



Agents of Chaos: The Shadow Campaign Against the West

**Cognitive Warfare and Covert Action by
Russian and Belarusian Intelligence Services**

September 2025

Maciej Filip Bukowski

Agents of Chaos: The Shadow Campaign Against the West

**Cognitive Warfare and Covert Action by
Russian and Belarusian Intelligence Services**

AUTHOR	Maciej Filip Bukowski
COVER PHOTO	
COPYRIGHT	© Fundacja im. Kazimierza Pułaskiego
PUBLISHER	Fundacja im. Kazimierza Pułaskiego ul. Oleandrów 6, 00-629 Warsaw www.pulaski.pl
GRAPHIC DESIGN	Dobry Skład

Contents

Executive Summary / 5

**1 FROM GREEN MEN TO MIND WAR: THE EVOLUTION OF HYBRID THREATS
TOWARD COGNITIVE WARFARE / 7**

2 COGNITIVE WARFARE AND THE EASTERN CANON OF DISRUPTION / 9

Key Thinkers / 10

Key Strategic Intent / 12

Key Intelligence Tactics / 13

Key Operational Concepts / 15

**3 CONCEPTUAL FRAMEWORK OF INTELLIGENCE-LED DISRUPTION BY RUSSIAN
AND BELARUSIAN SPECIAL SERVICES / 16**

Layer 1: Cognitive Infiltration / 17

Layer 2: Tokenization of Operatives / 18

Layer 3: Expanding Scalable Disruption / 19

4 TYPOLOGY OF OPERATIONS: FROM FIRES TO FALSEHOODS / 20

Sabotage & Diversion / 21

Outsourcing Espionage / 23

CogOps and Disinformation / 25

Weaponization of Diasporas / 27

Tech Advancements in Software / 30

Tech Advancements in Hardware / 32

Time: the Five Phases in Narrative and Operational Cycles / 34

5 WESTERN BLIND SPOTS, ADAPTIVE FAILURES AND HOW TO FIX THEM / 35

Cognitive Deficit: The Absence of Integrated Threat Comprehension / 36

Systemic Gap: Fragmentation of Counterintelligence, Cyber, and Domestic Policy / 37

Interoperability Deficit: Data Silos Between Member State Services / 38

Regulatory Void: Absence of Effective Legal Instruments to Address Foreign Influence / 39

Turning the Tables: Lawful Hybrid Action Against Russia and Belarus / 40

Poland: National Constraints and the Need for Institutional Paradigm Shift / 42

6 CONCLUSION / 44

Review 1 and Commentary: Dr. Anna Grabowska-Siwiec / 45

Review 2: Grzegorz Małecki / 48

Executive Summary

As of 2025, the transatlantic realm is under sustained assault not through open warfare, but through a diffuse, coordinated campaign of cognitive erosion and covert disruption. Russian and Belarusian intelligence services have deployed a hybrid strategy that merges sabotage, terrorism, psychological manipulation, and narrative infiltration into a long-term framework of destabilization of the West. The aim is to fragment trust, fracture resilience, and corrode collective sense-making both within NATO states and across the alliance itself. This is not a campaign to seize territory, but one designed to induce fragmentation of societies, establish antagonistic groups that destabilize states from within, and weaken the cognitive defenses of societies – one perception at a time.

This report shows that these operations are not isolated acts of espionage or sabotage and diversion, but elements of a systemic architecture of cognitive warfare. Russia and Belarus have fused reflexive control theory, narrative engineering, and networked disinformation into a doctrine aimed at the mental and emotional foundations of Western societies. The focus here is Europe, with particular attention to Poland, the Baltic states, and selected Western European countries, where such operations illustrate the scale and logic of a war fought below the threshold of NATO's Article 5, yet carrying existential consequences.

The report identifies three fundamental interlocking layers of this campaign waged against the West:

1. **Cognitive Infiltration:** Penetration of public discourse and digital ecosystems with psychologically potent, memetic narratives designed to erode trust in institutions, blur the lines between truth and fiction, and trigger emotional fatigue.
2. **Tokenized Execution:** Decentralized recruitment of unwitting or expendable operatives to carry out physical sabotage, including warehouse arsons and drone reconnaissance. This ensures plausible deniability while enabling scalable disruption via proxy agents [1] [2].
3. **Disruption via Micro-Operations:** Fragmented but cumulative low-intensity actions are synchronized with information warfare to amplify confusion, induce paralysis, and overload Western crisis response systems.

This report argues that **the West must abandon its purely reactive posture**. A defensive intelligence paradigm is insufficient against an adversary that targets perception, emotion, and decision-making itself. What is needed is a calibrated offensive posture that treats cognitive security as a core element of national and alliance-level defense.

Key recommendations include:

- Establishing a cognitive early warning system combining open-source intelligence, AI-based tools, narrative analysis, and emotional trend mapping;
- Activating diaspora-based counterintelligence assets, mobilizing Russian and Belarusian exiles as both operational and symbolic nodes of resistance;
- Creating a European registry of foreign influence and perception manipulation actors, modeled on FARA but tailored to hybrid threats;
- Deploying targeted counter-narratives and controlled disruption campaigns using symbolic inversion, memetic tactics, and agile communications;
- Institutionalizing cognitive warfare simulations within NATO and EU crisis planning to reflect the cross-domain nature of modern hybrid threats

Ultimately, the long-term effectiveness of the ongoing hybrid offensive depends not on the power of Moscow and Minsk, but on the inertia of the West. Victory in this war of perception will be achieved by those who understand that the battlefield is not terrain, but trust. Clarity of stance and societal coherence must be treated not as ideals, but as fundamentally strategic assets to be protected and reinforced.

1

From Green Men to Mind War: The Evolution of Hybrid Threats toward Cognitive Warfare

The concept of hybrid warfare has evolved from a model based on irregular military tactics and limited disinformation into a multi-layered strategy targeting the cognitive foundations of democratic societies. What began with the appearance of unmarked military personnel during the annexation of Crimea and the use of proxy militias in eastern Ukraine has matured into a campaign that seeks to destabilize public perception, disrupt emotional coherence, and corrode the very process by which societies distinguish truth from falsehood.

In its initial form, hybrid warfare focused on physical ambiguity [3] [4] [5]. Unattributed actors seized infrastructure, manipulated local political conflicts, and obscured state responsibility through plausible deniability [6]. These operations leveraged confusion in the legal and military grey zones that define responses below the threshold of open conflict. Their objective was material influence without conventional war. A major example includes the set of operations that preceded Russia's illegal seizure of Crimea [7] [8] [9].

Over time, however, and with advancements in technology, the focus has shifted toward psychological ambiguity. Today, Russian and Belarusian hybrid strategies aim at not just concealing (...) and making the attack indistinguishable from internal dysfunction. This is an approach that targets perception, interpretation, and emotion. Its goal is to fragment society's shared reality and overwhelm it with contradictions, false choices, and fatigue. It is designed to confuse and exhaust rather than to coerce through force.

In this new phase, hybrid threats rely less on the seizure of buildings or transport lines and more on the occupation of informational and emotional spaces. Weaponized narratives, destabilizing rumors, manipulated imagery, and algorithmically boosted sentiment floods are used to inject uncertainty into every layer of democratic life. The objective is no longer just strategic advantage but epistemic disorder.



Societies that cannot agree on what is real cannot act collectively or defend effectively.

This transformation has profound consequences. It means that intelligence services, influence operations, and information technology are now instruments of adverse offense. It also means that traditional deterrence frameworks, built on visibility and proportionality, are ill-suited to confront an adversary that operates through

invisibility and diffusion. The war now waged against the West has moved from the battlefield to the mind, and winning it requires understanding cognition not as an afterthought, but as the primary target of hostile action. Intelligence services, which traditionally operated in the shadows, are increasingly abandoning plausible deniability and conducting their activities in a practically overt manner.

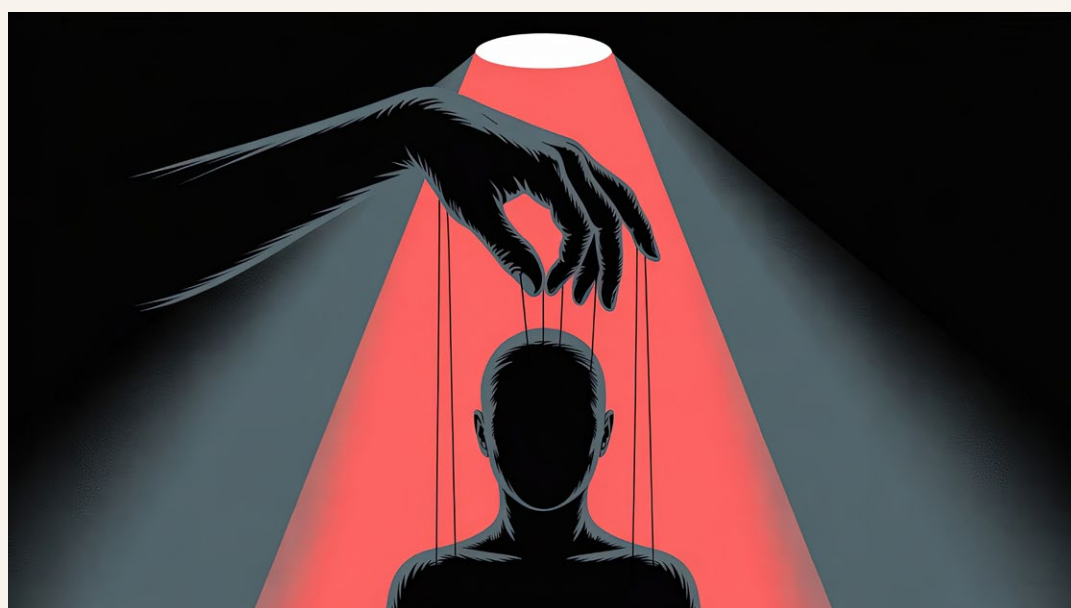
2

Cognitive Warfare and the Eastern Canon of Disruption

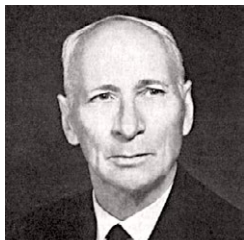
Russia's, and by extension Belarus's, cognitive warfare framework is instrumental, not teleological. Its ultimate goal remains geopolitical expansion and the revision of the international order. The cognitive arsenal is not an end in itself, but a means to disable resistance, erode cohesion, and shape the battlefield long before kinetic or political escalation. Russian and Belarusian intelligence strategies are underpinned by a body of theoretical work that functions not as an ideology, but as a toolkit. This canon

combines post-Soviet military thought with postmodern strategies of perception warfare and narrative control.

These doctrines view cognition as terrain, and emotion, fatigue, and confusion as weapons. The following theorists offer the intellectual scaffolding for contemporary influence operations, covert interventions, and ambient psychological disruption.



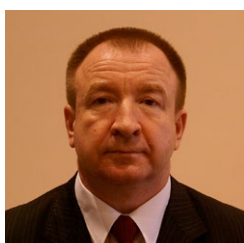
Key Thinkers



Evgeny Messner [10] [11] [12]

A Tsarist officer turned émigré theorist, Messner developed the concept of *мятежная война* (“mutinous war”), which framed modern conflict as a rebellion within the psyche of societies. He posited that wars would no longer be fought over territory or dominance between armies, but through the corrosion of civilizational will. Fear, disorientation, and loss of loyalty were his weapons of choice. Messner’s theory, developed in exile in Argentina, foresaw hybrid war decades before its doctrinal codification in Russia.

Photo source: Andrzej Turczyn Blog



Igor Panarin [13] [14] [15]

A former КГБ analyst and academic, Panarin advanced the idea that information-psychological warfare is a continuous and legitimate form of diplomacy. His works, including *Information Warfare and Geopolitics* (1999), advocate preemptive narrative saturation to shape adversary’s perception, stabilize domestic public opinion, and engineer a psychological buffer zone. Panarin normalizes the weaponization of media as a standard interstate behavior and calls for permanent readiness in the cognitive domain.

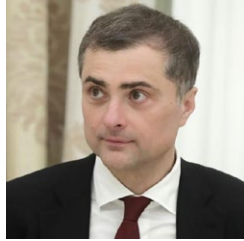
Photo source: Wikipedia



Gleb Pavlovsky [16] [17] [18] [19]

A former Soviet dissident turned Kremlin technologist, Pawłowski engineered the doctrine of *managed democracy* and conceptualized *virtual politics*. His suggested strategy was to flood the information environment with curated contradictions, fragmenting political discourse into performative confusion. Pavlovsky’s method does not rely on narrative control through censorship, but on the creation of emotional apathy and epistemic exhaustion through media theater.

Photo source: Wikipedia



Vladislav Surkov [20] [21]

Surkov, both playwright and power broker, formalized a methodology of chaos as governance. In *The Loneliness of the Half-Breed*, he advocates a vision of non-linear politics where the state orchestrates conflicting narratives to neutralize resistance and produce epistemic dependency. Surkov's technique relies on contradiction, ambiguity, and spectacle to create a society where every version of truth is plausible, but none is actionable.

Photo source: Wikipedia



Aleksandr Dugin [22] [23] [24] [25]

Dugin, the ideologue of Eurasianism, views information not as propaganda but as metaphysical warfare. His *Fourth Political Theory* advocates for civilizational conflict in which liberalism is dismantled through cultural, religious, and psychological infection. Information, fear, myths, and religious archetypes serve to undermine Enlightenment-based ontologies. While Dugin's institutional influence is debated, his civilizational framing permeates military-intellectual networks and nationalist media across the Russian state apparatus.

Photo source: Wikipedia



Valery Gerasimov [26]

Since 2012, the General has served as Chief of the General Staff of the Armed Forces of the Russian Federation. In his 2013 article *The Value of Science Is in the Foresight* he argued that modern conflicts increasingly hinge on non-military instruments. His concept, described as “a new approach to achieving political and military objectives,” emphasizes the coordinated use of political, economic, informational, and social tools to destabilize an adversary and erode its resilience well before the outbreak of open armed confrontation. These operations, envisioned as continuous and intertwined with limited military action, give rise to the distinctive grey zone that blurs the line between peace and war.

Photo source: Wikipedia

Key Strategic Intent

Moscow's end-state is not a classic territorial aggrandizement alone, but parity by subtraction: to narrow the gap with the West by degrading Western cohesion, capacity, and clarity faster than Russia must reform itself. As Timothy Snyder argued in *The Road to Unfreedom*, once the Kremlin internalized that convergence with the West was unattainable, it pivoted to demolition from within, seeking to make liberal democracies appear chaotic, self-contradictory, and unworthy of emulation. The strategic aims are regime preservation, restoration of a privileged sphere of influence, decoupling and exhaustion of support for Ukraine, and the creation of a permissive security environment where coercion

below the threshold becomes routine. Operationally, this translates into corrosion of trust in institutions, fragmentation of EU-NATO decision cycles, and the imposition of friction costs on innovation, logistics, and crisis response. Success is measured not by public victories but by delayed attribution, longer response times, rising defensive overheads, and recurrent political paralysis. Belarus functions as an auxiliary platform and risk buffer, extending reach while dispersing attribution. This intent explains why cognitive, criminal, and deniable kinetic lines of effort are synchronized to keep defenders reactive and societies emotionally fatigued.



Key Intelligence Tactics

Russian and Belarusian intelligence services operate as a distributed ecosystem where each agency cultivates its own area of specialization, yet overlaps are deliberately maintained to enable redundancy and plausible deniability. Understanding these differentiated roles is essential for mapping hybrid threat vectors.

The **Federal Security Service (FSB)** functions as both a domestic counterintelligence agency and an external operator. While its primary mandate is internal control, the FSB runs extensive operations abroad through Russian diplomatic cover, especially in Central and Eastern Europe. For instance, in 2017 Estonian authorities arrested a Russian national suspected of being an FSB agent preparing cyberattacks against Estonian state institutions [27].

The **Main Directorate of the General Staff (GU – formerly GRU)** provides the kinetic arm of Russian hybrid warfare. Its specialization lies in military sabotage, targeting critical infrastructure, logistics corridors, and energy systems. The most infamous example is the 2018 Skripal poisoning in Salisbury, conducted by GRU Unit 29155 using military-grade Novichok nerve agent [28]. GRU has also been tied to NotPetya (2017), a cyber-sabotage campaign disguised as ransomware that crippled Ukrainian and global infrastructure, causing billions in damage [29].

The **Foreign Intelligence Service (SVR)** pursues traditional long-term espionage and influence campaigns. Its hallmark operations involve technology theft and penetration of political circles. For instance, in 2020, the supply-chain hack of the SolarWinds firm was attributed to SVR's hackers group APT29 (Cozy Bear), which compromised U. S. federal agencies and corporations to harvest strategic intelligence without immediate disruption [30].

The **Federal Protective Service (FSO) and Spetssvyaz**, in turn ensure secure communications for Russia's leadership and military.

Open-source and intelligence analyses confirm their administration of SORM, Russia's mass surveillance and interception system, which simultaneously protects regime channels and monitors dissidents [31].

The **Belarusian KGB and its internal security branch GUBOPiK** operate in two interconnected spheres. Domestically, they conduct systemic repression, dismantling opposition structures and controlling civil society through coercion and infiltration. As such, it functions as a *de facto* political police. A high-profile example is the 2021 Ryanair Flight 4978 hijacking, when the Belarusian KGB orchestrated the forced landing of a civilian airliner in Minsk to arrest opposition journalist Raman Pratasevich [32]. Abroad, GUBOPiK has been infiltrating Belarusian exile communities abroad in exchange for permission to leave Belarus [33].

