SECURITY & DEFENCE QUARTERLY

# Russian-linked sabotage in Poland: Attribution, legal resilience, and public–private infrastructure security

**Michael S. Wisniewski**

wisniewskim@kean.edu

https://orcid.org/0009-0005-3093-719X

Professional Security Studies, Kean University, 2039 Kennedy Blvd, Jersey City, NJ, USA

## Abstract

*This article examines how recent Russian-linked sabotage and disruption in Poland became governance problems under conditions of attribution uncertainty, contested legal classification, and public–private infrastructure exposure. It asks how Polish authorities publicly interpreted, legally framed, and institutionally managed these incidents, and what they revealed about public–private resilience. The study uses qualitative content analysis within a focused comparative case-study design. It examines four Polish cases: the Marywilska 44 shopping-centre fire, the explosive parcel plot, the Warsaw–Lublin railway sabotage case, and the September 2025 drone-incursion and airport-disruption cluster. Open-source official statements, prosecutorial releases, legal materials, parliamentary sources, and public reporting were coded across three analytical dimensions: attribution, legal and institutional response, and public–private resilience. The cases show a shift from isolated-incident framing towards a broader campaign logic in which sabotage and disruption are treated as cumulative, networked, and strategically meaningful. Attribution developed unevenly across cases, while criminal-law responses were supplemented by diplomatic signalling, international investigation, protective mobilisation, airspace defence, and allied coordination. The cases also show that commercially ordinary systems can become strategically exposed when they support logistics, mobility, public confidence, continuity, or deterrence. Russian-linked sabotage operations create a governance problem because attribution, legal classification, and operational adaptation often move at different speeds. Public–private resilience therefore requires clearer reporting channels, baseline protective expectations, continuity planning, information-sharing mechanisms, and more explicit allocation of risk and responsibility between public authorities and private operators.*

**Keywords:**

Poland, critical infrastructure, hybrid warfare, national resilience, proxy sabotage

**Article info**
Received: 25 March 2026
Revised: 3 June 2026
Accepted: 10 June 2026
Available online: 17 July 2026

Citation: Wisniewski, M.S. (2026) 'Russian-linked sabotage in Poland: Attribution, legal resilience, and public–private infrastructure security', *Security and Defence Quarterly*, 55(3). doi: 10.35467/sdq/224401.

© 2026 M.S. Wisniewski published by War Studies University, Poland.
This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

# Introduction

Hybrid warfare is not a new form of conflict, but Russia's war against Ukraine has renewed attention to how states combine military, intelligence, cyber, informational, economic, legal, and deniable instruments, including active measures, proxy use, sabotage, and other forms of pressure below the threshold of open war (Filipec, 2021; Galeotti, 2016; Mumford and Carlucci, 2023; Sanz-Caballero, 2023; Stoddart, 2026; Wither, 2016). In this setting, ambiguity is not incidental. It is often part of the method. Uncertainty over authorship, intent, and legal classification can slow response and complicate escalation management (Sanz-Caballero, 2023; Sari, 2020; Wither, 2016). Attribution delays, however, are not simply evidentiary or semantic; they also reflect political, legal, diplomatic, and alliance-management costs that Russia can exploit as part of its wider modus operandi. Sabotage, arson, parcel disruption, railway interference, drone incursions, and other forms of physical or operational disruption may therefore operate as instruments of grey-zone pressure when they impose costs, test resilience, or signal capability while preserving a degree of deniability (Filipec, 2021; Sanz-Caballero, 2023; Sari, 2020).

This study examines how Russian-linked sabotage and disruption in Poland become governance problems when attribution is politically and evidentially sensitive, legal classification is contested, and strategically exposed infrastructure is partly owned, operated, or secured by private actors. These incidents do not fit neatly into a single category, such as ordinary crime, terrorism, espionage, sabotage, hostile intelligence activity, or armed attack. As a result, public authorities must interpret, classify, communicate, and respond before attribution is complete, while private and commercially operated systems may bear security burdens for which ordinary business-risk models are poorly suited. This creates a governance problem at the intersection of attribution, lawfare, legal resilience, and public–private infrastructure security (Ostrowski and Zych, 2024; Sanz-Caballero, 2023; Sari, 2020).

Poland is a particularly important case for examining this problem. Since Russia's full-scale invasion of Ukraine in 2022, Poland has functioned as a frontline North Atlantic Treaty Organisation (NATO) state and a major logistical corridor for support moving towards Ukraine (Ostrowski and Zych, 2024; Piekarski, 2022; Wosik, 2026). Its transport routes, logistics systems, commercial facilities, railway corridors, airports, and adjacent airspace have significance beyond domestic infrastructure management (Olech, 2025; Ostrowski and Zych, 2024; Piekarski, 2022; Sadowski and Maj, 2022). Disruption affecting such systems can generate wider security effects because commercial and civilian infrastructures are linked to mobility, supply, public confidence, alliance logistics, and deterrence (Ochyra-Żurawska *et al.*, 2024; Sadowski and Maj, 2022; Wosik, 2026).

Recent incidents in Poland illustrate the difficulty of separating ordinary criminality from state-linked coercion under the conditions of uncertainty. Polish authorities and public reporting have linked the Marywilska 44 shopping-centre fire to suspected Russian-directed arson after an initial period of more cautious public attribution (National Prosecutor's Office, 2025; Notes from Poland, 2024, 2025a, 2025b). The explosive parcel plot highlighted the vulnerability of transnational logistics systems, with Eurojust (2026) describing self-igniting parcels and suspects believed to have acted on behalf of Russian military intelligence. The Warsaw–Lublin railway case was publicly framed by Polish authorities as sabotage affecting transport infrastructure, with official statements emphasising coordination among prosecutors, police, and special services (Prime Minister of Poland, 2025b; Special Services Coordinator, 2025). The September 2025 drone-incursion and airport-disruption cluster raised a different but related problem: airspace violation, allied

coordination, airport disruption, and deterrence management in the absence of a conventional ground attack (North Atlantic Treaty Organisation [NATO], 2025a, 2025b; Prime Minister of Poland, 2025a; Reuters, 2025a, 2025b, 2025c, 2025d, 2025e).

These incidents became publicly legible as security problems before certainty was complete. The article does not attempt to prove clandestine command responsibility beyond the public record, rather it analyses how Polish authorities publicly interpreted, legally framed, and institutionally managed recent Russian-linked sabotage and disruption affecting economically and strategically significant infrastructure. This matters because political attribution, legal attribution, public communication, protective action, and private-sector resilience can develop on different timelines and under different evidentiary thresholds. This timing mismatch is the practical governance dilemma on which the article focuses (Ostrowski and Zych, 2024; Sanz-Caballero, 2023; Sari, 2020).

The existing literature provides important foundations for analysing these incidents. Recent holistic work has already examined Russian hybrid warfare, active measures, cyber espionage, cyber warfare, critical infrastructure, and societal resilience in an integrated way, including Stoddart's (2022, 2026) studies of Russia's hybrid warfare offensive and cyber warfare threats to critical infrastructure. Hybrid warfare research has examined ambiguity, deniability, grey-zone pressure, information operations, and the difficulty of attribution (Filipec, 2021; Sanz-Caballero, 2023; Sari, 2020; Wither, 2016). Legal scholarship has examined how hybrid threats test domestic and international legal categories, including the boundary between crime, sabotage, espionage, terrorism, hostile intelligence activity, and armed attack (Sanz-Caballero, 2023; Sari, 2020). Infrastructure and public–private governance research has examined resilience, risk allocation, coordination, and the limits of public–private partnerships in protecting critical systems (Ampratwum *et al.*, 2022; Bovis, 2015; Carr, 2016; Dunn Cavelty and Suter, 2009; Jiang *et al.*, 2024). The narrower contribution of this article is therefore not to claim theoretical novelty but to provide a focused empirical comparison of how these problems appear together in recent Polish cases.

