RUSSIAN HYBRID WARFARE AGAINST POLAND 2022–2025: FROM ESPIONAGE AND SABOTAGE TO DRONE INCURSION

DOI: https://doi.org/10.37458/nstf.27.1.1
Original scientific paper
Received: December 1, 2025
Accepted: February 25, 2026

Przemysław Gasztold*

Abstract: This article examines the evolution of Russian hybrid warfare against Poland between 2022 and 2025, arguing that Poland has become both a frontline target and a testing ground for Moscow's adaptive toolkit of coercion below the threshold of open war. It situates Russia's activities in the context of Poland's strongly pro-Ukrainian posture, its role as the principal logistics hub for Western military assistance, and the expanding presence of NATO infrastructure on its

* **Przemysław Gasztold,** PhD, Assistant Professor at the Faculty of National Security at War Studies University in Warsaw; Senior Research Fellow at the Historical Research Office of the Institute of the National Remembrance in Warsaw; Senior Fellow (Non-Resident) at Orion Policy Institute, DC, USA; e-mail: p.gasztold@akademia.mil.pl

territory. Conceptually, the article engages with debates on hybrid warfare and sabotage, treating Russian operations as part of a long-term continuum rooted in Soviet doctrine and updated for contemporary conflict. Empirically, the study combines analysis of official documents, media reporting and existing scholarship to reconstruct a sequence of operations: the weaponization of migration on the Polish-Belarusian, and a series of espionage and sabotage cases involving both classic HUMINT assets and expendable "single-use" agents. Particular attention is devoted to two recent incidents - the September 2025 drone incursion into Polish airspace and the November 2025 explosion on the Warsaw-Lublin railway line which are interpreted not as isolated episodes but as escalatory steps in a broader strategy of coercive ambiguity toward NATO's Eastern Flank. The article concludes that Russian hybrid operations in Poland pursue not only military and logistical objectives, but also the gradual re-engineering of public attitudes, especially toward Ukraine. It argues that effective responses require integrated counterintelligence, the protection of critical infrastructure, and allied fusion mechanisms, alongside careful management of public communication to avoid amplifying the Kremlin's narratives.

Keywords: Russian hybrid warfare; Poland; espionage, sabotage; NATO

Introduction

On the night of 9-10 September 2025 twenty-one Russian drones violated Polish airspace, marking the most serious incident between NATO and Moscow since the onset of Russia's full-scale invasion of Ukraine in 2022. In response, Prime Minister Donald Tusk stated

that "Poland is closer to military conflict than at any time since the Second World War" (Walker et al., 2025). Although earlier incursions by Russian drones had been reported, none had occurred on such a scale, nor had they been perceived as sufficiently threatening to warrant an air-defense response. While the Kremlin denied responsibility, and some military analysts, political commentators, and politicians, including U.S. President Donald Trump, attempted to frame the episode as accidental (Kayali, 2025; Bo Lillis et al., 2025), the incident nonetheless signaled a qualitative escalation in Russia's hybrid campaign against Poland and the broader NATO alliance. Just over a month later, on 16 November 2025, an explosion damaged a railway line used to transport supplies to Ukraine, an event Prime Minister Tusk described as an "unprecedented act of sabotage" (Reuters, 2025). Far from constituting isolated provocations, the drone incursion and railway attack exemplify Moscow's adaptive use of hybrid tactics designed to generate ambiguity, instill fear and confusion, probe NATO's response thresholds, and erode public confidence within allied societies.

The purpose of this article is to analyze the instruments of Russian hybrid warfare deployed to generate fear, uncertainty, and destabilization in Poland from the outset of Russia's full-scale invasion of Ukraine in 2022 through 2025. Although the literature on hybrid warfare has expanded significantly, no comprehensive study has examined the Kremlin's malign activities directed specifically at Poland during this period, particularly the most recent developments. This article therefore addresses the following research question: How has Russian hybrid warfare against Poland evolved between 2022 and 2025, and what does this reveal about

Moscow's strategy toward NATO's Eastern Flank? The analysis advances three core claims. It argues that Russian intelligence activities in Poland have shifted from a predominantly residency-based HUMINT model toward a mixed architecture that combines traditional assets with a "franchised" system of expendable, "single-use" agents recruited largely online. It contends that recent kinetic signals, in particular the September 2025 drone incursion and the November 2025 railway sabotage should be understood not as discrete anomalies but as escalatory additions to an already dense repertoire of hybrid tools. Finally, the article maintains that these operations pursue a dual objective: disrupting the logistical backbone of Western support for Ukraine and gradually re-engineering social attitudes within Poland, particularly by undermining the pro-Ukrainian consensus and amplifying perceptions of Ukraine as a security liability.

This study employs a qualitative, process-tracing approach that reconstructs the evolution of Russian hybrid operations through a structured narrative of escalation between 2022 and 2025. The analysis draws on multiple types of sources, including official statements and press releases issued by Polish state institutions; investigative reporting from local and international media; open-source intelligence materials; and academic as well as policy-oriented literature on hybrid warfare. Case selection follows a logic of analytical relevance, and incidents were included not for their exceptional or sensational character, but because they mark identifiable shifts in Russian methods and reveal broader patterns of adaptation. The objective is not to provide an exhaustive catalogue of all hostile activities, but to trace the mechanisms through which

Moscow recalibrated its hybrid toolkit in response to counterintelligence pressure and changes in the wider security environment.

The article begins by outlining Poland's foreign policy orientation and its support for Ukraine, before assessing the conceptual debate on hybrid threats and their domestic reception through selected Polish cases. The analysis then situates the September 2025 drone incursion not as an isolated incident but as part of a sustained and escalating sequence of hostile measures designed to undermine and challenge Western security. By embedding the incident within the broader continuum of hybrid operations targeting Poland, the article demonstrates how Moscow integrates tactical provocations into a wider strategy of coercive ambiguity and pressure along NATO's Eastern Flank. The second part examines Russian espionage, sabotage, and the growing reliance on expendable or "single-use" agents, drawing on several illustrative cases to show how Russian intelligence adapted its methods following the expulsion of Russian diplomats from Warsaw in 2022. The article concludes by reflecting on the evolving nature of Russian hybrid warfare and outlining potential future scenarios for regional security

Poland, the War in Ukraine, and Russia's Hybrid Warfare Strategy

Since the full-scale Russian invasion on Ukraine in February 2022 the Polish approach to the war in Ukraine has been characterized by a combination of consistency, historical consciousness, and political unity across the domestic spectrum. Both the Polish political elite and broader society demonstrated an unprecedented

consensus in offering unconditional support for Ukraine and Ukrainians resisting Russian aggression. This response was deeply rooted in Poland's own historical experiences of Kremlin imperial domination and in its enduring culture of distrust toward Moscow's revisionist ambitions (Dyduch and Góra, 2024, pp. 306-307). Whereas in the past warnings from Warsaw about the growing threat posed by Russia were frequently dismissed by Western governments, and at times characterized as expressions of Russophobia, the outbreak of the war demonstrated that NATO's Eastern Flank states had in fact accurately assessed and anticipated the Kremlin's behavior. As a result, these countries now command greater attention and credibility among Western European partners than they did previously (Akbik, 2025).

Consistent with its strongly pro-Ukrainian stance, the Polish government opened its borders to Ukrainian refugees following the beginning of the invasion. By mid-May 2022, approx. 3.5 million people had crossed into Poland seeking safety (Duszczyk and Kaczmarczyk, 2022, p. 164). Poland also emerged as one of Kyiv's staunchest allies in the field of arms transfers. Tens of thousands of Ukrainian soldiers were trained on Polish territory, and between 2022 and 2025, Warsaw provided Ukraine with 46 military aid packages amounting to a total value of over EUR 4 billion (USD 4.5 billion). Poland not only transferred its own post-Soviet weaponry but also actively lobbied within NATO to persuade more reluctant allies to increase their support for Kyiv. In January 2023, Poland broke the international deadlock over the delivery of Leopard 2 tanks to Ukraine by initiating the formation of the so-called "tank coalition." According to a government

report, between 2022 and 2024, Poland donated to Ukraine 318 tanks, 586 armored vehicles, 137 artillery systems, 10 aircraft (MiG-29), and 10 helicopters (Mi-24).

Due to its geographical location, Poland has also served as the main logistical hub for Western assistance, with over 90% of all military aid to Ukraine transiting through Polish territory, primarily via the Rzeszów Airport and border crossings (Rada do Spraw Współpracy z Ukrainą, 2025). Moreover, in February 2025 the NATO-Ukraine Joint Analysis, Training and Education Centre (JATEC) was established in Bydgoszcz with the aim of facilitating the exchange of operational experience between Ukrainian and allied forces (Ministerstwo Obrony Narodowe, 2025). This proactive stance combined with Warsaw's leadership in advocating stronger sanctions and deeper NATO engagement has elevated Poland from a previously peripheral EU member to a central actor within Europe's security architecture, exemplifying the eastward shift of the continent's political center of gravity (Sus, 2025, p. 1200).