Taken together, these agencies compose a **layered offensive system**: FSB for counterintelligence penetration on its own territory, where it serves a protective function against foreign intelligence, while abroad it conducts intelligence activities. GU is responsible for sabotage, SVR for influence, Belarusian KGB for repression and diaspora operations, and FSO/Spetssvyaz for operational security. This division of labor illustrates why hybrid operations remain sustainable and adaptable, as each service feeds into the others' activities while maintaining enough independence to obscure clear attribution.

The Russian and Belarusian KGB security services have shifted from collection-centric espionage to operations that engineer public belief at scale. The transition accelerated after 2014 as Russia fused online influence with deniable kinetic acts, iterating through networks through a series of operations known collectively as Secondary Infektion [34], and later cross-platform campaigns that exploited Telegram and fringe ecosystems. By 2023 and 2024, this model was stress-tested in the Baltics [35] [36] and Poland

through synchronized influence, sabotage, and criminal outsourcing. The metric of their efficiency is saturation of narratives and the manipulation of social attention rather than clandestine secrecy. Criminal and extremist proxies provide reach, deniability, and localized access while state services supply targeting, narratives, and money flows.

As explained in detail in Chapter 3 of this report, this systemic approach operates across three overlapping fields. First, fringe and semi-closed online spaces seed and amplify emotionally charged frames that target identity, grievance, and fear (Cognitive Infiltration). Second, diasporic and migrant communities are selectively targeted for both perception shaping and

low-cost tasking, with recruitment and payment routed through encrypted channels (Tokenization of Operatives). Third, local civic tensions and vulnerabilities are converted into strategic wedges through calibrated acts of disruption (Expanding Scalable Disruption).

The hallmark effect of these operations is ambient instability that erodes confidence and decision quality. The method blends symbolic offense with selective material damage to trigger disproportionate coverage and political friction. The battlefield is the collective emotional metabolism. The objective is steady corrosion of civic resolve and alliance cohesion rather than a single decisive breakthrough.

Key Operational Concepts

Reflexive control [37]: Originating in Soviet military science, this concept denotes the manipulation of an adversary's decisions by pre-conditioning their perceptions and responses. It involves engineered stimuli, such as false choices, decoy information, and tempo manipulation.

Deceptive masking (maskirovka – *маскировка*) [38]: A doctrine of layered deception in which decoys, distraction, and seemingly innocuous actions conceal the real operational aim. It works both tactically and narratively to misdirect detection and interpretation. Doctrinally, the concept first emerged within Russian military operations and was later integrated into the broader framework of hybrid warfare.

Perception shaping operations [39]: A long-term effort to transform how societies interpret events, assign meaning, and recognize threats. This involves subtle and repeated emotional stimuli, not always linked to explicit political messages.

Cognitive fracking: A novel concept proposed herein, referring to the exploitation of social vulnerabilities that already exist: identity fractures, class anger, historical grievances. The method involves psychological pressure designed to rupture dormant tensions and provoke self-destructive political behavior.



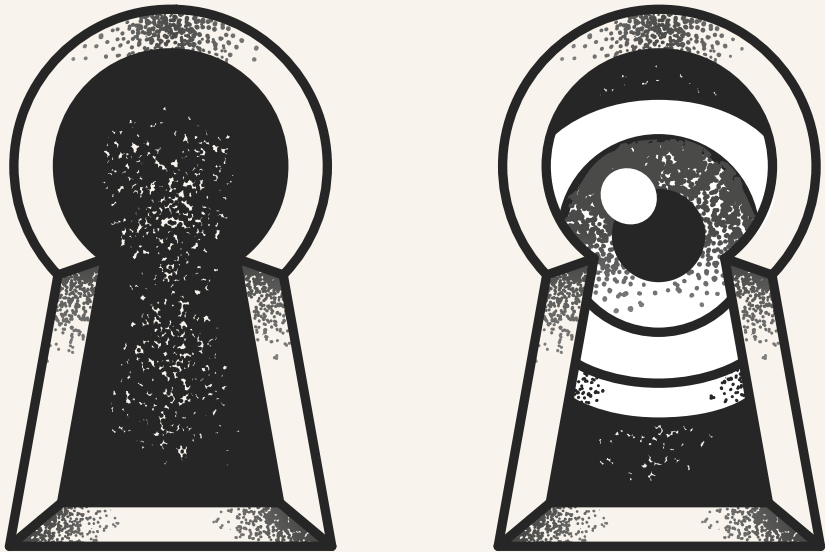
3

Conceptual Framework of Intelligence-Led Disruption by Russian and Belarusian Special Services

Russian and Belarusian intelligence operations across NATO's eastern flank are not reactive provocations. They are embedded within a deliberate architecture of conscious disruption, calibrated to exploit vulnerabilities without triggering open conflict. The animating principle is not to defeat Western states militarily, but to fragment them cognitively, exhaust them perceptually, and corrode them institutionally. Each layer operationalizes parity by subtraction:

infiltration corrodes trust, tokenization scales ambiguity, and micro-operations impose persistent friction on governance and logistics.

This operational philosophy privileges ambiguity over attribution and incoherence over escalation. What emerges is a layered, decentralized campaign targeting belief, legitimacy, and psychological resilience across time. Below are the three principal strata of this model.



Layer 1: Cognitive Infiltration

At its base is the systematic penetration of the informational ecosystem. The Russian information campaign proceeds in two distinct phases: first, social divisions and distrust for the institutions are built, and these tensions are subsequently escalated to enforce political and psychological reaction. This is not simply propaganda. It is a methodical repurposing of existing tensions, symbols, and anxieties to saturate public discourse with confusion, suspicion, and polarizing affect. Russian and Belarusian services use diasporic networks, digital influencers, and algorithmic cues to embed hostile messaging within domestic conversations.

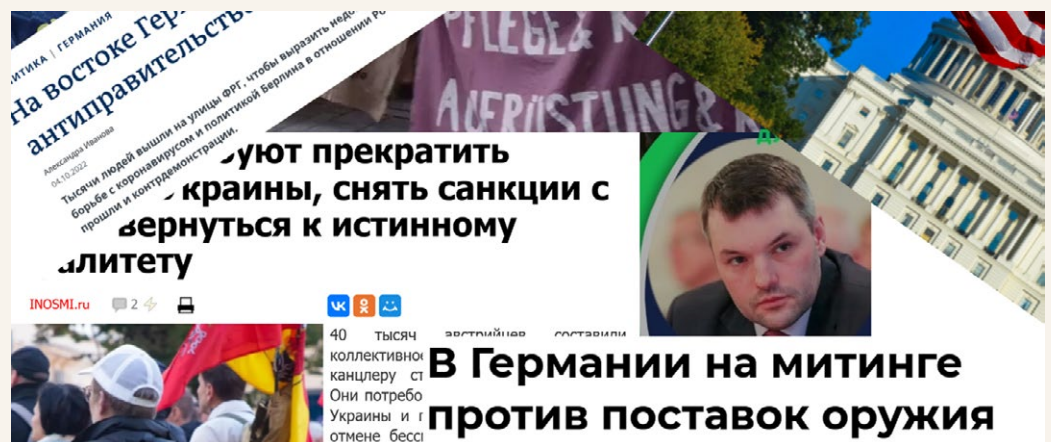
Narratives often exploit:

- Alleged victimhood of Russia or Belarus (“We are encircled by NATO”)
- National grievances (“Poland is a puppet”, “Ukrainians are privileged guests”)
- The decay of Western moral legitimacy (“Gender ideology”, “cultural suicide”)
- Historical Polish-Ukrainian antagonisms
- Aversion to “outsiders” within society

Case: In the run-up to Poland’s 2025 presidential election, Russia-aligned influence networks used X (formerly Twitter) and Telegram channels with Polish-language identities to circulate targeted disinformation portraying Ukrainian refugees as a burden on the state. These narratives included fabricated statistics and visual materials that framed refugees as distorting welfare systems and demographic stability. The campaign integrated content across multiple online communities to amplify its reach, leveraging localized branding to increase credibility while masking its coordinated and foreign origin [40].

Relevant concept: *Perception shaping operations* are not persuasive in the classical sense. They render truth relative by making every position feel ideologically contaminated, emotionally exhausting, or contextually unverifiable.

Examples of Russian propaganda about Ukraine



Source: gov.pl

Layer 2: Tokenization of Operatives

The middle layer consists of outsourcing of tactical tasks to low-visibility, low-cost individuals. This is a hallmark of the Russian and Belarusian shift toward scalable ambiguity. Rather than deploy trained operatives, intelligence services now “tokenize” labor by separating their intent from tactical execution.

Such actors include:

- Economic migrants recruited online, often through encrypted channels, who serve as proxy agents; this recruitment is sometimes linked to cryptocurrency payments and a sense of impunity
- Criminal elements motivated by cryptocurrency and impunity
- Disillusioned citizens convinced of corruption in national politics
- Individuals with personality disorders or mental health problems

Tasks are framed as logistical, ideological, or benign. A man photographing a military base is portrayed as a train enthusiast. A warehouse fire is linked to criminal turf wars. This method ensures that sabotage and diversion remain plausibly deniable, fragmentary, and depoliticized in the eyes of the public.

A defining feature of Russian and Belarusian intelligence methods is the increasing reliance on ad-hoc “disposable spies”: one-off operatives recruited for a narrowly defined task with minimal training and no long-term institutional attachment. This construct aligns with the intelligence industry’s concept of “throwaway” identities: agents used for a single mission and then discarded to preserve deniability and minimize

bureaucratic burden [41]. The use of disposable spies surged notably after the mass expulsions of Russian diplomats in early 2022, estimated at over 600 across Europe by mid-2022, including approximately 400 in just one wave. This forced the Kremlin to pivot away from embassy-based intelligence toward more precarious, ad hoc recruitment models using financial incentives or ideological persuasion [42]. In addition, other forms of agency are also employed, such as illegals operating under false identities, walk-ins who independently volunteer their cooperation, defectors providing information after switching sides, and agents of influence shaping public opinion and political decision-making.

Case: Between late 2023 and mid-2024, Poland, the United Kingdom, and Germany recorded a series of arson and sabotage incidents initially attributed to local disputes or criminal rivalries. In Poland, attacks on a Gdynia restaurant, a warehouse in Gdańsk, and a pallet storage site in Marki were first linked to organized crime but later tied to Russian intelligence tasking [43]. In the UK, a London warehouse fire and attempted arson at a Ukrainian-linked business were presented as isolated criminal acts until counterintelligence identified coordination with Russian handlers [44]. In both contexts, operatives were often recruited online from vulnerable social groups, paid in cryptocurrency, and kept unaware of the broader operational purpose, ensuring that each action appeared disconnected from a larger hostile campaign.

Relevant concept: *Deceptive masking* operates by layering incoherence of tactics over coherence of strategy. By dispersing execution across civilian proxies, the operation evades attribution while increasing scale.

Layer 3: Expanding Scalable Disruption

The upper layer of this model is temporal and symbolic. Its aim is not immediate crisis but cumulative degradation. Scalable disruption chains together minor events to create strategic effects: fear cycles, institutional embarrassment, public paralysis. The model is iterative and resilient. If one operation fails, another quietly replaces it.

Typical effects include:

- Psychosocial exhaustion from repeated low-level threats (e.g. bomb alerts, cyber hoaxes)
- Loss of institutional credibility through spectacle and contradiction
- Overextension of state response capacities by exploiting overreaction

Case: Since 2024, Poland has seen over a dozen coordinated arson attacks on logistics centers, including the large-scale Marywilska fire, where some 1,400 stores and service points were destroyed [45]. These incidents drew intense media attention and successfully redirected the national conversation, showing how physical sabotage can be exploited for political effect.

Relevant concept: *Cognitive fracking* involves tapping into latent societal fissures, such as cultural resentment, economic precarity, or post-pandemic distrust to trigger disproportionate psychological reactions. This is not about propaganda, but accelerating pre-existing entropy.

Russian hybrid-warfare activity by country and year, January 2018-June 2025



Source: International Institute for Security Studies

4

Typology of Operations: From Fires to Falsehoods

This chapter lays out six principal categories of hybrid operations conducted by Russian and Belarusian intelligence actors. Each category is illustrated with verified case studies.



Sabotage and Diversion

Russian and Belarusian intelligence services have progressively refined sabotage as a hybrid warfare tool to operate below the threshold of open conflict while producing maximum political and societal disruption. This approach draws on Soviet-era doctrine [46], but incorporates twenty-first-century operational flexibility, compartmentalization, and synchronization with information warfare. The change accelerated after 2022, when logistical corridors through Poland, the Baltics, and Germany became essential for sustaining Ukraine's defense. The 2025 IISS report indicates a fourfold increase in Russian sabotage operations against critical infrastructure in Europe between 2023 and 2024, with most actions having been conducted by decentralized, ad hoc contractors [47].

Rather than relying on high-profile kinetic attacks, these operations now favor a pattern of persistent, low-to-mid intensity actions that cumulatively erode public trust and institutional credibility of legally elected authorities. The night of September 9–10, 2025, when a dozen of Russian drones violated Polish air space, is to be treated as a case study of scalable sabotage: the enemy tested NATO procedures, probed reaction times, and assessed the psychological resilience of Polish institutions. The hallmark of this sabotage doctrine is plausible deniability. Operatives often work through unwitting intermediaries, recruited via social media and encrypted messaging apps and paid in cryptocurrency, with tasks framed as benign or apolitical to mask strategic intent. These assignments range from photographing military convoys to placing incendiary devices in civilian facilities. Such methods allow intelligence services to maintain distance from the physical act, complicating attribution while ensuring that the disruption coincides with politically sensitive moments. These activities operate in a gray space where the adversary's objective is to impose friction and uncertainty on decision-making processes rather than achieve an immediate battlefield advantage.

Norway experienced an underground cable channel fire between Asker and Drammen that disrupted rail services [48], and Oslo faced a wave of at least sixteen deliberate vehicle fires since April 2024 [49]. In **Finland**, there were at least eleven break-in attempts against municipal water supply systems in Turku, Tampere, Porvoo, and Sipoo, as well as fires at UPM's Joensuu plywood factory, the Santahamina garrison area, Ruovesi's municipal hall, an industrial hall in Lahti suspected to be arson, and a recycling facility in Oulu [50] [51].

Estonia saw the destruction of a PVC storage structure in Lööra and an explosion at a heavy fuel oil tank in North Tallinn's port area [52]. **Latvia** reported a hazardous waste facility fire in Riga's [53] Bolderaja district [54], while **Lithuania** recorded a fire at the Kaunas Aviation Factory near a disused military airfield [55].

Investigations revealed that recruitment and operational guidance had taken place through online platforms such as Telegram, where suspects received explicit reconnaissance and sabotage instructions.

Similar tradecraft emerged in **Germany**. In April 2024, German authorities arrested two dual nationals suspected of planning sabotage attacks on military bases on behalf of Russia [56]. In 2025, prosecutors brought to trial several men accused of participating in Russian-directed operations, including schemes to mail incendiary and explosive parcels [57]. Also in 2025, courier facilities in Germany and the **United Kingdom** were targeted with parcels disguised as everyday consumer goods such as massage devices and cosmetic kits, concealing incendiary compounds and timed ignition systems [58]. These devices caused limited material damage but were intended to test screening protocols, disrupt supply chains, and foster perceptions of systemic vulnerability.

In **Poland**, the scale of hostile activity detected in Poland between is unprecedented in post-Cold War Central Europe. At least 49 individuals have been arrested for espionage, sabotage, or cooperation with Russian or Belarusian services [59]. Those detained include foreign nationals, local proxies, and opportunistic recruits drawn in via encrypted messaging platforms, low-threshold online offers, or darknet intermediaries. Authorities dismantled 19 distinct operational groups, many compartmentalized and unaware of one another's tasks, reflecting a systemic effort to flood the environment with plausible operatives engaged in low-sophistication, high-frequency missions such as photographing military railways, monitoring airports, or setting fires near strategic warehouses.

Within just a few weeks in 2024, Poland experienced an unusually dense and varied series of incidents targeting industrial, military, logistical, economic, and symbolic assets. In May, Kremlin-linked operatives set fire to the Marywilka 44 shopping center in Warsaw, destroying more than 1,400 commercial units and causing losses estimated at hundreds of millions of zloty.

By late June, the tempo intensified. On June 28, a fire consumed diesel tanks at the LHS transshipment terminal in Sławków [60], threatening a key freight artery, while another blaze spread across seven hectares of the military training ground in Żagań [61]. Industrial damage included the destruction of two wood-processing halls in Klonowo [62] and a major fire at the Synthos chemical plant in Oświęcim, which required 25 firefighting brigades to contain.

Cultural and heritage sites were also struck, including the Stolberg Palace in Wrocław, a historic palace in Jelcz-Laskowice [63], and a 17th-century wooden church in Nowy Sącz. Economic and agricultural losses mounted with the destruction of 500 tons of grain in a warehouse in Sierpc [64] [65]. In Wrocław [66], police arrested a man attempting to ignite a paint factory; investigators found direct links to Russian intelligence handlers who had wired approximately 5,000 USD for the operation.