This study builds on this literature through a focused empirical comparison of the following four connected Polish cases: the Marywilska 44 shopping-centre fire in Warsaw, the explosive parcel plot, the Warsaw–Lublin railway sabotage case, and the September 2025 drone-incursion and airport-disruption cluster. These cases vary in target type, operational form, and degree of public attribution, but they illuminate the same broader problem: how Russian-linked sabotage and disruption affecting economically and strategically significant infrastructure are interpreted and managed under conditions of uncertainty (Olech, 2025; Ostrowski and Zych, 2024; Żywczyk, 2025). These cases are not treated as identical events or as proof of a single operational chain. Rather, they are examined comparatively to identify recurring patterns in attribution, legal framing, institutional response, and public–private resilience.

To answer these questions, the article compares the mentioned four cases through the following three analytical dimensions: attribution, legal and institutional response, and public–private resilience. This approach allows the study to trace how responsibility was publicly suggested or asserted, how legal and security mechanisms were activated under uncertainty, and how disruption exposed vulnerabilities, costs, and coordination burdens for private or commercially operated systems.

The study asks the following question: How have Polish authorities publicly interpreted, legally framed, and institutionally managed recent Russian-linked sabotage and disruption incidents affecting economically and strategically significant infrastructure? Two subsidiary questions guide the analysis. Firstly, how has attribution developed across cases

with different levels of uncertainty and evidentiary maturity? Secondly, what do these cases suggest about strengths and limits of public–private resilience when commercially ordinary systems become strategically consequential?

The article makes three contributions. These contributions are primarily empirical, analytical, and practical rather than claims of theoretical novelty. Empirically, it brings together four recent Polish cases that are usually discussed separately and compares them through a common analytical framework. Analytically, it argues that attribution, legal response, and resilience burdens do not move at the same speed, and that this misalignment is itself part of the governance problem created by Russian sabotage operations conducted within a broader hybrid warfare environment (Sanz-Caballero, 2023; Sari, 2020). Practically, it shows that resilience cannot be reduced to the protection of formally designated critical infrastructure alone. Commercially ordinary systems, including shopping centres, logistics networks, rail corridors, warehouses, airports, and private operators connected to them, may become strategically exposed when they sit within wider networks of mobility, supply, deterrence, and alliance support (Ampratwum *et al.*, 2022; Carr, 2016; Olech, 2025; Ostrowski and Zych, 2024). The article proceeds by reviewing the relevant literature, explaining the qualitative comparative method, presenting cross-case findings, and discussing implications for legal resilience and public–private infrastructure security.

# Literature review and theoretical framework

## Hybrid warfare, grey-zone pressure, and Russian active measures

Hybrid warfare is best understood in this article as a flexible repertoire of coercive activity below the threshold of open war, rather than as a wholly new form of conflict (Filipec, 2021; Sanz-Caballero, 2023; Sari, 2020; Wither, 2016). Many of the activities now discussed under the language of hybrid warfare resemble older practices of irregular warfare, active measures (*aktivnyye meropriyatiya*), later reframed in Russian law and practice as support measures (*meropriyatiyasodeistviya*), political warfare, psychological pressure, intelligence-enabled influence, and deniable coercion (Galeotti, 2018; Giles, 2016; Lasconjarias and Larsen, 2015; Stoddart, 2026). The contemporary significance of hybrid warfare lies less in novelty than in the way older instruments are combined with modern vulnerabilities, including digital communication systems, transnational logistics, privatised infrastructure, and politically constrained escalation thresholds (Filipec, 2021; Sanz-Caballero, 2023; Sari, 2020; Stoddart, 2022, 2026).

The concept remains contested. Hybrid warfare can describe military, paramilitary, intelligence, cyber, informational, legal, economic, and deniable activity, but its breadth can also weaken analytical precision (Filipec, 2021; Kresin, 2022; Sanz-Caballero, 2023; Sari, 2020). For this reason, the article uses the term descriptively and cautiously. It does not treat Russian sabotage operations as evidence of a single, fixed doctrine. Galeotti's (2019a) critique of the so-called Gerasimov Doctrine is useful here because it warns against overstating doctrinal coherence. As Galeotti (2019a, p. 159) argues, "This is no 'new way of war'. It is not Gerasimov's, and it is not a doctrine." The point is not that Russian active measures, sabotage, or deniable pressure is imaginary. Rather, it is that doctrinal labels can obscure the opportunistic, adaptive, and institutionally disruptive character of Russian activity (Galeotti, 2018, 2019b; Giles, 2016; Stoddart, 2026).

Ambiguity is central to this repertoire. Hybrid and grey-zone operations often seek to complicate attribution, delay response, and create disagreement over whether an incident

should be treated as crime, espionage, sabotage, terrorism, hostile intelligence activity, or armed attack (Sanz-Caballero, 2023; Sari, 2020; Wither, 2016). Sanz-Caballero (2023, p. 2) captures this legal difficulty by placing hybrid threats in a condition of "legal uncertainty" and emphasises that such threats are "not easy to detect, let alone attribute." This uncertainty is not merely a problem for later legal analysis. It shapes how authorities classify, communicate, and act upon it before attribution is complete. At the same time, attribution delays should not be treated as the product of ambiguity alone. Political and legal attribution also requires evidence, interagency coordination, alliance consultation, and assessment of possible diplomatic, retaliatory, or escalation costs.

Attribution is therefore not a single act. Technical attribution concerns how an incident occurred and what operational methods, devices, networks, or vulnerabilities were involved. Legal attribution concerns the evidentiary basis for assigning responsibility in criminal or judicial processes. Political attribution concerns public or diplomatic communication about responsibility, often under conditions in which intelligence cannot be disclosed completely (Sanz-Caballero, 2023; Sari, 2020). Political attribution is not simply a less certain version of legal attribution; it may also reflect strategic signalling, alliance management, deterrence, and the willingness to absorb diplomatic costs. These forms of attribution may overlap, but they do not move on the same timeline. A state may need to warn the public, reassure operators, or signal deterrence before it can disclose evidence suitable for prosecution. At the same time, premature attribution carries credibility, legal, and escalation risks.

This is especially relevant to Russian-linked sabotage because proxy use, cut-outs, informal intermediaries, online recruitment, and task fragmentation can separate immediate perpetrators from sponsoring or directing institutions (Filipec, 2021; Galeotti, 2018; Giles, 2016; Stoddart, 2026). Such methods can lower operational cost, preserve deniability, and complicate the distinction between ordinary criminality and state-linked coercion. They also give sabotage a transnational character. A plot may involve recruitment in one country, preparation in another, movement through logistics networks, and effects across several jurisdictions. This does not mean that every disruptive incident can be attributed directly to Kremlin decision-making on the basis of public evidence. It does mean that Russian-linked sabotage must be analysed with attention to intelligence direction, intermediaries, operational compartmentalisation, and the gap between suspicion and proof.

Legal resilience provides a second foundation for the analysis. Sari (2020) uses the concept to describe the capacity of legal and institutional systems to respond to grey-zone activity without either underreacting to strategically significant threats or overextending legal categories beyond their proper limits. Hybrid threats test this capacity because the same incident may be relevant to criminal law, counterterrorism, intelligence law, diplomatic practice, international law, and alliance security at once (Sanz-Caballero, 2023; Sari, 2020). If sabotage is treated only as an ordinary crime, its strategic significance may be missed. If it is classified too quickly as terrorism or armed attack, the state may move faster than public evidence supports. This is also where lawfare matters: contested legal categories, evidentiary thresholds, and uncertainty over attribution can become part of the operational environment rather than merely a later legal debate.

