EuropeanDefenceNetwork

NextGen Inspiring Europe's Defence
Shaping
Thinking
Connecting
Building

HYBRID WARFARE IN EUROPE

Publication 1 • April 2026

European Defence Network

NextGen Inspiring Europe's Defence
Shaping
Thinking
Connecting
Building

ABOUT US

The European Defence Network (EDN) brings together a new generation of Europeans working at the intersection of defence, security and policy.

It was created from a simple premise: Europe's security challenges cannot be addressed within national silos. They require shared thinking, cross-border cooperation and a common strategic culture.

EDN operates as a platform for analysis and exchange, producing research, organising seminars and fostering dialogue across academia, industry and institutions. Its work is driven by independence and a commitment to objective, high-quality insight, free from political or industrial bias.

At its core, EDN is about people. It connects students and young professionals across Europe, equipping them with the analytical tools, networks and perspective needed to engage with complex defence challenges.

By doing so, it contributes to the emergence of a more coherent, informed and forward-looking European defence ecosystem.

EuropeanDefenceNetwork

NextGen Inspiring Europe's Defence
Shaping
Thinking
Connecting
Building

THE AUTHORS

Agamemnon Logothetis

Andrea Cirelli

Carola Picconi

Eleni Panagakou

Matteo Anthony Carotti

Sofia Zanin

Renaud Laffourcade

Table of Contents

Introduction

Hybrid warfare, while not a new phenomenon, has become increasingly prevalent in recent years. There is no universally accepted definition, nor a fixed set of actions that clearly delineate what constitutes hybrid warfare. The term itself began to gain prominence in the early 2000s, when NATO used it to describe a blend of irregular tactics and methods of conflict, combining elements of conventional and non-conventional warfare. Hybrid warfare can be conducted by both state and non-state actors and extends beyond traditional military confrontation. Rather, it adopts a comprehensive, "all-domain" approach, targeting a state's political, societal, economic, and cyber spheres. These operations employ both kinetic and non-kinetic means, often simultaneously, with the aim of exploiting vulnerabilities across multiple sectors.

Hybrid methods of warfare have existed since antiquity, as evidenced by conflicts such as the Peloponnesian War. What has changed over the past two to three decades, however, is the normalization of hybrid warfare as a dominant mode of conflict. The traditional Westphalian concept of war, defined by state-to-state confrontation, clear distinctions between peace and conflict, and engagement between standing armies operating under established codes of conduct, has become increasingly blurred.

In the contemporary security environment, conflict is waged through a combination of cyberattacks, disinformation campaigns, the instrumentalisation of migratory flows, and the use of non-state or plausibly deniable actors, among other means. Formal declarations of war between nation-states have become rare. Instead, we have entered an era of persistent competition, in which adversarial actions occur continuously across multiple domains, often below the threshold of conventional warfare and without clear attribution.

This publication examines hybrid warfare and its impact on European defence and security, with a particular focus on developments over the past 10 to 15 years. It begins by outlining the different forms that hybrid warfare can take, before analysing the types of hybrid attacks Europe has faced since 2014. It then explores strategies for countering hybrid threats, assesses how hybrid warfare fits within the broader geostrategic objectives of state actors, and considers approaches to strengthening civil resilience.

Drawing on a wide range of sources, this work seeks to provide a comprehensive overview of how hybrid warfare has affected European states and societies. It also aims to raise awareness among readers, contributing to a more informed understanding of the challenge and, ultimately, to greater societal resilience.

As this is the first publication of this kind produced by the European Defence Network (EDN), I would like to express my sincere appreciation for your interest in and support for our work. Through the Network, we aim to connect and engage young professionals and students from across Europe who are involved in, or interested in, defence and security. Our goal is to foster dialogue with policymakers and to promote a stronger, more coordinated approach to European defence across national boundaries.

Agamemnon Sotirios Logothetis - Head of Publications

Section 1.
Different Types of Hybrid Warfare

While hybrid warfare has undergone significant strategic evolution and become increasingly relevant to European security, a more precise analytical framework is necessary to understand how it operates in practice. The difficulty in defining hybrid warfare is not merely semantic; rather, it reflects the deliberate nature of hybrid strategies, which are designed to blur traditional distinctions between war and peace, civilian and military domains, and state and non-state actors.

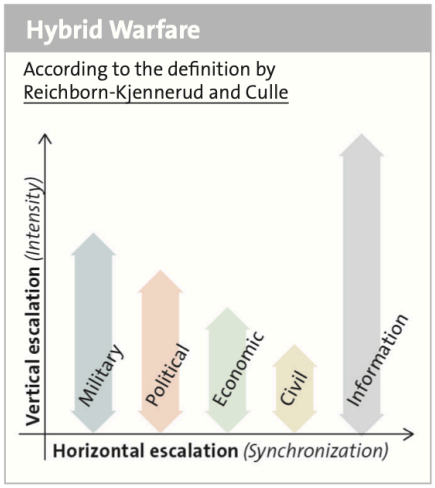

Figure 1. *Hybrid Warfare according to Reichborn-Kjennerud and Cullen.*
Source: Capaul (2024, p. 1)

Rather than treating hybrid warfare as an entirely new phenomenon, this section argues that it represents an evolution of twentieth-century conflict (Capaul, 2024). The difficulty in establishing a clear definition stems in part from the fact that this form of warfare relies on the systematic integration of multiple domains, coordinated to generate strategic effects below the threshold of conventional armed conflict. This shift has complicated both attribution and response. When actions occur within the hybrid domain, such as cyber intrusions, disinformation campaigns, the instrumentalisation of migratory flows, or economic coercion, it becomes inherently ambiguous whether an incident should be classified as an act of war, a criminal offence, or a form of political interference (Gardner, 2015).

Moreover, the objective of such operations is often cumulative and long-term: to erode social cohesion, distort democratic processes, undermine public trust, and weaken institutional resilience. For instance, China's strategic approach has generally sought to avoid direct military confrontation, instead emphasising the use of economic leverage and other forms of soft power to advance its interests (Bargués & Bourekba, 2022).

A clear illustration of the evolution of contemporary conflict can be found in the deployment of the so-called "Little Green Men" during the Annexation of Crimea (Gardner, 2015). These unmarked yet highly trained armed personnel—later acknowledged to be Russian special forces, operated without insignia, allowing Russia to deny direct involvement while maintaining effective control on the ground. Their rapid seizure of key infrastructure and government buildings unfolded alongside coordinated information and political operations, blurring the line between war and peace and delaying both domestic and international responses. This episode exemplifies the strategic logic of ambiguity: achieving concrete political and military objectives while remaining below the threshold that would typically trigger a conventional response.

1.1 Analytical Framework: Two Core Dimensions

Hybrid warfare can be split in two broad categories (Medina Llinàs, 2022):

1. information-based operations aiming at affecting perception
2. decision-making and actions affecting physical systems

An overview of both will be presented below.

1.1.1 Information-Based Operations

Information has long been recognised as a source of power. As noted in 1998 by Vladimir Slipchenko, then Vice President of the Russian Academy of Military Sciences, “it is a weapon just like missiles, bombs and torpedoes” (De Spiegelere et al., 2011). In this context, the weaponisation of information can generate significant disruption, particularly when amplified by contemporary technological capabilities.

The war in Ukraine provides a clear illustration of how narratives disseminated through social media can be deliberately manipulated. The conflict has highlighted a broader confrontation between competing models of digital governance, notably Russian and Chinese techno-authoritarian approaches vis-à-vis the ecosystem shaped by Silicon Valley (Colomina, 2022).

Disinformation, misinformation, and fabricated content act as key enablers in this environment, seeking to exploit and amplify existing societal vulnerabilities. The emergence of generative artificial intelligence has further accelerated this dynamic, enabling the rapid production of convincing text, images, and videos at scale, thereby extending both the reach and effectiveness of traditional propaganda (Bachmann et al., 2023).

Within the broader spectrum of hybrid activities, election interference remains one of the most destabilising tools. Recent cases, including reported interference in elections in Romania, Moldova, and France, demonstrate how external actors seek to exploit democratic processes in order to undermine institutional legitimacy. These efforts are often reinforced through coordinated disinformation campaigns and orchestrated social media activity. For instance, networks reportedly linked to Azerbaijan have promoted separatist narratives in French overseas territories through initiatives such as the Baku Initiative Group (Raufer, 2025).

Hybrid tactics also include symbolic provocations designed to inflame social divisions. Acts such as the vandalism of Holocaust memorials or the placement of pig heads outside mosques in the Paris region, incidents reported by *The Guardian* in 2025, may appear disconnected from traditional forms of warfare. However, such actions are often intended to provoke societal tensions, erode trust, and redirect political attention. Investigations into these incidents have pointed to possible foreign interference, suggesting a deliberate effort to exploit existing societal fault lines (The Guardian, 2025). In this context, social destabilisation is not incidental but instrumental to hybrid strategy.

These examples illustrate how information manipulation and symbolic disruption function as core tools of contemporary hybrid warfare. The following case study examines one of the most structured and technologically sophisticated manifestations of this approach.

1.1.1.1 Case study: Russian Disinformation Campaigns

Russian disinformation operations (*dezinformatsiya voïna*) pose a rapidly evolving threat to global information integrity and represent one of the most sustained and adaptive forms of

hybrid information warfare. In recent years, these campaigns have evolved from isolated influence efforts into highly organised, multilingual infrastructures designed to distort digital ecosystems at scale.

This paper selects the CopyCop operation as a case study due to its scale, organisational sophistication, and technical professionalism. The campaign has been attributed to Storm-1516, a Russian-linked disinformation network associated with coordinated influence operations targeting Western information environments. By 2025, it had built an infrastructure of over 300 websites, including 141 French-language platforms designed to mimic legitimate news sources (NewsGuard, 2025).