A specific domain of strategic importance where Poland is grappling with Russian sabotage concerns fiber-optic cable disruption. Recent incidents in Warsaw, including large-scale damage to underground lines in Warsaw [67], illustrate

how foreign intelligence services may be shifting from maritime operations against Baltic undersea cables to land-based attacks on critical telecommunication infrastructure.

This clustering of diverse incidents in such a compressed period appears designed to overwhelm national response capacity and maintain a constant sense of vulnerability. Russia and Belarus have been refining a generation of hybrid tools on Polish soil, treating the country as a testbed for persistent operations targeting cognition, infrastructure, diaspora vulnerability, and societal confidence. These actions are not aimed at decisive breakthroughs but at incremental corrosion, with each probe producing high-volume institutional, informational, or psychological reverberations. Over time, the logic becomes systemic: normalize infiltration, stretch institutional bandwidth, and alter societal perceptions of stability and sovereignty.

Taken together, these incidents reveal a coherent operational doctrine in which high-value military, energy, and industrial sites are targeted alongside culturally significant and civilian assets. The pattern is designed to coerce security forces into constant reaction mode, create visible evidence of state weakness, and sustain an undercurrent of public insecurity that can be exploited in the information domain.

From a theoretical perspective, these acts are not isolated but form part of a systemic campaign logic in which physical attacks are sequenced and distributed to create ambient instability. The operational effect comes from sustained tempo and geographic dispersion, forcing security services to overextend their monitoring and investigative capacity. Each act is amplified by accompanying information operations that either exaggerate state incompetence or fuel conspiracy narratives, further magnifying the psychological impact.

This integration of sabotage and diversion into a broader hybrid framework demonstrates how Moscow and Minsk have adapted old tradecraft to modern vulnerabilities. They are blending low-visibility physical disruption with tailored narrative exploitation to create a feedback loop in which each incident primes the information environment for the next. The result is an enduring erosion of societal resilience, achieved without crossing the conventional thresholds that would trigger direct military retaliation.

Outsourcing Espionage

Outsourcing espionage is one of the key elements of the current hybrid warfare strategy employed by Russian and Belarusian intelligence services, but it does not signify a complete departure from traditional methods. Intelligence officers operating under diplomatic cover as well as illegals using false identities remain active. What is new, however, is the growing importance of recruiting low-visibility individuals, often migrants or citizens of third countries, who are approached through encrypted communication platforms such as Telegram, WhatsApp, or online forums.

This model does not replace traditional intelligence but rather complements it by creating flexible and harder-to-detect networks. It allows the combination of operations carried out by career officers with cheap and ad hoc missions performed by individuals recruited on the spot, which together strengthen the ability to conduct large-scale influence and sabotage operations.

Recruits, often migrants, newly arrived refugees, or economically marginalized individuals, are given strictly defined tasks such as surveillance, infiltration, or minor sabotage. Payments range from symbolic sums for simple activities to several hundred dollars or cryptocurrency for more complex operations. These missions are designed to be deniable, scalable, and difficult to trace back to central command structures.

Investigations have revealed cases in which many recruits were effectively treated as disposable assets. Some mistook their handlers for business partners or nationalist sympathizers, agreeing to tasks such as distributing anti-NATO leaflets or installing cameras to monitor military transport headed for Ukraine. In return, they received cryptocurrency payments ranging from 5 to 400 dollars [68]. Victims of recruitment were often approached through gig-work platforms where migrants searched for temporary jobs, which made the recruitment process harder to



Photo: primagi – stock.adobe.com



detect. They were engaged in such a way that they did not know or understand who they were truly working for, which may have also resulted from the limited intellectual capacity of some recruits. This is a routine operational technique; even in classical agent recruitment, the process is conducted under a cover story so that the recruited individual does not realize they are being recruited.

In 2024, a 17-year-old Canadian was recruited by FSB and directed to conduct espionage tasks before his arrest led to the exposure of cryptocurrency wallets linked to FSB money laundering network [69]. Czech intelligence documented cases in which migrants outside the European Union were hired via Telegram under the pretext of criminal activities or legitimate jobs, often without realizing they were aiding foreign intelligence, which contributed to a climate of distrust within communities [70].

A similar pattern appeared in the United Kingdom, where a Bulgaria-based spy ring led by Orlin Roussev used intermediaries to recruit operatives for surveillance on dissidents, journalists, and Ukrainian military personnel. These operatives were financially motivated, with some claiming they had been deceived and held no ideological alignment with the mission [71]. Such

groups demonstrate how criminal and informal networks can be converted into intelligence assets, further blurring the boundaries between espionage and organized crime.

This model extends into sabotage or diversion operations. In March 2024, a British court convicted three men for setting fire to a warehouse containing Ukrainian aid supplies. Their handler, believed to have ties to Russian intelligence, coordinated the operation via Telegram and praised them in Russian once the fire began [72]. The case highlights the deliberate use of untrained and easily replaceable operatives to conduct destabilizing acts under remote guidance, with minimal exposure for the directing intelligence service.

The outsourcing approach fits within hybrid warfare doctrine, which prioritizes cumulative erosion of trust and institutional credibility over direct confrontation. By distributing tasks among loosely connected individuals who are not part of formal networks, Russian and Belarusian intelligence reduces operational vulnerability while maintaining continuity of action. This method sustains a constant operational presence, shaping both the physical environment and the information space without engaging in open conflict.

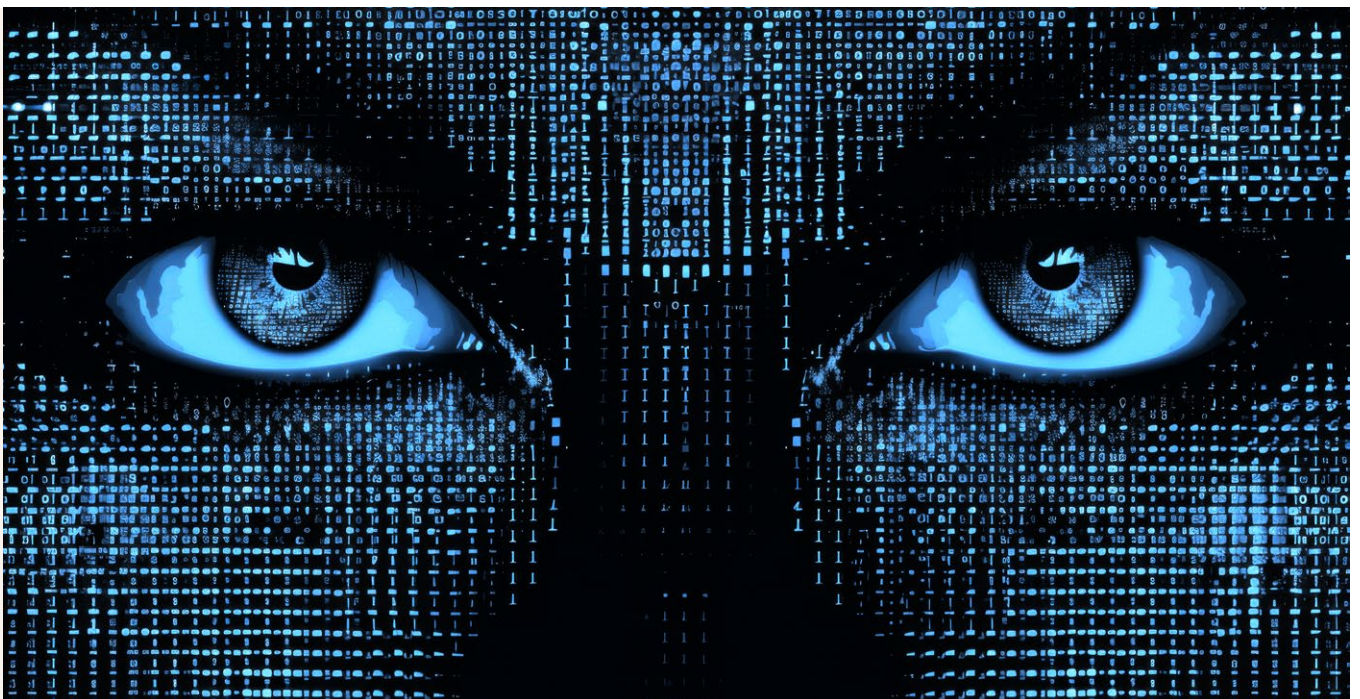
CogOps and Disinformation

Cognitive operations seek to shape what people notice, feel, and conclude, now running on a production line that blends inauthentic personas, synthetic media, and cross-platform choreography. The goal is saturation and uncertainty rather than persuasion in a single message. Investigators in Europe describe a repeatable pipeline that seeds a claim in fringe channels, launders it through impersonation sites and pseudo-local outlets, and then boosts it with automation and coordinated posting, increasingly using consumer AI to multiply volume and cadence [73].

In Poland, analysts documented a cross-platform effort that fused Russia-aligned clusters with Operation Overload techniques to inflame sentiment against Ukrainian refugees during the 2025 presidential cycle, including AI-generated visuals and impersonation sites that mimicked local outlets to heighten credibility and reach. The operation timed bursts around campaign milestones and used diaspora-adjacent Telegram channels to mimic grassroots anger [74]. Independent monitors tracking the same

architecture across Europe found the network spiking during elections and crisis moments, while exploiting enforcement gaps on large platforms to keep narratives circulating [75].

In France, state investigators mapped large pro-Russia content farms that cloned mainstream media brands and pushed tailored falsehoods, a pattern that Paris linked to a persistent network of 193 fake news sites and to the broader “Portal Kombat” and “Doppelgänger” ecosystems targeting French information space and the Paris 2024 Olympics. Authorities published technical details, attribution notes, and examples of fabricated videos and spoofed articles designed to appear native to the French media environment [76] [77] [78]. A follow-on national brief detailed how generative AI accelerated the same ecosystem by producing synthetic anchors, cloned voices, and templated videos at scale, while repackaging content for Telegram, X, and smaller video platforms to bypass moderation [79].





In the United Kingdom, the government sanctioned Russian disinformation contractors and executives after documenting attempts to incite anti-Ukraine protests and run coordinated influence assets that impersonated British news outlets and local civic pages. Public designations named the Social Design Agency and related entities, and tied them to cloned domains and narrative operations that targeted UK audiences and allies [80] [81]. Research teams also tracked the Overload network using free AI tools to flood British and European platforms with synthetic images, cloned-voice clips, QR-code redirects, and template websites, including mass submissions to fact-checkers that appeared designed to hijack attention cycles [82] [83].

In the United States, the Department of Justice and partner agencies disrupted an artificial-intelligence-enhanced bot farm built with software from Russia's state-run RT and operated by the FSB, which was designed to seed and amplify divisive narratives at scale across X and other platforms. In a separate action, the department seized 32 Doppelgänger domains that spoofed legitimate media and government sites to launder Russian state narratives into the American information space [84] [85]. A joint FBI and CISA advisory added technical detail on the "Meliorator" automation stack, describing how account creation, content scheduling, and audience targeting were integrated to drive engagement while masking coordination [86].

Across these theaters, generative AI has shifted disinformation from artisanal work to an automated process. Investigations show adversaries using off-the-shelf models to create synthetic visuals, clone voices, translate and localize at speed, and then A/B test copy and persona scripts to converge on the most anger-eliciting variants. Analysts who followed Overload across Europe and the UK documented that free consumer tools were sufficient to mount a continuous "content explosion," which multiplied the number of assets and channels faster than enforcement could adapt [87] [88]. European strategic reporting adds that these cognitive lines of effort are synchronized with physical and cyber events, for example drone incursions, sabotage scares, or service outages, to blur situational awareness and keep institutions reactive rather than anticipatory.

Finally, several governments and research bodies stress that the headline impact on election outcomes is not the only measure of threat. Studies of the 2024 UK and EU elections found limited direct vote effects from AI deepfakes while still warning about corrosive side effects, including intimidation of candidates, confusion about what sources to trust, and the normalization of synthetic rumor cycles that persist beyond the campaign period [89]. That distinction matters for policy because cognitive operations aim to degrade confidence and cohesion over time, even when short-term polling shifts are hard to detect.

Weaponization of Diasporas

Diaspora communities across Europe have become operational terrain for Russian and Belarusian intelligence, providing language access, trust networks, and civic cover that enable recruitment, surveillance, logistics, and narrative work within otherwise open social spaces [90]. A recurring mechanism is the use of front charities and “compatriots” structures that present themselves as legal aid or cultural support while channeling money, legal assistance, and messaging to assets embedded in diasporas; the best documented case is Pravfond, which internal emails and financial records tie to convicted spies, propagandists, and points of influence across Europe [91]. This infrastructure operates in parallel with direct pressure on émigré communities by homeland security services, where intimidation and surveillance are conducted abroad through visits, online harassment, and threats to relatives, producing a chilling effect on civic participation and opposition activity in host states.

Diaspora spaces are also used to outsource low-visibility tasks to people who are not trained intelligence officers but who possess the right mix of access and deniability. Czech counterintelligence reports that recruiters have turned to migrants and non-EU nationals contacted over Telegram and paid in small sums or cryptocurrency to carry out acts that range from reconnaissance to sabotage and intimidation, with the explicit goal of eroding trust in government and creating ambient fear within societies [92]. This pattern appears in Poland as well, where analysts have documented outreach to immigrants and economically insecure civilians for espionage and arson tasks that can be compartmentalized and replaced quickly if exposed [93] [94]. The cumulative effect is a distributed, low-signature human network that is hard to map and harder to deter because much of the activity blends into legitimate diaspora life.





Diasporas are also exploited through criminal intermediaries that already move people, cash, and goods across borders. Europol's 2025 threat assessment describes a growing shadow alliance between state actors and organized crime, where criminal logistics are repurposed for political sabotage, espionage, and influence, providing both plausible deniability and resilient supply chains inside the EU [95]. In practice these are cash couriers, forged documents, rented accommodations, and vehicle fleets tied to crime groups but serving hybrid operations that target infrastructure, activists, and diaspora organizations. Because criminal activity is often investigated separately from foreign-interference cases, the same networks can continue to function even when individual operatives are arrested, which preserves the adversary's operational tempo.

Concrete prosecutions show how diaspora cover and outsourced roles converge. In the United Kingdom, Metropolitan Police investigations and court proceedings detailed a Russia-directed spy unit run by Orlin Roussev, who received tasking connected to the Wirecard fugitive Jan Marsalek and coordinated Bulgarian nationals living in Britain to collect sensitive information and support operations under everyday

social and professional guises within migrant communities; Roussev was sentenced to nearly eleven years after pleading guilty, and the case record shows thousands of messages linking diaspora presence to covert tasking [96] [97]. In a separate UK case, a jury convicted three men of arson at an East London warehouse that stored equipment for Ukraine, where the conspirators were recruited and directed over Telegram by a Russia-linked handler and justified their actions within diaspora-adjacent online ecosystems that normalized collaboration as paid gigs rather than espionage. This illustrates how diaspora channels can be leveraged for kinetic outcomes while maintaining distance between the attack and its sponsor [98].

Belarusian services use similar tools against their communities abroad but add coercion that explicitly targets family members who remain in Belarus. Lithuania's annual threat assessment reports that Belarusian intelligence coerces members of the sizeable Belarusian diaspora in Lithuania by threatening relatives at home, then tasks coerced individuals to gather information, infiltrate organizations, or pressure activists, using embassy and consular resources as cover and diaspora events as access points [99]. European parliamentary resolutions also record

transnational intimidation by the Belarusian Investigative Committee and related structures, which seek to extend domestic repression into EU member states by opening cases in absentia and using public lists that stigmatize activists and make them more vulnerable to surveillance and harassment inside diaspora circles [100].

Journalistic and analytical reconstructions of Russia's recent sabotage and diversion surge further clarify the human pipelines that run through diaspora networks. A cross-border investigation found that online recruiters working from Russia or Belarus identified economically precarious migrants inside EU states and laundered tasking through Telegram channels and gig-work forums, which resulted in a string of arsons and reconnaissance assignments executed by people who neither knew nor cared about the strategic aim, only the payment. These narratives were repeatedly corroborated by court files, chat logs, and payment records obtained by reporters and law enforcement [101]. Where prosecutions reach the handler layer, they typically reveal a small set of remote coordinators who move among diaspora-linked chats, nationalist channels, and criminal brokers, shifting identities while keeping the same recruiting scripts and payment methods, which is consistent with a resilient, replaceable labor model rather than the older, officer-heavy agent running of the Cold War era [102] [103].

The strategic effect of exploiting diasporas is cumulative. Community institutions that should serve integration and mutual aid become contested spaces where cultural programming and benevolent legal aid are indistinguishable from covert messaging and asset protection. Individuals who join groups for support find themselves targeted for recruitment or intimidation, which corrodes trust within diaspora communities and between them and host-state authorities. Security services must devote scarce resources

to investigate ambiguous activities that sit at the edge of legality, while adversaries can claim plausible civic intent even as they harvest intelligence and stage low-level sabotage. This is why European security bodies now frame diaspora interference as a priority threat to democratic resilience: it attacks the connective tissue of open societies using the very freedoms those societies extend to newcomers and exiles.

Targeting diaspora communities is a direct inheritance from Soviet intelligence practice, where émigré networks were seen both as threats and as reservoirs of recruitment [104]. The KGB systematically infiltrated exile groups during the Cold War, and today's FSB, SVR, and Belarusian KGB continue this line of effort with updated tools and contexts. The pattern is especially visible in Poland, Lithuania, and Germany, where émigré organizations are closely monitored, infiltrated, and sometimes coerced into collaboration.