The multidimensional nature of Poland's support for Ukraine, the expanding presence of NATO infrastructure and troops, together with its deeply entrenched distrust of Russia and the absence of any illusions about the Kremlin's intentions, has made Poland one of the principal targets of hybrid operations. This, however, does not imply that Warsaw had previously been free from espionage or disinformation activities. During the Cold War, Poland was part of the Soviet sphere of influence, but after 1990 it adopted a distinctly pro-Atlantic and pro-Western orientation, culminating in its accession to NATO in 1999 and the

European Union in 2004 (Palczewska, 2024). Even during the 1990s, when Russia faced severe internal crises and many Western analysts anticipated its gradual democratic transformation, the Kremlin did not abandon offensive intelligence operations against Poland (Nyzio, 2023, p. 7; Bułhak and Friis, 2025, p. 11). Following Vladimir Putin's rise to power, these activities not only continued but intensified, steadily taking the form of hybrid warfare aligned with Moscow's revisionist policies toward Georgia (2008) and Ukraine (since 2014). In this context, as Daniela Richterova (2024) emphasized, Russia's current operations such as disinformation, espionage, and sabotage should not be viewed as isolated reactions to NATO's stance on the war in Ukraine, but rather as integral components of a long-standing repertoire rooted in the tradition of Soviet warfare doctrines and continually adapted to the hybrid paradigm of modern conflict.

Indeed, there are numerous parallels between the Kremlin's Cold War strategies designed to influence, disrupt, and destabilize adversaries in times of potential conflict, and Russia's contemporary modus operandi, which is commonly conceptualized within the framework of hybrid warfare. The concept itself has been defined in multiple ways and has become institutionalized within the doctrines of NATO, the EU, and several member states. It now serves as a key reference point for a growing body of studies, policy analyses, and scholarly publications, occupying a central place in contemporary security discourse (Libiseller, 2023). Scholars have developed a wide range of approaches and interpretations, focusing on aspects such as non-kinetic operations, asymmetric threats, and the blurring of war and peace while simultaneously

deconstructing earlier frameworks and debating overlapping terminology (Murray and Mansoor, 2012; Schroefl and Kaufman, 2014; Banasik 2015; Lanoszka, 2016; Johnson, 2017; Fridman, 2018; Elak and Śliwa, 2019; Caliskan, 2019; Almäng, 2019; Bērziņš, 2019; Rauta, 2019; Mumford, 2020; Janičatová and Mlejnková, 2021; Iskandarov and Gawliczek, 2022; Genini, 2025).

Over time, hybrid warfare has evolved into an umbrella term, comparable in its conceptual ambiguity to terrorism, encompassing a wide array of phenomena that scholars and policymakers link to contemporary security challenges - most recently, to sabotage, with some incidents now being described through both lenses. (Gasztold and Gasztold, 2020; Maniszewska, 2024). However, many scholars doubts its usefulness as a concept for explaining Russia's actions, its foreign agenda, and the future trajectory of warfare (Pynnöniemi and Jokela, 2020, p. 829; Renz, 2016, p. 186). Others, such as Tad Schnaufer (2017), argue that the concept of hybrid warfare does not adequately capture the nature of Russian operations in Ukraine since 2014. Instead, he proposed the notion of non-linear warfare, understood as a form of conflict without clear front lines or distinct friendly and enemy zones, unfolding through fluid and overlapping spheres of influence and operating by subverting and fragmenting an opponent's social and political structures, thereby enabling an aggressor to exploit opportunities through flexible, often minimally planned actions that extend beyond conventional military force. While current literature offers vast definitions and frameworks in which hybrid warfare may be conceptualized, one might look at Jacobs and Lasconjarias (2025, p. 3) who interpret this phenomenon

as form of "violent conflict that simultaneously involves state and non-state actors, with the use of conventional and unconventional means of warfare that are not limited to the battlefield or a particular physical territory".

Despite its acknowledged conceptual ambiguity, this article employs the term "hybrid warfare" as a pragmatic umbrella category, primarily because it has become institutionalized in NATO and EU documents and is widely used within Polish security discourse (Biuro Bezpieczeństwa Narodowego, 2025). Its adoption therefore provides a shared analytical vocabulary for examining contemporary forms of coercive behavior that operate below the threshold of armed conflict. At the same time, the article treats the concept not as a precise theoretical model but as a heuristic framework that captures the adaptive and flexible nature of Russian operations, namely their capacity to integrate new forms of coercion, such as drone incursions or controlled airspace violations, into an existing repertoire of hostile activities including disinformation, deception, sabotage, cyber operations, instrumentalized migration, and terrorism. When viewed comprehensively, these methods delineate the contours of Russia's broader strategy of "neither war nor peace," the quintessential hybrid modus operandi.

A substantial body of scholarship has examined the multifaceted nature of Russian hybrid warfare directed against Poland, cumulatively offering a detailed picture of both its instruments, short and long-term objectives. Existing research highlights the implications of Russian activities for the security of NATO's Eastern Flank (Śliwa, 2022; Banasik, 2020; Sadowski et al., 2023; Miszczuk, 2025) and analyses their effects on the

operational environment of the Polish armed forces (Piekarski, 2019). Scholars have also explored specific operational tools, including radio-frequency jamming (Westbrook, 2024), a range of Russian tactical approaches (Żywczyk, 2025; Starosta, 2024), and the deployment of disinformation and propaganda strategies (Wenzel et al., 2023; Zadorożna and Butuc, 2024; Wóycicki et al., 2017). Another strand of research focuses on the diffusion of Russian narratives within the Polish academic space (Gajos and Wyciszkiewicz, 2025), the use of terrorism and coercive violence as components of hybrid operations (Piekarski, 2022), and the employment of cyberspace as a domain of contestation (Stodolnik, 2025; Duda and Kowalska, 2025; Pelc, 2024). Complementing these perspectives is emerging work on Russian cognitive warfare techniques, which seek to shape perceptions, decision-making, and public sentiment (Bukowski, 2025). Within the broader information domain, particular attention has been devoted to the "battle for memory", the Kremlin's efforts to manipulate historical narratives as a means of influencing contemporary political attitudes. In this context, Russia attempts to exploit long-standing historical tensions between Poland and Ukraine, seeking to exacerbate divisions and intensify societal polarization (Kiera, 2024; Olech and Dobrowolska, 2022; Darczewska, 2019). Taken together, this literature demonstrates a broad scholarly consensus: Russian hybrid warfare against Poland is multidimensional, strategically adaptive, and deeply embedded in both physical and cognitive domains, with historical memory and identity politics constituting key arenas of contestation.

Even before the Russian invasion of Ukraine, Poland became the target of a complex, state-orchestrated operation at its border with Belarus, which involved facilitating and directing migrants from the Global South to attempt illegal crossings into the EU. This instrumentalization of migration served multiple objectives. Its primary aim was to destabilize the internal situation in Poland by generating acute humanitarian and security pressures on state institutions. Simultaneously, it sought to polarize Polish society by deepening political and moral divisions over the country's approach to foreigners, asylum seekers, and border protection. More broadly, sought to diminish public trust in state authorities, generate friction within the EU and NATO, and probe the resilience of Poland's border-management system (Wawrzusiszyn, 2022; Wawrzusiszyn, 2025; Filipec, 2022; Łubiński, 2022; Sari, 2023; Jakubiak, 2024).

There were also additional benefits that Minsk derived from the weaponization of migration, ones it may not have anticipated when initiating this pressure. When Polish soldier Emil Czeczko, deployed on the border, defected to Belarus in December 2021, the Lukashenka regime quickly integrated his case into its disinformation campaign. The migration pressure became a vehicle for amplifying false narratives, for example, Czeczko claimed on Belarusian state television that Polish Border Guard officers were intoxicated and repeatedly opened fire on refugees before burying them in mass graves (Kuśmirek, 2022, p. 316; Yeliseyeu, 2024). Czeczko died in Belarus under unexplained circumstances in March 2022. The regime in Minsk continues to exploit his defection for propaganda purposes. In March 2023, it established the Emil Czeczko International Charitable

Foundation, which introduced the "Peace and Human Rights Award," conferred on pro-Belarusian and pro-Russian politicians and journalists. The border pressure also led to numerous injuries among Polish border guards and soldiers, who were attacked by migrants in several incidents. There were lethal events as well, including the June 2024 attack in which a Polish soldier was fatally wounded while performing his duties at the border (Żywczyk, 2025, pp. 66–67).

In 2023, the Polish Border Guard registered approx. 26,000 attempts to illegally cross the Belarus-Poland border; in 2024 this figure increased to roughly 30,000 (Polskie Radio Białystok, 2025). From January to late November 2025, the service recorded an additional 27,700 such attempts (Bura, 2025). The situation coincided with the joint Russian-Belarusian military exercise Zapad 2025, during which Poland temporarily closed the border to all passenger and freight traffic. Although the decision carried economic costs for both sides, it was intended as a form of pressure on Minsk to cease instrumentalizing migration. On 17 November 2025, Poland reopened an additional border crossing with Belarus (Infosecurity24, 2025). Following this step, the Border Guard did not report a single new attempt to cross the border illegally, which may suggest the existence of an informal understanding between Warsaw and Minsk (Wprost, 2025). In return for reopening the border, Belarus was likely expected to reduce or halt the engineered migration flow. Whether these expectations will be met remains to be seen, and further observation is required to assess Belarus's long-term compliance.

While cyberattacks, disinformation, and border pressure had failed to provoke unrest or weaken public trust in

state institutions, the Kremlin turned to another, far more dramatic instrument from its hybrid warfare toolkit. The events of 9-10 September 2025 marked a critical inflection point in Russia's hybrid confrontation with NATO. Over the course of a single night, twenty-one Russian drones violated Polish airspace constituting the first large-scale breach of NATO airspace by Russia since the onset of its full-scale invasion of Ukraine (Polska Agencja Prasowa, 2025).