Employing a "carpet-bombing" strategy, the network flooded digital spaces with content of varying credibility in order to confuse audiences and manipulate AI training datasets. One documented operation generated approximately 55 million views in four months, alongside the dissemination of over 38,000 messages across social media platforms. The campaign's influence extended even to artificial intelligence systems, with chatbots inadvertently reproducing its false narratives.

Its adaptability and multilingual focus further distinguish it from more traditional disinformation efforts. By tailoring narratives to local contexts, the operation exploits cultural and linguistic nuances to undermine trust in democratic institutions. For example, it has impersonated regional media outlets such as *L'Écho Rhône-Alpes*, blending fabricated content with legitimate reporting to shape public opinion across different audiences.

Among CopyCop's most notorious activities is the creation of fraudulent websites mimicking trusted media outlets (Insikt Group, 2025). In October 2025, the fake site *BrutInfo* impersonated *Brut* and *Le Monde*, publishing a fabricated story alleging that French President Emmanuel Macron was building a €148 million bunker, accompanied by an AI-generated video that reportedly amassed 800,000 views on X. Another outlet, *Enquête du Jour*, impersonated *Le Monde* and *StreetPress journalists*, disseminating a conspiracy theory concerning Brigitte Macron's gender identity through a hybrid of AI-generated voiceovers and repurposed archival footage. These cases illustrate CopyCop's use of generative AI to scale disinformation operations and exploit the credibility of established media organisations.

At the core of CopyCop and Storm-1516 is John Mark Dougan, a former U.S. sheriff now based in Russia, who has been identified as playing a central role in the publication and amplification of disinformation narratives (Viginum, 2025). Dougan's activities are reportedly supported by the Center for Geopolitical Expertise (CGE) and elements linked to Russia's GRU, which are alleged to provide technical and organisational assistance, including infrastructure capable of supporting large-scale content generation. Another key figure is Simeon Boikov, an Australian pro-Kremlin influencer reportedly financed by Pravfond, a Russian legal aid fund linked to intelligence networks.

Since its emergence, Storm-1516 has continuously evolved, conducting both reactive and long-term influence campaigns. Between 2023 and March 2025, Viginum documented 77 disinformation operations targeting France, Ukraine, and broader Western audiences (Viginum, 2025). While the real-world impact of these campaigns is difficult to quantify, some narratives have achieved significant visibility, occasionally being amplified by political figures and online influencers.

Notably, CopyCop does not operate in isolation. It forms part of a broader and increasingly integrated ecosystem of Russian-linked information operations designed to maximise narrative penetration across digital platforms. Beyond individual campaigns, networks such as InfoDefense on Telegram rely on coordinated accounts and aligned influencers to amplify messaging at scale. Portal KOMBAT, which emerged in 2024, operates as a centralised hub for pro-Russian content, synchronising efforts with CopyCop and the broader Lakhta ecosystem (Insikt Group, 2025; EU DisinfoLab, 2024). Financial backing is often attributed to entities such as Pravfond, which funds influencers and is reported to have links to Russian state-affiliated structures (Viginum, 2025). The Pravda Network further repackages and amplifies false narratives, ensuring their dissemination across both fringe and mainstream information environments (NewsGuard, 2025).

The Lakhta Project, initially led by Yevgeny Prigozhin, initially focused on influence operations targeting Western democracies before expanding under Russian-aligned state structures to include broader anti-Western campaigns in regions such as Africa and the Middle East, often in coordination with the Wagner Group (U.S. Department of Justice, 2018; Insikt Group, 2025).

Within this ecosystem, strategic methodologies such as the "Matryoshka" model demonstrate increasing operational sophistication. This approach typically unfolds in three stages: first, the creation of AI-generated or fabricated content attributed to a purported whistleblower; second, dissemination through cloned or deceptive websites designed to impersonate legitimate institutions; and third, amplification via aligned influencers, expatriate networks, and sympathetic public figures (Viginum, 2025; EU DisinfoLab, 2024).

In 2025, this method was used to circulate false claims regarding Ukrainian President Volodymyr Zelensky's property purchases, exploiting domains such as casinohotelvunipalace.com (Viginum, 2025). Similar impersonation tactics targeted the German Ministry of Defence and the U.S.-based Institute for the Study of War, through fabricated platforms including wehrpflicht.de and warstudiescentre.co.uk (Insikt Group, 2025; ISW, 2025).

1.1.2 Operations Targeting Physical Systems (Sabotage)

As noted above, hybrid warfare is not limited to the manipulation of information or the destabilisation of political processes. As Ofer Fridman argues in *Russian Hybrid Warfare: Resurgence and Politicization* (2018, p. 11), the Russian concept of *Gibridnaya Voyna*, which emerged following the "New-Generation War" framework developed by Sergey Chekinov and Sergey Bogdanov in the 2010s, can be understood as an "amplification of any possible social, political, economic, or ideological divisions in the adversary's society that would help to undermine its political, economic, and military cohesion and resilience".

This conceptualisation also extends to direct physical sabotage targeting critical infrastructure, military assets, and civilian systems. Such activities, often characterised by deniability and asymmetry, are designed to disrupt state operational capacity while eroding public confidence in institutional resilience. Unlike conventional military operations, sabotage within a hybrid framework is frequently conducted through proxy actors, combining technological and human vectors to achieve strategic effects while minimising attribution risks.

European Union security officials have noted a "shift in scale" in hybrid threats, including a rise in sabotage and arson incidents across Eastern Europe and the United Kingdom. While no foreign state has been officially attributed responsibility in these cases, the pattern of incidents, when considered alongside documented Russian use of drones and hybrid tactics in Ukraine, has raised significant concern. The International Institute for Strategic Studies (IISS) has similarly highlighted this trend in its research paper *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure* (IISS, 2025), published on 19 August 2025.

1.1.3 Cyberattacks and Electronic Warfare

One of the most pervasive contemporary forms of physical sabotage is the use of cyberattacks and electronic warfare to disrupt essential services and military operations. In 2025, widespread GPS jamming campaigns affected both civilian and military systems across Europe, significantly impacting navigation, logistics, and communication networks, including reported interference with the aircraft carrying Ursula von der Leyen (BBC News, 2025). These disruptions, attributed by European authorities to Russian electronic warfare activity, have raised concerns regarding the safety of civilian aviation and maritime traffic, while also complicating NATO's operational readiness.

In parallel, ransomware attacks attributed to groups such as LockBit and APT28, both widely linked in security reporting to Russian state-aligned cyber activity, have disrupted critical infrastructure, including healthcare systems. Notably, hospitals in Corbeil-Essonnes, France, were affected by a ransomware incident that temporarily paralysed services (Le Parisien, 2022). These cases illustrate how cyber operations function as a form of hybrid sabotage, targeting both civilian resilience and state operational capacity through non-kinetic means.

1.1.4 Airspace Incursions and Drone Threats

The violation of national airspace by foreign military aircraft and unmanned systems represents another dimension of physical hybrid warfare. Russian fighter jets have repeatedly conducted unauthorised flights near the borders of Poland, Romania, and Estonia, testing NATO air defence systems and probing for potential vulnerabilities (France 24, 2025). While often framed as routine training activities in earlier years, such incursions can also serve broader strategic purposes, including signalling intent, exerting pressure on neighbouring states, and normalising the presence of military activity near allied airspace. More recently, the use of civilian drones over sensitive sites, including airports in Denmark, Norway, Belgium, and Germany, as well as French military installations such as Mourmelon and L'Île-Longue, the Eurenco explosives depot in Dordogne, and NATO convoy movements near Mulhouse, has become an increasingly recurring pattern (Le Figaro, 2025). These activities reflect the expanding role of unmanned systems in hybrid operations, particularly in probing critical infrastructure and assessing response capabilities.

1.1.5 Sabotage of Critical Infrastructure

The sabotage of critical infrastructure, particularly in the Baltic Sea and on industrial sites, has emerged as a defining feature of hybrid warfare in Europe. Over the past two years, at least six suspected sabotage incidents have damaged or destroyed eleven underwater cables (Politico, 2025), severely disrupting digital and energy connectivity across the region. The 2024 sabotage of Baltic Sea cables, likely involving the *Eagle S*, a vessel operating under the Cook Islands flag but suspected of links to Russia's shadow fleet, illustrates the use of proxy

maritime assets to target strategically significant infrastructure (Sud-Ouest, 2025). Similarly, the increasing presence of so-called "ghost tankers" in the Baltic Sea, often operating under flags of convenience and with limited regulatory oversight, has heightened the risk of both accidental and deliberate damage to underwater pipelines and communication cables, further undermining regional security.

However, such tactics are not exclusive to Russian-linked actors. The 2022 sabotage of the Nord Stream pipelines, widely attributed in open-source reporting to non-Russian state actors, underscores that infrastructure sabotage is a tool employed by multiple parties within broader geopolitical competition.

On land, industrial and military facilities have also been recurrent targets. In 2023, cables were deliberately severed on the *Amiral Ronarc'h* frigate at the Lorient naval shipyard in France (Ouest-France, 2023), while a similar incident occurred at BAE Systems' Govan shipyard in the United Kingdom, where approximately sixty cables were cut (AirCosmos, 2023). These acts of sabotage, often assessed as involving insider facilitation or recruited operatives, appear designed to delay military production timelines and increase operational and maintenance costs.