Recent cases show that this legacy has been recalibrated toward "disposable spy" recruitment among vulnerable migrant populations. For instance, in 2024, German authorities disrupted networks in which Russian services recruited Latin American migrants to carry out low-cost sabotage, including arson attacks against logistical and commercial targets tied to Ukraine's defense supply chain [105]. In 2025, courts in the UK (...) also convicted individuals tasked by Russian handlers with torching a warehouse linked to aid shipments [106]. These operatives were chosen for their anonymity and expendability, with no expectation of long-term intelligence careers. Meanwhile, in Poland in 2023 a network consisting of 16 individuals was dismantled after being recruited for espionage activities, including monitoring transport infrastructure and installing tracking devices [107] [108].

Tech Advancements in Software

Artificial intelligence and modern algorithmic tools have expanded hybrid warfare from a manual, craft industry into an automated, adaptive system that scales across languages, platforms, and audiences. European threat assessments now document how foreign information manipulation uses AI to industrialize content creation, accelerate targeting, and fuse psychological operations with low-cost technical probes against infrastructure and public services [109]. Research findings by RAND [110] point out that the side that best combines mass, deception, mission command, and network resilience will benefit most from AI, since these technologies reward rapid iteration and flexible C2 systems¹.

Generative media has become the workhorse of influence operations. Investigations of Russia's campaigns since 2022 show routine use of AI image and video generators, voice cloning, and automated translation to fabricate local proof points, seed new rumors at high velocity, and tailor narratives for different linguistic communities, including within the EU [111]. NATO StratCom COE's Virtual Manipulation Briefs track a measurable rise in AI-created assets across ten platforms, with adversaries testing copy, visuals, and messenger personas to capture engagement and to stress fact-checking capacity during crises [112]. RUSI's analysis details how Russian military-adjacent ecosystems have experimented with bespoke chatbots and synthetic spokespersons that imitate authoritative voices in order to anchor fabricated claims, then recycle those claims back into closed-loop channels for apparent corroboration [113].

Automation is not limited to content generation. Campaigns now use full "influence pipelines" where AI agents and scripts create, label, translate, schedule, and A/B-test thousands of assets while botnets route the best-performing variants into audience segments identified by platform

and open-source data signals. A 2025 investigation into Operation Overload, also known as Matryoshka, documented how pro-Russia actors leveraged free, consumer-grade AI tools to drive a content explosion across Telegram, X, and other networks, including deepfake videos with cloned voices, while even spamming fact-checkers to game visibility dynamic [114]. Brookings research on elections explains why this matters for democracies, since algorithmic targeting and synthetic personalization lower the cost of running parallel micro-campaigns that harden polarization and exploit preexisting grievances rather than trying to persuade the undecided [115].

A newer front is model and data poisoning that aims to shape the outputs of AI systems themselves. Reporting and analysis in 2025 describe a Russian-aligned network that saturates the open web with pseudo-journalistic pages and edits auxiliary knowledge bases so that general-purpose chatbots repeat planted falsehoods, a tactic researchers call LLM grooming [116]. The Atlantic Council also highlights coordinated efforts to "poison" AI models by flooding crawler-visible content on topics like bioweapons narratives, which over time biases the response distribution of less-guarded systems [117]. Technical literature underscores the feasibility and impact of such poisoning on model behavior, indicating that even small percentages of tainted data can degrade safety filters and steer outputs toward targeted narratives [118].

AI also tightens the loop between digital operations and activity against physical targets. RAND work on sense-making shows how machine-assisted triage of open-source streams can accelerate the identification of vulnerable assets, crowd behavior, and media event windows, which shortens the planning cycle for hybrid actions that seek attention effects rather

1 C2 (*command and control*) refers to a command structure in which decisions are made centrally, but execution and adaptation take place in a decentralized manner, ensuring flexibility and resilience against disruptions.

**Pro-Russian
bot farm ceased
by Ukrainian
authorities**

Source: Wikimedia



than decisive kinetic results [119] [120]. European security reporting further documents how deepfakes and generative assets are paired with cyber probing or low-cost drone incursions to produce multi-vector pressure that distracts defenders, triggers false alarms, and then exploits the confusion online, especially around Poland and the Baltic region.

Countermeasures are evolving but are uneven and contested. Europe's policy response stresses provenance and transparency, including the C2PA standard for cryptographically attesting content origin and edits, which major platforms and publishers have begun to adopt in news workflows and tooling [121] [122]. Security agencies also point to "content credentials" as a cornerstone of multimedia integrity programs in the generative era [123]. At the same time, analysts warn that provenance alone will not fix attention hijacking or the ability of adversaries to manipulate uncredentialed content and platform recommendation systems, which calls for multi-layer defenses that combine provenance,

model hardening, botnet disruption, and civic resilience [124] [125].

The emerging consensus is that AI does not merely add speed to existing disinformation, it changes the production function of influence. It enables adversaries to scale multilingual assets, autogenerate synthetic personas that converse rather than broadcast, and tune messaging with reinforcement signals gathered in real time, while simultaneously corrupting the knowledge substrate that downstream AI systems consult [126] [127]. For frontline states like Poland and allies on NATO's northeastern flank, the implication is clear. Airspace probes, parcel-borne incendiaries, sabotage and diversionary actions and cyber intrusions are now synchronized with algorithmic campaigns and model-level tampering that collectively impose attention costs, exploit institutional friction, and erode trust at scale. Effective defense requires treating AI-enabled manipulation not as a media problem, but as an operational threat that links the informational, cyber, and physical domains in a single concept of operations.

Tech Advancements in Hardware

Russian and Belarusian services have retooled their hybrid operations with a rotating toolkit of unmanned systems, improvised munitions, and digital coordination channels that privilege deniability and scale. The emphasis is not on a single breakthrough technology but on iterative, low-cost innovations that pressure European defenses from multiple directions at once, especially along the Poland–Baltics frontier where airspace, rail, and logistics nodes are most exposed. Recent incidents show a pattern of using reconnaissance and kamikaze-style drones to probe response times, stress air defenses, and generate attention effects that amplify parallel information operations, while cyber probing and app-mediated tasking create a seamless bridge between the physical and cognitive theaters [128].

A clear marker of this evolution is the appearance of Russian “Gerbera” drones over NATO territory, including the July 10, 2025 incursion that crossed from Belarus into Lithuania and crashed about one kilometer inside the border. Lithuanian authorities described the aircraft as a wooden copy of an Iranian Shahed, optimized for low cost and deception against radar, and later confirmed that a similar platform found at the Gaižiūnai training area carried an explosive device that required disposal by specialists. The incidents prompted Vilnius to press for additional anti-drone assets from NATO and to accelerate national counter-UAS plans [129] [130] [131]. Within weeks, officials again reported a likely crossing from Belarus, underscoring the intent to normalize pressure on NATO airspace and to test allied coordination in a gray zone that stops short of kinetic escalation [132].

This airborne pressure coincides with an industrial push inside Belarus to scale unmanned production close to NATO borders. In March 2025, Belarusian and Russian officials floated plans for a drone plant inside Belarus capable of high-volume output, a proposal echoed in subsequent media and expert reporting that tracked

site activity in Minsk and framed the initiative as part of a broader bid to relocate sensitive manufacturing under Belarusian cover. Public statements in Minsk about creating dedicated “drone troops” as an independent service branch reinforced the institutionalization of this capability and its integration into reconnaissance, strike, and targeting functions across the Belarusian force structure [133] [134] [135]. Analysts have warned that even “civilian” lines can be dual-used, a point highlighted by reporting that the project would initially focus on agricultural UAVs while preserving pathways to military adaptation in a wartime economy [136].

On the Polish side, authorities have confronted a blend of air and cyber probes that illustrate how technological innovation serves cumulative disruption. After a cluster of 2024 alerts about possible drone incursions during Russian strikes on Ukraine, Poland activated searches and air defense posture, later walking back one widely reported case following forensic review. The episode nevertheless exposed the burden of rapid-reaction cycles in a contested air picture and the difficulty of discriminating genuine intrusions from sensor anomalies in real time, especially when adversaries exploit that ambiguity for narrative effect [137] [138]. In parallel, Poland reports sustained cyber pressure against essential services, including a foiled attempt to compromise a major city’s water system that officials attributed to the broader campaign targeting Poland’s role as a logistics hub for Ukraine. The incident illustrates how cyber and unmanned probing operate as a single operational continuum that seeks both access and attention, forcing defenders to invest heavily in resilience while dealing with persistent uncertainty in attribution and intent [139].

In this environment, technological innovation (...) is deliberately incremental. Cheap GPS trackers and consumer electronics can be repurposed as timing or triggering modules for incendiary devices routed through courier systems, while



low-cost drones built from commercial components can be configured for reconnaissance, payload delivery, or symbolic fly-bys that generate exaggerated public anxiety. European casework in early 2025 documented parcels disguised as consumer goods that contained homemade incendiaries and timer assemblies derived from off-the-shelf trackers, delivered to distribution centers to probe screening and disrupt operations while staying within a cost envelope that encourages repetition. The same logic informs the choice of wooden or composite airframes for drones like the Gerbera, which complicate conventional radar discrimination and allow adversaries to “spend down” the defender’s attention budget at minimal expense [140] [141].

Regional defense responses are starting to adapt around this technological churn. Lithuania has asked for allied counter-UAS reinforcements and launched public drone training and education programs to build a civilian reserve of operators and spotters, a step that acknowledges how a society-wide sensor network can compress response times and complicate adversary planning. Authorities describe a phased rollout of training centers, curricula for both adults and students, and integration with national civil

defense plans to raise the floor of competence across the population [142]. Poland, for its part, has accelerated work on airspace hardening and drone force structure while public messaging emphasizes the frequency of Russian cyberattacks and the need for fused civil-military defenses, a framing consistent with the hybrid nature of the threat and the cost-imposition logic behind it [143].

Taken together, these developments show that technological innovation in the current hybrid campaign is less about headline systems and more about the adversary’s willingness to iterate. Low-cost drones that blur reconnaissance and psychological signaling, parcel-routed incendiaries that test supply chains, and persistent cyber probing of essential services all function as interlocking lines of effort. They compel European governments to spend money and political capital on protections that are hard to see and harder to measure, while the initiator preserves deniability and freedom to escalate or pause at will. The strategic effect flows from attrition in attention and resources, not from any single strike, which is made possible by a procurement and innovation cycle that treats consumer technology as a ready-made arsenal [144] [145] [146].

Time: the Five Phases in Narrative and Operational Cycles

These five operational typologies are not isolated acts but integrated nodes within a larger hybrid campaign calibrated for cumulative destabilization across multiple domains. Fragmentation ensures that each incident, though minor and plausible on its own, contributes to a broader atmosphere of perceptual chaos. Masking obscures attribution by cloaking operations in the guise of criminal or local activity, providing plausible deniability.

Timing aligns events with political debates, NATO troop movements, or symbolic anniversaries, maximizing psychological impact. Narrative coupling amplifies every physical disruption through synchronized information operations, multiplying confusion and deepening public distrust. When sequenced, these modalities create feedback loops: an incident triggers an information campaign, the official response becomes a media spectacle, and trust erodes incrementally, producing degradation without the escalation of open conflict.

The operation types described above are structured in phased sequences that stretch over weeks or months. The rhythm appears random but follows an orchestrated cognitive logic:

Phase one initiates narrative priming. This may include planting rumors, memes, leaks, or framing events through micro-influencers. The content often revolves around NATO “provocations,” Western hypocrisy, or institutional incompetence.

Phase two introduces kinetic markers. These are often minor sabotage actions such as warehouse fires, drone incursions, or disruptions in railway logistics. The intent is not mass destruction but psychological intrusion and ambiguity.

Phase three links the incident to the narrative frame. This is done through diasporic diffusion, sabotage and diversion, automated resharing, and targeted rumors. Emotional narratives are seeded and looped to create interpretive stickiness. The same fire becomes evidence of NATO escalation, state failure, or elite indifference, depending on the audience.

Phase four exploits institutional reaction. Any contradictions in communication, inconsistencies in attribution, or slow public response are interpreted as proof of deception or impotence. This is where cognitive terrain becomes most vulnerable.

Phase five resets the loop. A new micro-incident or message is launched, building on the erosion achieved previously. As this cycle repeats, it creates a sustained cognitive environment of suspicion, exhaustion, and perceptual overload.

Through repetition, these five phases sustain an environment of suspicion, exhaustion, and perceptual overload, gradually weakening societal cohesion even in the absence of large-scale attacks.

5

Western Blind Spots, Adaptive Failures and How to Fix Them

Despite years of exposure to Russian and Belarusian hybrid campaigns, the West continues to operate with critical structural and cognitive deficits. These blind spots are not merely technical oversights. They are systemic, institutional,

and conceptual, rooted in outdated threat models and fragmented governance frameworks. This chapter identifies four main fault lines: the cognitive deficit, the system gap, the interoperability vacuum, and the regulatory void.



Cognitive Deficit: The Absence of Integrated Threat Comprehension

A significant weakness demonstrated by Western states lies in the inability to conceptually integrate subperceptual and hybrid threats into national security frameworks. Western institutions often treat sabotage, disinformation, espionage, and symbolic coercion as discrete phenomena rather than as expressions of a coherent strategic architecture.

Counterintelligence services continue to prioritize kinetic and technical threats over long-term perception management. This is particularly visible in the handling of Russian information operations, which are still often dismissed as “mere propaganda” or treated as isolated election interference, rather than as cognitive preparation for broader destabilization. The lack of a shared cognitive map across institutions impedes the ability to recognize patterns in narrative diffusion, cross-border mimicry, and psychological disruption [147]. Similarly, the lack of horizontal state strategy to counter disinformation and the tolerance shown to political micro-targeting leave the state vulnerable to manipulation that undermines social cohesion and information security.

Moreover, few governments have institutionalized anticipatory monitoring of narrative environments. Open-source intelligence (OSINT) capabilities are underdeveloped, and the analyst profiles needed for long-term perception analysis remain rare in national security bureaucracies. Russia and Belarus exploit this lag by shaping discourse long before crises formally emerge [148].

Recommendation:

- *National governments should establish permanent special service units for hybrid threats as integrated centers combining military counterintelligence, cyber defense, counterintelligence, and strategic communication. In the case of Poland, the most appropriate location would be the Government Security Center or the Chancellery of the Prime Minister to ensure cross-ministerial coordination.*
- *These cells should detect and analyze sub-threshold aggression by fusing multiple information streams, including social media patterns preceding disinformation campaigns, anomalies indicating cyber intrusions, and signs of proxy sabotage against critical infrastructure.*
- *Within NATO, the focus should be on identifying “left of launch” indicators to provide early warning before hybrid operations materialize.*
- *In the EU, national units should be networked and coordinated through the Hybrid Fusion Cell, the Union’s focal point for hybrid threat analysis.*
- *Governments must resource these cells with advanced analytic training and AI-assisted tools to enhance detection and pattern recognition across domains.*
- *Continuous cross-border sharing of insights should be institutionalized to accelerate attribution, reduce the ambiguity exploited by adversaries, and enable timely, coordinated responses.*

Systemic Gap: Fragmentation of Counterintelligence, Cyber, and Domestic Policy

Russian and Belarusian operations seamlessly cross administrative boundaries. A single campaign may involve recruiting diaspora actors, deploying bots on Telegram, penetrating local media, and manipulating protests. Meanwhile, Western responses are divided among ministries, agencies, and mandates, with little horizontal integration or real-time coordination. The result is operational slippage. Intelligence collected by national services rarely reaches local authorities in time. Cyber command centers are often disconnected from the socio-political context and unable to assess the narrative impact of breaches. In Poland, NASK combines these two spheres. Such segmentation creates an exploitable gap between detection and response.

Recommendations:

- *Governments must integrate all relevant actors into a unified defensive framework to close systemic gaps in countering hybrid threats.*
- *At the national level, states should establish interagency coordination centers that bring together counterintelligence, cyber defense, strategic communications, and policy officials to assess threats and coordinate responses.*
- *Models from the UK and Baltic states (especially Estonia's) demonstrate effective approaches and should be shared across NATO and EU forums.*
- *At the EU level, the 2025 Internal Security Strategy's call for a "true European concert" should be operationalized through a standing Hybrid Threats Coordination Council linking security, home affairs, and foreign policy institutions.*
- *NATO should complement this effort by promoting comprehensive resilience frameworks that integrate civil, military, and informational defenses.*
- *Proposals such as President Sauli Niinistö's call for an EU-level intelligence cooperation service and an "anti-sabotage" network highlight the need for cross-border structures to close institutional seams.*
- *Allies should conduct joint exercises with counter-hybrid scenarios that require cyber forces, special services, police, and policy officials to collaborate in the security domain real time.*

Fusing these efforts should allow NATO and EU members to form a unified counter-force able to detect and disrupt hybrid operations quickly, strengthening resilience and reinforcing deterrence.



NATO Cyber Defence Pledge Conference at The Hague, Netherlands on 17 May 2024

Source: Wikimedia

Interoperability Deficit: Data Silos Between Member State Services

Among EU and NATO states, data and intelligence and counterintelligence (or otherwise coming from special services) related to hybrid threats remain unevenly shared or not shared at all. The problem is not only technical, but also legal, political, and cultural.