Polish and Dutch aircrafts, specifically Polish F-16s and Dutch F-35s, intercepted and shot down four of the unmanned aerial vehicles, which were later identified as decoy systems consistent with the Geran/Gerbera family of drones. In response to the scale and nature of the incursion, Poland initiated consultations under NATO's Article 4, signaling both the seriousness of the event and its broader implications for Alliance cohesion and deterrence posture (Olech, 2025). Although some commentators initially raised the possibility that the drones had strayed unintentionally due to navigational failures, the pattern and concentration of the incursion strongly suggested an intentional act. The incident appeared consistent with a deliberate Russian effort to probe Western air-defense systems, test reaction times, and assess NATO's political, military, and societal responses to a controlled breach of its airspace. This interpretation aligns with Russia's established preference for operating within the grey zone between provocation and overt aggression, maintaining plausible deniability while pursuing strategic gains. The deployment of decoy drones further reinforces the view that the operation was choreographed to appear accidental while simultaneously yielding operational

intelligence on allied detection and interception capabilities (van den Berg and Stijnman, 2025).

The incursion also generated political repercussions within Poland, intensifying pre-existing tensions between the president, his administration, and the government, and thereby further complicating the domestic management of the crisis. At the same time, Russian-linked disinformation campaigns exacerbated societal anxieties by promoting narratives that framed the incident as a Ukrainian provocation (Ministerstwo Cyfryzacji, 2025). From a wider perspective, the drone incursion represented a new echelon of Russian hostile actions, one that is relatively inexpensive yet capable of exerting disproportionate psychological and political effects. By orchestrating an intentional act designed to appear unintentional, Russia simultaneously advanced multiple objectives: collecting intelligence, testing NATO's thresholds, exploiting divisions within Polish society, and complicating Ukraine's security environment. The incident illustrates a central feature of Russia's contemporary modus operandi: the deliberate creation of crises that occupy an ambiguous space between accident and attack, allowing Moscow to weaken its adversaries while maintaining plausible deniability. The incursion also occurred less than a month after the Putin-Trump summit in Alaska, at a time when the United States was attempting to encourage Moscow to engage in a negotiated settlement of the war in Ukraine. Its timing underscored the Kremlin's hardline position and Putin's unwillingness to offer concessions, an aspect of Russian strategic behavior that the current U.S. administration has yet to fully grasp (Gasztold, 2025).

Espionage, Sabotage, and Expendable Agents

After the World War II, when Poland was incorporated into the Soviet sphere of influence, the Polish state has been a persistent target of intensive intelligence activity directed from Moscow. In the immediate post-war years, Soviet intelligence prioritized the infiltration and dismantling of the anti-communist underground and its domestic networks, as well as the detection of clandestine links between Polish émigré communities and Western intelligence services. Although most armed independence formations were suppressed by the early 1950s, Soviet services did not halt their operations on Polish territory (Poleszak, 2021).

Formally, they cooperated with Polish security institutions, and an official KGB residency operated in Warsaw (Bagieński, 2023). At the same time, Soviet operatives pursued independent recruitment, cultivating human sources in sensitive sectors, including within the officer corps of the Polish People's Army. Intelligence activity intensified during periods of political crisis for the communist regime, most notably during the legal functioning of "Solidarity" between 1980 and 1981, when even the structures of the Polish United Workers' Party were subject to infiltration (Bułhak and Friis, 2025, p. 2). Neither the collapse of communism nor the subsequent systemic transformation marked a decisive break in these practices. Soviet, and later Russian services continued to operate in Poland through both legal and illegal residencies, maintaining an largely uninterrupted intelligence presence (Świerczek, 2025).

Since the resurgence of Russian imperial ambitions and the unlawful annexation of Crimea in 2014, the threat

posed by Russian intelligence activities has acquired increasing importance for Poland's national security. At that time, however, the security agenda remained dominated by concerns over international terrorism, which tended to overshadow issues related to Russian espionage. This balance shifted markedly after the 2022 invasion of Ukraine, when Poland's counterintelligence service - the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego, ABW) began systematically exposing and dismantling a series of espionage networks, several of which had been operating clandestinely for many years.

One of the earliest and most illustrative cases is that of Pablo González, also known as Pavel Rubtsov, a Spanish freelance journalist detained during the night of 27-28 February 2022 in Przemyśl by the ABW on suspicion of acting on behalf of Russian military intelligence. From 2019 onwards, he lived in Warsaw with the Polish freelance journalist Magdalena Ch., while conducting extensive reporting trips across Spain, Eastern Europe, and the post-Soviet region (Buniatian and Smbatian, 2024). Over several years, González embedded himself in environments of particular interest to Russian intelligence, cultivating access to Russian opposition circles from 2016 onward, notably through his close relationship with Zhanna Nemtsova and his regular participation in meetings involving prominent Kremlin critics such as Alexei Navalny, Ilya Yashin, and Vadim Prokhorov. His ability to operate discreetly within these groups, supported by his fluency in Russian and his facility for building trust, enabled the systematic collection of sensitive information on dissident actors. According to case materials, the evidence includes intelligence-style reports attributed to González

containing detailed observations on Russian opposition figures, their routines, home addresses, and communication patterns, as well as information gathered during his frequent visits to frontline areas in Ukraine. Polish, Ukrainian, and multiple Western security services had already identified him as a person of interest. Following his arrest, it emerged that he had supplied assessments of military positions, personnel, and infrastructure that could have supported Russian targeting, while also collecting information relevant to Polish and NATO security. Although González publicly presented himself as a Spanish journalist of Russian descent, investigators maintain that he exploited his dual identity and the mobility afforded by journalistic work to conduct intelligence-gathering operations under the cover of professional reporting (Walker, 2024).

Although Rubtsov had already been under the scrutiny of Spanish and Ukrainian counterintelligence services for some time, his arrest, subsequent detention, and the protracted duration of investigative proceedings triggered a series of protest campaigns in Western countries. These campaigns, directed and supported by organizations such as Reporters Without Borders and Amnesty International, expressed solidarity with the "journalist," frequently asserting his innocence and calling for his release (Keeley, 2022; RSF, 2023; IFJ–EFJ, 2023). To the surprise of many of his supporters, Rubtsov was seen in Moscow on 1 August 2024 participating in the largest spy swap between the West and Russia since the Cold War, finding himself among the 24 people involved in the prisoner exchange (Murphy and Khalil, 2024; Mineeva, 2024). His release under this deal clearly demonstrated that he was of

considerable value to the Kremlin, whose intelligence services evidently did not forget his prior activities.

Shortly after González's arrest, Polish counterintelligence services succeeded in uncovering yet another Russian spy. On 17 March 2022, they detained Tomasz L., who was accused of engaging in espionage activities since 2017 (Onet, 2025). According to the evidentiary material, while employed in the Archival Division of the Civil Registry Office of the Capital City of Warsaw and having access to its document collections and information systems, he copied official records onto private storage devices and photographed them using his mobile phone. The materials he illicitly obtained included civil status records of Polish citizens and foreign nationals, correspondence with diplomatic missions, official templates, guidelines, and a range of other sensitive data. Such information might enable Russian intelligence services to produce legalization documents used to construct the identities of so-called "illegals." He subsequently transmitted the collected data to an identified intelligence officer through concealed radio communications - methods in which he had previously been trained by Russian handlers (Nowak, 2025a).

Another illustrative case concerns Igor R., who arrived in Poland with his wife following the onset of Russia's invasion of Ukraine and, with assistance from the Polish Ministry of Foreign Affairs, obtained political refugee status. Presenting himself as an opposition activist and outspoken critic of Vladimir Putin, he established contacts within the Russian opposition community based in Warsaw. Supported by a government scholarship, the couple began university studies and rented an apartment.

In reality, however, Igor R. had been recruited by the FSB while still a student in Russia, and his relocation to Poland was intended to facilitate the infiltration and monitoring of Russian opposition networks abroad. He also allegedly collected information on officials from the Polish Ministry of Foreign Affairs who had assisted him, on individuals involved in the programmes of the National Agency for Academic Exchange, and on lecturers at the University of Silesia who provided Polish-language instruction to Russian nationals. He was arrested in late July 2024 after his wife - having discovered his extramarital affair - began disclosing his ties to the FSB. According to investigators, he communicated with his handler through an old mobile phone rather than a smartphone, as well as via Telegram. His case illustrates the extent to which Russian intelligence services prioritize surveillance of the Russian diaspora in Warsaw. It also highlights the need for heightened vigilance in interactions with Russian refugees, among whom additional intelligence assets may be operating (Molga, 2025).

While in the cases of González, Tomasz L., and Igor R. it was not disclosed whether they were handled directly by case officers from the Russian residency in Warsaw or managed through alternative channels, this station had been involved in extensive offensive intelligence-gathering. In response, Polish counterintelligence decided in March 2022 to dismantle such operations by expelling 45 Russian diplomats identified as intelligence officers (Bułhak and Friis, 2025, p. 11). Poland was not unique in adopting this approach. Between 2018, following the Skripal poisoning, and 2025, more than 700 Russian “diplomats” were expelled from Western countries (Rękawek et al., 2025, p. 16; Riehle 2024b, p.