A broader pattern of arson and explosive incidents further illustrates the systematic targeting of economic and logistical infrastructure. These include fires affecting Bundeswehr logistics assets in Germany (AFP, June 2025), the Marywilska shopping centre in Poland (AFP, March 2024), and a DHL logistics facility in Birmingham in the United Kingdom (The Guardian, July 2024). The use of expendable agents, including individuals recruited through encrypted messaging applications such as Viber (Le Figaro, 2025), has enabled the execution of dispersed sabotage campaigns, including the reported destruction of hundreds of vehicles in Germany in 2025.

1.1.6 Targeting Human Life and Symbolic Violence

Beyond material damage, hybrid warfare increasingly involves actions that directly endanger human life and exploit symbolic violence to sow fear and division. Reported assassination plots against high-profile figures, such as Armin Papperger, CEO of Rheinmetall, illustrate concerns regarding the targeting of key actors in the defence industrial base. The placement of explosive devices, such as the booby-trapped package discovered in Leipzig in 2024, reflects a calculated strategy to disrupt supply chains and instil public anxiety.

Symbolic acts, including the daubing of red paint on Holocaust memorials in Paris and the placement of pig heads outside mosques, are widely interpreted as designed to exacerbate social tensions and amplify existing fault lines within societies. These tactics, while seemingly disconnected from traditional warfare, serve to weaken societal cohesion and divert attention from broader strategic objectives.

1.2 Operational Logic of Hybrid Warfare

All in all, Hybrid warfare combines different approaches that still remain in the gray zone below the armed combat threshold. Then again, to understand the classification system it is important to keep in mind the deep connection between the vector, the perpetrator and the aim of the attack. On this note, the attack vector can vary in intensity on the basis of 3 criteria:

- **Asymmetry**: the domain in which the attack is carried out;
- **Intensity**: the level of potential escalation relative to conventional warfare;
- **Deniability**: the extent to which the state perpetrating the attack can deny involvement or intent.

The combination of these three characteristics, at different levels and in varying proportions, produces a wide range of possible attack scenarios. For further clarity, the figure below provides a summary of the different categories (Ball, 2018).

Categorization of Hybrid Threats in line with the Definition Criteria of the Hybrid Attack Vector

Term	Deniability	Asymmetry	Intensity	Examples
Hybrid Interference	High: *plausible deniability*	Strongly asymmetrical	Below the threshold of war	Disinformation via social media
Hybrid Operations	Medium: *somewhat plausible deniability*	Asymmetrical	Below the threshold of war	Sabotage of critical infrastructure
Hybrid Warfare	Low: *implausible deniability*	Paramilitary	Conflicts in the "gray zone" (close to the threshold of war)	Little green men, weaponized migration
Conventional Warfare	No deniability	Military (symmetrical warfare)	Threshold of war exceeded	Russia's full invasion of Ukraine since 2022

Source: Author's categorization based on terminology used in Wigell, Mikkola and Juntunen.

Figure 2. *Categorization of Hybrid Threats.* Source: Adapted from Capaul (2024, p. 2).

Section 2.
Hybrid Warfare Attacks in Europe Between 2014-2025

This chapter examines how hybrid warfare has been operationalised against Europe between 2014 and 2025. Rather than providing an exhaustive inventory, it focuses on recurring patterns across three domains: migration manipulation, technological disruption (including cyber operations and airspace incursions), and election interference.

These cases illustrate how hybrid tools are combined across domains to exert sustained pressure while remaining below the threshold of open conflict. Together, they reveal a strategic logic based on cumulative destabilisation rather than decisive confrontation.

2.1 Weaponization of Migration

Conceptual Framework: Coercive Engineered Migration

Migration is inherent to human history, and population movements across borders are a constant feature of human societies. However, when state or non-state actors deliberately exploit or manipulate such movements to destabilise neighbouring regions for strategic gain, this enters the realm of coercive engineered migration (CEM), a tool of hybrid warfare. The term and theoretical framework were originally developed by Kelly M. Greenhill (2010). CEM forms part of the broader category of strategic engineered migration, defined as "those in- or out-migrations that are deliberately induced or manipulated by state or non-state actors, in ways designed to augment, reduce, or change the composition of the population residing within a particular territory, for political or military ends" (Greenhill, 2008). While the exploitation of displaced populations is not new, it remains understudied despite its increasing use.

Strategic engineered migration includes multiple subtypes, each with different objectives. Coercive engineered migration, the focus of this paper, is used as a foreign policy instrument to induce behavioural change in a target state (Greenhill, 2008). CEM requires at least two actors - a coercer and a target - and relies on generating a credible threat of, or directly initiating, migration flows that overwhelm the target's capacity to absorb arrivals ("capacity swamping") and/or trigger internal social unrest ("political agitation"). Either mechanism can destabilise the target's domestic equilibrium.

Democracies are particularly vulnerable due to two force multipliers: hypocrisy costs (reputational damage incurred when restricting borders or engaging with abusive regimes) and political polarisation. CEM succeeds or fails largely based on perception. Polarised societies, split between anti-refugee "rejectionists" and pro-refugee "promoters", create pressure points that coercers can exploit. Democracies also incur high reputational costs when violating humanitarian norms, increasing their susceptibility. However, targets can resist through deterrence, externalising flows, or reshaping public narratives.

Within the 2014–2025 timeframe, the EU has been targeted by multiple CEM attempts. On the southern front, these include Türkiye's use of Syrian refugee flows in 2016, where Ankara acted as an opportunistic coercer (Greenhill, 2010; Gökalp Aras & Nefise Ela Gokalp Aras, 2019); and Morocco's 2020–21 pressure on Spain following the hospitalisation of the Polisario leader, which triggered mass crossings into the Ceuta enclave (Álvarez-Miranda &

Brey, 2023). Increasingly, however, EU institutions view the eastern front as the core threat axis, with Russia and Belarus at the centre. This includes Russia's role in the 2015–2016 Finnish border episode and the 2021–22 Belarus-orchestrated crisis along the borders of Lithuania, Poland, and Latvia. EU institutions have primarily assessed the weaponisation of migration in relation to the eastern front, as Russia is identified as the most immediate security threat to Europe. Consequently, the next case studies provide a historical breakdown of the two most prominent Russia-linked CEM cases.

2.1.1 Case Study: Finland (2015–2016)

Between 1 September 2015 and 16 March 2016, Finland was subjected to a Russian influence operation through coercive migration engineering. At two northern border crossings between Russia and Finland, as well as Norway, authorities observed a sudden influx of Middle Eastern migrants lacking proper visas. The flow abruptly stopped in late February 2016, immediately prior to the announcement of a Russia–Finland bilateral agreement. In January 2016, Finnish agencies reported that at the Kandalaksha crossing, Russian services were directing migrant movements, indicating potential state involvement.

Political figures and Members of the European Parliament quickly accused Russia of using migration flows to influence Helsinki's foreign policy. The influx not only placed diplomatic pressure on Finland but also triggered domestic social tension. A vigilante group, the "Soldiers of Odin", linked to Finnish nationalist circles, formed in response to the arrivals. Violent attacks against reception centres intensified anti-immigration rhetoric already heightened by the broader Syrian refugee crisis. Far-right mobilisation was met with far-left counter-mobilisation, deepening polarisation—one of CEM's core force multipliers.

As the situation deteriorated, Finland initiated diplomatic talks with Russia, despite Moscow's international isolation following the 2014 annexation of Crimea. Immediately after contacts were announced, migration flows ceased. Russia thus leveraged coercive migration dynamics to pressure Finland into diplomatic engagement, diverging from the EU's broader isolation posture and avoiding closer alignment with NATO-related practices (Wojnowski, 2022, pp. 282–292).

The Finnish case illustrates a scenario in which coercive engineered migration can alter target-state behaviour, particularly where the coercer confronts a single state with concentrated domestic pressure points. By contrast, the Belarus case demonstrates the limits of CEM when the target is a supranational actor such as the EU, where decision-making is diffuse, costs are distributed, and political cohesion reduces the likelihood of unilateral concessions.

2.1.2 Case Study: Belarus–EU Border Crisis (2021–2022)

The 2021 case of coercive engineered migration is among the clearest contemporary examples of migration used as a hybrid tool in Europe, and it contributed to EU institutions explicitly recognising the weaponisation of migration. At the time, the EU framed Belarus's actions, politically supported by Russia, as the instrumentalisation of migrants within the civilian domain rather than through direct military escalation.

In mid-2021, Belarus employed CEM as retaliation for EU sanctions imposed following the repression of mass protests after contested elections. Shortly after the sanctions, President Alexander Lukashenko warned that Belarus would no longer prevent migrants from reaching

Europe. Soon after, a surge in arrivals from Middle Eastern and West African countries was recorded at the borders with Lithuania, Poland, and Latvia. It is worth noting that Belarus had issued similar threats between 2002 and 2004 and had previously exploited migration routes during earlier phases of the European migration crisis, making engineered migration a recurring feature of eastern-front hybrid dynamics (Talik, 2024).

The crisis intensified rapidly. In July 2021, Lithuania accused Belarus of facilitating irregular crossings from Iraq, Afghanistan, and African countries and declared a state of emergency. In early August, Lithuania reported approximately 4,000 crossings (Reuters, 2021a), and days later Belarusian border personnel were accused of pushing migrants across the border into Lithuanian territory. Latvia declared a local state of emergency, while Lithuania began constructing a border fence with support from Estonia (Euractiv, 2021). On 18 August, Lithuania accused Minsk of flying migrants into Belarus, a claim which Belarus denied.

In early September 2021, Poland declared a state of emergency (Reuters, 2021b) and began installing barbed wire along its border. These measures triggered reactions from both pro-refugee and anti-migration groups, fuelling polarisation similar to that observed in the Finnish case during 2015–16. Escalation continued in October, when Arabic-language advertisements circulated on Facebook and messaging applications promoting simplified travel and tourist visas to Belarus, from where migrants were then transported to the border and crossed on foot (Adams, 2021).