Security services remain bound by national mandates and are hesitant to share ongoing investigations, especially in politically sensitive domains such as disinformation or domestic radicalization. Moreover, differing definitions of what constitutes a hybrid threat lead to incompatible classification systems. A sabotage or diversion incident labeled terrorism in one country may be treated as petty crime in another. This misalignment creates blind spots across borders that adversaries can traverse with ease.

Joint situational awareness platforms exist, such as the EU Hybrid Fusion Cell or NATO's Hybrid Threats Division, but they lack both enforcement authority and deep analytical capacity. Their outputs are often limited to threat bulletins rather than operational integration. This fosters reactive posture and inhibits preemptive counter-hybrid capabilities.

Recommendations:

- *NATO, the EU, and member states must prioritize secure and proactive intelligence-sharing to repair current interoperability gaps.*
- *Practical fixes, including routing intelligence through the NATO Office of Security as a neutral conduit, can ensure data reaches all stakeholders without requiring full treaties.*

- *NATO should fully implement its data-centric strategy by treating shared data as a strategic asset, developing interoperable classified networks, and adopting common tagging standards.*
- *National agencies should adopt a “dare to share” culture by strengthening bilateral and multilateral exchanges, conducting joint operations, and seconding officers to partner services. At the same time, it is necessary to develop mechanisms addressing the costs of their maintenance, the protection of state secrecy, and the building of trust, which is particularly important despite the fact that joint operations with partners are already being conducted.*
- *Frameworks such as the G7 Rapid Response Mechanism and NATO's Counter Hybrid Support Teams should be made permanent and expanded.*
- *NATO and EU member states should develop mechanisms for the secure exchange of data on hybrid threats that will not replace in-person meetings, but will allow for the rapid sharing of technical alerts. This can be supported by post-quantum cryptographic algorithms, elements of quantum cryptography for key channels, distributed authentication systems, and AI-based early warning networks.*

Institutionalizing this culture of intelligence exchange will close exploitable seams, enable faster attribution and response, and strengthen deterrence by ensuring hostile operations are collectively exposed.

Regulatory Void: Absence of Effective Legal Instruments to Address Foreign Influence

Unlike the United States, which possesses legal tools like the Foreign Agents Registration Act (FARA), most European countries lack institutional mechanisms to track, regulate, or expose foreign influence operations.

Russian and Belarusian actors exploit this legal absence by embedding influence structures into think tanks, church networks, cultural institutions, and pseudo-media. These nodes function as multipliers of disinformation and conduits for soft coercion but remain legally protected as civil society actors. Western democracies often hesitate to impose disclosure or transparency requirements for fear of infringing on freedom of speech or association [149].

The result is a paradox. Liberal norms become shields for illiberal intervention. States are paralyzed not by direct threat, but by the friction between their legal openness and the strategic opacity of the opponent. Even when malign influence is suspected, the absence of legal categories to classify or prosecute it results in procedural inertia.

Recommendations:

Addressing this vacuum requires decisive legislative and policy measures that expose and counter foreign influence networks without undermining democratic freedoms.

- *NATO and EU leaders should recognize transparency in foreign political activities as a core security requirement, not an optional measure.*
- *Member states should enact or strengthen foreign influence registration laws, modeled on FARA in the US and the UK's Foreign Influence Registration Scheme.*

- *Such laws must require individuals or entities acting on behalf of foreign governments to register activities including lobbying, media operations, NGO funding, and other influence efforts.*
- *Non-compliance should trigger significant penalties, including fines and potential criminal liability.*
- *The EU should accelerate development of its foreign influence transparency mechanism, ensuring national and EU registries complement each other rather than create fragmentation.*
- *NATO and the EU should establish a joint legal task force to align best practices and close loopholes exploited by hostile actors.*
- *Enforcement must be backed by well-resourced investigative units empowered to demand disclosure and sanction covert influence, including deceptive media outlets or organizations linked to foreign intelligence.*
- *Laws must be adaptable, with regular updates to cover emerging tactics such as AI-driven disinformation, covert influencer financing, and deepfakes.*
- *Transparency requirements should be coupled with systematic analysis, with NATO and EU centers of excellence processing registry data to identify malign campaigns.*
- *When appropriate, malign influence operations should be publicly exposed, transforming transparency into a tool of deterrence.*

Building enforceable FARA-style registries, coordinating internationally, and adapting to technological change can allow allies to strip away the anonymity Moscow and Minsk rely on, reinforcing democratic resilience and protecting open societies from hostile infiltration.

Turning the Tables: Lawful Hybrid Action Against Russia and Belarus

Western responses have been overwhelmingly reactive. Yet the West holds vast underused resources that can impose sustained cognitive, legal, financial, and operational friction on Russian intelligence ecosystems without mirroring illicit tactics or targeting civilians. These resources include, among others, the unparalleled financial intelligence capabilities of banks and payment networks, which make it possible to identify financial links, track suspicious fund flows, and block money laundering mechanisms that support intelligence operations. Also important are export controls in semiconductor and machine tool supply chains, maritime leverage through insurance and port state control, as well as investigative journalism consortia and OSINT communities. The latter cannot be formally tasked by states with covert activities, but they can be supported through funding, data access, and information-sharing mechanisms, which enhances their effectiveness and complementarity with institutional efforts.

Another resource is access to digital platforms through binding transparency regimes and trusted flagger programs, diaspora networks, and anti-regime Russians and Belarusians in exile, as well as the use of universal jurisdiction, meaning the ability to prosecute perpetrators of the most serious crimes regardless of the place of commission or the perpetrator's nationality. Additional tools include sanctions modeled on the Magnitsky Act², law enforcement cyber capabilities enabling the takeover of infrastructure and blocking of domains – already practiced in joint Polish-Czech and U. S. operations – as well as satellite data and the AIS system used for real-time attribution. These are further reinforced by the convening power of NATO, the EU, and the G7 in synchronizing exposure and sanctions.

When employed coherently, these tools enable an offensive grounded in truth that disrupts the logistics of Russia's covert operations, raises the costs of tasks outsourced to proxies, and weakens regime control over narratives both domestically and abroad, while remaining consistent with international and domestic law.

Recommendations:

- *NATO, the EU, and member states should stand up an Offensive Transparency and Disruption Initiative that fuses financial intelligence units, export control authorities, maritime regulators, cyber law enforcement, and open source investigators to map and publicly expose Russian proxy networks, front companies, logistics routes, and disinformation supply chains on a rolling basis.*
- *Create a joint sanctions and lawfare cell to convert each exposure into coordinated actions, including Magnitsky designations, asset freezes, export denial listings, civil forfeiture, and litigation against facilitators.*
- *Use port state control, classification societies, and insurance leverage to interdict the shadow fleet and deny services to vessels and operators tied to sanctions evasion.*
- *At national level, task dedicated cyber disruption teams, under legal authorities and judicial oversight, to seize botnets, deplatform impersonation clusters, and sinkhole domains that enable hostile influence.*
- *Expand support for independent Russian language media, circumvention tools, and safe digital channels for whistleblowers to power a truth offensive aimed at corruption, casualty*

2 Magnitsky sanctions lists are compilations of individuals and entities subject to travel bans and asset freezes under Magnitsky laws, which allow perpetrators of serious human rights violations and corruption to be punished regardless of where the crimes were committed. Such mechanisms have been implemented by the United States, Canada, the United Kingdom, the European Union, and the Baltic states. The name comes from Sergei Magnitsky, a Russian lawyer who exposed a major corruption scandal in Russia and died in 2009 in a Moscow detention center as a result of torture.

concealment, and elite privilege, coordinated with diaspora partners and exile organizations.

- *Require large platforms to implement verifiable provenance and transparency APIs that allow trusted researchers and regulators to track cross platform narrative laundering, with rapid takedown pathways for coordinated inauthentic behavior.*
- *Build an Allied Procurement Shield that tags high risk components and machine tools, embeds end use verification, and prosecutes diversion through transshipment hubs.*
- *Institutionalize an Allies for Exposure forum across NATO, the EU, and the G7 that announces monthly joint attributions, coordinated penalties, and case studies of disrupted*

operations to impose reputational and operational costs.

- *Finally, create vetted channels for responsible collaboration with anti-regime Russians and Belarusians in the West, focusing on witness testimony, document leads, and civic outreach that delegitimizes the security services while safeguarding participants.*

Taken together, these measures can shift the initiative, forcing Russia to defend its networks under continuous legal and informational pressure, increasing the cost of subthreshold aggression and strengthening deterrence without abandoning democratic principles.

Poland: National Constraints and the Need for Institutional Paradigm Shift

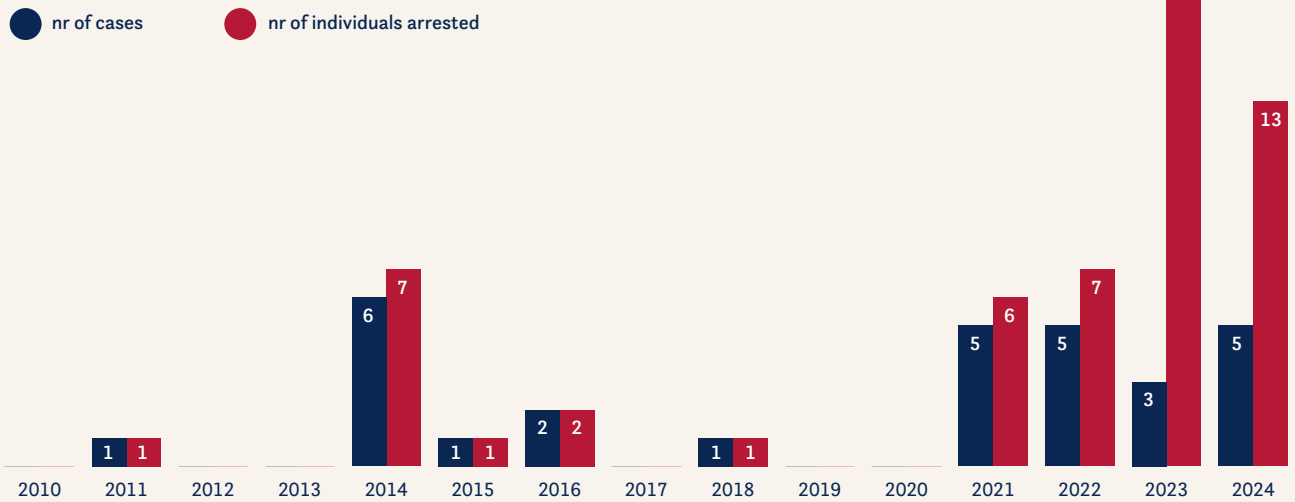
Poland's intelligence and security system continues to operate on inherited logic designed for the Cold War era rather than the realities of twenty-first-century hybrid conflict. The architecture is defined by silos, with counterintelligence, cyber defense, law enforcement, and crisis management each working within narrow mandates that prevent rapid, integrated action. Adversaries exploit this fragmentation through low-cost, tokenized operatives, disposable espionage cells, and narrative saturation techniques that can overwhelm reactive bureaucracies. Instead of anticipatory defense, the system privileges collection and procedure, which means hostile operations are often understood only after they have already produced effects in the cognitive or infrastructural domain. The result is a structural lag: Russia and Belarus iterate operations faster than Poland's institutions can process, investigate, and respond.

In this context, the government's proposal to reform the Internal Security Agency and the Foreign Intelligence Agency introduces additional procedural oversight by expanding judicial control over operational methods and access to intelligence materials [150]. Although these steps are intended to increase transparency, which is one of the reasons for many delays and the lack of dynamism in the work of intelligence services, they "leave the deeper deficits of flexibility, integration, and anticipatory capacity. The draft law proposes to improve these processes, but it does not alter the fundamental inertia of structures inherited from the Cold War, risking the paradox of reinforcing a system that adversaries have already learned to circumvent. However, positive signals should also be noted: the 2025 detention of a Belarusian citizen suspected of a sabotage activity in Poland, and simultaneous expulsion of a Belarusian diplomat indicate stronger regional counterintelligence cooperation also covering the Czech Republic, Hungary, Romania and Moldova [151].

An important but interrupted source of insight into Russian and Belarusian influence operations was the work of the **Parliamentary Commission on Russian and Belarusian Influence (2004–2024)**. The commission collected and analyzed nearly 17,000 pages of documents and prepared case studies on disinformation campaigns, electoral interference, and migration-driven destabilization at the Polish–Belarusian border [152] [153]. As noted by Professor Irena Lipowicz, its findings could have served as a valuable foundation for systemic reform and a more integrated approach to countering cognitive warfare [154]. Yet the commission was dissolved before its full materials were released, interrupting the process of institutional knowledge consolidation and preventing the utilization of its collected evidence for policy and operational change.

It is also worth highlighting the activities of NASK, which fill the gap left by the discontinued work of the Parliamentary Commission. In its reports, the institute systematically documents disinformation and cyber operations. The 2023 CERT Polska report points to a sharp increase in incidents, including a wave of DDoS attacks linked to elections in Poland, as well as the activity of Russia-related APT groups that interfered with infrastructure and political campaigns [155]. In addition, NASK analyses from 2023 document destabilizing narrative campaigns on the Polish–Belarusian border, combining migration disinformation with actions in cyberspace [156]. These materials today represent one of the most comprehensive publicly available sources of knowledge on the tools of cognitive warfare targeting Poland and its surroundings. Meanwhile, NASK's 2024 Global Election Disinformation Report (*Dezinformacja w wyborach na świecie*) shows how Russia and China adapt narratives to local contexts, in Mexico through deepfakes, in Taiwan through systematic campaigns by Beijing, and in the United States by reinforcing social polarization [157].

Russian espionage and sabotage arrests in Poland, 2018–2025



Source: Polish Internal Security Agency (ABW)

Recommendations:

- *Build a Cognitive Early-Warning Program housed in the National Media Council and integrated with CERT-PL. This program would fuse open source intelligence, real-time platform telemetry (via mandatory API access for large platforms), and forensic media analysis. Narrative spikes on themes such as refugee inflows or alleged security failures would trigger pre-defined protective protocols: e.g. heightened monitoring of railway yards, reinforcement of police presence at logistics nodes, or activation of counter-narratives through trusted local media.*
- *Stand up sector task forces for logistics corridors (ports, rail junctions, cross-border hubs) and telecommunications backbones. Each task force would pair infrastructure operators with ABW, Police, and CERT-PL, meeting monthly for red-team simulations of hostile methods: Telegram recruitment of couriers, incendiary devices disguised as parcels, low-signature drone attacks. Findings would feed directly into sector-specific defensive playbooks.*
- *Construction of a low-cost anti-drone defense layer which includes acoustic sensors, mobile interceptors and jamming systems should become a modernization priority for Central Europe in order to mitigate the cost asymmetry relative to Russian attacks.*
- *Mandate joint training and quarterly cross-agency exercises supervised by the Government Centre for Security. These exercises would rehearse pre-activation disruption of hostile cells, evidentiary handoffs between ABW and prosecutors, and coordinated public messaging to avoid adversary exploitation of institutional missteps.*
- *Equip agencies with AI-assisted detection and case correlation platforms developed through NASK and trusted vendors. All special services would be required to adopt common TTPs (tactics, techniques, procedures) for parcel screening, drone interdiction, and rapid takedown of enabling infrastructure such as burner accounts and illicit procurement chains.*
- *Align legal reform with operational mandates by pairing new oversight provisions with enforceable fusion obligations and accountability metrics. Independent parliamentary oversight would coexist with binding requirements for anticipatory defense and transparent reporting on disruption effectiveness, ensuring legality does not come at the expense of agility.*

Taken together, these measures convert procedural refinement into operational transformation, closing the structural gaps that recent Polish cases have exposed and raising the cost of hybrid campaigns before they activate.

6

Conclusion

The evidence across domains makes it clear that Russia and its proxies are waging a decades long strategy of subthreshold warfare designed to corrode cohesion, exploit seams, and exhaust allied resilience. Sabotage, diversion, espionage, disinformation, and legal manipulation form a coordinated offensive that thrives on Western hesitation. Russia seeks parity by subtraction, not by modernization, and will therefore continue to export entropy until democracies harden cognition and coordination. In contrast, the West remains bound by short electoral cycles, too often resetting priorities while Moscow sustains pressure without pause. There is a stark imbalance between Russia and its proxies' intensive, well-resourced efforts to understand and influence the West and the West's limited, overly academic, and sluggish approach to studying Russia [158]. This asymmetry defines the battlefield.

The West, however, remains bound by short electoral cycles, too often resetting priorities or failing to maintain consistent, long-term action and cross-party consensus, while Moscow sustains constant pressure due to the continuity and permanence of its power and priorities.

This asymmetry defines the battlefield. It cannot abandon the rule of law, which is the foundation of its legitimacy and strength. Yet clinging to legal and procedural comfort while adversaries operate in the shadows means surrendering the initiative. The pressure of civil rights and freedom of speech, cardinal for the perception of Western strength and values, also plays a significant role in this regard. NATO, the EU, and national governments already possess unrivaled resources in financial intelligence, legal powers, cyber capabilities, and narrative reach. What is lacking is only the determination to integrate them into a lasting strategy that treats hybrid threats as a continuum of warfare rather than isolated incidents.