The literature on lawfare reinforces this point. Drawing on Bachmann and Muñoz Mosquera, 2015; Sanz-Caballero (2023, p. 4) defines lawfare as using law to "twist and bend legal paradigms." This does not mean that every legal dispute in a hybrid context is lawfare. Rather, it indicates that legal argument, procedural ambiguity, and contested classification can themselves become part of the conflict environment. In attribution contexts, lawfare is relevant because uncertainty over whether an incident should be categorised as

crime, espionage, sabotage, terrorism, hostile intelligence activity, or armed attack can be exploited to slow response, preserve deniability, and impose political costs on the target state. Public authorities must therefore preserve legal credibility while responding to the acts that may be designed to exploit legal restraint. This also explains why signalling matters. In this article, signalling refers to public, diplomatic, legal, or military communication intended to convey resolve, reassurance, attribution, or deterrence to multiple audiences, including domestic publics, private operators, allies, and hostile actors.

Attribution and signalling also raise problems of responsible disclosure. Authorities may need to inform affected operators, warn the public, or expose hostile activity without compromising intelligence sources, ongoing investigations, or judicial proceedings. False-flag possibilities further complicate this problem because hostile actors may seek not only to deny involvement but also to manipulate the evidentiary environment or provoke misdirected responses (Sanz-Caballero, 2023; Sari, 2020). For this reason, the public handling of sabotage requires a balance between transparency, evidentiary caution, deterrence, and operational security.

Infrastructure scholarship adds the third dimension. Recent work emphasises that infrastructure vulnerability should be understood systemically rather than asset by asset (Ampratwum, *et al.*, 2022; Ostrowski and Zych, 2024; Stoddart, 2022). Transport, logistics, energy, communications, aviation, commercial facilities, and public administration are interdependent. Disruption in one sector can produce cascading effects in another, especially when the affected system supports mobility, supply, public confidence, or security functions (Olech, 2025; Ostrowski and Zych, 2024; Stoddart, 2022, 2026). This systems-based view is important because sabotage does not need to destroy a military target to create strategic effects. It may instead impose precautionary costs, force visible mobilisation, test response procedures, or reveal coordination gaps. Stoddart's (2026) work is useful here because it connects Russian hybrid warfare and cyber warfare to the vulnerability of critical infrastructure and the wider problem of societal resilience.

The public–private dimension is central to this problem. Many exposed systems are not owned, operated, insured, secured, or maintained solely by the state. Shopping centres, warehouses, logistics firms, parcel networks, rail contractors, airports, insurers, and private security providers may all become involved in prevention, detection, reporting, continuity planning, or recovery after hostile disruption (Ampratwum *et al.*, 2022; Bovis, 2015; Carr, 2016; Dunn Cavelty and Suter, 2009; Jiang *et al.*, 2024). Public–private partnerships are necessary to infrastructure resilience, but the literature also warns that they are not a simple solution unless risk allocation, information sharing, reporting duties, and operational responsibilities are clearly defined (Carr, 2016; Dunn Cavelty and Suter, 2009; Jiang *et al.*, 2024). For that reason, societal resilience depends not only on state capacity, but also on whether private operators can detect, report, absorb, and recover from disruption that carries national-security consequences.

For this study, public–private resilience refers to the capacity of state institutions and private or commercially operated systems to share information, absorb disruption, allocate risk, maintain continuity, and adapt security practices when ordinary infrastructure becomes strategically exposed. The private dimension includes ownership, operational cost, duty of care, insurance exposure, security preparedness, incident reporting, business continuity, and cooperation with public authorities (Ampratwum *et al.*, 2022; Bovis, 2015; Carr, 2016; Jiang *et al.*, 2024). This definition matters because Russian-linked disruption may place national-security burdens on operators whose ordinary risk models were designed for crime, accident, or business interruption rather than hostile state-linked activity.

Poland brings these issues together. It is not unique in facing Russian-linked sabotage or grey-zone pressure, but it is a high-value case because of its role as a frontline NATO state and logistical corridor for Ukraine (Olech, 2025; Ostrowski and Zych, 2024; Piekarski, 2022; Wosik, 2026). Its commercial, logistics, rail, and aviation systems sit at the boundary between civilian operation and strategic function. This makes Poland useful for examining how sabotage is interpreted when the affected infrastructure is commercially ordinary but security-significant.

These literatures already provide a substantial theoretical foundation, including holistic work on Russian hybrid warfare, cyber warfare, critical infrastructure, and resilience (Stoddart, 2022, 2026). The need addressed here is therefore not a claim of wholly new theory, but a more focused empirical comparison of how these dynamics appear in recent Polish sabotage and disruption cases. Hybrid-threat scholarship emphasises the movement from identification to effective response, but response cannot be understood without examining legal classification, public attribution, and institutional activation (Filipec, 2021; Sari, 2020; Sanz-Caballero, 2023). Legal-resilience scholarship shows that states must respond to grey-zone activity without either underreacting or overextending legal categories, but it leaves room for closer analysis of how this balance is managed in concrete cases (Sari, 2020; Sanz-Caballero, 2023). Infrastructure-resilience and public–private partnership scholarship calls for clearer responsibility, information sharing, risk allocation, and continuity planning, but these recommendations are rarely examined in relation to Russian-linked sabotage operations affecting commercially operated systems (Ampratwum, *et al.*, 2022; Bovis, 2015; Carr, 2016; Dunn Cavelty and Suter, 2009; Jiang *et al.*, 2024). The Polish cases therefore provide a useful setting for connecting these recommendations to empirical incidents in which attribution, legal response, and public–private resilience developed together under conditions of uncertainty.

The article's contribution follows from this empirical focus rather than from a claim that the underlying theoretical problems have been neglected altogether. Hybrid warfare scholarship explains ambiguity, deniability, proxy use, and sub-threshold coercion. Legal scholarship explains how grey-zone activity tests attribution rules and legal categories. Infrastructure-resilience scholarship explains why public authorities depend on private and semi-private actors to manage risk and continuity. What remains especially valuable is case-based analysis of how these issues develop together in concrete sabotage cases affecting commercially ordinary but strategically consequential systems. This article addresses that gap by comparing four Polish incidents across three analytical dimensions: attribution, legal and institutional response, and public–private resilience.

The first dimension, attribution, examines how responsibility was publicly suggested, qualified, or asserted. The second dimension, that is legal and institutional response, examines how authorities used criminal-law, intelligence, diplomatic, mobilisation, and international-coordination mechanisms. The third dimension, public–private resilience, examines how incidents exposed vulnerabilities, costs, coordination demands, and preparedness gaps for private or commercially operated systems. Together, these dimensions allow the article to analyse Russian sabotage operations not as isolated criminal episodes but as governance problems at the intersection of hybrid warfare, lawfare, legal resilience, and infrastructure security.

## Research design and method

This study uses qualitative content analysis within a focused comparative case-study design to examine how Polish authorities publicly interpreted, legally framed, and institutionally

managed recent Russian-linked sabotage and disruption affecting economically and strategically significant infrastructure. The method is appropriate because the article examines public institutional meaning-making rather than attempting to prove non-public operational direction beyond the public record. It traces how incidents were described, attributed, classified, and acted upon while facts remained incomplete.

The study examines four Polish cases: the Marywilska 44 shopping-centre fire in Warsaw, the explosive parcel plot, the Warsaw–Lublin railway sabotage case, and the September 2025 drone-incursion and airport-disruption cluster. These cases were selected because they vary in target type, operational form, and degree of public attribution while addressing the same broader problem: Russian-linked sabotage and disruption affecting strategically significant infrastructure in Poland. The comparison is analytical rather than statistical; the cases are treated as related instances in a common strategic setting, not as identical events or proof of a single operational chain.