As flows increased, Poland began constructing a full border wall. By early November, several thousand migrants were stranded in freezing conditions. With approximately 15,000 Polish troops deployed, the crisis evolved into a humanitarian emergency marked by repeated attempts to breach the border. Germany's Foreign Minister Heiko Maas stated that the EU would not yield to Belarusian blackmail and called for further sanctions (BBC News, 2021).

By late 2021, Lithuania also introduced a state of emergency, and arrivals peaked across the eastern border (European Union Agency for Asylum, 2022). In January 2022, Poland began constructing a reinforced border wall, which - once completed in mid-2022 - significantly reduced crossings (Deutsche Welle, 2022). Arrivals declined further in 2023, although the crisis did not fully end, as humanitarian concerns persisted for those stranded in border regions, and affected states maintained strict control measures.

While Belarus's coercive action destabilised the border and generated a severe humanitarian crisis, it ultimately failed as a foreign policy instrument. Minsk sought sanctions relief, political recognition, and economic concessions; however, the EU remained unified, expanded sanctions, and refused both negotiation and legitimacy. In contrast to the Finnish case, where a single state faced concentrated domestic pressure and ultimately modified its behaviour, the Belarus episode highlights the limits of coercive engineered migration when the target is a supranational actor capable of distributing political costs across multiple member states.

2.2 Cyber and Space Domain Disruption

In hybrid warfare, human and political vulnerabilities are frequently exploited, and this logic extends into the technological and spatial domains.

Relevant principles governing this sphere include state sovereignty, non-intervention, due diligence, and the prohibition of the use of force in cyberspace. In addition, space-based

assets and the air domain more broadly are central to strategic deterrence and constitute both civilian and military infrastructure across Europe and globally. In this context, the militarisation of outer space has created opportunities for both state and non-state actors to generate disruption across interconnected systems.

2.1.1 Case Study: KA-SAT Cyberattack (2022)

At the beginning of 2022, in parallel with Russia's invasion of Ukraine, a large-scale cyberattack disrupted broadband satellite internet services provided by Viasat Inc.'s KA-SAT network. The attack affected tens of thousands of modems across Ukraine and parts of Europe, disrupting connectivity for civilian, governmental, and commercial users (CyberPeaceInstitute, 2022). Following assessments by Viasat and the U.S. government, the most plausible hypothesis is that the primary objective of the attack was disruption rather than information theft. In this context, and given the timing of the operation, the likely intent was to hinder Ukrainian command and control capabilities during the initial phase of the invasion.

In the words of Victor Zhora, Chief Digital Transformation Officer at the State Service of Special Communication and Information Protection of Ukraine, "Russia is attacking not just with missiles and with bombs, but with cyber weapons" (Satter, 2022), underscoring the hybrid nature of the operation and its relevance to the principles enshrined in the Council of Europe Convention on Cybercrime (Budapest Convention).

A more detailed technical analysis attributed the disruption to malware known as *AcidRain*, designed to remotely erase modem data and render devices inoperable. However, the incident also produced spillover effects across Europe. A major German company reportedly lost remote monitoring access to over 5,800 wind turbines, while numerous French broadband users were left offline, in some cases for extended periods (Kerttunen; Schuck; Hemmelskamp, 2023).

NetBlocks, through its Cost of Shutdown Tool, recorded a significant outage across the KA-SAT network during the period of the attack, further confirming the scale of the disruption (Swinhoe, 2022).

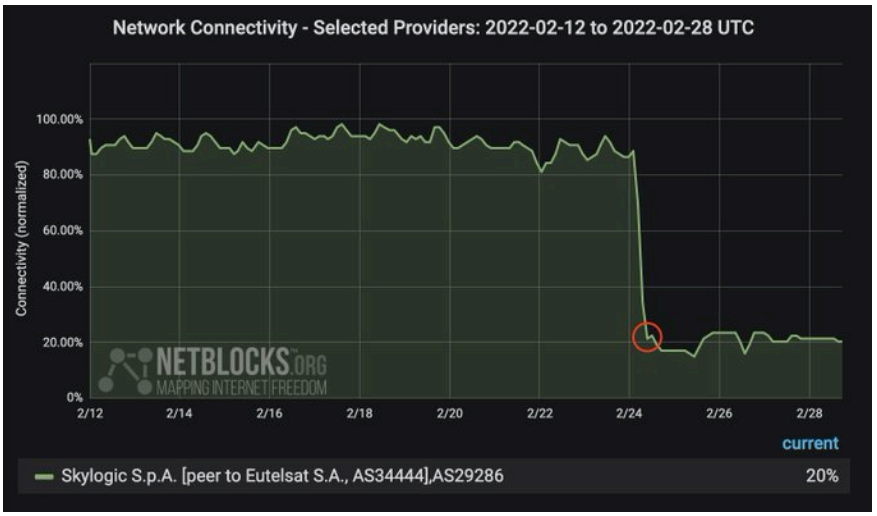

Figure 3. *Network Connectivity - Selected Providers.* Source: Netblocks (2022)

The KA-SAT incident forms part of a broader pattern of deliberate interference with civilian and commercial satellite systems. Similar activities have been recognised by both the European Union and NATO as instruments of hybrid warfare. Since 2022, European institutions and member states have recorded increased instances of jamming and spoofing against global navigation satellite systems, particularly GPS, across large parts of Europe—from the Baltic to the Black Sea. These disruptions have affected civil aviation, critical infrastructure, and government operations (Burrows, 2025).

Taken together, these developments suggest that the KA-SAT cyberattack was not an isolated incident, but part of a broader effort to undermine the reliability of space-based and satellite-enabled services on which contemporary societies increasingly depend. Large-scale cyber operations against satellite communications, combined with persistent interference in navigation systems, illustrate how modern conflict is extending into the cyber and space domains. These activities have tangible consequences for civilian populations and raise complex legal questions under international law, including issues of state responsibility and the protection of civilian infrastructure during armed conflict.

2.3 Airspace Violations and Drone Incursions

Where the KA-SAT cyberattack was characterised by limited formal attribution due to plausible deniability, recent years have seen a growing number of airspace violations and drone incursions that have produced tangible security effects across Europe, extending beyond disruptions to communications into direct challenges to national security and territorial integrity.

These drone incursions constitute violations of airspace sovereignty and are generally considered to be in breach of the principles set out in the Chicago Convention on International Civil Aviation, which establishes the foundational legal framework for international aviation law. In a broader normative context, such activities also contradict the principles of responsible state behaviour as articulated in UN General Assembly Resolution 73/266 on Advancing responsible State behaviour in cyberspace in the context of international security.

2.3.1 Case Studies: Poland and Belgium

As also indicated by NetBlocks, the consequences of drone-related incidents can extend beyond physical airspace violations to include measurable disruptions in network connectivity across affected regions (Swinhoe, 2022). In this broader context, Russian-linked incursions have reportedly contributed to localised infrastructure disruptions, including a power outage affecting Sumy, Ukraine on 8 December 2025.

Figure 4. *Network Connectivity by Region: Ukraine*. Source: Netblocks (2025)

These incidents illustrate the increasing frequency of airspace violations targeting European and neighbouring states' critical infrastructure. However, it is important to distinguish between different categories of drone incursions. In the case of Poland, numerous incidents have occurred in the context of the war in Ukraine and can be understood as cross-border, highly deniable operations aimed at testing air defence systems and probing escalation thresholds. By contrast, more recent incursions affecting several EU and NATO member states appear primarily designed to generate disruption and reinforce perceptions of insecurity, while simultaneously accelerating political momentum toward strengthening air defence capabilities (Lendon; Yee, 2025).

In response, Poland has announced plans to develop a national "drone wall", conceived as a multilayered defence system combining early detection technologies, electronic warfare capabilities (including jamming of control and navigation signals), kinetic interception systems relying on anti-drone missiles, and an integrated command-and-control architecture linked to existing artillery, reconnaissance, and air defence assets. At the European level, these incidents have also revived discussions on a broader "European drone wall", although the EU's implementation timeline remains more gradual. The EU currently aims to operationalise a networked drone defence capability by the end of 2027 (Kozatskyi, 2025).

Figure 5. *9-10 September 2025 Russian air attack on Ukraine.* Source: ППО радар - monitorwar (2025)

In parallel, visual mapping of drone and missile trajectories, such as those circulated by Polish media outlets including Telewizja Republika and political figures such as Anna-Maria Żukowska of the political party Lewica (The Left), has illustrated the pathways of aerial threats originating from Russian territory into Polish airspace during the war in Ukraine.

Belgium has also recently been affected by airspace incursions, particularly in proximity to airports and nuclear facilities, raising concerns about the broader strategic intent behind such operations. These incidents contribute to a narrative in which the Russian Federation is perceived as willing to extend the conflict deeper into European territory through incremental and deniable actions. However, while incursions in Poland are widely interpreted as linked to its logistical and political support for Ukraine, Belgium is more frequently viewed as a strategic signalling target, particularly in light of frozen Russian assets held in Brussels (Clapson, 2025).

2.4 Election Interference as a Hybrid Warfare Tool

Another important dimension of hybrid warfare that warrants analysis is election and political interference. Often described as a "test" to be faced by Western nations, hybrid warfare increasingly targets the electoral integrity of democratic systems. As noted by CYIS (2025), "election interference has evolved into a multidimensional threat, ranging from AI-generated disinformation to authoritarian states deploying cyber operatives."

Election interference can therefore be understood as a key instrument through which hybrid warfare is operationalised, shaping political processes and influencing strategic decision-making. In this context, the primary objective is often the destabilisation of democratic systems, with downstream effects including the weakening of European states and, consequently, their domestic cohesion and external policy coherence. Some scholars further argue that the ultimate aim of such interference is to disrupt domestic policy formation, thereby reducing a state's ability to act cohesively in the international arena.