1258). Declassified documents from the Cold War era, including those from Polish military and civilian residencies operating until 1990, clearly demonstrate that expelling a substantial number of intelligence officers working under diplomatic cover can halt, disrupt, and disorganize an intelligence network. Assets become cut off from routine contact with their handlers, communication channels are compromised, tasking and reporting are delayed, and, in many cases, contact is frozen altogether. The removal of such a large contingent of potential intelligence operatives compelled Russian services to seek new means of acquiring information and recruiting assets. This challenge was, to some extent, mitigated by an increased reliance on the cyber domain.

In the aftermath of the large-scale expulsions of its intelligence officers, Russia increasingly sought to compensate for the loss of professional operatives by relying on "disposable" or "single-use" agents, usually civilians who were recruited largely through online channels and were frequently unaware of the state actor directing their actions (Richterova et. al, 2024, p. 7; Riehle, 2024a, p. 458). These recruits, drawn from a range of nationalities (including Ukrainians, Russians, Moldovans, Estonians, Bulgarians, Belarusians, and Poles), were assigned limited, low-skill tasks in exchange for modest financial compensation. Many were identified through online employment platforms used by migrants seeking part-time work, which made the recruitment process difficult to detect. While these activities typically involved minor disruptive actions, such as distributing anti-NATO or anti-Ukraine stickers and graffiti, in some instances instructions transmitted via encrypted messaging applications, particularly

Telegram, escalated to more serious acts of sabotage, including attempted arson. This strategy enabled Moscow to partially rebuild its operational capacity at minimal expense while maintaining a high degree of plausible deniability, consistent with the broader logic of hybrid warfare (Rękawek et al., 2025, pp. 16, 23; Bukowski, 2025, pp. 23–24; Walker, 2025; Jeznach et al., 2024).

In 2023, for example, the ABW dismantled the largest Russian espionage network ever identified in Poland, consisting of sixteen members. The organization operated in cell structures, each headed by individuals trusted by Russian intelligence. Although Polish counterintelligence had detected part of the group earlier and placed its members under surveillance, arrests were carried out only after intercepted communications revealed an active plan to sabotage weapons shipments bound for Ukraine. The investigation showed that the operatives had been monitoring critical sites, including Jasionka Airport, the Naval Port of Gdynia, and the Rzeszów railway station. They were also tasked with distributing leaflets aimed at fostering hostility toward Ukrainians and NATO. Officials noted that these propaganda activities served both to stimulate anti-Ukrainian sentiment within Polish society and to test recruits' readiness to engage in actions against the host state.

In addition, members of the network received instructions to set fire to buildings and vehicles and, in at least one instance, to commit an assassination. Some provided access to their bank accounts to enable transfers used to finance the group's operations. Participants were compensated in cryptocurrency, with

payments typically confirmed through photographs documenting completed assignments. All communication with Russian handlers took place via encrypted Telegram channels, while payments, ranging from 20 to 50 PLN (approx. 5-10 EUR) per sticker were made in Bitcoin, leaving no traceable record. Most operatives had been recruited in Ukraine and later entered Poland under the guise of war refugees, though they were in fact assets of Russian intelligence. The network's core consisted of thirteen Ukrainians, supplemented by two Belarusian students and one Russian national - a hockey player for a club in Sosnowiec. Sentences ranged from one year and three months to six years of imprisonment; one minor was placed in a juvenile detention centre (Miller et al., 2023; Kacprzak and Zawadka, 2023). Interestingly, four of the convicted sought later asylum in Poland, likely fearing deportation to Ukraine, where they would have faced additional imprisonment and the confiscation of their property for espionage on Russia's behalf (Kacprzak and Zawadka, 2025).

This case highlights the growing threat posed by Russian sabotage operations, yet the concept of sabotage itself is interpreted differently across scholarly disciplines. A recent reconceptualization by Rovner et al. (2025) defines sabotage as the "weaponization of friction to degrade the performance of a target's system from within," akin to introducing sand into the gears of an organization. While sabotage has limited value as a stand-alone instrument, it functions as an enabler that strengthens and complements other policy tools. Within the framework of hybrid warfare, sabotage encompasses a broad spectrum of activities from arson to the destruction of railway infrastructure - incidents that may

appear isolated and dispersed across unrelated locations. Considered collectively, however, such actions gradually and systematically erode state capacity. In Poland, their growing frequency suggests a deliberate attempt to generate disruption and cultivate fear and uncertainty within society, particularly given that the selected targets frequently serve civilian or dual-use functions. These hostile acts were further reinforced by parallel Russian disinformation campaigns seeking to attribute responsibility to Ukrainians. This narrative gained plausibility from the fact that some people conducting operations on behalf of the Kremlin were indeed recruited from among Ukrainian nationals, including both refugees and those who had arrived in Poland for other reasons. For example, in September 2025 three Ukrainian citizens received prison sentences ranging from one to five years for their involvement (at various times between 2023 and 2024) in an organized group operating in Poland, Lithuania, Latvia, Ukraine, and Russia, whose purpose was to carry out acts of sabotage and terrorism, specifically the arson of large-scale facilities within EU member states. The investigation covered, among other incidents, the arson of an OBI store in Warsaw on 14 April 2024; the arson of an IKEA store in Vilnius on 9 May 2024; the burning of the Marywilska shopping centre in Warsaw on 12 May 2024; as well as preparations for an arson attack on an IKEA store in Riga (Nowak, 2025b).

While earlier arson incidents had already indicated a mounting pattern of escalation, the drone incursion accelerated this trend and moved it into a more overtly hostile phase. The trajectory intensified further on 16 November 2025, when an explosion on the Warsaw-Lublin railway line damaged a section of track. This

attack marked a significant escalation in the scale and ambition of hybrid operations conducted on Polish territory, signaling a shift toward more disruptive and potentially lethal forms of sabotage. Since 2022, railway infrastructure has become a recurrent target of Russian operations, owing to its logistical importance for transporting Western military assistance to Ukraine. Until recently, Russian intelligence efforts had focused primarily on monitoring arms shipments, and planned acts of sabotage were typically disrupted by counterintelligence at an early stage (Bryjka, 2025).

The November incident, however, unfolded differently. According to government statements, the explosion occurred on a stretch of track near Mika and was first detected when a train driver reported structural irregularities. Subsequent on-site police assessments confirmed one explosion and revealed a second act of sabotage involving damage to the traction infrastructure. As the line is routinely used to transport military equipment and humanitarian supplies to Ukraine, officials stressed that the blast posed a direct threat to Poland's security and carried the potential for mass casualties. At a press conference, four senior ministers, including the Ministers of Defense and the Interior, announced that substantial forensic evidence had been secured, enabling investigators to pursue the identification of the perpetrators (Reuters, 2025).

Polish security services identified two Ukrainians - Yevhenii Ivanov and Oleksandr Kononov as the direct perpetrators of the attack, both allegedly recruited by Russian military intelligence. The men entered Poland from Belarus using passports issued under false identities. Having executed the operation, they swiftly

returned to Belarus, leading Polish intelligence services to focus their efforts on uncovering their domestic facilitators (Harłukowicz and Stankiewicz, 2025; Bahgat, 2025). In response, the Polish government launched Operation Horizon, deploying 10,000 troops in an effort to bolster the security of critical infrastructure, expand joint patrols, and enhance coordination across state services in the face of escalating diversionary threats (Halicki, 2025).

While the growing reliance on so-called "single-use" agents has become increasingly evident, the railway-track explosion illustrates that such operations are not always executed by untrained amateurs. In this case, the perpetrators demonstrated clear proficiency in handling explosives, indicating a higher level of competence than is typically associated with ad hoc recruits. This suggests important gradations within the category of "single-use" agents: although Ivanov and Kononov still fit this classification, since their identities were exposed and it is highly unlikely, they will be redeployed for further operations in Poland, their conduct, as well as the effectiveness of their escape plan, points to Russian training, guidance, or operational support. Accordingly, they should not be viewed as individuals randomly recruited online for low-skill tasks, but rather as expendable assets entrusted with more complex assignments and operating under closer direction from a case officer (Gruszka and Nyzio, 2025).

Although "single-use" agents offer Moscow a low-cost tool that ensures plausible deniability, Russia continues to pursue traditional HUMINT targets as well, particularly people with access to sensitive state information. These efforts are frequently conducted in

close coordination with Belarusian intelligence, which, unlike its Russian counterpart, had for many years not been treated as a priority target by the ABW. This oversight enabled Belarusian services to operate with greater freedom and expand clandestine activities directed not only at the Belarusian diaspora but also at Polish state institutions (Kociubiński and Shadurski, 2024). One of the most consequential incidents occurred in 2024 with the defection of Tomasz Szmydt, a judge of the Provincial Administrative Court in Warsaw, serving since 2012. In May 2024, Szmydt fled to Minsk, requested political asylum, and publicly denounced Polish authorities while endorsing Belarusian and Russian narratives on regional security. His defection was unprecedented in post-1989 Poland, not merely because it involved a sitting judge, an office typically shielded from abrupt political realignments, but also because it occurred at a moment of intensifying hybrid pressures directed against Poland.

Subsequent disclosures by Polish authorities revealed that Szmydt had handled cases concerning the denial of security clearances, giving him insight into very sensitive administrative procedures and potentially privileged information about people assessed as security risks. This raised credible concerns about whether such material might have been transferred to Belarusian or Russian intelligence. His case illustrates the continued priority Moscow and Minsk place on cultivating assets within critical state institutions. It also demonstrates how the hybrid toolkit integrates psychological, informational, and political operations designed to discredit Poland both domestically and internationally, amplifying the impact of defections far beyond their immediate operational value (Rogalewicz, 2024).