The source base consists of forty-eight open-source documents, including official statements, prosecutorial releases, legal texts, parliamentary materials, and selected public reporting. These materials were selected through criterion-based sampling. Documents were included if they met at least one of the three criteria: they addressed one of the four cases directly, documented a formal institutional response, or provided legal, policy, or operational context necessary to interpret the state's public handling of the incident. The corpus was determined by analytical relevance and comparative coverage rather than statistical representativeness, and sources were added until the main public institutional statements, legal framings, and response measures across the four cases were captured without substantial repetition (Malterud *et al.*, 2016).

The document was the unit of collection. The unit of analysis was the relevant passage within each document. A passage was coded when it addressed one or more of the study's three analytical dimensions: attribution, legal and institutional response, or public–private resilience. Incident characteristics, including kinetic action, reconnaissance, and resilience testing, were also recorded as descriptive context. Attribution codes captured whether responsibility was publicly ambiguous, cautiously suggested, or directly linked to Russian or hostile-state activity. Legal and institutional-response codes captured criminal-law framing, diplomatic action, international coordination, and protective mobilisation. Public–private resilience codes captured infrastructure vulnerability, coordination demands, precautionary or operational costs, and possible proxy or disposable-agent patterns.

The coding framework combined deductive and inductive elements. Deductively, the coding followed four analytical lenses: incident characteristics, attribution, legal and institutional response, and public–private resilience. Inductively, the analysis remained open to recurring themes not fully specified in advance, including foreign intelligence involvement, deterrence, institutional adaptation, resilience testing, precautionary cost, and possible disposable-agent patterns (Ostrowski and Zych, 2024; Sanz-Caballero, 2023; Sari, 2020). A single passage could receive more than one code, where it addressed multiple themes. To reduce methodological repetition in the main text, the full codebook is retained in the Appendix (Table A1) rather than reproduced here in detail.

Coding proceeded in two stages. Firstly, the documents were read closely and tagged according to the four main analytical lenses. Secondly, coded segments were compared across cases to identify recurring patterns, meaningful contrasts, and areas in which attribution, legal framing, or resilience burdens diverged. The analysis focused on the presence and relative salience rather than on raw frequency. Descriptive code counts were used as heuristic aids to comparison, not as measures of effect size, causal weight, or formal

statistical association. The interpretive weight of the findings therefore comes from how the underlying documents framed each incident.

This study has four limitations. Firstly, it relies on open-source material and therefore cannot access classified intelligence, sealed case files, or internal deliberations. Secondly, public statements may reflect strategic communication as well as evidentiary assessments, especially in cases involving foreign-state attribution. Thirdly, the cases differ in timing, maturity, and operational form, which limit any effort to treat them as directly equivalent. Finally, the descriptive distributions presented later are not inferential statistics and should not be read as a proof of causal weight by themselves (Ostrowski and Zych, 2024; Sanz-Caballero, 2023). These limitations define the scope of the article. It does not reconstruct sabotage operations exhaustively or establish classified command responsibility. Instead, it examines how sabotage and disruption become publicly legible as governance problems when attribution, legal classification, political signalling, and operational response overlap (Ostrowski and Zych, 2024; Sanz-Caballero, 2023). This scope is consistent with the article's focus on public institutional interpretation rather than forensic reconstruction.

## Results

The qualitative content analysis suggests that the four Polish cases should not be read as isolated security episodes. They differ in target type, operational form, and evidentiary maturity but share a common governance problem: each required Polish authorities to interpret disruption under conditions of uncertainty while deciding whether the incident should be treated as ordinary criminality, foreign-linked sabotage, infrastructure vulnerability, or a wider security challenge. Across the cases, official and public framing increasingly connected discrete incidents to a broader pattern of Russian-linked pressure on infrastructure, public security, and state resilience, while attribution and response remained conditioned by evidentiary, diplomatic, and operational costs (Olech, 2025; Wosik, 2026; Żywczyk, 2025). Table 1 summarises the main cross-case findings.

The first pattern concerns attribution. Attribution developed unevenly across the four cases. Marywilska provides the clearest example of movement from cautious suspicion to direct public attribution. Initial reporting described Prime Minister Donald Tusk as saying that the Russian-related "threads" being examined were "quite probable" (Notes from Poland, 2024).

**Table 1. Cross-case summary of incident and attribution patterns.**

| Case | Dominant incident pattern | Attribution pattern | Main analytical result |
|---|---|---|---|
| Marywilska 44 fire | Kinetic destruction | Delayed shift from cautious suspicion to direct public attribution | Commercial infrastructure becomes explicitly securitised. |
| Parcel plot | Kinetic disruption with a networked logistics dimension | Networked attribution emphasising handlers, proxies, and cross-border coordination | Logistics systems emerge as transnational hybrid vulnerabilities. |
| Warsaw–Lublin rail sabotage | Kinetic disruption to transport infrastructure | More direct strategic attribution | Rail infrastructure is framed as both economic and strategic. |
| Drone/airport-disruption cluster | Testing and reconnaissance rather than destruction | Security framing under continued evidentiary and escalation-management caution | Airspace incidents are framed as resilience and deterrence challenges. |

Note. The table summarises the article's coded findings across incident characteristics and attribution patterns.

By May 2025, the public language had hardened. A later statement reported that Polish authorities said they knew "the fire was the result of arson instructed by the Russian secret services" (Notes from Poland, 2025b). This shift matters because it shows attribution as a staged process rather than a single moment of naming. Investigative caution, public suspicion, and later direct attribution unfolded on different timelines rather than resolving into one immediate public attribution decision.

The explosive parcel plot followed a different pattern. Rather than moving from one ambiguous claim to one later direct claim, the case was framed through a distributed operational chain. Eurojust (2026) described the case as involving "self-igniting parcels" and reported that suspects were believed to have acted "on behalf of the military-intelligence service of the Russian Federation." The public record emphasised task division, recruitment, cross-border movement, and international investigation. This makes the parcel case especially important for understanding proxy-based and transnational forms of Russian-linked sabotage. Attribution in this case was not centred only on the immediate perpetrators but on the relationship among handlers, intermediaries, logistics systems, and foreign intelligence direction.

The Warsaw–Lublin railway case moved more directly in strategic framing. Polish authorities described the incidents as sabotage affecting railway infrastructure and emphasised the likelihood of foreign-service involvement (Prime Minister of Poland, 2025b; Special Services Coordinator, 2025). Compared with Marywilska, the railway case was more immediately legible as a security problem because rail infrastructure connects civilian mobility, freight movement, economic continuity, and possible alliance-support functions. Public framing moved quickly towards a security interpretation. The drone and airport-disruption cluster widened the attribution problem further because the public response had to balance claims about deliberate targeting with airspace defence, allied coordination, airport disruption, and escalation management (NATO, 2025a, 2025b; Prime Minister of Poland, 2025a; Reuters, 2025a, 2025b, 2025c, 2025d, 2025e).

The second pattern concerns legal and institutional response. Criminal-law investigation remained central, especially in the the Marywilska, parcel, and railway cases, but prosecution was not the only relevant pathway. Once incidents were linked publicly to Russian services, foreign intelligence direction, transnational logistics, or airspace violation, their institutional meaning extended beyond ordinary criminal investigation. The Marywilska case combined criminal-law framing with later diplomatic and strategic significance (National Prosecutor's Office, 2025; Notes from Poland, 2025a, 2025b). The parcel plot required international legal coordination because the suspected devices moved through cross-border logistics networks and involved suspects in more than one jurisdiction (Eurojust, 2026). The Warsaw–Lublin railway case linked prosecution with protective mobilisation, as authorities emphasised both investigation and security of citizens and infrastructure (Special Services Coordinator, 2025).

The drone cluster activated a different institutional pathway. Rather than centring on ordinary criminal prosecution, the response emphasised airspace defence, allied coordination, public communication, and NATO consultation rather than ordinary criminal prosecution (NATO, 2025a, 2025b; Prime Minister of Poland, 2025a; Reuters, 2025d, 2025e). This distinction matters because it shows that Russian-linked disruption may activate different legal and institutional mechanisms depending on whether the incident is framed as sabotage, reconnaissance, airspace violation, terrorism, hostile intelligence activity, or escalation management. Across the cases, the common feature was institutional layering: prosecutors, police, intelligence services, diplomatic channels, international bodies, NATO-linked mechanisms, and private operators, all became relevant to the response.

