok and Instagram) and podcasts. It is worth noting the niche character of sources such as the abw.gov.pl website. Research conducted by the Author on a defined cohort of students showed that potential audiences seeking knowledge about Polish special services via their websites amounted to between 30% and 50% (depending on gender and year of study)[25]. Notably, these were individuals who already possessed preliminary knowledge of Poland's special services and were self-motivated to expand it.

To date, Poland has not seen a public-awareness campaign informing citizens about the threats posed by proxy networks and the desired patterns of behaviour. Citizens do not know how to react when they observe individuals behaving suspiciously – for example, installing cameras along railway routes. The fact that ABW, which most frequently issues statements on this subject, does not employ the term "proxy network" has a desensitising effect: the phenomenon lacks rigorous, clear and socially recognisable definitional framing.

The detection, prosecution and prevention of proxy-network activity conducted on behalf of foreign intelligence services also requires appropriate tools and personnel resources on the part of ABW and SKW. Staffing continuity

25 A. Grabowska-Siwiec, *Służby specjalne – czy są atrakcyjnym miejscem pracy dla młodych Polaków?*, „Special OPS" 2023, no. 2, p. 28–33.

in Poland's special services, including counterintelligence, is subject to cyclical disruption associated with the electoral cycle. This does not favour effective action against foreign intelligence services operating in the country, whose activities are inherently long-term – an aspect often poorly understood by both political decision-makers and the general public. As Stanisław Hoc argues, it is essential to enhance counterintelligence effectiveness in combating espionage by ensuring a proper standard of operational work, utilising both technical and human assets, and fostering close cooperation between the operational and investigative branches, among other measures[26].

The prosecution of proxy networks – which also exhibit transnational characteristics – requires cooperation between Polish special services, the Police, and the prosecutor's office, as well as their counterparts in NATO and EU member states. ABW declares intensive international cooperation, including with the authorities of Lithuania, Germany and the United Kingdom. The exchange of experience and knowledge regarding the adversary's modus operandi is crucial to preventing and combating proxy-network activity.

Bibliography

Aleksandrowicz T.R., *Służby specjalne w strategicznym zapewnieniu bezpieczeństwa państwa*, [in:] *Strategia bezpieczeństwa narodowego Polski*, ed. J. Gryz, Warszawa 2013.

Bryjka F., *Rosyjskie działania dywersyjne wobec państw NATO*, „Biuletyn PISM" 2024, no. 112.

Burczaniuk P., *Przestępstwo szpiegostwa po nowemu, czyli w świetle nowelizacji Kodeksu karnego z 17 sierpnia 2023 roku*, „Przegląd Bezpieczeństwa Wewnętrznego" 2024, no. 30.

Grabowska-Siwiec A., *Służby specjalne – czy są atrakcyjnym miejscem pracy dla młodych Polaków?*, „Special OPS" 2023, no. 2.

Hoc S., *Siatki szpiegowskie w kontekście art. 130 kk*, [in:] *Prawo karne na przełomie wieków. Księga jubileuszowa profesora Ryszarda A. Stefańskiego*, eds. M. Rogalski, J. Kosonoga, J.A. Dąbrowski, Warszawa 2025.

Hoc S., *Szpiegostwo w znowelizowanym Kodeksie karnym*, „Nowa Kodyfikacja Prawa Karnego" 2023, no. 67.

26 S. Hoc, *Szpiegostwo w znowelizowanym…*, p. 120.

Kozera C.A. et al., *Game of Proxies – Towards a new model of warfare: Experiences from the CAR, Libya, Mali, Syria, and Ukraine*, „Security and Defence Quarterly" 2020, vol. 31, no. 4.

Wither J.K., *Outsourcing warfare: Proxy forces in contemporary armed conflicts*, „Security and Defence Quarterly" 2020, vol. 31, no. 4.