Before examining empirical cases, it is important to clarify key conceptual distinctions. As J. Davies notes, election interference has long been used as a foreign policy tool, defined as "a deliberate attempt by a foreign government to change the electoral rule or the election outcome" (Bubeck and Marinov, p. 45). In fact, some estimates suggest that up to 65% of post-World War II elections have experienced some form of foreign interference, highlighting its historical prevalence. However, a distinction must be made between traditional election interference as a foreign policy instrument and what can be defined as *hybridised election interference*.

While conventional election interference may aim to influence specific policy outcomes or political alignments, hybridised election interference is embedded within a broader hybrid warfare strategy. Its primary objective is not merely influence, but structural damage: undermining institutional trust, polarising societies, and weakening a target state's long-term capacity for coherent policy implementation (Davies, 2021).

One of the most widely analysed examples of this phenomenon is Russian interference in the 2016 United States presidential election. While scholars debate the extent to which these operations influenced the final outcome, the case is particularly significant for the diversity of methods employed, including data leaks, misinformation campaigns, and targeted propaganda efforts. According to Darin Johnson, it was crucial for the United States, in the context of foreign interference, to recognise domestic societal cleavages as strategic vulnerabilities

rather than purely internal political issues. He argues that "racial division was fundamental to Russia's interference campaign" (Johnson, 2019, p. 203), with over half of Russian-linked Facebook advertisements reportedly designed to amplify racial and social divisions (Davies, 2021).

Further analysis by Keating and Schmitt suggests that while propaganda and disinformation were central tools, their effectiveness was amplified by deeper structural conditions, including ideological receptiveness within segments of the population. In particular, they highlight the role of emerging populist currents and a growing ideological affinity toward certain forms of conservatism, which created an environment in which external messaging could gain greater traction (Keating & Schmitt, 2021).

2.4.1 Case Study: Moldovan Elections (2024–2025)

Already in 2023 the Authority for European Political Parties and European Political Foundations requested an analysis on how foreign electoral interferences affect EU democratic processes. The report shows that there are three main tools used for this specific aim: financial interference, information manipulation and cyber-enabled electoral interference (Authority for European Political Parties and European Political Foundations, 2023).

Concerning Moldova, it should be underlined that the election interference had been started already in October 2024 when the first round of presidential elections occurred and carried on until September 2025, key date for the outcome of the Moldovan future. The election options have been described as a final run between the West and Russia since in 2024, together with the first round of parliamentary elections, a referendum on the possible accession to the EU was also carried out (European Parliament Research Service, 2024). Given the general framework, the pro-European candidate Maia Sandu—from the Party of Action and Solidarity (PAS)—found herself and Moldova to fight against a wave of Russian electoral interference (Freedom House, 2025).

Already in 2024, the European Parliament adopted a resolution issuing a strong warning against Russian attempts to derail Moldova's pro-European trajectory, highlighting that Russia has spent approximately €100 million to influence the outcome of Moldovan elections in favour of a more Russia-aligned government (European Parliament, 2024). According to the EU Parliament, "On 3 October 2024, Moldovan authorities uncovered a large-scale voter fraud scheme financed by Moldovan oligarch Ilan Shor, involving $15 million being transferred to 130,000 Moldovans as part of a voter bribery operation" (European Parliament, 2024). It has to be highlighted that Ilan Shor is part of the Russian oligarchic networks sanctioned by the EU, thus the money was exchanged in the black market through Turkey, the UAE and Lebanon and then recycled in Moldova, showing a clear example of financial interference (European Council, 2024; Transparency International, 2025).

On another level, information manipulation was another tactic largely used. According to Sandu, "Russia has deployed AI-enabled disinformation campaigns that fuse micro-targeting, bot networks, deepfakes, and fabricated news articles," strongly directed to target the youth through social media platforms such as TikTok (Sandu, 2025; EU DisinfoLab, 2025).

Moreover, Russia also targeted embassies and diaspora voting sites with massive vote-buying practices and bomb threats already in the first round of presidential elections in 2024 (OSCE, 2024; Reuters, 2024).

In conclusion, despite the Russian interference, Maia Sandu reached the majority necessary to win the elections; however, she warned EU officials that "Moldova may have been the testing ground but Europe was the target," well aware of the complete toolkit used by Moscow to undermine Moldova's path towards the European Union (Sandu, 2025; European Parliament, 2025).

2.5 Conclusion

Overall, the cases analysed in this chapter demonstrate that hybrid warfare in Europe operates through cumulative pressure rather than decisive blows. Migration manipulation, cyber and space disruption, airspace violations, and election interference function as mutually reinforcing tools that exploit legal ambiguity, societal divisions, and technological dependence while preserving deniability. Between 2014 and 2025, these practices did not aim at immediate territorial gains, but instead at shaping strategic environments and eroding political cohesion over time.

Looking ahead, such hybrid activities are likely to intensify and expand across additional domains, from energy systems and supply chains to information ecosystems and emerging technologies. Their gradual, cross-sectoral nature makes them difficult to detect, attribute, and counter, posing growing challenges for policymakers and existing security frameworks as threats increasingly emerge below the threshold of open conflict.

Against this backdrop, the key question is no longer only how hybrid warfare manifests in practice, but how it can be effectively identified, deterred, and countered. The following section therefore turns to the main tactics and methods currently employed by states and international organisations to respond to hybrid threats, assessing their effectiveness and limitations in an increasingly complex and multidomain security environment.

Section 3.
Tactics and Methods of Countering Hybrid Warfare

The rise of hybrid warfare as a defining feature of contemporary conflict has compelled European states to fundamentally reassess their security paradigms (European External Action Service [EEAS], 2022; North Atlantic Treaty Organization [NATO], 2022). Rather than focusing solely on the infliction of material damage or the disruption of operations, hybrid warfare is primarily designed to erode the cohesion, resilience, and trust underpinning societies and institutions from within. By systematically exploiting political, social, technological, and informational vulnerabilities, adversaries aim to generate fragmentation, undermine democratic processes, and weaken the capacity of states and organisations to respond effectively (NATO StratCom COE, 2021; EEAS, 2022).

Countering hybrid threats therefore requires more than technical or legislative adjustments; it necessitates the development of resilient societies capable of absorbing shocks, adapting to disruptive pressures, and maintaining functional integrity under sustained stress. This resilience rests on two interrelated pillars: institutional robustness and digital sovereignty (European Commission, 2020; ENISA, 2023). Institutional robustness refers to the ability of political and administrative systems to coordinate effectively, respond rapidly, and maintain legitimacy in the face of multi-domain threats. Digital sovereignty, in turn, reflects the capacity of states and regional organisations to secure critical infrastructures, control data flows, and reduce strategic dependence on external technological actors (European Commission, 2020; ENISA, 2023).

In response to the growing complexity of hybrid threats, European institutions and Member States have begun developing a multi-layered strategic approach that combines legislative innovation, technological investment, intelligence coordination, and international cooperation (EEAS, 2022; European Commission, 2023). This evolving framework seeks not only to mitigate the immediate effects of hybrid operations, but also to enhance long-term resilience against their cumulative and adaptive nature.

3.1 Protecting Critical Infrastructure

The resilience of critical infrastructure is central to mitigating the physical and systemic impacts of hybrid warfare. In this regard, the European Union's Critical Entities Resilience (CER) Directive, adopted in December 2022, represents a significant paradigm shift (European Union, 2022a). It requires Member States to conduct comprehensive risk assessments and implement robust protection measures across sectors deemed essential, including energy grids, water supply systems, transport networks, and healthcare facilities. The directive's emphasis on prevention, protection, response, and recovery reflects a holistic understanding of resilience, recognising that hybrid threats often exploit the interdependencies between these sectors (European Commission, 2023; ENISA, 2023).

For example, the sabotage of underwater cables in the Baltic Sea does not only disrupt digital communications, but can also affect energy distribution and financial transactions, producing cascading effects across economies and societies (ENISA, 2023). In response, the EU has increasingly focused on identifying vulnerabilities in critical supply chains and promoting the diversification of strategic reserves as a means of reducing systemic exposure to disruption (European Commission, 2023).

Alongside regulatory measures, the EU has also expanded its use of restrictive measures. The 2024 sanctions regime targeting individuals and entities involved in sabotage and destabilisation serves both as a deterrent and as a mechanism to disrupt ongoing hybrid campaigns (Council of the European Union, 2024). These measures are particularly relevant in the context of the weaponisation of irregular migration, where state actors exploit migratory flows as instruments of political pressure (European External Action Service [EEAS], 2023). While the long-term effectiveness of these sanctions remains difficult to assess at this stage, their strategic objective is to constrain the financial and logistical networks that enable hybrid operations, while preserving the integrity of EU asylum systems. Particular attention has also been directed towards overseas territories, which, due to their geographic isolation and limited resources, remain more exposed to cyberattacks and disinformation campaigns (European Commission, 2023).

At the operational level, recent drone incursions over sensitive sites - including military bases, ammunition depots, and NATO logistical convoys - have further exposed regulatory and capability gaps. In response, the French government is currently revising its legal framework to enable more effective neutralisation of hostile drones (Le Monde, 2025; Ministère des Armées, 2025). While larger military systems such as Iranian Shahed or Russian Geran drones can generally be detected and tracked through France's national radar network and NATO surveillance assets, the primary challenge stems from small, commercially available drones capable of evading detection and operating with relative impunity under existing legal constraints (ENISA, 2023).