The third pattern concerns public–private resilience. The cases show how civilian or commercial systems can become strategically exposed because of their location within wider networks of mobility, supply, public confidence, and deterrence. Marywilska involved a shopping centre, tenants, workers, insurers, and commercial owners, but once publicly linked to Russian-directed arson, it became more than a private or local loss. It became an example of how civilian–commercial infrastructure could be targeted or exploited within a wider hostile campaign (National Prosecutor's Office, 2025; Notes from Poland, 2025a, 2025b). The resilience issue was therefore not only physical protection but also the allocation of security burdens, reporting duties, continuity costs, and public–private coordination when a commercially ordinary site became strategically meaningful.

The parcel plot provides the clearest example of private-sector exposure. The suspected devices moved through logistics systems that depend on private operators, cross-border movement, sorting facilities, transport schedules, cargo interfaces, and cross-border movement. Limited incendiary devices could therefore create wider costs through inspection, delay, screening, insurance concerns, and reputational risk across logistics networks (Eurojust, 2026). The case also suggests a proxy or disposable-agent pattern, in which low-cost intermediaries and divided tasks make the operation harder to attribute and easier to deny. This does not prove a settled doctrine on the basis of public evidence, but it does show how suspected Russian-linked operations can exploit both vulnerable individuals and commercially open systems.

The Warsaw–Lublin railway case shows a different version of public–private exposure. Rail infrastructure is more visibly strategic than a shopping centre or parcel chain but its operation still depends on multiple public, commercial, technical, and contractor relationships. Disruption to a rail corridor can affect passengers, freight, infrastructure managers, security services, and cross-border support routes. The case therefore supports a systems-based view of resilience in which a single disruption may create cascading operational and security effects (Ostrowski and Zych, 2024; Special Services Coordinator, 2025).

Three findings follow from the cross-case comparison. Firstly, public framing moved from isolated-incident logic towards campaign logic. The cases were not identical and the evidence differed across them, but public discourse increasingly treated fires, logistics disruption, railway sabotage, and drone incursions as part of a wider pattern of Russian-linked pressure against Poland and other European states (Olech, 2025; Wosik, 2026). This campaign logic should not be read as a proof of one single operational chain; it instead reflects how similar forms of disruption can accumulate strategic meaning across separate incidents.

Secondly, attribution, legal classification, and operational response did not move at the same speed. Public attribution hardened unevenly. Criminal-law tools remained central in some cases, while diplomacy, international investigation, protective mobilisation, airspace defence, and NATO-linked consultation became more important in others. The uneven tempo was not simply the result of ambiguity; it also reflected the evidentiary, diplomatic, alliance-management, and resource costs attached to naming, classifying, and responding to suspected state-linked sabotage. This supports the legal-resilience argument that grey-zone incidents may remain formally domestic in a legal procedure while becoming functionally international in security significance (Sanz-Caballero, 2023; Sari, 2020).

Thirdly, resilience pressures were greatest where infrastructure appeared ordinary in administrative terms but strategic in systemic effect. A shopping centre, parcel network, railway line, airport, or logistics node did not need to be a military site to become security significant. These systems became targets, conduits, witnesses, or cost-bearers

because they sat within networks that connect commerce, mobility, deterrence, and alliance support.

Overall, the results support the article's central claim: Russian-linked sabotage and disruption in Poland should be analysed not only as a problem of attribution or criminal investigation but as a public–private governance problem under conditions of uncertainty. The descriptive code distributions, reported in the Appendix (Table A2), support this comparison by showing that vulnerability appeared across all four cases, while direct attribution was strongest in both Marywilska and railway cases, international coordination was most prominent in the parcel case, and mobilisation was most visible in the railway and drone cases. The results therefore prepare the discussion by showing that Russian-linked disruption forces authorities and operators to spend resources, manage uncertainty, and coordinate across legal, diplomatic, security, and commercial domains before full certainty is available.

# Discussion

The findings suggest that recent Russian-linked sabotage and disruption in Poland are best understood not as isolated incidents but as governance problems produced by Russian active measures, attribution costs, institutional seams, lawfare, and infrastructure interdependence (Filipec, 2021; Olech, 2025; Ostrowski and Zych, 2024; Sanz-Caballero, 2023; Sari, 2020; Stoddart, 2026). Across the four cases, Polish authorities had to act before all relevant facts were settled publicly. This should not be read because of ambiguity alone. Political and legal attribution takes time, requires evidence and interagency coordination, and may generate diplomatic, alliance-management, retaliatory, and escalation costs. Attribution, legal classification, public communication, and operation protection must proceed under uncertainty while hostile actors could benefit from the delay, confusion, and resource diversion this produced (Olech, 2025; Ostrowski and Zych, 2024; Sanz-Caballero, 2023; Sari, 2020).

The first implication concerns attribution. The Polish cases show that attribution in sabotage settings is not a single legal or political act. It develops across technical, legal, intelligence, diplomatic, and public-communication domains. Marywilska case illustrates delayed movement from suspicion to direct attribution. The parcel plot shows how attribution can be distributed across handlers, intermediaries, logistics systems, and international investigative bodies. The rail case shows faster securitisation of infrastructure disruption. The drone cluster shows how attribution may be tied to deterrence and allied consultation even when public evidence remains incomplete. Political attribution is often a strategic choice as well as an evidentiary judgement, because naming Russia publicly may impose diplomatic costs, invite hostile counter-signalling, and require allied coordination. This supports the broader literature's view that hybrid threats are difficult to detect and attribute, but it also adds an empirical point: different forms of attribution may coexist rather than resolve into one definitive public statement (Sanz-Caballero, 2023; Sari, 2020).

The second implication concerns Russian intelligence practice and proxy use. The parcel case is particularly important because it points towards a transnational operational pattern involving recruitment, task division, logistics exploitation, and suspected links to Russian military intelligence (Eurojust, 2026). This does not prove, on the public record alone, a direct Kremlin command chain behind every disruptive incident. It does, however, show how Russian-linked sabotage can operate through cut-outs, recruited intermediaries, and low-cost disposable agents. Such methods lower operational risk, complicate

attribution, and allow hostile actors to exploit the space between criminal prosecution and state responsibility (Galeotti, 2018; Giles, 2016; Stoddart, 2026). This is consistent with a broader Russian modus operandi in which active measures, proxy activity, and deniable disruption are used to impose costs, force protective expenditure, and sow confusion without necessarily crossing the threshold of open war. The result is a form of pressure that may look locally criminal while functioning strategically.

The third implication is transnationality. Russian-linked sabotage in Poland cannot be understood only through domestic criminal law or national infrastructure protection. The parcel plot moved through cross-border logistics systems and required Eurojust coordination. Drone incursions involved NATO-linked airspace defence and allied consultation. Rail and logistics vulnerabilities matter because Poland is part of a broader corridor supporting Ukraine and European security. These cases therefore show that sabotage may be legally domestic at the point of investigation but operationally and strategically international in its causes, pathways, and consequences (Filipec, 2021; Kresin, 2022; Olech, 2025; Wosik, 2026). They also indicate why Poland should be treated as a focused frontline case within a wider European and Euro-Atlantic pattern rather than as an isolated national anomaly. This wider pattern matters for interpretation. Similar forms of sabotage, cyber-enabled disruption, information operations, infrastructure pressure, and societal resilience testing appear in broader analyses of Russian hybrid activity against Western states and critical infrastructure (Olech, 2025; Stoddart, 2022, 2026). The Polish cases are therefore valuable not because they exhaust the phenomenon but because they show how a frontline NATO state publicly manages attribution, legal framing, protective mobilisation, and public–private resilience when these pressures converge.