The stakes could not be higher. Either Europe and its allies act decisively, uniting intelligence, law, and operational power into a seamless defense and offense, or Russia will continue to erode trust and cohesion from within. The war is already underway. The choice is to remain locked in reactive cycles or to demonstrate that liberal democracy, rooted in the rule of law, can fight and prevail against authoritarian hybrid warfare.

Review 1 and Commentary:

Dr. Anna Grabowska-Siwiec

The report by Maciej Filip Bukowski, prepared for the Pułaski Foundation, addresses the issue of contemporary hybrid threats originated by the Russian Federation and the Republic of Belarus. The document represents an attempt at a comprehensive account of phenomena situated within the spectrum of hybrid warfare, with particular emphasis on the implications for the security of NATO and EU member states.

The report addresses matters of fundamental importance for contemporary international security studies. The problem of hybrid threats, particularly in the context of Russian-Belarusian influence operations, constitutes one of the key areas of analysis in the field of national security of Western states. The author rightly identifies a research gap in the systematic study of phenomena that remain below the threshold of open armed conflict.

Of particular scientific value is the conceptualisation of a “calibrated offensive posture” as a response to hybrid activities. This proposal goes beyond the traditional reactive approach to security threats and advocates a proactive counter-strategy, which represents a significant contribution to the development of security theory.

The report makes a meaningful contribution to the academic discourse through its analysis of the transformation brought about by artificial intelligence in the field of information operations. The thesis on the shift of disinformation activities from “artisanal work to an automated process” is a highly accurate observation that merits further scholarly exploration. This finding has major implications for both the theory and practice of information security, pointing to the need for a redefinition of existing approaches to countering disinformation.

The author introduces a valuable concept of “feedback loops,” whereby “an incident triggers an information campaign, the official response becomes a media spectacle, and trust erodes

step by step.” This mechanism offers a systematic analysis of the processes through which seemingly isolated events become instruments of erosion of social trust and institutional cohesion.

The report presents an important observation concerning the nature of contemporary hybrid threats. The author rightly identifies that the effectiveness of these activities does not derive from the scale of individual attacks but rather from their repetitiveness and capacity to “sustain an atmosphere of suspicion, fatigue, and perceptual overload.” This observation represents a significant contribution to the theoretical understanding of the mechanisms of hybrid warfare.

Particularly valuable is the identification of the problem of a lack of analytical integration between criminal activities and the intelligence operations of foreign states. The author correctly points out that delays in recognising these linkages “allow the adversary to maintain operational momentum,” which constitutes a serious gap in security systems.

The document provides an important contribution to the understanding of the challenges faced by contemporary counterintelligence services. The analysis of structural and procedural limitations in the face of evolving hybrid threats is of great value to the practice of national security.

The report formulates ambitious, though not always easily achievable, postulates concerning the “institutionalisation of a culture of intelligence and counterintelligence information exchange.” These proposals, while discussed in various international fora, have yet to be fully implemented, which underscores their practical relevance.

A key value of the report lies in its potential contribution to strengthening societal resilience against hybrid activities. Through its systematic

analysis of the mechanisms and methods employed by Russian and Belarusian intelligence services, the document may help raise public awareness regarding the nature and scale of contemporary threats.

The document fills an important gap in the Polish academic discourse on security by offering a systematic analysis of phenomena previously described only in a fragmented manner in the literature. Particularly noteworthy is the interdisciplinary character of the analysis, which combines perspectives from security studies, social psychology, communication sciences, and computer science. Such an approach enables a holistic understanding of hybrid warfare as a multidimensional phenomenon requiring comprehensive responses at both national and international levels.

Commentary by Dr. Anna Grabowska-Siwiec on the Report *Agents of Chaos: The Shadow Campaign Against the West Cognitive Warfare and Covert Action by Russian and Belarusian Intelligence Services* (*Agenci chaosu: ukryta kampania przeciwko Zachodowi*)

Contemporary intelligence threats are marked by a significant shift in the operational field from the traditionally understood domain of secrecy to the socially accessible and perceptually visible sphere. This transformation does not represent an incidental evolution but rather a deliberate operational strategy aimed at maximising psychological impact while preserving credible state-level deniability. Ukraine's territory was used as a testing ground for institutionalised hybrid operations. The mechanisms developed in the process of destabilising Ukraine were subsequently adapted and directed against Western states after their unequivocal opposition to Russian aggression. This progression demonstrates the systematic nature of hybrid doctrine's development.

The use of overt or only loosely camouflaged actions does not signify an operational deficit of intelligence services but rather a deliberate method of achieving psychosocial effects. This strategy aims to generate: perceptual chaos – disruption of society's ability to rationally assess threats; a climate of fear – the systematic heightening of social anxiety and the sense of being besieged through the impression of the omnipresence of Russian and Belarusian

intelligence threats; and institutional distrust – the systematic undermining of the credibility of state structures.

The long-term intentionality of the described activities is focused on: weakening social cohesion; discrediting democratic values – undermining the legitimacy of democratic systems; and ultimately reshaping the political configuration – bringing to power parties favourable to Russian policy. This sequence of objectives points to the systemic nature of hybrid operations generated by Russia, extending beyond short-term tactical gains.

Given that intelligence aggression is detected and neutralised by counterintelligence services, the key modernisation postulates should concentrate on this segment of the state's security apparatus. This requires strengthening the resources of counterintelligence services, providing solid legal foundations for their operational powers, and ensuring integration with independent analytical centres to enhance expert capacity. It is equally necessary to clearly distinguish between the activities of intelligence and counterintelligence services. The definitional conflation of competencies and tools of both types of services creates both informational chaos and a negative public image of domestic agencies, which directly undermines their effectiveness. Counterintelligence services are embedded in the legal order of the state, as they operate within its territory. Their competencies and operational tools must be grounded in law and must instil in society a sense of the effectiveness and importance of counterintelligence for collective security.

The transnational character of hybrid and disinformation activities also implies the need for the development of international cooperation mechanisms. However, the effectiveness of cooperation between intelligence services encounters significant systemic constraints, such as the handling of highly classified data, limited trust even among allied partners, and the risk of revealing operational methods and sources. Any proposed changes in this regard must take these limitations into account.

In many states, including Poland, intelligence services are subject to political fluctuations and pressures, transforming them into instruments for strengthening ruling parties. This

instrumentalisation weakens their operational capacities and international credibility. The structural weaknesses of intelligence agencies include underfunding (budgets inadequate to the scale of challenges), lack of qualified personnel, limited cooperation with the private and academic sectors, and lack of access to cutting-edge technological solutions. These systemic shortcomings curtail the capacity to respond effectively to complex threats, particularly in cyberspace. To effectively counter hybrid threats, the starting point must be the resolution of these internal problems of the intelligence services.

An essential element of counterintelligence effectiveness lies in the development of communication channels between the services and society. Without public support, the services cannot effectively carry out their protective functions.

The discourse on strengthening the competencies of intelligence services is inevitably linked

to the potential restriction of civil rights and freedoms. Striking the optimal balance between the effectiveness of protection against hostile intelligence activities and the preservation of the fundamental liberties characteristic of democratic societies is extraordinarily difficult. Democratic societies therefore face the paradox of having to restrict their own freedoms in order to protect themselves from external threats, as those very freedoms are exploited by hostile intelligence services as vectors of attack.

We are currently witnessing a fundamental transformation in the nature of intelligence threats, which requires an appropriate adaptation of the defensive systems of democratic states. The key challenge lies in developing effective response mechanisms that will not compromise fundamental democratic values while at the same time ensuring robust protection against hybrid activities.

Review 2: Grzegorz Małecki

The report vividly and convincingly presents the dynamically escalating phenomenon of broadly defined aggressive operations within the so-called hybrid warfare, conducted in recent years by Russian and Belarusian intelligence services on the territory of Poland as well as other European Union and NATO countries. It contains an exhaustive description of their objectives and methodological foundations, along with a meticulous catalogue of the mechanisms and instruments employed by the Russian and Belarusian intelligence services in their undeclared war against the West. This evocative account enables the reader to grasp the origins and essence of the phenomena we have witnessed in recent years, whose purpose is the destruction of the sense of security among Western societies and the provocation of internal conflicts that diminish their capacity to defend themselves against external threats.

An important added value of the report lies in its skillful combination of a concise theoretical description with a wide array of the most current, striking examples of such operations across the entire European continent (not only in Poland), many of which are completely unknown in Poland. The picture that emerges from this compilation reveals a disturbing scale of threats of an existential nature for the security of Poland and Europe. Their societies are often unaware of this danger, deprived of the comprehensive overview presented in the report. Only by placing individual events, which are the result of hostile intelligence activities, within a broader framework of hybrid operations does their destructive potential become visible, allowing for a proper understanding of the scale of the peril we are facing.

This troubling picture naturally raises questions about the capacity of the state apparatus and the Euro-Atlantic community to neutralise these threats and defend against them. With cold precision, the report depicts the grim reality that Poland, the EU, and NATO are clearly on the defensive in this field, while Russia and Belarus are dynamically expanding their offensive without facing an adequate response. The reaction remains largely passive, focused on minimising the effects and prosecuting the physical perpetrators of sabotage and diversion, rather than pre-emptively neutralising these activities along with their instigators and command structures. The report aptly highlights the negligence, errors, and systemic deficits of Western countries, including Poland, in combating the hybrid aggression of Russia and Belarus, emphasising in particular the anachronistic attachment to outdated operational patterns of the distant past that characterise most European intelligence services.

The greatest strength of the report, however, lies in its highly accurate recommendations, which point to specific measures that would enable the West to effectively repel attacks from Russia and Belarus and move into an offensive posture in hybrid warfare. Fully agreeing with these proposals, I would place particular emphasis on the recommendation to undertake active counter-offensive operations that would shift the operational field onto the adversary's territory. Without launching aggressive offensive operations by European intelligence services acting in unison, there is no chance of effectively neutralising the intelligence apparatus of Russia and Belarus.

Endnotes

- [1] Wither, J. (2020). *Outsourcing warfare: Proxy forces in contemporary armed conflicts*. Security and Defence Quarterly, 31(4), 17–34. <https://doi.org/10.35467/sdq/127928>
- [2] Kozera, C., Bernat, P., Güler, C., Popławski, B., & Sözer, M. (2020). *Game of Proxies – Towards a new model of warfare: Experiences from the CAR, Libya, Mali, Syria, and Ukraine*. Security and Defence Quarterly, 31(4), 77–97. <https://doi.org/10.35467/sdq/131787>
- [3] Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies. http://www.potomac institute.org/images/stories/publications/potomac_hybridwar_0108.pdf
- [4] Bilal, A. (2021, November 30). *Hybrid Warfare – New Threats, Complexity, and “Trust” as the Antidote*. NATO Review. <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>
- [5] Cordesman, A. H. (2016, May 4). *The future of hybrid warfare*. Center for Strategic and International Studies (CSIS). <http://csis.org/analysis/future-hybrid-warfare>
- [6] Horn, C. B. (2016). *On hybrid warfare*. Publications.gc.ca; Royal Canadian Air Force Centre for Operational Research and Analysis. https://publications.gc.ca/collections/collection_2017/mdn-dnd/D4-10-19-2016-eng.pdf
- [7] Connable, B., Young, S., Pezard, S., Radin, A., Cohen, R., Migacheva, K., & Sladden, J. (2020). *Russia's Hostile Measures Combating Russian Gray Zone Aggression Against NATO in the Contact, Blunt, and Surge Layers of Competition*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2500/RR2539/RAND_RR2539.pdf
- [8] Canada's Security Intelligence Service. (2025). *The Military Aspects of Russian Grey Zone Activities*. Canada.ca; Government of Canada. <https://www.canada.ca/en/security-intelligence-service/corporate/publications/hybrid-methods-in-the-grey-zone/military-aspects-russian-grey-zone-activities.html>
- [9] Mumford, A., & Carlucci, P. (2022). *Hybrid warfare: The continuation of ambiguity by other means*. European Journal of International Security, 8(2), 1–15. <https://doi.org/10.1017/eis.2022.19>
- [10] Messner, E. (2004). *Forma przyszłych wojen*. Bellona.
- [11] Klutz, A. (2016). *Myatezh Voina: The Russian Grandfather of Western Hybrid Warfare*. Small Wars Journal. <https://archive.smallwarsjournal.com/jrnl/art/myatezh-voina-the-russian-grandfather-of-western-hybrid-warfare>
- [12] Messner, E. (2007). *Mutiny War as a New Form of Armed Struggle*. In Rácz, A. (2015). *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*. Finnish Institute of International Affairs. <https://www.fia.fi/wp-content/uploads/2017/01/fiareport43.pdf>
- [13] Rácz, A. (2015). *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist* (pp. 1–104). The Finnish Institute of International Affairs. <https://www.fia.fi/wp-content/uploads/2017/01/fiareport43.pdf>
- [14] Panarin, I. (2003). *Information Warfare and Geopolitics*. Cited in Darczewska, J. (2014). *The Anatomy of Russian Information Warfare*. osw Studies. https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf
- [15] Tsygankov, A. (2015). Vladimir Putin's last stand: the sources of Russia's Ukraine policy. Post-Soviet Affairs, 31(4), 279–303. <https://doi.org/10.1080/1060586x.2015.1005903>
- [16] Pomerantsev, P. (2019). *This Is Not Propaganda*. Faber & Faber.
- [17] Pavlovsky, G. (2014). *Putin's World Outlook [Interview]*. In New Left Review.; Wilson, A. (2005). *Virtual Politics: Faking Democracy in the Post-Soviet World*. Yale University Press.
- [18] Pomerantsev, P. (2014). *Nothing is true and everything is possible: the surreal heart of the new Russia*. PublicAffairs.
- [19] Pavlovsky, G. [Interview]. (2012). *The Reality We Create*. In Walker, S. (2016). *The Long Hangover*. Oxford University Press. <https://www.penguinrandomhouse.com/books/553053/the-long-hangover-by-shawn-walker/>
- [20] Surkov, V. (2019). *The Loneliness of the Half-Breed*. Russia in Global Affairs. <https://eng.globalaffairs.ru/articles/the-loneliness-of-the-half-breed/>
- [21] Snyder, T. (2018). *The Road to Unfreedom*. Tim Duggan Books.
- [22] Dugin, A. (2012). *The Fourth Political Theory*. Arktos.
- [23] Dugin, A. (1997) *Osnovy geopolitiki (Foundations of Geopolitics)*. Arktogeja.
- [24] Laruelle, M. (2015). *Eurasianism and the Ideology of Russian Empire*. Woodrow Wilson Center.
- [25] Fridman, O. (2018). *Russian Hybrid Warfare: Resurgence and Politicization*. Oxford University Press.
- [26] Bartles, C. K. (2016). Getting Gerasimov Right. *Military Review*, 96(1), 30–38. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf
- [27] Reuters Staff. (2017, November 7). Estonia arrests suspected Russian FSB agent. *Reuters*. <https://www.reuters.com/article/world/estonia-arrests-suspected-russian-fsb-agent-idUSKBN1D71HZ/>
- [28] UK Government. (2018, September 5). *PM statement on the Salisbury investigation: 5 September 2018*. gov.uk. <https://www.gov.uk/government/speeches/pm-statement-on-the-salisbury-investigation-5-september-2018>
- [29] UK Government. (2018, February 15). *Foreign Office Minister condemns Russia for NotPetya attacks*. gov.uk. <https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks>
- [30] National Cyber Security Centre. (2021, April 15). *UK and US Call out Russia for SolarWinds Compromise*. Wwww.ncsc.gov.uk. <https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise>
- [31] Popescu, N., Secieru, S., Alatalu, S., Borogan, I., Chernenko, E., Hergip, S., Jonsson, O., Kurowska, X., Limnell, J., Pawlak, P., Pernik, P., Reinhold, T., Reshetnikov, A., Soldatov, A., & Vilmer, J.-B. (2018). *Hacks, leaks and disruptions Russian cyber strategies* EDITED BY Chaillot Papers. European Union Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/EuissFiles/cp_148.pdf
- [32] U. S. Department of Justice. (2022, January 20). *Belarusian Government Officials Charged with Aircraft Piracy for Diverting Ryanair Flight 4978 to Arrest Dissident Journalist in May 2021*. Justice.gov. <https://www.justice.gov/archives/opa/pr/belarusian-government-officials-charged-aircraft-piracy-diverting-ryanair-flight-4978-arrest>
- [33] Gerdžiūnas, B., & Valkauskas, T. (2024, August 15). *Belarusian exiles in Vilnius fight off kgb infiltration, recruitment attempts*. Lrt.lt. <https://www.lrt.lt/en/news-in-english/19/2337733/belarusian-exiles-in-vilnius-fight-off-kgb-infiltration-recruitment-attempts>
- [34] Nimmo, B., François, C., Eib, C. S., Ronzaud, L., Ferreira, R., Hernon, C., & Kostelancik, T. (2020). *Secondary Infektion*. Graphika. <https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf>
- [35] Praks, H. (2024, May 30). *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage – Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats*. Hybrid CoE – the European Centre of Excellence for Countering Hybrid Threats. <https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-32-russias-hybrid-threat-tactics-against-the-baltic-sea-region-from-disinformation-to-sabotage/>