At present, security forces are often limited to the use of jamming systems or firearms within restricted perimeters, and in many cases require prior authorisation from the gendarmerie, resulting in procedural delays. To address these shortcomings, the French government - under Prime Minister Sébastien Lecornu, in coordination with the Secretariat-General for Defence and National Security (SGDSN) - is developing reforms to expand engagement rules, including allowing pre-emptive neutralisation in proximity to high-risk sites and accelerating procurement procedures for counter-drone technologies such as jammers and kinetic interceptors (Ministère des Armées, 2025).

A key innovation under consideration is the 2026 deployment of the Proteus system, a 20mm anti-aircraft cannon mounted on military vehicles and equipped with thermal imaging and AI-assisted targeting, with an effective range of up to 1,500 metres (Le Monde, 2025). Germany's 2025 legal reforms permitting the Bundeswehr to shoot down threatening drones provide an important comparative precedent (Reuters, 2025), although France remains more cautious due to concerns over collateral damage and the legal constraints of peacetime operations (Reuters, 2025).

Despite the tightening of drone regulations since 2016, including mandatory registration for drones above 250 grams and electronic identification requirements for those above 800 grams, attribution and enforcement challenges persist (European Commission, 2023). Malicious actors continue to exploit increased drone range, autonomy, and spoofed identifiers to evade detection. While Denmark has publicly attributed recent airport overflights to Russian activity, France has refrained from formal attribution, citing insufficient forensic certainty and the risk of escalation through public accusation (Le Monde, 2025). Although agencies such as the DGSI and DRSD systematically investigate these incidents, public attribution remains rare, reflecting a broader strategic caution in addressing hybrid threats within ambiguous legal and evidentiary environments (EEAS, 2022).

Taken together, these measures illustrate that European counter-hybrid strategy is not based on a single defensive layer, but on a multi-level logic combining resilience-building, disruption, and deterrence-by-denial. Regulatory frameworks such as the CER Directive aim to reduce systemic vulnerability by strengthening structural resilience, while sanctions regimes and financial restrictions seek to increase the operational costs for actors engaging in hybrid activities (Council of the European Union, 2024; European Commission, 2023). At the same time, legal and operational adaptations, particularly in the field of counter-drone capabilities and engagement rules, reflect an effort to close capability gaps in real time as new threats emerge. However, a persistent feature of this approach is the tension between rapid response and legal-institutional constraint, especially in relation to attribution and escalation management (EEAS, 2022; NATO, 2022). As a result, countering hybrid warfare in Europe is best understood as an evolving and adaptive security ecosystem rather than a fixed doctrinal response.

3.2 Countering Disinformation: Legal Frameworks and Operational Responses

The manipulation of information has become a defining feature of hybrid warfare, with adversaries increasingly leveraging social media platforms, synthetic media such as deepfakes, and coordinated influence campaigns to undermine public trust and deepen societal polarisation. In response, the European Union has progressively strengthened its regulatory architecture through instruments such as the Digital Markets Act (DMA) and the Digital Services Act (DSA). These frameworks impose stricter obligations on online platforms to monitor, mitigate, and report the dissemination of disinformation, particularly in cases involving systemic risks to democratic processes.

Among their key provisions are enhanced transparency requirements for political advertising, obligations for the rapid removal of verified illegal or harmful content, and the introduction of mechanisms enabling users to flag manipulative material. However, enforcement remains a significant challenge, particularly in relation to large, predominantly US-based platforms. The effectiveness of these measures is constrained by the scale and velocity of online content, the complexity of cross-border regulatory coordination, and the substantial technical and institutional resources required to identify and counter coordinated influence operations. The establishment of specialised bodies such as the European Digital Media Observatory has therefore been instrumental in strengthening the EU's capacity to detect, analyse, and respond to foreign information manipulation and interference (FIMI). Overall, these developments reflect an ongoing attempt to close regulatory gaps while balancing operational effectiveness with fundamental rights considerations, particularly freedom of expression.

Alongside legal instruments, operational responses play a crucial role in countering disinformation campaigns. National and European agencies increasingly rely on public attribution and technical reporting to expose ongoing influence operations. For instance, the French counter-disinformation agency VIGINUM has published detailed analyses of pro-Russian and other state-linked campaigns, documenting their tactics, techniques, and procedures. Similarly, the exposure of the "CopyCop" operation, linked to Russian intelligence, highlighted the use of extensive networks of fake news websites and coordinated social media accounts designed to amplify polarising narratives across Europe.

These forms of public attribution serve multiple strategic purposes. They not only increase public and institutional awareness of ongoing manipulation efforts but also contribute to the creation of evidentiary records that can support future regulatory or sanction-based responses. In addition, enforcement tools under the DSA, including the suspension of accounts and the

imposition of financial penalties on non-compliant platforms, provide further leverage to reduce the reach and effectiveness of coordinated disinformation campaigns. Taken together, these measures illustrate a dual-track approach in which regulatory governance and operational exposure work in tandem to limit the strategic impact of information-based hybrid threats.

3.3 Building Cyber Resilience: Policy, Technology, and Training

The manipulation of information has become a defining feature of hybrid warfare, with adversaries increasingly leveraging social media platforms, synthetic media such as deepfakes, and coordinated influence campaigns to undermine public trust and deepen societal polarisation (NATO StratCom COE, 2021; European External Action Service [EEAS], 2022). In response, the European Union has progressively strengthened its regulatory architecture through instruments such as the Digital Markets Act (DMA) (Regulation (EU) 2022/1925) and the Digital Services Act (DSA) (Regulation (EU) 2022/2065). These frameworks impose stricter obligations on online platforms to monitor, mitigate, and report the dissemination of disinformation, particularly in cases involving systemic risks to democratic processes (European Commission, 2023).

Among their key provisions are enhanced transparency requirements for political advertising, obligations for the rapid removal of verified illegal or harmful content, and the introduction of mechanisms enabling users to flag manipulative material. However, enforcement remains a significant challenge, particularly in relation to large, predominantly US-based platforms. The effectiveness of these measures is constrained by the scale and velocity of online content, the complexity of cross-border regulatory coordination, and the substantial technical and institutional resources required to identify and counter coordinated influence operations (EEAS, 2022; European Commission, 2023). The establishment of specialised bodies such as the European Digital Media Observatory (EDMO) has therefore been instrumental in strengthening the EU's capacity to detect, analyse, and respond to foreign information manipulation and interference (FIMI) (European Commission, 2023). Overall, these developments reflect an ongoing attempt to close regulatory gaps while balancing operational effectiveness with fundamental rights considerations, particularly freedom of expression.

Alongside legal instruments, operational responses play a crucial role in countering disinformation campaigns. National and European agencies increasingly rely on public attribution and technical reporting to expose ongoing influence operations. For instance, the French counter-disinformation agency VIGINUM has published detailed analyses of pro-Russian and other state-linked campaigns, documenting their tactics, techniques, and procedures (VIGINUM, 2023). Similarly, the exposure of the "CopyCop" operation, linked to Russian intelligence, highlighted the use of extensive networks of fake news websites and coordinated social media accounts designed to amplify polarising narratives across Europe (NATO StratCom COE, 2024).

These forms of public attribution serve multiple strategic purposes. They not only increase public and institutional awareness of ongoing manipulation efforts but also contribute to the creation of evidentiary records that can support future regulatory or sanction-based responses. In addition, enforcement tools under the DSA, including the suspension of accounts and the imposition of financial penalties on non-compliant platforms, provide further leverage to reduce the reach and effectiveness of coordinated disinformation campaigns (European Commission, 2023). Taken together, these measures illustrate a dual-track approach in which

regulatory governance and operational exposure work in tandem to limit the strategic impact of information-based hybrid threats.

3.4 Strengthening EU-NATO Cooperation: A Unified Front Against Hybrid Threats

The transnational nature of hybrid warfare necessitates a coordinated response from international organisations. The strategic partnership between the European Union and NATO, formalised through successive joint declarations and structured dialogues, has become increasingly vital in addressing hybrid threats (European Council, 2016, 2018, 2023; NATO, 2022). This cooperation reflects a shared recognition that hybrid threats cut across internal and external security domains, requiring integrated responses that combine civilian, military, and informational tools.

Initiatives such as the Parallel and Coordinated Exercises (PACE) framework enable both organisations to test their resilience and response mechanisms in simulated hybrid crisis scenarios. These exercises are designed to improve interoperability, enhance crisis coordination, and identify gaps in joint response capabilities under conditions of ambiguity and multi-domain pressure (NATO StratCom COE, 2021). This cooperation is particularly important for supporting countries on the EU's eastern flank, such as Moldova, Ukraine, and Georgia, which face persistent hybrid threats from regional adversaries (European External Action Service [EEAS], 2023).

By aligning their strategies, the EU and NATO can leverage their respective strengths: the EU's regulatory, legal, and economic instruments complement NATO's military, deterrence, and intelligence capabilities (NATO, 2022; EEAS, 2022). This synergy enhances the collective ability to deter hybrid aggression, attribute malicious activities, and respond effectively to crises. The partnership also facilitates the sharing of best practices and the development of common standards, ensuring that all Member States are equipped to counter hybrid threats in a cohesive and coordinated manner.

Section 4.
Hybrid Warfare as Part of the Strategic Plan of State Actors

Figure 6. *The New Battlefront: Hybrid Warfare in Europe (2014–2025).*
Source: Original illustration created by the author using Google NotebookLM.

The growing reliance on hybrid forms of conflict is rooted in a deep dissatisfaction with the post–Cold War liberal order, which has been increasingly contested in contemporary strategic competition (European External Action Service [EEAS], 2022). States that benefited materially from integration into this system while rejecting its normative and institutional constraints have increasingly turned to indirect, sub-threshold strategies to contest it (NATO StratCom COE, 2021). Hybrid warfare thus emerges not as an ad hoc tactic but as a strategic response to an order perceived as structurally biased and politically restrictive (EEAS, 2022).