The fourth implication concerns legal resilience. Criminal law remains necessary because sabotage produces concrete harms, perpetrators, evidence, and prosecutorial pathways. Yet criminal law alone cannot capture the whole governance problem when incidents also involve foreign intelligence links, diplomatic consequences, alliance reassurance, infrastructure protection, and public–private coordination. The Polish cases show that legal resilience requires neither underreaction nor overclassification. Treating sabotage only as ordinary crime may miss its strategic function. Treating every ambiguous incident as an act of war may exceed the available evidence and create escalation risks. Lawfare is central to this problem because hostile actors can exploit legal thresholds, evidentiary uncertainty, attribution standards, and classification disputes as part of the conflict environment. The difficult task is to preserve legal credibility while allowing protective and diplomatic responses to proceed before certainty is complete (Sanz-Caballero, 2023; Sari, 2020).

This creates a related problem of signalling. In this article, signalling refers to public, diplomatic, legal, or military communication intended to convey resolve, reassurance, attribution, or deterrence to multiple audiences. Those audiences include domestic publics, private operators, allies, adversaries, and potential perpetrators. The Polish cases suggest that signalling is not separate from institutional response. Public attribution, protest notes, NATO consultation, security deployments, and official reassurances, all communicate how the state understands the incident and what kind of response it is prepared to make. The risk is that signalling can move faster than legal proof. The benefit is that silence or excessive caution may also invite further probing. This tension is precisely where attribution, lawfare, and deterrence intersect: the state must communicate enough to impose costs and reassure audiences without undermining prosecution, intelligence protection, or alliance management.

Responsible disclosure is therefore central to sabotage governance. Authorities may need to warn private operators, reassure the public, and expose hostile activity without

compromising classified intelligence, ongoing investigations, sources, methods, or future prosecutions. This is particularly important where private firms operate the systems through which hostile activity moves. Logistics companies, airports, rail contractors, shopping-centre owners, insurers, and private security providers need usable threat information, but public authorities may not be able to disclose everything they know. A practical resilience framework must therefore distinguish between public attribution, confidential operator warnings, classified intelligence-sharing, and evidentiary disclosure for prosecution.

False-flag possibilities further complicate this balance. The possibility that an adversary may mislead investigators, manipulate evidence, or exploit premature public claims reinforces the need for careful attribution. This does not mean that authorities should avoid public attribution altogether. Rather, attribution should be staged, evidence-based, and calibrated to the purpose it serves. A criminal indictment, diplomatic statement, public warning, NATO consultation, and operator advisory may each require different levels of evidentiary detail. Such calibration also reduces the risk that Russia can turn legal caution, evidentiary uncertainty, or public disagreement into additional confusion.

The public–private dimension is the most important practical implication of the study. The Polish cases show that commercially ordinary systems can become strategically consequential when they support mobility, supply, public confidence, or alliance logistics. Marywilska involved a commercial site. The parcel plot exploited logistics networks. The rail case affected transport infrastructure. The drone cluster disrupted aviation and airport operations. In each case, private or commercially operated systems became targets, conduits, witnesses, or cost-bearers in a wider security problem (Ampratwum *et al.*, 2022; Carr, 2016; Jiang *et al.*, 2024).

This means that public–private resilience cannot depend on general calls for vigilance alone. Private operators in exposed sectors need clearer reporting channels, baseline protective expectations, continuity plans, and access to timely threat information. Public authorities, in turn, need mechanisms for receiving reports from commercial actors, distinguishing ordinary incidents from hostile probing, and sharing actionable guidance without disclosing sensitive intelligence. The relevant policy question is not whether private actors should replace the state. They should not. The question is how public authorities and private operators can coordinate when the target is privately operated but the threat is geopolitical. This is also a resource problem: forcing public authorities and private operators to spend time, money, personnel, and political attention on protective adaptation is itself one of the effects Russian hybrid operations seek to produce.

Cost allocation is part of this problem. Screening, closures, delays, insurance disputes, security upgrades, staff training, and business interruption may fall on private actors even when the underlying threat is state-linked. If those costs are treated only as ordinary commercial risk, private operators may underinvest in security or fail to report suspicious activity. If all costs are shifted to the state, resilience becomes fiscally and operationally unrealistic. A stronger model would clarify minimum protective standards, reporting duties, liability expectations, and channels for public support in sectors exposed to hostile state-linked disruption (Bovis, 2015; Dunn Cavelty and Suter, 2009; Jiang *et al.*, 2024).

The Polish cases also point to a need for professionalisation. Security preparedness in exposed commercial systems should include staff training, incident documentation, suspicious-activity reporting, continuity planning, and coordination exercises with public authorities. Professional security standards and certification frameworks are not a substitute for national strategy, but they can help private operators build defensible preparedness

and improve cooperation with state agencies. The key issue is not any single credential. It is the development of recognisable standards and trained personnel capable of operating at the boundary between commercial risk management and national security.

Overall, the discussion supports the study's central argument: Russian-linked sabotage operations create a governance problem because attribution, legal classification, and operational adaptation move at different speeds. That misalignment is not simply an accidental by-product of ambiguity; it is one of the ways hybrid pressure works, because Russia can exploit evidentiary delay, legal caution, institutional division, and resource strain. The state must investigate carefully, communicate credibly, deter further action, protect infrastructure, and coordinate with allies and private operators before the evidentiary picture is complete. That misalignment is not an administrative failure. It is a defining feature of sabotage conducted within a hybrid-warfare environment.

## Conclusions

This article examined how Polish authorities publicly interpreted, legally framed, and institutionally managed recent Russian-linked sabotage and disruption affecting economically and strategically significant infrastructure, and what those cases suggested about the strengths and limits of public–private resilience under conditions of attributional uncertainty (Sari, 2020; Wosik, 2026; Żywczyk, 2025). Across the four cases, the findings indicated a shift from isolated-incident framing towards a broader campaign logic, in which sabotage was treated as cumulative, networked, and strategically meaningful. The article's contribution is therefore best understood as a focused empirical and case-based analysis of Polish experience, rather than as a claim to introduce a wholly new theory of Russian hybrid warfare. At the same time, attribution, legal classification, and operational adaptation did not move in parallel (Sari, 2020; Wosik, 2026; Żywczyk, 2025). That misalignment appears to be part of the challenge rather than a temporary flaw in otherwise settled governance.

Public attribution hardened at different speeds across the cases, while legal and institutional responses expanded according to the character of each incident. Criminal-law tools remained central, but they were supplemented by diplomatic signalling, international investigation, protective mobilisation, airspace defence, and allied consultation. This supports the article's central argument that Russian-linked sabotage operations create a governance problem that cannot be reduced to attribution alone. Nor should delayed attribution be read as a product of ambiguity alone. It also reflects evidentiary thresholds, political choice, alliance consultation, diplomatic risk, possible retaliation, and the practical costs of naming a hostile state publicly. The more difficult issue is how authorities act responsibly before certainty is complete.

The findings also show that resilience in this environment cannot be limited to formally designated critical infrastructure. Commercially ordinary systems may become strategically exposed when they support logistics, mobility, public confidence, continuity, or deterrence. Shopping centres, parcel networks, rail corridors, airports, warehouses, contractors, insurers, and private security providers may become targets, conduits, witnesses, or cost-bearers in a wider security problem. This means that public–private resilience requires more than general calls for vigilance. It requires clearer reporting channels, baseline protective expectations, continuity planning, information-sharing mechanisms, and more explicit allocation of risk and responsibility between public authorities and private operators. These measures matter because resource diversion, precautionary cost, and uncertainty management are themselves part of the pressure produced by Russian hybrid activity.