- [36] Estonian Internal Security Service. (2025). *Annual Review 2024-2025*. KAPO. https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf
- [37] Thomas, T. (2004). *Russia's Reflexive Control Theory and the Military*. The Journal of Slavic Military Studies, 17(2), 237–256. <https://doi.org/10.1080/13518040490450529>
- [38] Dąbrowska, I. (2021). *Maskowanie operacyjne (maskirowka) jako rosyjska zdolność zaskakiwania przeciwnika*. Przegląd Bezpieczeństwa Wewnętrznego, 25(13), 293–321. <https://ejournals.eu/czasopismo/przeglad-bezpieczenstwa-wewnetrznego/artukul/maskowanie-operacyjne-maskirowka-jako-rosyjska-zdolnosc-zaskakiwania-przeciwnika>
- [39] Fridman, O. (2018). *Russian "Hybrid Warfare"*. Oxford University Press. <https://doi.org/10.1093/oso/9780190877378.001.0001>
- [40] Institute for Strategic Dialogue. (2025, May 20). *Investigation: Russia-aligned campaigns amplify negative sentiment towards Ukrainians in Poland ahead of a decisive presidential vote*. ISD. https://www.isdglobal.org/digital_dispatches/russia-aligned-campaigns-amplify-negative-sentiment-towards-ukrainians-in-poland-ahead-of-a-decisive-presidential-vote
- [41] Lucas, E. (2019). *The Spycraft Revolution*. Foreign Policy. <https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/>
- [42] Riehle, K. P. (2023). *Soviet and Russian Diplomatic Expulsions: How Many and Why?* International Journal of Intelligence and Counterintelligence, 37(4), 1–26. <https://doi.org/10.1080/08850607.2023.2272216>
- [43] Reuters Staff. (2025, August 13). *Poland charges group with sabotage on behalf of foreign intelligence*. Reuters. <https://www.reuters.com/world/poland-charges-group-with-sabotage-behalf-foreign-intelligence-2025-08-13/>
- [44] Burrows, E. (2025, July 8). *UK court convicts 3 men over arson attack authorities say was organized by Russian intelligence*. AP News. <https://apnews.com/article/russia-ukraine-london-arson-warehouse-intelligence-a00f7429e0688731ff1718d2c3bb855f>
- [45] Gera, V. (2025, May 11). *Poland blames Russian intelligence for Warsaw shopping center arson attack*. AP News. <https://apnews.com/article/poland-russia-420187f5755036f6f1c65122c11348f>
- [46] Radin, A., Demus, A., & Marcinek, K. (2020). *Understanding Russian Subversion: Patterns, Threats, and Responses* (pp. 1–32). RAND Corporation. <https://www.rand.org/pubs/perspectives/PE331.html>
- [47] Reynolds, S. (2025, August 14). *The scale of Russian operations against Europe's critical infrastructure*. International Institute for Strategic Studies. <https://www.iiss.org/research-paper/2025/08/the-scale-of-russian-sabotage-operations-against-europes-critical-infrastructure/>
- [48] Øvrebø, E. F. (2024, June 13). *Brann ved Lieråstunnen: – Mye innstillinger og forsinkelser*. VG. <https://www.vg.no/nyheter/i/EywVrl/brann-ved-lieraaesen-tunnel-togstrekning-mellom-asker-og-drammen-stengt>
- [49] Langvik, S. (2024, June 19). *Ingen pågrepet etter bilbranner i Oslo*. VG. <https://www.vg.no/nyheter/i/4B7L4q/bilbrann-paa-haugerud-i-oslo>
- [50] Jegoroff, M. (2024, June 30). *Yhtäkkiä alkoi hämähien vesihuolto-kohteiden murtosarja – tämä tapauksista tiedetään*. Ilta-Sanomat. <https://www.is.fi/kotimaa/art-2000010531133.html>
- [51] Is. (2024, June 30). *Pääkirjoitus: Onko Putinin Venäjä siirtynyt Suomen häirinnässä jo vakavammalle tasolle? Salamurhat ja sabotaasit eivät välttämättä ole enää pelkkää mielikuvitusta*. Ilta-Sanomat. <https://www.is.fi/paakirjoitus/art-2000010532602.html>
- [52] Kusma, E. (2024, June 3). *Kose vallas põles viihhall, päästjad reageerisid suurte jõududega*. Ohtuleht.ee. https://www.ohtuleht.ee/1108159/fotod-kose-vallas-poles-viihall-paastjad-reageerisid-suurte-joududega?utm_source=ground.news&utm_medium=referral
- [53] Moulson, G. (2025, May 14). *Germany and Switzerland arrest 3 over suspected plans to send explosive parcels to Ukraine*. Apnews.com. <https://apnews.com/article/germany-ukraine-russia-packages-arson-explosives-arrests-c032a532ffc94585d70501ff6a4d4bda>
- [54] LETA. (2024, June 29). *Bolderājā notikušais ugunsgrēks izcēlies bistamo atkritumu apsaimniekotāja teritorijā*. Tv3.Lv. <https://tv3.lv/degpunkta/ugunsdrošiba/vides-piesarņojuma-izplatīšanas-ugunsgrēka-bolderaja-ierobežota/>
- [55] Matonis, J. (2024, June 24). *Pranešama apie gaisrų Kauno aviacijos gamykloje*. Delfi. <https://www.delfi.lt/news/daily/crime/pranesama-apie-gaisra-kauno-aviacijos-gamykloje-120031866>
- [56] Sychev, A., & Ratz, A. (2024, April 18). *Germany arrests two for alleged military sabotage plot on behalf of Russia*. Reuters. <https://www.reuters.com/world/europe/germany-arrests-two-alleged-military-sabotage-plot-behalf-russia-2024-04-18/>
- [57] Moulson, G. (2025, May 14). *Germany and Switzerland arrest 3 over suspected plans to send explosive parcels to Ukraine*. Apnews.com. <https://apnews.com/article/germany-ukraine-russia-packages-arson-explosives-arrests-c032a532ffc94585d70501ff6a4d4bda>
- [58] Koper, A., Strzelecki, M., Lebedev, F., & Sytas, A. (2025, April 10). *Insight: Sex toys and exploding cosmetics: anatomy of a "hybrid war" on the West*. Reuters. <https://www.reuters.com/world/europe/sex-toys-exploding-cosmetics-anatomy-hybrid-war-west-2025-04-05/>
- [59] Kang-Stryker, A., & Bugajski, J. (2025). *Poland on the Frontlines Against Russia's Shadow War*. Eurasia Daily Monitor, 22(66). <https://jamestown.org/program/poland-on-the-frontlines-against-russias-shadow-war>
- [60] Todur, W. (2024, June 28). *Pożar w Sławkowie nie był przypadkowy? "Trzeba brać pod uwagę ten fatalny rosyjski ślad"*. Wyborcza.pl Sosnowiec. <https://sosnowiec.wyborcza.pl/sosnowiec/7,93867,31101652,pozar-w-slawkowie-nie-byl-przypadkowy-trzeba-brac-pod-uwage.html>
- [61] Kozioł, M. (2024, June 28). *Samoloty gaśnicze i strażacy walczy z ogniem na poligonie w Żaganii. Pożar pojawił się podczas ćwiczeń*. Wyborcza.pl Zielona Góra. <https://zielonagora.wyborcza.pl/zielonagora/7,35182,31101980,samoloty-gasnicze-i-strazacy-walczą-z-ogniem-na-poligonie-w.html>
- [62] Gruszczyński, A. (2024, June 27). *Wielki pożar pod Działdowem. Stł. strażaków walczy z ogniem*. Wyborcza.pl Olsztyn. <https://olsztyn.wyborcza.pl/olsztyn/7,48726,31096605,wielki-pozar-pod-dzialdowem-100-strazakow-walczą-z-ogniem.html>
- [63] Danielewicz, M. (2024, June 26). *Ogromny pożar zabytkowego pałacu w Jelczu-Laskowicach. Dym było widać z odległości kilku kilometrów*. Wyborcza.pl Wrocław. <https://wroclaw.wyborcza.pl/wroclaw/7,35771,31094238,strazacy-walczą-z-pozarem-neogotyckiego-palacu-w-jelczu-laskowicach.html>
- [64] MG. (2024, June 24). *Pożar magazynu ze zbożem. Podano przypuszczalną przyczynę*. TvN24.PL; TVN Warszawa. <https://tvn24.pl/tvnwarszawa/najnowsze/gozdowo-sierpc-pozar-magazynu-ze-zbozem-st7977366>
- [65] Matusiak, T. (2024, June 24). *Pożar magazynu na zboże. Chmura ciemnego dymu w okolicach Sierpca i Płocka*. Wyborcza.pl Płock. <https://plock.wyborcza.pl/plock/7,35681,31088324,pozar-magazynu-na-zboze-chmura-ciemnego-dymu-w-okolicach-sierpca.html>
- [66] Kijek, K., & Zieliński, R. (2024, June 17). *Ogromny pożar zabytkowego pałacu Stolbergów we Wrocławiu. Strażacy przez całą noc walczyli z ogniem*. Wyborcza.pl Wrocław. <https://wroclaw.wyborcza.pl/wroclaw/7,35771,31065769,pozar-zabytkowego-palacu-stolbergow-we-wroclawiu-strazacy-przez.html>
- [67] Informacja prasowa. (2025, August 6). *Sabotaż światłowodów w Warszawie – szybka reakcja Intelligent Technologies*. Elektrotechnik Automatyk. <https://elektrotechnikautomatyk.pl/artykuly/sabotaz-swiatlowodow-w-warszawie-szybka-reakcja-intelligent-technologies>
- [68] Walker, S. (2025, May 4). *"These people are disposable": how Russia is using online recruits for a campaign of sabotage in Europe*. The Guardian. <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>
- [69] Saito, M., Koper, A., Zverev, A., Lebedev, F., & Nikolskaya, P. (2025, June 12). *Russia recruited a teenage spy. His arrest led to a crypto money trail*. Reuters. <https://www.reuters.com/investigates/special-report/europe-espionage-teen-spy/>
- [70] Johecová, K. (2025, July 10). *Russia hires migrants to wreak havoc, Czech intel report says*. POLITICO. <https://www.politico.eu/article/russia-hiring-migrants-fear-weaken-trust-state-czech-republic-secret-service-telegram-arson-military/>
- [71] Warrell, H., & Mosolova, D. (2025, May 12). *Bulgarian who led Russia-backed spy ring in the UK jailed for 10 years*. Financial Times. <https://www.ft.com/content/65c17f2f-64ad-42f3-b035-fef3f22c6bda>

- [72] Burrows, E. (2025, July 9). *European intelligence officials warn that a Russian sabotage campaign is escalating*. AP News. <https://apnews.com/article/russia-sabotage-europe-ukraine-13ee37cf869139839f0d4a3ebe7bd80d>
- [73] Strategic Communications. (2024). *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*. EEAS. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en
- [74] Institute for Strategic Dialogue. (2025, May 20). *Investigation: Russia-aligned campaigns amplify negative sentiment towards Ukrainians in Poland ahead of a decisive presidential vote*. ISD. https://www.isdglobal.org/digital_dispatches/russia-aligned-campaigns-amplify-negative-sentiment-towards-ukrainians-in-poland-ahead-of-a-decisive-presidential-vote
- [75] Atanasova, A., Poldi, F., & Kuster, G. (2025). *Operation Overload: More Platforms, New Techniques, Powered by AI*. (pp. 1–138). Check First. https://checkfirst.network/wp-content/uploads/2025/06/Overload%C2%A0-%20Main%20Draft%20Report_compressed.pdf
- [76] VIGINUM. (2024). *Summary of the Information Threat to the Paris 2024 Olympic and Paralympic Games Public report*. General Secretariat for Defence and National Security. https://www.sgdns.gouv.fr/files/files/Publications/20240919_NP_SGDSN_VIGINUM_Summary%20information%20threat%20Paris2024Games_EN_0.pdf
- [77] Hinnant, L. (2024, July 4). *Russian-linked cybercampaigns put a bull's-eye on France. Their focus? The Olympics and elections*. AP News. <https://apnews.com/article/france-election-disinformation-russia-olympics-be18d688677240686df200096018f221>
- [78] Reynaud, F., & Ricard, P. (2024, February 12). *France uncovers vast network of Russian disinformation sites*. Le Monde. https://www.lemonde.fr/en/pixels/article/2024/02/12/france-uncovers-vast-network-of-russian-disinformation-sites_6518362_13.html
- [79] VIGINUM. (2025). *Challenges and opportunities of artificial intelligence in the fight against information manipulation* (pp. 1–28). General Secretariat for Defence and National Security. https://www.sgdns.gouv.fr/files/files/Publications/20250207_NP_SGDSN_VIGINUM_Rapport%20menace%20informationnelle%20IA_EN_0.pdf
- [80] Foreign, Commonwealth & Development Office. (2024, October 28). *UK sanctions Putin's interference actors*. GOV.UK. <https://www.gov.uk/government/news/uk-sanctions-putins-interference-actors>
- [81] Reuters Staff. (2024, October 28). *UK sanctions Russian "disinformation agencies"*. Reuters. <https://www.reuters.com/world/uk/uk-sanctions-russian-disinformation-agencies-2024-10-28/>
- [82] Gilbert, D. (2025, July 1). *A Pro-Russia Disinformation Campaign Is Using Free AI Tools to Fuel a "Content Explosion."* WIRED. <https://www.wired.com/story/pro-russia-disinformation-campaign-free-ai-tools/>
- [83] Bergmanis-Koräts, G., Isupova, M., & Vecmanis, R. R. (2025). *Virtual Manipulation Brief 2025: From War and Fear to Confusion and Uncertainty*. Stratcomcoe.org; StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia. <https://stratcomcoe.org/publications/virtual-manipulation-brief-2025-from-war-and-fear-to-confusion-and-uncertainty/320>
- [84] U. S. Department of Justice. (2024, July 9). *Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm*. Justice.gov. <https://www.justice.gov/archives/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners>
- [85] U. S. Department of Justice. (2024, September 4). *Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere*. Justice.gov. <https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence>
- [86] Federal Bureau of Investigation, Cyber National Mission Force, Netherlands Military Intelligence and Security Service, Netherlands General Intelligence and Security Service, Netherlands National Police, & Canadian Centre for Cyber Security. (2024). *State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity* (pp. 1–14). Cisa.gov. <https://www.ic3.gov/csa/2024/240709.pdf>
- [87] Gilbert, D. (2025, July 1). *A Pro-Russia Disinformation Campaign Is Using Free AI Tools to Fuel a "Content Explosion."* WIRED. <https://www.wired.com/story/pro-russia-disinformation-campaign-free-ai-tools/>
- [88] Bergmanis-Koräts, G., Isupova, M., & Vecmanis, R. R. (2025). *Virtual Manipulation Brief 2025: From War and Fear to Confusion and Uncertainty*. Stratcomcoe.org; StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia. <https://stratcomcoe.org/publications/virtual-manipulation-brief-2025-from-war-and-fear-to-confusion-and-uncertainty/320>
- [89] Stockwell, S. (2024). *AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections*. Centre for Emerging Technology and Security; The Alan Turing Institute. <https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-threat-analysis-2024-uk-and-european-elections>
- [90] General Intelligence and Security Service of the Netherlands, & National Coordinator for Counterterrorism and Security. (2024). *Crossing borders: State-sponsored interference in diaspora communities in the Netherlands* (pp. 20–21). AIVD and NCTV. <https://english.aivd.nl/binaries/aivd-en/documenten/publications/2025/03/25/phenomenon-analysis-crossing-borders/Crossing-Borders-AIVD-NCTV.pdf>
- [91] Lozovsky, I., & Laine, M. (2025, May 21). *Russian Foundation, Aimed at Helping "Compatriots" Abroad, Supports Spies, Criminals, and Propagandists*. OCCRP. <https://www.occrp.org/en/project/dear-compatriots/russian-foundation-aimed-at-helping-compatriots-abroad-supports-spies-criminals-and-propagandists>
- [92] Jochecová, K. (2025, July 10). *Russia hires migrants to wreak havoc, Czech intel report says*. POLITICO. <https://www.politico.eu/article/russia-hiring-migrants-fear-weaken-trust-state-czech-republic-secret-service-telegram-arson-military/>
- [93] Agencja Bezpieczeństwa Wewnętrzznego. (2024, October 25). *Komunikat dotyczący działalności dywersyjnej FR*. Abw.gov.pl. <https://www.abw.gov.pl/pl/informacje/2569,Komunikat-dotyczacy-dzialalnosci-dywersyjnej-FR.html>
- [94] Lelonek, A. (2025, April 9). *Russia's recruitment of immigrants to carry out spying and sabotage is a new threat to Poland*. Notes from Poland. <https://notesfrompoland.com/2025/04/09/russias-recruitment-of-immigrants-to-carry-out-spying-and-sabotage-is-a-new-threat-to-poland/>
- [95] EUROPOL. (2025). *European Union Serious and Organised Crime Threat Assessment" The Changing DNA of Serious and Organised Crime*. European Union Agency for Law Enforcement Cooperation. <https://www.europol.europa.eu/cms/sites/default/files/documents/eu-socta-2025.pdf>
- [96] Reuters Staff. (2025, May 12). *Russian spy ring leader jailed in UK for nearly 11 years*. Reuters. <https://www.reuters.com/world/europe/russian-spy-ring-leader-jailed-uk-nearly-11-years-2025-05-12/>
- [97] Holden, M., & Tobin, S. (2025, March 7). *Bulgarians convicted in UK of being Russian spies working for Wirecard fugitive*. Reuters. <https://www.reuters.com/world/europe/three-bulgarians-convicted-spying-russia-after-uk-trial-2025-03-07/>
- [98] Burrows, E. (2025, July 8). *UK court convicts 3 men over arson attack authorities say was organized by Russian intelligence*. AP News. <https://apnews.com/article/russia-ukraine-london-arson-warehouse-intelligence-a00f7429e0688731ff1718d2c3bb855f>
- [99] State Security Department of the Republic of Lithuania, & Defence Intelligence and Security Service under the Ministry of National Defence. (2025). *2025 National Threat Assessment*. Ministry of National Defence. https://kam.lt/wp-content/uploads/2025/03/2025-GR-ENG-02-21-El-be-uzraso_.pdf
- [100] European Parliament. (2025, April 3). *European Parliament resolution of 3 April 2025 on the immediate risk of further repression by Lukashenko's regime in Belarus – threats from the Investigative Committee (2025/2629(RSP))*. www.europarl.europa.eu. https://www.europarl.europa.eu/doceo/document/TA-10-2025-0063_EN.html
- [101] European Parliament. (2025, April 3). *Resolution of 3 April 2025 on the immediate risk of further repression by Lukashenko's regime in Belarus – threats from the Investigative Committee (P10_TA(2025)0063)*. European Parliament. http://www.europarl.europa.eu/doceo/document/TA-10-2025-0063_EN.html