Although Szmydt now resides in Belarus and periodically travels to Moscow, he has been fully incorporated into the Belarusian state propaganda apparatus. He is employed by International Radio Belarus, where he co-produces Free Word for Poland, a six-hour programme designed to persuade Polish audiences of the supposed advantages of life under Alexander Lukashenka's rule (Belsat, 2025a). Despite being the subject of a European Arrest Warrant issued by Poland in connection with an espionage investigation, the asylum granted to him effectively shields him from extradition.

The broader context in which his case unfolds is one of sharply escalating intelligence and sabotage activity since 2022. According to the ABW, between February 2022, the outset of Russia's full-scale invasion of Ukraine, and November 2025, the agency launched 71 criminal investigations related to espionage conducted on behalf of Russia or Belarus. These cases extend beyond classic intelligence-gathering to include diversionary operations, acts of sabotage, and coordinated disinformation efforts. Investigators have identified 73 suspects, 67 of whom have been formally charged, with 55 currently in detention. Those implicated are predominantly citizens of Ukraine, Belarus, Russia, and Poland (Belsat, 2025b). Given the emergence of several high-profile incidents in recent months, including the recent railway bombing, it is highly probable that the number of individuals charged with espionage and sabotage will continue to increase.

Conclusions

Since 2022, Russian hybrid activities targeting Poland have not only intensified but also diversified, revealing Poland's transformation from a peripheral target into a key laboratory for Russian experimentation with hybrid tools. Poland's role as one of Ukraine's strongest political and military supporters, and as the principal logistical hub for Western assistance, has made it a central arena in which Moscow tests how far it can challenge NATO without triggering a conventional response. The trajectory from long-standing espionage and disinformation, through instrumentalized migration and low-intensity sabotage, to the 2025 drone incursion and the railway explosion, illustrates an incremental but deliberate escalation. These measures have been calibrated to remain below the threshold of open conflict while probing allied response mechanisms and cultivating ambiguity over attribution.

The expulsion of forty-five Russian diplomats in 2022 significantly disrupted traditional intelligence networks and forced an adaptation of Russian tradecraft. While classical HUMINT targeting individuals with access to sensitive information has continued, often in coordination with Belarusian services and supported by "illegals" operating outside embassy structures, Moscow has simultaneously shifted toward a more "franchised" model of operations. This model relies heavily on "single-use" or expendable agents recruited online, typically remunerated through small cryptocurrency transfers and assigned relatively simple disruptive tasks ranging from graffiti and leaflet distribution to arson and infrastructure sabotage. Recent incidents, however, demonstrate that such assets can also be employed in

more sophisticated operations, including the deliberate destruction of railway infrastructure. The disproportionate involvement of Ukrainian nationals, among them refugees and labour migrants, serves a dual function: it strengthens Russia's plausible deniability and simultaneously furnishes material for disinformation narratives depicting Ukrainians as a security threat.

In this sense, Russian hybrid operations in Poland function not only as instruments of coercion but also as mechanisms of social re-engineering. Rather than attempting to foster pro-Russian sentiment in a society shaped by the historical legacies of Soviet domination and imperial ambition, Moscow seeks instead to erode the foundations of the pro-Ukrainian consensus. Recent surveys indicate that Poles most frequently express aversion toward Russians (72%), with only 8% reporting sympathy. By orchestrating activities that can be plausibly attributed to Ukrainians and amplifying them through coordinated disinformation campaigns, the Kremlin seeks to normalize anti-Ukrainian attitudes, exploit war fatigue, and portray solidarity with Kyiv as a source of risk and instability. Emerging data suggest that this approach may be having an effect: polling from February 2025 indicates a decline in sympathy toward Ukrainians from 40% to 30%, accompanied by an increase in unfavourable views from 30% to 38% (Omyła-Rudzka, 2025, p. 2). Yet this shift may also reflect broader dynamics, not only potential Russian influence operations, but also war fatigue, economic pressures, and intensified domestic political competition.

Within this context, Kremlin-aligned proxies disseminate narratives suggesting that Kyiv seeks to draw Poland into the war despite clear public opposition to any direct military involvement. Recent polling indicates that 65 percent of Poles oppose sending troops to the Ukrainian-Russian border as part of a stabilization mission (Laboratorium Badań Medioznawczych, 2025). The defection of a sitting judge, the mobilization of pro-Russian online bot networks, and the systematic targeting of diaspora communities illustrate how external operations and internal vulnerabilities are increasingly intertwined. The boundary between internal and external security is increasingly porous, as hybrid instruments are directed simultaneously at critical infrastructure, political institutions, and social cohesion.

These developments present complex dilemmas for Poland and its allies. On the one hand, dismantling espionage networks, disrupting sabotage plots, and publicly exposing hostile operations are indispensable components of deterrence and national resilience. On the other hand, actions that explicitly associate Ukrainians or other foreign communities with security risks may unintentionally reinforce the very perceptions that Russian information campaigns seek to embed. Likewise, an overly securitized domestic political or media environment can be instrumentalized by Moscow to portray Poland as repressive or unstable. Effective responses must therefore integrate robust counterintelligence activity and strengthened protection of critical infrastructure with deliberate management of public communication and community relations, ensuring that defensive measures do not inadvertently amplify the adversary's strategic narratives. In this context, Polish counterintelligence requires not only

additional resources but also a more proactive and selectively offensive operational posture.

At the allied level, NATO and EU member states should resist treating acts of sabotage, disinformation, and espionage as discrete or episodic events. Instead, they must recognize them as interlocking components of a coherent Russian strategy. This, in turn, necessitates the establishment of integrated fusion cells capable of synthesizing intelligence and operational information across domains. Moreover, the West, still possessing substantial financial and regulatory leverage should adopt a more assertive and anticipatory approach to countering hybrid threats, rather than relying primarily on reactive measures (Bukowski, 2025, pp. 35-43).

Looking ahead, several plausible trajectories emerge. A first and most likely scenario is one of managed escalation in the grey zone, in which Russia continues to employ low-cost, deniable tools such as limited drone incursions, cyber operations, and infrastructure sabotage to maintain constant pressure on Poland while avoiding direct military confrontation. A second scenario involves horizontal escalation, where methods refined in Poland are replicated across the region, turning the country into both a primary target and a hub for regional counter-hybrid coordination. A third, more worrying scenario centers on deeper institutional penetration and political polarization within Poland, with hybrid operations increasingly indistinguishable from domestic contestation. Finally, a shock scenario, such as a mass-casualty incident or a serious mishap involving NATO forces, cannot be excluded, and would test both Polish crisis management and allied solidarity.

In sum, the Polish case underscores that Russian hybrid warfare is best understood as a long-term, adaptive strategy that blends intelligence collection, targeted disruption, and societal manipulation. It seeks not only to impede the flow of arms to Ukraine, but also to reshape political preferences and security debates inside Poland and across NATO's Eastern Flank. Addressing this challenge will require not just technical fixes and episodic crisis responses, but a sustained, whole-of-society effort to strengthen institutional resilience, preserve political cohesion, and protect the social foundations of Poland's role as a key supporter of Ukraine.

Literature:

1. Akbik, A. (2025). "From historical bias to historical insight: shifting stereotypes about Central and Eastern Europe after the invasion of Ukraine", Cambridge Review of International Affairs, pp. 1–23. doi: 10.1080/09557571.2025.2579251.
2. Almäng, J. (2019). "War, Vagueness and Hybrid War", Defence Studies 19(2), pp. 189–204. DOI:10.1080/14702436.2019.1597631.
3. Bagieński, W. (2023). "Współpraca służb wywiadowczych PRL i Związku Sowieckiego jako element relacji dwustronnych KGB z MSW (1956–1990)", Aparat Represji w Polsce Ludowej 1944-1989, 21, pp. 15-38, DOI: 10.48261/arprl232101
4. Bahgat, F. (2025). "Poland says Ukrainians working for Russia behind rail blast, Deutche Welle", 18 November, available at: https://www.dw.com/en/poland-railway-sabotage-suspects-ukrainians-working-for-russia/a-74790998 (accessed: 18.11.2025).

5.Banasik, M. (2015). “How to understand the hybrid war”, Securitologia, 1(21), pp. 19-34. DOI: 10.5604/18984509.1184214

6.Banasik, M. (2020). “The challenges for Central Europe posed by the rivalry of the Russian Federation below the threshold of war”, Rocznik Instytutu Europy Środkowo-Wschodniej 18(39), pp. 9-26, DOI: https://doi.org/10.36874/RIESW.2020.3.1.

7.Belsat (2025a). ”Z czego utrzymuje się zbiegły do Łukaszenki były polski sędzia Tomasz Szmydt”, 12 June, available at: https://pl.belsat.eu/87242862/z-czego-utrzymuje-sie-zbiegly-do-lukaszenki-byly-polski-sedzia-tomasz-szmydt (accessed: 18.11.2025).

8.Belsat (2025b). ”Dobrzyński: 73 podejrzanych o szpiegostwo na rzecz Rosji i Białorusi od lutego 2022 r.”, 3 November 2025, available at: https://pl.belsat.eu/89823593/dobrzynski-73-podejrzanych-o-szpiegostwo-na-rzecz-rosji-i-bialorusi-od-lutego-2022-r (accessed: 18.11.2025).