The Polish experience therefore offers a wider lesson for frontline and transit states facing deniable coercion below the threshold of war. Russian sabotage operations conducted within a broader hybrid-warfare environment exploit the gap between suspicion and proof, domestic law and international security, and public responsibility and private ownership. They also exploit lawfare, attribution costs, and institutional seams between criminal investigation, intelligence assessment, alliance signalling, and privately operated infrastructure security. Future research could extend this analysis through interviews with public officials and infrastructure operators, judicially developed case materials where available, and comparative cases from other European states facing similar Russian-linked disruption. Such work would help clarify how legal resilience and public–private infrastructure security can be strengthened before the next ambiguous incident occurs.

**Funding**

This research received no external funding.

**Data Availability Statement**

The data presented in this study is available on request from the author.

**Disclosure Statement**

No potential conflict of interest was reported by the author. The author read and agreed to the published version of the manuscript.

## References

**Ampratwum, G., Osei-Kyei, R. and Tam, V.** (2022) 'Exploring the concept of public–private partnership in building critical infrastructure resilience against unexpected events: A systematic review', *International Journal of Critical Infrastructure Protection*, 39, p. 100556. doi: 10.1016/j.ijcip.2022.100556.

**Bachmann, S.D. and Muñoz Mosquera, A.B.** (2015) 'Lawfare and hybrid warfare—how Russia is using the law as a weapon', *Amicus Curiae*, 102, pp. 25–28.

**Bovis, C.** (2015) 'Risk in public–private partnerships and critical infrastructure', *European Journal of Risk Regulation*, 6(2), pp. 200–207. doi: 10.1017/s1867299x00004505.

**Carr, M.** (2016) 'Public–private partnerships in national cyber-security strategies', *International Affairs*, 92(1), pp. 43–62. doi: 10.1111/1468-2346.12504.

**Dunn Cavelty, M. and Suter, M.** (2009) 'Public–private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection', *International Journal of Critical Infrastructure Protection*, 2(4), pp. 179–189. doi: 10.1016/j.ijcip.2009.08.006.

**Eurojust** (2026) 'Joint investigation team disrupts group using self-igniting parcels for terrorist attacks', 6 March. Available at: https://www.eurojust.europa.eu/news/joint-investigation-team-disrupts-group-using-self-igniting-parcels-terrorist-attacks (Accessed: 17 May 2026).

**Filipec, O.** (2021) 'Preventing hybrid threats: From identification to an effective response', *European Studies: The Review of European Law, Economics and Politics*, 8(1), pp. 17–38. doi: 10.2478/eustu-2022-0063.

**Galeotti, M.** (2016) 'Hybrid, ambiguous, and non-linear? How new is Russia's "new way of war"?', *Small Wars & Insurgencies*, 27(2), pp. 282–301. doi: 10.1080/09592318.2015.1129170.

**Galeotti, M.** (2018) 'I'm sorry for creating the "Gerasimov Doctrine"', *Foreign Policy*, 5 March. Available at: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ (Accessed: 17 May 2026).

**Galeotti, M.** (2019a) 'The mythical "Gerasimov Doctrine" and the language of threat', *Critical Studies on Security*, 7(2), pp. 157–161. doi: 10.1080/21624887.2018.1441623.

**Galeotti, M.** (2019b) *Russian political war: moving beyond the hybrid*. Abingdon: Routledge. doi: 10.4324/9780429443442.

**Giles, K.** (2016) *Russia's "new" tools for confronting the west: continuity and innovation in Moscow's exercise of power*. London: Chatham House. Available at: http://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf (Accessed: 17 May 2026).

**Jiang, W., Jiang, J., Martek, I. and Jiang, W.** (2024) 'Critical risk management strategies for the operation of public–private partnerships: A vulnerability perspective of infrastructure projects', *Engineering, Construction and Architectural Management*, 32(7), pp. 4771–4795. doi: 10.1108/ecam-12-2023-1292.

**Kresin, O.** (2022) 'Recognition, regulation and countering hybrid threats in NATO and the EU', *Pravovaderzhava: Yearly Journal of Scientific Articles*, 33, pp. 516–529. doi: 10.33663/1563-3349-2022-33-516-529.

**Lasconjarias, G. and Larsen, J.A.** (eds.) (2015) *NATO's response to hybrid threats*. Forum paper 24. Rome: NATO Defense College. Available at: www.files.ethz.ch/isn/195405/fp_24.pdf (Accessed 26 June 2026).

**Malterud, K., Siersma, V.D. and Guassora, A.D.** (2016) 'Sample size in qualitative interview studies: Guided by information power', *Qualitative Health Research*, 26(13), pp. 1753–1760. doi: 10.1177/1049732315617444.

**Mumford, A. and Carlucci, P.** (2023) 'Hybrid warfare: The continuation of ambiguity by other means', *European Journal of International Security*, 8(2), pp. 192–206. doi: 10.1017/eis.2022.19.

**National Prosecutor's Office [Prokuratura Krajowa]** (2025) *Zarzuty w związku z pożarem hali przy ul. Marywilskiej 44*, *Gov. Pl*, 12 May. Available at: https://www.gov.pl/web/prokuratura-krajowa/zarzuty-m44 (Accessed 26 June 2026).

**North Atlantic Treaty Organisation (NATO)** (2025a) 'Statement by NATO secretary general Mark Rutte on the violation of Polish airspace by Russian drones', 10 September. Available at: https://www.nato.int/en/news-and-events/events/transcripts/2025/09/10/statement (Accessed: 17 May 2026).

**North Atlantic Treaty Organisation (NATO)** (2025b) 'Joint press conference', 12 September. Available at: https://www.nato.int/en/news-and-events/events/transcripts/2025/09/12/joint-press-conference (Accessed: 17 May 2026).

**Notes from Poland** (2024) 'Russia "likely" behind fire that destroyed Warsaw shopping centre, says Tusk', *Notes from Poland*, 21 May. Available at: https://notesfrompoland.com/2024/05/21/russia-likely-behind-fire-that-destroyed-warsaw-shopping-centre-says-tusk/ (Accessed: 17 May 2026).

**Notes from Poland** (2025a) 'Tusk: Lithuanian evidence shows Russia behind fire that destroyed Warsaw shopping centre', *Notes from Poland*, 17 March. Available at: https://notesfrompoland.com/2025/03/17/tusk-lithuanian-evidence-shows-russia-behind-fire-that-destroyed-warsaw-shopping-centre/ (Accessed: 17 May 2026).

**Notes from Poland** (2025b) 'Poland confirms Russia behind fire that destroyed Warsaw's biggest shopping centre', *Notes from Poland*, 12 May. Available at: https://notesfrompoland.com/2025/05/12/poland-confirms-russia-behind-fire-that-destroyed-warsaws-biggest-shopping-centre/ (Accessed: 17 May 2026).

**Ochyra-Żurawska, K., Skwarek, Z., Zygo, K. and Ochyra, P.** (2024) 'Bezpieczeństwo zewnętrzne Polski—Współczesne wyzwania i zagrożenia' [Poland's external security – modern challenges and threats], *Prawo i Bezpieczeństwo [Law and Security]*, 1(2), pp. 58–75. doi: 10.4467/29567610pib.24.004.19840.

**Olech, A.** (2025) 'Hybrid threats to critical infrastructure in the European Union. Selected hybrid CoE analyses', *Terrorism – Studies, Analyses, Prevention*, Special Issue, pp. 138–158. doi: 10.4467/27204383ter.25.017.21520.

**Ostrowski, P. and Zych, R.** (2024) 'State's resilience to critical infrastructure threats: The example of the Russian war on Ukraine', *Teka Komisji Prawniczej PAN Oddział w Lublinie [Journal of the Legal Sciences Commission of the Polish Academy of Sciences, Lublin Branch]*, 17(2), pp. 349–363. doi: 10.32084/tkp.9050.