- [102] Walker, S. (2025, May 4). "These people are disposable": how Russia is using online recruits for a campaign of sabotage in Europe. The Guardian. <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>
- [103] EUROPOL. (2025). *European Union Serious and Organised Crime Threat Assessment* "The Changing DNA of Serious and Organised Crime". European Union Agency for Law Enforcement Cooperation. <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>
- [104] Central Intelligence Agency. (1987). *Soviet active measures in the United States*. U. S. Department of State. <https://www.cia.gov/readingroom/docs/cia-rdp11M01338R000400470089-2.pdf>
- [105] Sychev, A., & Ratz, A. (2024, April 18). *Germany arrests two for alleged military sabotage plot on behalf of Russia*. Reuters. <https://www.reuters.com/world/europe/germany-arrests-two-alleged-military-sabotage-plot-behalf-russia-2024-04-18/>
- [106] Reuters Staff. (2025, May 12). *Russian spy ring leader jailed in UK for nearly 11 years*. Reuters. <https://www.reuters.com/world/europe/russian-spy-ring-leader-jailed-uk-nearly-11-years-2025-05-12/>
- [107] Counter Terrorism Policing. (2025, July 11). *Group convicted after Russian-ordered arson attack in London*. Counter Terrorism Policing. <https://www.counterterrorism.police.uk/group-convicted-after-russian-ordered-arson-attack-in-london/>
- [108] Walker, S. (2025, May 4). "These people are disposable": how Russia is using online recruits for a campaign of sabotage in Europe. The Guardian. <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>
- [109] Strategic Communications. (2024). *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*. EEAS. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en
- [110] Burdette, Z., Phillips, D., Heim, J. L., Geist, E., Frelinger, D. R., Heitzenrater, C., & Mueller, K. P. (2025, July 3). *An AI Revolution in Military Affairs? How Artificial Intelligence Could Reshape Future Warfare*. Rand.org; RAND Corporation. https://www.rand.org/pubs/working_papers/WRA4004-1.html
- [111] Osadchuk, R. (2024, July 9). *AI tools usage for disinformation in the war in Ukraine*. DFRLab. <https://dfrlab.org/2024/07/09/ai-tools-usage-for-disinformation-in-the-war-in-ukraine/>
- [112] Bergmanis-Korāts, G., Isupova, M., & Vecmanis, R. R. (2025). *Virtual Manipulation Brief 2025: From War and Fear to Confusion and Uncertainty*. Stratcomcoe.org; StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia. <https://stratcomcoe.org/publications/virtual-manipulation-brief-2025-from-war-and-fear-to-confusion-and-uncertainty/320>
- [113] Wallner, C., Copeland, S., & Giustozzi, A. (2025). *Emerging Insights Russia, AI and the Future of Disinformation Warfare*. Royal United Services Institute for Defence and Security Studies. <https://static.rusi.org/russia-ai-and-the-future-of-disinformation-warfare.pdf>
- [114] Gilbert, D. (2025, July 1). *A Pro-Russia Disinformation Campaign Is Using Free AI Tools to Fuel a "Content Explosion."* WIRED. <https://www.wired.com/story/pro-russia-disinformation-campaign-free-ai-tools/>
- [115] Pita, A., & Wirtschafter, V. (2024, June 26). *What role is AI playing in election disinformation?* Brookings. <https://www.brookings.edu/articles/what-role-is-ai-playing-in-election-disinformation/>
- [116] Menn, J. (2025, April 17). *Russia seeds chatbots with lies. Any bad actor could game AI the same way*. The Washington Post. <https://www.washingtonpost.com/technology/2025/04/17/llm-poisoning-grooming-chatbots-russia/>
- [117] Châtelet, V. (2025, April 18). *Exposing Pravda: How pro-Kremlin forces are poisoning AI models and rewriting Wikipedia*. Atlantic Council. <https://www.atlanticcouncil.org/blogs/new-atlanticist/exposing-pravda-how-pro-kremlin-forces-are-poisoning-ai-models-and-rewriting-wikipedia/>
- [118] Alber, D. A., Yang, Z., Alyakin, A., Yang, E., Rai, S., Valliani, A. A., Zhang, J., Rosenbaum, G. R., Amend-Thomas, A. K., Kurland, D. B., Kremer, C. M., Eremiev, A., Negash, B., Wiggan, D. D., Nakatsuka, M. A., Sangwon, K. L., Neifert, S. N., Khan, H. A., Save, A. V., & Palla, A. (2025). Medical large language models are vulnerable to data-poisoning attacks. *Nature Medicine*, 31. <https://doi.org/10.1038/s41591-024-03445-1>
- [119] Marcellino, W., Welch, J., Clayton, B., Webber, S., & Goode, T. (2025, July 22). *Acquiring Generative Artificial Intelligence to Improve U.S. Department of Defense Influence Activities*. Rand.org; RAND Corporation. https://www.rand.org/pubs/research_reports/RRA3157-1.html
- [120] Warren, K., Menthe, L., Kane, B. R., Kessler, S., Lee, M., Lumpkin, D., Snyder, D. J., Zhang, L. A., Hartunian, A. E., & Konetzki, S. (2025). *Improving Sense-Making with Artificial Intelligence*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA3152-1.html
- [121] Coalition for Content Provenance and Authenticity. (2025). *Advancing digital content transparency and authenticity*. C2pa.org. <https://c2pa.org/>
- [122] European Broadcasting Union. (2024, December 18). *EBU joins early implementers of new standard to track media content provenance*. Tech.ebu.ch. <https://tech.ebu.ch/news/2024/12/ebu-joins-early-implementers-of-new-standard-to-track-content-provenance>
- [123] National Security Agency, Australian Signals Directorate, Australian Cyber Security Centre, Canadian Centre for Cyber Security, & National Cyber Security Centre. (2025). *Content Credentials: Strengthening Multimedia Integrity in the Generative AI Era* (pp. 1–25). National Security Agency. <https://media.defense.gov/2025/Jan/29/2003634788/-1/-1/0/CSI-CONTENT-CREDENTIALS.PDF>
- [124] Revitsky Locker, A., Heitzenrater, C., & Helmus, T. C. (2025, June 4). *Overpromising on Digital Provenance and Security*. Rand.org; RAND Corporation. <https://www.rand.org/pubs/commentary/2025/06/overpromising-on-digital-provenance-and-security.html>
- [125] European Commission. (2023). *Strategic communication and countering information manipulation*. European Commission. https://commission.europa.eu/topics/countering-information-manipulation_en
- [126] Bergmanis-Korāts, G., Isupova, M., & Vecmanis, R. R. (2025). *Virtual Manipulation Brief 2025: From War and Fear to Confusion and Uncertainty*. Stratcomcoe.org; StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia. <https://stratcomcoe.org/publications/virtual-manipulation-brief-2025-from-war-and-fear-to-confusion-and-uncertainty/320>
- [127] Galicia, B. (2025, July 3). *In the fight against foreign information manipulation, the US can't afford to disarm*. Atlantic Council. <https://www.atlanticcouncil.org/blogs/new-atlanticist/in-the-fight-against-foreign-information-manipulation-the-us-cant-afford-to-disarm/>
- [128] Reuters Staff. (2025, August 14). *Poland foiled cyberattack on big city's water supply, deputy PM says*. Reuters. <https://www.reuters.com/en/poland-foiled-cyberattack-big-citys-water-supply-deputy-pm-says-2025-08-14/>
- [129] Gerdžiūnas, B. (2025, July 11). *Russian drone crashed in Lithuania – what you should know*. Lrt.lt. <https://www.lrt.lt/en/news-in-english/19/2606122/russian-drone-crashed-in-lithuania-what-you-should-know>
- [130] Jakučionis, S. (2025, August 5). *Explosive device found in drone from Belarus that crashed in Lithuania*. Lrt.lt. <https://www.lrt.lt/en/news-in-english/19/2634744/explosive-device-found-in-drone-from-belarus-that-crashed-in-lithuania>
- [131] Biržietis, D. (2025, August 6). *Lithuania asks NATO to deploy anti-drone systems after explosive drone incident*. Lrt.lt. <https://www.lrt.lt/en/news-in-english/19/2635106/lithuania-asks-nato-to-deploy-anti-drone-systems-after-explosive-drone-incident>
- [132] Bajarūnas, E. (2025, July 31). *Flight Risk: Baltics Scramble to Counter Hybrid Drone Threat*. CEPA. <https://cepa.org/article/flight-risk-baltics-scramble-to-counter-hybrid-drone-threat/>
- [133] The Moscow Times. (2025, March 6). *Russia to Build Drone Factory in Belarus*. The Moscow Times. <https://www.themoscowtimes.com/2025/03/06/russia-to-build-drone-factory-in-belarus-a88273>
- [134] Taradiuk, Y. (2025, March 7). *Russia proposes to build drone factory in Belarus to "ensure security."* The Kyiv Independent. <https://kyivindependent.com/russia-proposes-to-build-drone-factory-in-belarus-to-ensure-security/>
- [135] BelTA. (2025, June 13). *Lukashenko briefed on creation of drone troops in Belarus*. Eng.belta.by. <https://eng.belta.by/president/view/lukashenko-briefed-on-creation-of-drone-troops-in-belarus-168907-2025/>

- [136] Loh, M. (2025, March 7). *Russia gearing up to build 100,000 drones on NATO's doorstep*. Business Insider. <https://www.businessinsider.com/russia-gearing-up-produce-drones-nato-doorstep-belarus-2025-3?ir=T>
- [137] Erling, B., & Charlish, A. (2024, August 26). *Poland says drone likely entered its airspace during Russian attack on Ukraine*. Reuters. <https://www.reuters.com/world/europe/polish-army-says-object-entered-poland-during-russian-attack-ukraine-2024-08-26/>
- [138] Reuters Staff. (2024, September 5). *Poland backs off claim drone violated airspace during Russian attack on Ukraine*. Reuters. <https://www.reuters.com/world/europe/poland-backs-off-claim-drone-violated-airspace-during-russian-attack-ukraine-2024-09-05/>
- [139] Reuters Staff. (2025, August 14). *Poland foiled cyberattack on big city's water supply, deputy PM says*. Reuters. <https://www.reuters.com/en/poland-foiled-cyberattack-big-citys-water-supply-deputy-pm-says-2025-08-14/>
- [140] Koper, A., Strzelecki, M., Lebedev, F., & Sytas, A. (2025, April 10). *Insight: Sex toys and exploding cosmetics: anatomy of a "hybrid war" on the West*. Reuters. <https://www.reuters.com/world/europe/sex-toys-exploding-cosmetics-anatomy-hybrid-war-west-2025-04-05/>
- [141] Gerdžiūnas, B. (2025, July 11). *Russian drone crashed in Lithuania – what you should know*. Lrt.lt. <https://www.lrt.lt/en/news-in-english/19/2606122/russian-drone-crashed-in-lithuania-what-you-should-know>
- [142] Desmarais, A. (2025, August 14). *Lithuania joins Baltic neighbours in teaching children to build and fly drones*. Yahoo News. <https://ca.news.yahoo.com/lithuania-joins-baltic-neighbours-teaching-110216590.html?guccounter=1>
- [143] Adamowski, J. (2024, April 8). *Polish defense leaders push "dronization" of the armed forces*. Defense News. <https://www.defensenews.com/global/europe/2024/04/08/polish-defense-leaders-push-dronization-of-the-armed-forces/>
- [144] Koper, A., Strzelecki, M., Lebedev, F., & Sytas, A. (2025, April 10). *Insight: Sex toys and exploding cosmetics: anatomy of a "hybrid war" on the West*. Reuters. <https://www.reuters.com/world/europe/sex-toys-exploding-cosmetics-anatomy-hybrid-war-west-2025-04-05/>
- [145] Biržietis, D. (2025, August 6). *Lithuania asks NATO to deploy anti-drone systems after explosive drone incident*. Lrt.lt. <https://www.lrt.lt/en/news-in-english/19/2635106/lithuania-asks-nato-to-deploy-anti-drone-systems-after-explosive-drone-incident>
- [146] Reuters Staff. (2025, August 14). *Poland foiled cyberattack on big city's water supply, deputy PM says*. Reuters. <https://www.reuters.com/en/poland-foiled-cyberattack-big-citys-water-supply-deputy-pm-says-2025-08-14/>
- [147] Fried, D., & Polyakova, A. (2018, March 5). *Democratic defense against disinformation*. Atlantic Council. <https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation/>
- [148] Lanoszka, A. (2019, January). *Disinformation in international politics*. Cambridge University Press. <https://www.cambridge.org/core/journals/european-journal-of-international-security/article/abs/disinformation-in-international-politics/49121D3134C4079B51E5012E6B6E247A>
- [149] Cornelissen, M. (2015, April 1). *The Baltic States' struggle for hearts and minds*. Latvian Institute of International Affairs. <https://www.liia.lv/en/opinions/the-baltic-states-struggle-for-hearts-and-minds-440>
- [150] Ministerstwo Sprawiedliwości. (2025). *Raport Zespołu ds. Dezinformacji Komisji ds. badania wpływów rosyjskich i białoruskich – Ministerstwo Sprawiedliwości – Portal Gov.pl*. Ministerstwo Sprawiedliwości. <https://www.gov.pl/web/sprawiedliwosc/raport-zespołu-ds-dezinformacji-komisji-ds-badania-wplywow-rosyjskich-i-bialoruskich>
- [151] Grabowska-Siwiec, A. (2025, September 11). *ABW zatrzymała obywatela Białorusi podejrzanego o działalność szpiegowską*. LinkedIn. https://www.linkedin.com/posts/anna-grabowska-siwiec-mjr-dr-phd-b68265113_msz-bis-ah-activity-7371262983597023234-ffRI
- [152] Górnicka, B. (2025, August 8). *Obywatel Rosji legalnie kupuje uczelnię a potem rekrutuje żołnierzy*. Gazeta Wyborcza – Magazyn. <http://wyborcza.pl/magazyn/7,124059,32159950,obywatel-rosji-legalnie-kupuje-uczelnie-a-potem-rekrutuje-zolnierzy.html>
- [153] Kancelaria Prezesa Rady Ministrów. (2025). *Projekt ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu oraz niektórych innych ustaw – Kancelaria Prezesa Rady Ministrów – Portal Gov.pl*. Kancelaria Prezesa Rady Ministrów. <https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-agencji-bezpieczenstwa-wewnetrznego-oraz-agencji-wywiadu-oraz-niektorych-innych-ustaw>
- [154] Ministerstwo Sprawiedliwości. (2025). *Raport Zespołu ds. Dezinformacji Komisji ds. badania wpływów rosyjskich i białoruskich – Ministerstwo Sprawiedliwości – Portal Gov.pl*. Ministerstwo Sprawiedliwości. <https://www.gov.pl/web/sprawiedliwosc/raport-zespołu-ds-dezinformacji-komisji-ds-badania-wplywow-rosyjskich-i-bialoruskich>
- [155] CERT. (2024). *Raport roczny z działalności CERT Polska 2023*. NASK. https://www.nask.pl/media/2024/10/Raport_CERT_2023.pdf
- [156] Gwozdowska, A., Doleśniak-Harczuk, O., Rutke, G., Biernat, J., Oksińska, P., Jarka, I., Gromada, M., & Majka, A. (2023). *Wojna informacyjna 2022-2023: Przebieg i wnioski* (pp. 1–78). NASK. https://www.nask.pl/media/2024/10/Raport__wojna_informacyjna.pdf
- [157] Nawrotkiewicz, J., Majchrowski, T., Chorny Elizalde, V., Badji, S. D., & Mikulski, K. (2024). *Dezinformacja w wyborach na świecie* (pp. 1–135). NASK. https://www.nask.pl/media/2024/12/Raport_Disinformation_PL_28112024_02.pdf
- [158] Myslovskiy, I. (2025, August 18). *European academia studies Russia too little, too refined, and too slowly*. New Eastern Europe. Retrieved from New Eastern Europe. <https://neweasterneurope.eu/2025/08/18/european-academia-studies-russia-too-little-too-refined-and-too-slowly/>