This section first outlines this logic and the strategic reasoning underpinning it, before turning to Russia as the most immediate and operationally significant case for Europe, where these dynamics translate into sustained pressure on security, institutions, and political cohesion (NATO, 2022).

4.1 Structural Dissatisfaction with the Post–Cold War Liberal Order

The post-1991 international system was marked by the end of the Cold War and the emergence of a liberal, "rules-based" global order underpinned by American hegemony (European External Action Service [EEAS], 2022). With the collapse of the Soviet Union, the Eastern Bloc, formerly led by Moscow, lost its position at the forefront of great power competition, leaving the United States and its allies in a dominant strategic position (NATO, 2022).

In the aftermath of the Second World War, the victorious powers, the United States and the Soviet Union, had already emerged as the principal architects of the international system,

entering into a prolonged period of strategic rivalry known as the Cold War. Although this competition never escalated into direct large-scale conflict between the two powers, it was characterised by sustained geopolitical tension and a series of proxy wars across multiple regions.

To stabilise the international system and foster interdependence among states, a number of international organisations were established during this period. Institutions such as the United Nations (UN), the World Trade Organization (WTO), and the World Health Organization (WHO) were intended to provide frameworks for cooperation, reduce the likelihood of conflict, and embed states within a shared system of governance (WTO, 2020; United Nations, 2021).

Over time, a prevailing assumption emerged that integrating rival powers into these institutions would encourage their gradual alignment with liberal norms and reduce systemic competition. This approach was particularly evident in the case of China, which gained recognition within the United Nations in 1971 and later joined the World Trade Organization in 2001 (WTO, 2020). Increased economic integration, the movement of people, and deepening trade relationships were expected to anchor states within the liberal order, thereby reinforcing stability while facilitating the diffusion of Western political and economic values (EEAS, 2022).

However, the structure of these institutions, and the broader global order they supported, has been largely shaped by Western norms and standards, reflected in the dominance of the US dollar as the world's primary reserve currency and the centrality of Western-developed financial infrastructure such as the SWIFT payment system (NATO, 2022). This is also evident in the concentration of key standard-setting bodies, credit rating agencies, and major investment institutions within the West.

From the perspective of states such as Russia and China, this system has conferred a structural advantage on Western powers while placing others at a relative disadvantage (EEAS, 2023). Following the collapse of the Soviet Union, the expansion and consolidation of this liberal order proceeded with limited resistance, reinforcing the predominance of Western norms in international relations.

Consequently, the post-Cold War environment, characterised by the erosion of a more multipolar balance and the consolidation of Western-led institutions, has contributed to growing dissatisfaction among revisionist powers. This discontent has, in part, driven states such as Russia and China to challenge and undermine the existing order, increasingly employing asymmetric tools, including hybrid warfare, to contest Western influence and reshape the international system (NATO StratCom COE, 2021; EEAS, 2022).

4.2 Reaping the Benefits of the Established Order While Building Alternatives

In seeking to challenge the liberal international order, Russia and China have not operated outside it, but rather within it, leveraging its structures to strengthen their own positions while simultaneously laying the groundwork for alternative frameworks (European External Action Service [EEAS], 2022; NATO, 2022). This strategy is particularly evident in China's post-1978 reform trajectory under Deng Xiaoping, which prioritised economic integration and positioned China as a central node in the globalisation process. Over time, China developed into the world's primary manufacturing hub, combining low-cost labour with export-driven growth to secure a critical role in global supply chains, particularly following

its accession to the World Trade Organization in 2001 (WTO, 2020).

Russia pursued a parallel, though distinct, pathway. After a protracted accession process, it joined the World Trade Organization in 2012. In the intervening period, Russia consolidated its economic influence through the export of hydrocarbons, becoming a major supplier of oil and gas, particularly to Europe (NATO, 2022). By embedding itself within global energy markets, Russia was able to exploit interdependence within the international system, using trade relationships to generate state revenue while reinforcing its domestic political model and strategic autonomy.

In both cases, integration into the post-Cold War global economy enabled Russia and China to accumulate wealth, expand state capacity, and deepen their influence, all while maintaining and, in some respects, strengthening illiberal governance structures (EEAS, 2023). Rather than converging with liberal norms, these states used the system's openness to pursue their own geopolitical objectives, including efforts to contest and reshape the Western-led order.

A key manifestation of this shift towards a more multipolar vision of global governance has been the emergence of alternative multilateral groupings. The formation of BRICS in 2009, comprising Brazil, Russia, India, and China, and later joined by South Africa in 2011, represented an early attempt to institutionalise cooperation among major non-Western powers. The group has since expanded into "BRICS+", incorporating additional states such as Egypt, the United Arab Emirates, Ethiopia, Iran, and others, reflecting a broader effort to amplify the voice of the so-called "Global South" within international politics (EEAS, 2023).

Beyond political coordination, BRICS has also sought to replicate and compete with existing Western-led financial institutions. The establishment of the New Development Bank serves as a notable example, providing development financing with fewer political conditions than institutions such as the World Bank (NATO StratCom COE, 2021). This reflects a broader strategy of adapting the institutional logic of the liberal order to create parallel structures aligned with alternative norms and priorities.

Complementing these efforts is the Shanghai Cooperation Organization, founded in 2001 by China, Russia, and several Central Asian states. Initially focused on regional security and coordination, the organisation has expanded significantly, with members including India, Pakistan, and Iran. It has provided a platform for advancing strategic initiatives, most notably China's Belt and Road Initiative, while reinforcing non-Western approaches to governance, sovereignty, and regional order (NATO StratCom COE, 2021).

Taken together, these developments illustrate a dual-track strategy: participation in the existing international system to extract economic and political benefits, alongside the gradual construction of alternative institutions designed to reflect and promote non-Western norms. Through this approach, Russia and China are not only contesting Western dominance but actively contributing to the evolution of a more fragmented and multipolar global order (EEAS, 2022; NATO, 2022).

Forum name	First meeting	Policy focus	Participants
China Development Forum	2000	Economic development	Government representatives, international organization representatives, academics
Boao Forum for Asia	2002	Regional economics, trade, integration	Governments of 26 Asian and Pacific countries
Beijing Xiangshan Forum	2006	Global and Asia-Pacific security and defence	Defence ministers, chiefs of staff, military officials from Asian and Pacific countries
Beijing Forum on Human Rights	2008	Human rights	Government representatives, civil society, academics
World Peace Forum	2012	Global security and peacebuilding	Former heads of state, government representatives, academics, civil society
World Internet Conference	2014	Internet governance, cybersecurity, information technology	Government representatives, business, civil society
Belt and Road Summit	2016	Economic development, investment	Government representatives, business, civil society
South-South Human Rights Forum	2017	Human rights	Government representatives, civil society, academics
COVID-19 Vaccine Cooperation Forum	2021	Global vaccine access and health	Government representatives, including health ministers, international organization representatives, vaccine manufacturers
Global Human Rights Governance Forum	2023	Human rights	Government representatives, civil society, academics

Figure 7. *China-sponsored transnational policy forums.* Source: Stephen (2025).

4.3 Weakening the established order

These efforts ultimately converge on a single strategic objective: the gradual weakening of the existing liberal international order (European External Action Service [EEAS], 2022; NATO, 2022). This is pursued through the expansion of influence and the promotion of an alternative, illiberal vision of state sovereignty, one that rejects supranational constraints and minimises institutional checks on state power. This constitutes the first pillar of a broader revisionist strategy aimed at reshaping global governance (EEAS, 2023). The second pillar is the use of hybrid warfare and systemic disruption to erode the effectiveness and legitimacy of existing institutions (NATO StratCom COE, 2021).

Such disruption operates across a spectrum, often within the "grey zone" between peace and open conflict, but also through the formal mechanisms of the international system itself (NATO, 2022). One notable example is the strategic use of veto power within the United Nations Security Council by Russia and China. Since the mid-2000s, there has been a marked increase in both the frequency and coordination of veto usage, reflecting a shift away from earlier patterns of cautious multilateral engagement toward a more assertive, obstructionist posture (United Nations, 2021). This behaviour limits the ability of international institutions to function effectively, undermining their credibility and reinforcing perceptions of systemic paralysis.

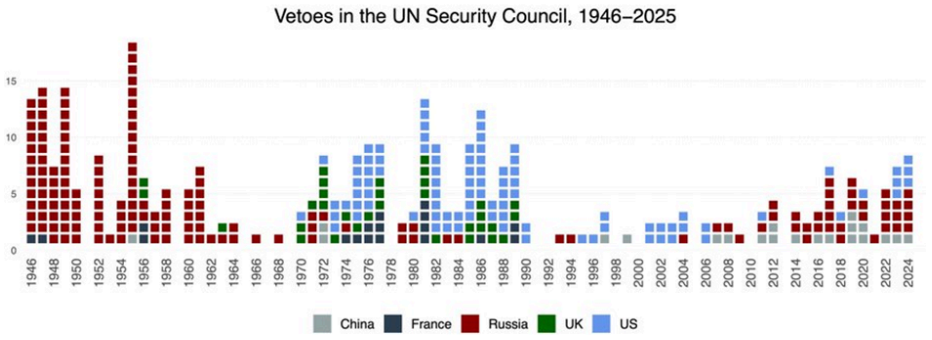

Figure 8. *Vetoes in the UNSC, 1946-2025.* Source: Lundgren (2025)

In parallel with efforts to build alternative multilateral frameworks, these actions allow revisionist states to project power and position themselves as credible challengers to Western dominance. Disrupting the current order, however, requires more than obstruction—it necessitates demonstrating both one's own capabilities and the vulnerabilities of others. This is pursued through a wide range of hybrid tactics, including attacks on critical infrastructure (such as submarine cables), cyber and digital disruption, and covert operations conducted within foreign territories (NATO, 2022).