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

**Prime Minister of Poland** (2024) 'Polish secret services need to be bolstered', Gov.pl, 14 May. Available at: https://www.gov.pl/web/primeminister/polish-secret-services-need-to-be-bolstered (Accessed: 17 May 2026).

**Prime Minister of Poland** (2025a) 'Airspace violation repelled: Poland's procedures prove effective', Gov.pl, 10 September. Available at: https://www.gov.pl/web/primeminister/airspace-violation-repelled-polands-procedures-prove-effective (Accessed: 17 May 2026).

**Prime Minister of Poland** (2025b) 'PM Tusk in Parliament: Russia behind sabotage attacks in Poland', Gov.pl, 18 November. Available at: https://www.gov.pl/web/primeminister/pm-tusk-in-parliament-russia-behind-sabotage-attacks-in-poland (Accessed: 17 May 2026).

**Reuters** (2025a) 'Poland downs drones in its airspace, becoming first NATO member to fire during war', *Reuters*, 10 September. Available at: https://www.reuters.com/business/aerospace-defense/poland-downs-drones-its-airspace-becoming-first-nato-member-fire-during-war-2025-09-10/ (Accessed: 17 May 2026).

**Reuters** (2025b) 'Poland downs drones after its airspace is violated', *Reuters*, 10 September. Available at: https://www.reuters.com/business/aerospace-defense/poland-downs-drones-after-its-airspace-is-violated-2025-09-10/ (Accessed: 17 May 2026).

**Reuters** (2025c) 'Russian drones in Poland's airspace stir worries for Europe's civil aviation', *Reuters*, 11 September. Available at: https://www.reuters.com/business/aerospace-defense/russian-drones-polands-airspace-stir-worries-europes-civil-aviation-2025-09-11/ (Accessed: 17 May 2026).

**Reuters** (2025d) 'US vows to defend NATO territory after suspected Russian drone incursion into Poland', *Reuters*, 12 September. Available at: https://www.reuters.com/business/aerospace-defense/us-vows-defend-nato-territory-after-suspected-russian-drone-incursion-poland-2025-09-12/ (Accessed: 17 May 2026).

**Reuters** (2025e) 'UN Security Council to meet Friday on drone incursions in Poland', *Reuters*, 11 September. Available at: https://www.reuters.com/world/europe/un-security-council-meet-friday-drone-incursions-poland-2025-09-11/ (Accessed: 17 May 2026).

**Sadowski, A. and Maj, J.** (2022) 'Interoperability and complementarity of civil defense as crucial problems of regional security: The case of the Suwalki Corridor', *The Journal of Slavic Military Studies*, 35(2), pp. 205–225. doi: 10.1080/13518046.2022.2139576.

**Sanz-Caballero, S.** (2023) 'The concepts and laws applicable to hybrid threats, with a special focus on Europe', *Humanities and Social Sciences Communications*, 10, p. 360. doi: 10.1057/s41599-023-01864-y.

**Sari, A.** (2020) 'Legal resilience in an era of grey zone conflicts and hybrid threats', *Cambridge Review of International Affairs*, 33(6), pp. 846–867. doi: 10.1080/09557571.2020.1752147.

**Special Services Coordinator** (2025) 'Act of sabotage on the railway. The safety of citizens and infrastructure as a government priority', Gov.pl, 17 November. Available at: https://www.gov.pl/web/special-services/act-of-sabotage-on-the-railway-the-safety-of-citizens-and-infrastructure-as-a-government-priority (Accessed: 17 May 2026).

**Stoddart, K.** (2022) *Cyberwarfare: Threats to critical infrastructure*. Cham: Palgrave Macmillan. doi: 10.1007/978-3-030-97299-8.

**Stoddart, K.** (2026) *Russia's hybrid warfare offensive against the west*. Berlin: De Gruyter Brill. doi: 10.1515/9783111583464.

**Wither, J.K.** (2016) 'Making sense of hybrid warfare', *Connections: The Quarterly Journal*, 15(2), pp. 73–87. doi: 10.11610/Connections.15.2.06.

**Wosik, P.** (2026) 'Defense against invisible enemies: Poland in the face of Russian hybrid warfare', *Wschód Europy. Studia Humanistyczno-Społeczne*, 11(1), pp. 11–20. doi: 10.17951/we.2025.11.1.11-20.

**Żywczyk, A.** (2025) 'Ataki hybrydowe wobec Polski: Analiza narzędzi i strategii Rosji', *Krakowskie Studia Małopolskie*, 46(2), pp. 62–73. doi: 10.15804/ksm20250203.

# Appendix

**Table A1. Coding framework used for qualitative content analysis.**

| Code family | Code | Definition | Illustrative meaning in this study |
|---|---|---|---|
| Incident characteristics | IC-KIN | Kinetic or physically destructive action | Fire, explosives, direct material damage, or physical disruption. |
| Incident characteristics | IC-TEST | Resilience testing or probing activity | Actions revealing response gaps, preparedness weaknesses, or monitoring limits. |
| Incident characteristics | IC-RECON | Reconnaissance- or surveillance-related activity | Drone incursions, probing, observation, or preparatory exposure of vulnerabilities. |
| Attribution | AF-AMB | Ambiguous or cautious attribution | Official reluctance to name a perpetrator or state link directly. |
| Attribution | AF-DIR | Direct attribution | Explicit public linkage to Russian services or a hostile state actor. |
| Legal/institutional response | LR-KK130 | Criminal-law framing | Use of sabotage-related criminal provisions and prosecutorial process. |
| Legal/institutional response | LR-DIP | Diplomatic response | Expulsions, diplomatic retaliation, or interstate signalling. |
| Legal/institutional response | LR-INT | International coordination | Eurojust, NATO-linked coordination, cross-border investigation, and allied cooperation. |
| Legal/institutional response | LR-MOB | Mobilisation/protective deployment | Visible deployment, increased security posture, and operational protective action. |
| Public–private resilience | PR-VULN | Infrastructure vulnerability | Monitoring gaps, exposed corridors, weak points, and systemic dependencies. |
| Public–private resilience | PR-COOR | Coordination demands | Information-sharing, interagency cooperation, and operator-state coordination. |
| Public–private resilience | PR-COST | Precautionary or operational cost | Delays, business disruption, compliance burdens, or security expenditures. |
| Public–private resilience | PR-DISP | Disposable agent pattern | Use of proxies, intermediaries, or low-cost deniable operatives. |

Note. The coding framework combines deductive categories derived from the study's four analytical lenses with inductive attention to emergent patterns in the source base (Ostrowski and Zych, 2024; Sanz-Caballero, 2023; Sari, 2020).

**Table A2. Descriptive distribution of selected codes across four Polish cases.**

| Codes | Marywilska 44 | Parcel plot | Rail sabotage | Drone cluster |
|---|---|---|---|---|
| AF-AMB (ambiguous/cautious attribution) | 2 | 1 | 1 | 3 |
| AF-DIR (direct attribution) | 4 | 2 | 4 | 1 |
| LR-KK130 (sabotage/terrorism provisions) | 3 | 0 | 2 | 0 |
| LR-DIP (diplomatic retaliation) | 2 | 0 | 0 | 0 |
| LR-INT (international coordination) | 1 | 6 | 1 | 3 |
| LR-MOB (mobilisation/protective deployment) | 0 | 0 | 2 | 2 |
| PR-COOR (state–private coordination) | 2 | 2 | 3 | 0 |
| PR-VULN (identified vulnerability) | 3 | 3 | 3 | 3 |
| PR-DISP (disposable agent model) | 3 | 1 | 1 | 0 |
| PR-COST (economic/operational drag) | 0 | 1 | 0 | 2 |

Note. Values indicate the number of coded source rows within each case in which the code appeared. These counts are descriptive and based on the current workbook's title-based coding; so, they should be presented as supporting indicators rather than definitive measures.