9.van den Berg, B., Stijnman E. (2025). “What the Russian drone incursion into Poland means for NATO. Testing the threshold”, Clingendael Alert, 23 September, available at: https://www.clingendael.org/sites/default/files/2025-09/Alert_Russian_drone_incursion_into_Poland_means_for_NATO.pdf (accessed:. 18.11.2025).

10.Bērziņš, J. (2019). “Not ‘Hybrid’ but New Generation Warfare”. Russia's Military Strategy and Doctrine, [in] Glen E. Howard, Matthew Czekaj (eds.), Boulder, USA: Lynne Rienner Publishers, pp. 157-184. https://doi.org/10.1515/9781735275284-009

11. Biuro Bezpieczeństwa Narodowego (2025). Podsumowanie działań Biura Bezpieczeństwa Narodowego w sprawach bezpieczeństwa w latach 2015-2025, BBN: Warsaw, available at: https://www.bbn.gov.pl/download/1/32139/BiuroBezpieczenstwaNarodowego2015-2025.pdf

12. Bo Lillis, K., Khurshudyan I., Bertrand N. (2025). "Intel officials are split on whether Russia deliberately flew drones into Poland but agree Putin is getting more aggressive", CNN, 19 September, available at: https://edition.cnn.com/2025/09/19/politics/intelligence-assessments-russian-drones-poland (accessed: 18.11.2025).

13. Bryjka, F. (2025). "Linie kolejowe są celem rosyjskiego sabotażu", Polski Instytut Spraw Międzynarodowy, 18 November, available at: https://pism.pl/publikacje/linie-kolejowe-sa-celem-rosyjskiego-sabotazu?s=03 (accessed: 18.11.2025).

14. Bukowski, M. F. (2025). Agenci chaosu: ukryta kampania przeciwko Zachodowi. Wojna kognitywna i ofensywne operacje rosyjskich oraz białoruskich służb specjalnych, Fundacja im. Kazimierza Pułaskiego: Warsaw, available at: https://pulaski.pl/wp-content/uploads/2025/10/Report_Agents-of-Chaos_PL_17-10.pdf

15. Bułhak, W., Friis, T.W. (2025). "Russian Intelligence in Czech Republic, Poland, and Slovakia at the Outbreak of War in Ukraine", International Journal of Intelligence and CounterIntelligence, pp. 1-24. DOI:10.1080/08850607.2025.2498270.

16. Buniatian, H., Smbatian H. (2024). "How An Accused Russian Spy Traversed Nagorno-Karabakh And Armenian Politics As A Journalist", 22 August, Radio Free Europe, available at: https://www.rferl.org/a/pablo-gonzalez-russian-spy-pavel-rubtsov-nagorno-karabakh-armenia-pashinian/33087059.html (accessed: 14.11.2025).

17. Bura, M. (2025). "Do Polski wbrew przepisom", Podlaski Oddział Straży Granicznej, 14 November, available at: https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/69014%2CDo-Polski-wbrew-przepisom.html?utm_source=chatgpt.com (accessed: 24.11.2025).

18. Caliskan, M., (2019). “Hybrid Warfare through the Lens of Strategic Theory”, Defense & Security Analysis 35(1), pp. 40–58. DOI:10.1080/14751798.2019.1565364.

19. Libiseller, C. (2023). “‘Hybrid warfare’ as an academic fashion”, Journal of Strategic Studies, 46(4), pp. 858-880. DOI: 10.1080/01402390.2023.2177987

20. Darczewska, J. (2019). ”‘Wojny pamięci’: historia, polityka i służby specjalne Federacji Rosyjskiej”, Przegląd Bezpieczeństwa Wewnętrznego, 11(20), pp. 13-41.

21. Duda, D., Kowalska, J. (2025). “The Concept Of Warfare in Cyberspace As En Example of Hybrid Warfare of the Russian Federation”, Studia Bezpieczeństwa Narodowego, 35, pp. 11-26. DOI: 10.37055/sbn/196886.

22. Duszczyk, M., Kaczmarczyk P. (2022). “The War in Ukraine and Migration to Poland: Outlook and Challenges”, Intereconomics, 57(3), pp. 164-170, DOI: 10.1007/s10272-022-1053-6.

23. Dyduch, J., Góra, M. (2024) “Polish Reactions to Russian Aggression Against Ukraine” in: Mihr A., Pierobon C. (eds) Polarization, Shifting Borders and Liquid Governance Studies on Transformation and Development in the OSCE Region, Springer: Cham, Switzerland, available at: https://link.springer.com/book/10.1007/978-3-031-44584-2

24. Elak, L., and Śliwa, Z. (2019). ”Hybridity – a ‘new’ method to accomplish dominance”, Security and Defence Quarterly, 23(1), pp.3-22. https://doi.org/10.35467/sdq/103347

25. Filipec, O. (2022). “Multilevel analysis of the 2021 Poland-Belarus Border Crisis in the Context of Hybrid Threats.” Central European Journal of Politics 8(1), pp. 1-18. DOI: 10.24132/cejop_2022_1

26. Fridman, O. (2018). Russian “Hybrid Warfare”. Resurgence and Politicisation, London, UK: Hurst & Company.

27. Gajos, B., Wyciszkiewicz E. (2025). Narracje polityczne w duchu rosyjskiej propagandy. Raport na temat ich występowania w polskiej literaturze naukowej w latach 2014–2024, Centrum Mieroszewskiego: Warsaw, available at: https://mieroszewski.pl/upload/2025/10/narracje-polityczne-w-duchu-rosyjskiej-propagandy-online.pdf

28. Gasztold, P. (2025) "Rising Tensions: The U.S.–Russia Standoff and Its Consequences for NATO and Ukraine", Orion Policy Institute, 18 November, available at: https://orionpolicy.org/rising-tensions-the-u-s-russia-standoff-and-its-consequences-for-nato-and-ukraine/ (accessed: 24.11.2025)

29. Gasztold, A., Gasztold, P. (2020). "The Polish Counterterrorism System and Hybrid Warfare Threats", Terrorism and Political Violence, 34(6), pp. 1259–1276. DOI: 10.1080/09546553.2020.1777110.

30. Genini, D. (2025). "Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine", New Perspectives, 33(2), 122-149. https://doi.org/10.1177/2336825X251322719

31. IFJ-EFJ, (2023) "Poland: Spanish journalist Pablo González in custody for one year on charges of spying for Russia and no trial in sight", International and European Federations of Journalists, 28.02.2023, available at: https://europeanjournalists.org/blog/2023/02/28/poland-spanish-journalist-pablo-gonzalez-in-custody-for-one-year-on-charges-of-spying-for-russia-and-no-trial-in-sight/ (accessed: 14.11.2025).

32. Halicki, P. (2025). "Operacja 'Horyzont' w praktyce. Wyjaśniamy, gdzie będzie można spotkać żołnierzy", Onet.pl, 21 November, available at: https://wiadomosci.onet.pl/warszawa/rusza-operacja-horyzont-polacy-maja-o-niej-mylne-wyobrazenie-wyjasniamy/9zldrr9 (accessed: 24.11.2025).

33. Harłukowicz, J., Stankiewicz, A. (2025) "Frustracja służb po dywersji na kolei. Kierowca terrorystów wyszedł na

wolność", Onet.pl, 24 November, available at: https://wiadomosci.onet.pl/kraj/dywersja-na-kolei-agenci-sluzb-sfrustrowani-decyzja-prokuratury/pgxqt69 (accessed: 24.11.2025).

34. Infosecurity24, (2025). "Polska otwiera przejścia graniczne z Białorusią", 14 November, available at: https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/polska-otwiera-przejscia-graniczne-z-bialorusia (accessed: 24.11.2025)

35. Iskandarov, K., and Gawliczek, P. (2022) "Economic coercion as a means of hybrid warfare: The South Caucasus as a focal point". Security and Defence Quarterly, 40(4), pp. 47-57. DOI: 10.35467/sdq/151038

36. Jacobs, A. and Lasconjarias, G., (2015). "NATO's Hybrid Flanks Handling Unconventional Warfare in the South and the East", Research Paper No. 112, Research Division - NATO Defense College, Rome (available at: https://www.files.ethz.ch/isn/190786/rp_112.pdf)

37. Jakubiak, E. (2024). "Legal Implications of the Hybrid Warfare on the Polish-Belarusian Border", Europejski Przegląd Prawa i Stosunków Międzynarodowych, 3(71), 144-155. DOI: 10.52097/eppism.9270

38. Janičatová, S., Mlejnková P., (2021). "The Ambiguity of Hybrid Warfare: A Qualitative Content Analysis of the United Kingdom's Political-Military Discourse on Russia's Hostile Activities", Contemporary Security Policy 42(3), pp. 312–44. DOI:10.1080/13523260.2021.1885921.

39. Jeznach, K., Grove, T., Pancevski, B. (2024). "The Misfits Russia Is Recruiting to Spy on the West", The Wall Street Journal, 15 May, available at: https://www.wsj.com/world/europe/the-misfits-russia-is-recruiting-to-spy-on-the-west-7417b2b5 (accessed: 18.11.2025).

40. Johnson, R. (2017). "Hybrid War and Its Countermeasures: A Critique of the Literature". Small Wars & Insurgencies 29(1), pp. 141–63. DOI:10.1080/09592318.2018.1404770.

41. Kacprzak, I., Zawadka, G. (2023). ”Rosyjscy szpiedzy planowali wysadzenie pociągu w Polsce. Nie zostaną deportowani?”, Rzeczpospolita, 17 November, available at: https://www.rp.pl/przestepczosc/art39576581-rosyjscy-szpiedzy-planowali-wysadzenie-pociagu-w-polsce-nie-zostana-deportowani (accessed: 4.11.2025).

42. Kacprzak, I., Zawadka, G. (2025). ”Szpiedzy chcą azylu. Zaskakujący finał największej afery wywiadowczej w Polsce”, Rzeczpospolita, 5 September, available at: https://www.rp.pl/sluzby/art42957981-szpiedzy-chca-azylu-zaskakujacy-final-najwiekszej-afery-wywiadowczej-w-polsce (accessed: 4.11.2025).

43. Kayali, L. (2025). “Poland to Trump: Russian drones were no mistake”, Politico, 12 September, available at: https://www.politico.eu/article/not-a-mistake-poland-rebukes-trumps-doubts-about-russian-drone-incursion/ (accessed: 4.11.2025).

44. Keeley, G. (2022). “Spanish Journalist Marks 100 Days in Prison on Spy Claim”, Voice of America, 7 June, Available at: https://www.voanews.com/a/spanish-journalist-marks-100-days-in-prison-on-spy-claim/6607075.html (accessed: 17.11.2025).

45. Kiera, J. (2024) ”Polityka historyczna jako instrument wojny informacyjnej w polityce zagranicznej Federacji Rosyjskiej wobec Polski w latach 2015-2023 - casus Sputnik News Polska”, Wschodni Rocznik Humanistyczny, 21(4), pp. 7-35. DOI: 10.36121/jkiera.21.2024.4.007

46. Kociubiński, K., Shadurski, V. (2024). ”Zagrożenia hybrydowe dla bezpieczeństwa Polski ze strony Białorusi po 2020 r.”, Wschodnioznawstwo, 18, pp. 231-253, DOI: 10.4467/20827695WSC.24.015.20630

47. Kuśmirek, K. (2022). “Information Activities during the Migration Crisis on the Polish-Belarusian Border as a Threat to Society’s Resilience”, Bezpieczeństwo. Teoria i praktyka, 3(48), pp. 311-321. DOI: 10.48269/2451-0718-btip-2022-3-023

48. Laboratorium Badań Medioznawczych (2025). ”Badanie opinii Polaków na temat polskiego wojska - sondaż CATI” , 22 May, available at: https://www.lbm.uw.edu.pl/publikacje/newsy/622-badanie-opinii-polakow-na-temat-polskiego-wojska-sondaz-cati (accessed: 18.11.2025)

49. Lanoszka, A. (2016). “Russian Hybrid Warfare and Extended Deterrence in Eastern Europe”, International Affairs 92(1), pp. 175-95. DOI:10.1111/1468-2346.12509.

50. Łubiński, P. (2022). “Hybrid Warfare or Hybrid Threat - The Weaponization of Migration as an Example of the Use of Lawfare - Case Study of Poland”, Polish Political Science Yearbook, 51, pp. 43–55; DOI: https://doi.org/10.15804/ppsy202208

51. Maniszewska, K., (2024). Towards a New Definition of Terrorism: Challenges and Perspectives in a Shifting Paradigm, Springer: Cham.

52. Mineeva, Y. (2024). “An illusion of mercy: Decoding Russia's prisoner swap strategy”, Chatham House, 6 August, available at: https://www.chathamhouse.org/2024/08/illusion-mercy-decoding-russias-prisoner-swap-strategy (accessed: 17.11.2025).

53. Ministerstwo Cyfryzacji (2025). ”Uwaga na dezinformację związaną z naruszeniem polskiej przestrzeni powietrznej przez drony”, 10 September 2025, available at: https://www.gov.pl/web/cyfryzacja/uwaga-na-dezinformacje-zwiazana-z-naruszeniem-polskiej-przestrzeni-powietrznej-przez-drony (accessed: 18.11.2025).

54. Ministerstwo Obrony Narodowej (2025). “NATO – Ukraine Joint Analysis, Training and Education Centre opens!”, 17 February, available at: https://www.gov.pl/web/national-defence/nato--ukraine-joint-analysis-training-and-education-centre-opens (accessed: 24.11.2025).

55. Miszczuk, M. (2025). “The Security of the NATO’s Eastern Flank in the Perspective of the Military Threats Posed by the Russian Federation”, National Security Studies, 35, pp. 27-62, DOI: 10.37055/sbn/193671

56. Molga, T. (2025). ”Polska zapewniła mu mieszkanie i stypendium. Rosjanin Igor nadawał prosto do FSB”, Wirtualna Polska, 3 November, available at: https://wiadomosci.wp.pl/polska-zapewnila-mu-mieszkanie-i-stypendium-rosjanin-igor-nadawal-prosto-do-fsb-7217889395604064a (accessed: 17.11.2025).

57. Mumford, A. (2020). “Understanding Hybrid Warfare.” Cambridge Review of International Affairs 33(6), pp. 824–27. DOI:10.1080/09557571.2020.1837737.

58. Murray, W., Mansoor, P.R. (2012). Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge: Cambridge University Press.

59. Miller, G., Morris, L., Ilyushina M. (2023). “Russia recruited operatives online to target weapons crossing Poland”, The Washington Post, 18 August, available at: https://www.washingtonpost.com/world/2023/08/18/ukraine-weapons-sabotage-gru-poland/ (accessed: 4.11.2025).

60. Gruszka, P., Nyzio, A. (2025). ”‘Jednorazowi szpiedzy w Polsce. Ekspert o kulisach: wystarczy jedna rozmowa”, Onet.pl, 23 November, available at: https://wiadomosci.onet.pl/kraj/jednorazowi-szpiedzy-w-polsce-ekspert-o-kulisach-wystarczy-jedna-rozmowa/cm10bzr (accessed: 24.11.2025).

61. Murphy, M., Hafsa, K. (2024). “Who are the prisoners in the Russia-West swap?”, BBC, 2 August, available at: https://www.bbc.com/news/articles/cjjwexqj11xo (accessed: 17.11.2025).

62. Nowak, P. (2025a) ”Akt oskarżenia przeciwko Tomaszowi L. za szpiegostwo na rzecz rosyjskiego wywiadu”, Prokuratura Krajowa, 9 October, available at: https://www.gov.pl/web/prokuratura-krajowa/akt-oskarzenia-przeciwko-tomaszowi-l-za-szpiegostwo-na-rzecz-rosyjskiego-wywiadu2 (accessed: 17.11.2025).

63. Nowak, P. (2025b). ”Wyrok skazujący trzy osoby za udział w zorganizowanej grupie przestępczej o charakterze sabotażowo-terrorystycznym”, Prokuratura Krajowa, 24 October, available at: https://www.gov.pl/web/prokuratura-krajowa/wyrok-skazujacy-trzy-osoby-za-udzial-w-zorganizowanej-grupie-przestepczej-o-charakterze-sabotazowo-terrorystycznym (accessed: 17.11.2025).

64. Nyzio A., (2023). ‘O szpiegach, szpiegostwie i polskim kontrwywiadzie’, Analiza KBN, 13(128), pp. 1-59,

65. Olech, A. (2025). “Poland Triggers NATO’s Article 4”, Defence24, 10 September, available at: https://defence24.com/geopolitics/poland-triggers-natos-article-4, (accessed: 18.11.2025).

66. Olech, A., Dobrowolska, J. (2022). ”Polsko-Ukraińskie relacje a rosyjskie działania dezinformacyjne”, Studia Bezpieczeństwa Narodowego 26(4), pp. 63–72. doi:10.37055/sbn/156978.

67. Omyła-Rudzka, M. (2025). ”Stosunek Polaków do innych narodów”, Komunikat z badań, 13, Centrum Badania Opinii Społecznej: Warsaw, available at: https://www.cbos.pl/SPISKOM.POL/2025/K_013_25.PDF

68. Onet.pl (2025). ”Szpieg w warszawskim ratuszu. Jest akt oskarżenia przeciwko Tomaszowi L.”, 9 October 2025, available at: https://wiadomosci.onet.pl/kraj/szpieg-w-warszawskim-ratuszu-jest-akt-oskarzenia-przeciwko-tomaszowi-l/sdjvb3w (accessed: 4 November 2025).

69. Palczewska, M. (2020). “The security perception and security policy of Poland, 1989–2017”, Defense & Security Analysis, 37(1), pp. 80–95. DOI: 10.1080/14751798.2020.1831237.

70. Pelc, P. (2024). ”Cyberprzestrzeń jako element walki informacyjnej – doświadczenia z konfliktu w Ukrainie”, Bezpieczeństwo Narodowe, 45(2), pp.89–109. DOI: 10.59800/bn/196691

71. Piekarski, M. (2019) “Polish Armed Forces and hybrid war: current and required capabilities”, The Copernicus

Journal of Political Studies, 1, pp. 42–64. DOI: 10.12775/CJPS.2019.003.

72. Piekarski, M. (2022). "Possible scenarios of terrorist attacks in Republic of Poland in the context of hybrid threats", Terrorism – Studies, Analyses, Prevention, 2(1), pp. 259-279, DOI:10.4467/27204383TER.22.026.16346

73. Poleszak, S. (2021). „Podziemie niepodległościowe w Polsce w latach 1947–1953. Próba syntezy", Annales Universitatis Mariae Curie-Skłodowska, sectio F – Historia, 76, 327-365, DOI: 10.17951/f.2021.76.327-365

74. Polska Agencja Prasowa (2025). "Odnaleziono ostatniego drona, który wleciał do Polski z Rosji", 20 September, available at: https://www.pap.pl/aktualnosci/w-woj-warminsko-mazurskim-odnaleziono-ostatniego-drona-ktory-wlecial-do-polski-z-rosji (accessed: 18.11.2025).

75. Polskie Radio Białystok (2025). "Straż Graniczna: w zeszłym roku było 30 tys. prób przekroczenia granicy", 4 January, available at: https://www.radio.bialystok.pl/wiadomosci/index/id/246121 (accessed: 24.11.2025).

76. Pynnöniemi, K., Jokela, M. (2020). "Perceptions of Hybrid War in Russia: Means, Targets and Objectives Identified in the Russian Debate", Cambridge Review of International Affairs 33(6), pp. 828–45. DOI:10.1080/09557571.2020.1787949.

77. Rada do Spraw Współpracy z Ukrainą (2025), Polska pomoc Ukrainie 2022-2023, Warszawa.

78. Rauta, V. (2019). "Towards a Typology of Non-State Actors in 'Hybrid Warfare': Proxy, Auxiliary, Surrogate and Affiliated Forces." Cambridge Review of International Affairs 33(6), pp. 868–87. DOI:10.1080/09557571.2019.1656600.

79. Renz, B. (2018). Russia's Military Revival,. Cambridge, UK: Polity Press.

80. Reuters (2025). “Polish railway track blast an ‘unprecedented act of sabotage’, PM says”, 17 November, available at: https://www.reuters.com/world/explosion-polish-railway-track-was-caused-by-sabotage-pm-says-2025-11-17/ (accessed: 17.11.2025).

81. Rękawek, K., Lanchès, J., Zotova, M., Bowser, D. (2025). Russia’ Crime–Terror Nexus. Criminality as a Tool of Hybrid Warfare in Europe, Globsec – ICCT.

82. Richterova, D., Grossfeld E., Long, M., Bury, P. (2024). “Russian Sabotage in the Gig-Economy Era”, The RUSI Journal, pp. 1-23, DOI:10.1080/03071847.2024.2401232

83. Richterova, D., (2024). “The Long Shadow of Soviet Sabotage Doctrine?”, War on the Rocks, 19 August, available at: https://warontherocks.com/2024/08/the-long-shadow-of-soviet-sabotage-doctrine/ (accessed: 4.11.2025).

84. Riehle, K. (2024a). ‘The Ukraine war and the shift in Russian intelligence priorities’, Intelligence and National Security, 39(3), pp. 458–474. DOI: 10.1080/02684527.2024.2322807.

85. Riehle K. (2024b). “Soviet and Russian Diplomatic Expulsions: How Many and Why?”, International Journal of Intelligence and CounterIntelligence, 37(4), pp. 1238-1263, DOI: 10.1080/08850607.2023.2272216.

86. Rogalewicz, M. (2024). ”Dezinformacja białoruska z wykorzystaniem byłego polskiego sędziego”, Warsaw Institute, 20 June, available at: https://warsawinstitute.org/pl/dezinformacja-bialoruska-z-wykorzystaniem-bylego-polskiego-sedziego/ (accessed: 18.11.2025).

87. Rovner, J., Cormac, R., Maschmeyer, L. (2025). “Sand in the Gears: Sabotage in World Politics.” European Journal of International Security, https://doi.org/10.1017/eis.2025.10025

88. RSF (2023). “RSF regrets the Polish judge’s decision to further extend the year-long detention of a Spanish

journalist", Reporters sans frontières, 27 February, available at: https://rsf.org/en/rsf-regrets-polish-judge-s-decision-further-extend-year-long-detention-spanish-journalist (accessed: 14.11.2025).

89. Sadowski, A., Wąsowska, K., Maj, J., Pietrek G. (2023), "Operational analysis of threats to the security of NATO's eastern flank. Context of hybrid activities", Journal of Modern Science, 53(4), pp. 680-699. DOI:10.13166/jms/176680.

90. Sari, A. (2023). "Instrumentalized migration and the Belarus crisis: Strategies of legal coercion", Hybrid CoE Paper 17, available at: https://www.hybridcoe.fi/publications/hybrid-coe-paper-17-instrumentalized-migration-and-the-belarus-crisis-strategies-of-legal-coercion/

91. Schnaufer, T. A. II. (2017). "Redefining Hybrid Warfare: Russia's Non-linear War against the West". Journal of Strategic Security 10(1), pp. 17-31. DOI: http://doi.org/10.5038/1944-0472.10.1.1538

92. Schroefl, J., Kaufman, S.J. (2014). "Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War." Studies in Conflict & Terrorism 37(10), pp. 862–80. doi:10.1080/1057610X.2014.941435.

93. Starosta, J. (2024). ed. Wszystko jest wojną. Rosyjskie działania hybrydowe wobec państw Trójmorza, Instytut Nowej Europy: Warsaw, available at: https://ine.org.pl/wp-content/uploads/2024/12/RUS-dzialania-hybrydowe-PL.pdf

94. Stodolnik, M. (2025). "Cyber threats as hybrid activity against the European Union in light of the current geopolitical situation", Terrorism – Studies, Analyses, Prevention, special edition, pp. 225–248. DOI: 10.4467/27204383TER.25.021.21524

95. Sus, M. (2025) "Status-seeking in wartime: Poland's leadership aspirations and the response to the Russian invasion of Ukraine", The British Journal of Politics and International Relations, 27(4), pp. 1199-1222. DOI: 10.1177/13691481251329767

96. Śliwa, Z. (2022). “Poland as a Front-line Nation in the Wake of Russian Aggression in Ukraine”, Sõjateadlane (Estonian Journal of Military Studies), 20, pp. 123–140.

97. Świerczek, M. (2025). Śpiące psy Rosyjskie gry agenturalne wobec Urzędu Ochrony Państwa początkiem lat 90. XX w., LTW: Warszawa.

98. Walker, S., (2024). “Journalist or Russian spy? The strange case of Pablo González”, The Guardian, 15 October, available at: https://www.theguardian.com/world/2024/oct/15/journalist-russian-spy-pablo-gonzalez-kremlin-illegal (accessed: 14.11.2025).

99. Walker, S. (2025). “‘These people are disposable’: how Russia is using online recruits for a campaign of sabotage in Europe”, The Guardian, 4 May, available at: https://www.theguardian.com/world/ng-interactive/2025/may/04/these-people-are-disposable-how-russia-is-using-online-recruits-for-a-campaign-of-sabotage-in-europe (accessed: 17.11.2025).

100. Walker, S., Sabbagh, D., Krupa, J., Saue, P. (2025) “Poland ‘closer to military conflict than at any time since WW2’ as Nato allies weigh response to Russian drones”, The Guardian, 10 September, available at: https://www.theguardian.com/world/2025/sep/10/poland-shoots-down-drones-over-its-territory-amid-russian-attack-on-ukraine-says-military (accessed: 3.11.2025).

101. Wawrzusiszyn, A. (2022). ”Kryzys migracyjny na granicy polsko-białoruskiej i jego wpływ na bezpieczeństwo Polski”, Nowa Polityka Wschodnia, 2(33), pp. 45-65. DOI: 10.15804/npw20223303

102. Wawrzusiszyn, A. (2025). “Russian-Belarusian hybrid activities on the borders of the European Union and NATO”, Journal of Modern Science, 1(61), pp. 10-32, DOI:10.13166/jms/203108

103. Wenzel, M., Stasiuk-Krajewska, K., Macková, V., Turková, K. (2023). ”The penetration of Russian disinformation related to the war in Ukraine: Evidence from Poland, the Czech Republic and Slovakia”,

International Political Science Review, 45(2), pp. 192-208. DOI: 10.1177/01925121231205259

104. Westbrook, T. (2024). “Aircraft vulnerability to politically motivated Radio Frequency Interference (RFI) in Eastern Europe”, Security and Defence Quarterly, 46(2), pp. 104–117. DOI: 10.35467/sdq/178249

105. Wprost (2025). ”‘Nagła cisza’ na granicy polsko-białoruskiej. Takiej sytuacji nie było od ośmiu miesięcy”, 22 November, avaliable at: https://www.wprost.pl/kraj/12183055/przelom-na-granicy-polski-i-bialorusi-pulkownik-o-zniknieciu-migrantow.html (accessed: 24.11.2025).

106. Wóycicki, K., Kowalska, M., Lelonek, A. (2017) Rosyjska wojna dezinformacyjna przeciwko Polsce, Fundacja im. Kazimierza Pułaskiego: Warsaw, available at: https://pulaski.pl/wp-content/uploads/2023/06/RAPORT-Rosyjska-wojna-dezinformacyjna-przeciwko-Polsce.pdf

107. Yeliseyeu, A. (2024). “Belarus’s Coercive Engineered Migration Case of 2021–2022: Categorisation of State Media Narratives”, Migration Studies – Review of Polish Diaspora, pp. 79-99. DOI: 10.4467/25444972SMPP.23.030.19145

108. Zadorożna, M., Butuc, M. (2024). “Russian disinformation in Moldova and Poland in the context of the Russo-Ukrainian war”, Security and Defence Quarterly, 46(2), pp.47–65. DOI: 10.35467/sdq/189686

109. Żywczyk, A. (2025). ”Ataki hybrydowe wobec Polski: analiza narzędzi i strategii Rosji”. Krakowskie Studia Małopolskie, 2(46), pp. 62–73. DOI: 10.15804/ksm20250203