Examples of such activities include symbolic or psychological operations, as well as more direct actions, including targeted assassinations such as the poisoning of Sergei and Yulia Skripal, which has been formally attributed by UK and allied investigations to Russian state actors. Additionally, probing actions designed to test state responses, such as irregular cross-border incursions or unconventional aerial activities, serve to expose weaknesses in national resilience and crisis management systems (NATO StratCom COE, 2021).

At the political level, one of the most consequential tools of disruption has been interference in democratic processes. Efforts to influence elections, shape public discourse, and amplify societal divisions represent a direct challenge to the principle of popular sovereignty and the liberal democratic model (European External Action Service [EEAS], 2023). In Europe, Russia has also been linked to networks of Eurosceptic political movements, in some cases extending to financial support for parties such as the National Rally, thereby seeking to fragment political cohesion within the European Union.

Economic coercion constitutes another key instrument. China, in particular, has demonstrated a willingness to employ retaliatory measures against states whose policies contradict its strategic narratives. For example, following Lithuania's decision to deepen ties with Taiwan, Beijing imposed trade restrictions aimed at deterring similar actions by other countries (EEAS, 2022). More broadly, China has leveraged its dominance in critical supply chains, especially rare earth elements, to exert pressure on larger economies, signalling the potential costs of political divergence (NATO, 2022).

While the use of unilateral sanctions and coercive economic tools is not unique to Russia and China, their application in this context reflects a broader rejection of liberal norms governing international conduct. Such measures constrain the ability of states, particularly smaller ones, to pursue independent foreign policies without facing economic or political retaliation, thereby reinforcing a more hierarchical and power-centric vision of the international system.

4.4 Russia and the Strategic Logic of Hybrid Warfare

Illiberal powers dissatisfied with the post-Cold War liberal order have increasingly turned to alternative instruments to reshape norms, institutions, and influence structures. Russia stands at the centre of this trend. As scholars note, Moscow views the liberal order as both restrictive and eroding, and therefore seeks to contest it through tools that maximise ambiguity while minimising the risk of escalation (EEAS, 2022; NATO, 2022). Hybrid warfare has become its primary foreign-policy instrument, allowing the Kremlin to project power beyond its material limits and compensate for conventional weaknesses. Operating below the threshold of open conflict enables Russia to sustain continuous strategic pressure, test the cohesion of EU and NATO members, and exploit domestic political vulnerabilities inside adversary states (NATO, 2022). In this sense, hybrid warfare is not an auxiliary tactic but a structural component of Moscow's long-term ambition to reshape the European security environment.

The use of a combination of hybrid warfare techniques - that is, measures which, due to their non-conventional nature, do not amount to direct acts of war but nevertheless destabilise their targets - lies at the core of the Russian Federation's foreign policy and strategic objectives. Citing Surkov, long-term advisor to President Vladimir Putin, Wojnowski (2022) reports that the pursuit of an expansionist foreign policy was framed as a matter of survival for the Russian Federation, while simultaneously serving to alleviate domestic social tensions. According to Surkov, Russia's expansionist posture relies on "projecting chaos" onto neighbouring states, thereby enabling internal consolidation and the creation of divisions among external actors. The West is not blind to this approach. The NATO 2030 report identifies Russia as the primary threat to the Alliance's security and stability, highlighting how Moscow has engaged not only in military activity but also in the systematic use of unconventional means to undermine cohesion within NATO (NATO 2030, p. 25).

For over a decade, Russia's strategic objectives have remained consistent: divert attention, fracture alliances, and destabilise the internal cohesion of states it perceives as strategic competitors. To this end, the Kremlin deploys a diversified toolkit encompassing drone incursions, engineered migration flows, cyber and information operations, and interference in political processes. Together, these instruments form an integrated web of hybrid strategies designed to exploit vulnerabilities across multiple domains (Wojnowski, 2022, pp. 267–268).

To further illustrate Russia's reliance on non-kinetic actions, often referred to as active measures, Russian military officials themselves emphasise that the centre of gravity of modern conflict has shifted toward the integrated use of so-called non-military means, the scope of which is virtually unlimited (Wojnowski, 2022, p. 282). As this report has shown, while Moscow is directly engaged in military operations in Ukraine, it simultaneously targets the European Union across multiple domains, including disinformation campaigns, cyberattacks, airspace violations affecting critical infrastructure, and the exploitation of migration flows as a tool of political destabilisation.

These strategic premises help explain why hybrid warfare has become particularly attractive to Moscow and why it has proven so effective in practice.

Why is hybrid warfare so strategically relevant for Russia, and why does it work so well?

1. *It compensates for structural weaknesses*

Unconventional forms of warfare have often been employed in asymmetrical contexts as force multipliers. Their appeal lies partly in lower economic costs and partly in their effectiveness, as such means are difficult to counter using conventional response mechanisms (Chivvis, 2017, p. 2). In the case of Russia, this logic still partially applies. Conducting cyber operations, political disinformation campaigns, or exploiting pre-existing migration flows is far less costly than deploying large-scale conventional forces across borders. In this sense, hybrid warfare allows Russia to economise the use of force while maintaining strategic pressure.

2. *It fits Russia's historical intelligence tradition*

Russia's reliance on hybrid instruments also reflects a deeply embedded intelligence tradition. Long before "hybrid warfare" entered Western strategic vocabulary, Moscow employed *aktivnye meropriyatiya* (active measures)—covert operations designed to blur attribution, manipulate political environments, and undermine adversaries without triggering direct

confrontation (Wojnowski, 2022, pp. 267–268). Contemporary hybrid operations modernise these methods through digital networks, private military intermediaries, and large-scale information manipulation. This continuity reflects a strategic culture that has consistently favoured ambiguity and indirect action as central tools of statecraft (Clark, 2020, p. 13).

3. *It exploits vulnerabilities inherent to open societies*

Hybrid tactics are particularly effective because they target fault lines that liberal democracies cannot easily seal. As Greenhill explains, open societies possess inherent pressure points, political polarisation, humanitarian obligations, and pluralistic information environments, that hostile actors can exploit at relatively low cost (Greenhill, 2010). Russia leverages precisely these characteristics through disinformation, cyber operations, and the amplification of domestic political divides.

4. It operates below the threshold of war, complicating response

A defining advantage of Russia's hybrid approach lies in its ability to remain below the formal threshold of armed conflict. By calibrating operations just short of what would trigger NATO Article 5 responses, Moscow exploits legal ambiguity and political hesitation (NATO, 2022). Sub-threshold actions such as cyber intrusions, GPS jamming, and disinformation campaigns generate sustained pressure without triggering collective military retaliation.

4. *It creates a cumulative, multi-domain effect*

Hybrid operations derive strength from convergence. Russia synchronises actions across cyber, information, energy, and political domains so that each reinforces the others. The resulting effect is cumulative rather than linear, overwhelming adversaries' ability to compartmentalise crises.

4.5 Conclusion

Russia conceptualises hybrid warfare not merely as a set of methods, but as a form of conflict in its own right (Clark, 2020, p. 13). European and Western actors often underestimate Moscow's objectives by classifying hybrid activities as actions falling just below the threshold of war. However, viewed through Russian strategic thinking, hybrid warfare encompasses both indirect active measures and selective forms of direct confrontation aimed at destabilising and undermining adversaries. The European Union's vulnerability to such operations - stemming from its democratic nature and the interconnection of political, economic, and informational systems - renders this multifaceted threat particularly difficult to detect and mitigate. From Moscow's perspective, hybrid warfare therefore represents an optimal instrument for generating instability and projecting influence.

Section 5.
Building Civil Resilience & Response

The capacity of societies to withstand and adapt to hybrid threats hinges on the resilience of their civilian infrastructure, the preparedness of their institutions, and the engagement of their citizens. Unlike traditional military conflicts, hybrid warfare targets the fabric of daily life, disrupting essential services, manipulating information, and exploiting societal vulnerabilities (NATO, 2022; European External Action Service [EEAS], 2022). Building civil resilience therefore requires combining the protection of critical civilian services, the enhancement of public awareness, and the empowerment of local communities. This strategy ensures that societies can absorb shocks, maintain operational continuity, and recover swiftly from disruptions, whether they originate from cyberattacks, sabotage, or disinformation campaigns (EEAS, 2023).

Looking at the latest geopolitical and international developments, covering several crises of any kind, one might say it was a matter of time before, on both a national and international level, societies were forced to confront the issue of crisis management and civilian resilience.

5.1 Civilian Resistance on a NATO level

At the end of 2024, NATO increasingly framed its strategic posture in terms of a "wartime mindset" (Martisiute, 2025), particularly in response to persistent hybrid incidents affecting the Baltic region and critical infrastructure in Northern Europe. This shift reinforces the importance of Article 3 of the North Atlantic Treaty, which states that: "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack." (North Atlantic Treaty, Article 3). This reflects a broader recognition that deterrence and defence must be complemented by civilian preparedness as part of a comprehensive resilience framework (NATO, 2022).

According to NATO doctrine, military efforts in deterrence and defence must coexist with and be reinforced by civilian preparedness, structured around three core pillars: continuity of government, continuity of essential services to the population, and civil support to military operations (NATO, 2022). The NATO Resilience Committee, established in 2022, provides strategic and policy direction for these efforts, building on developments initiated after the 2016 Warsaw Summit and further consolidated under the NATO 2030 Agenda, which places strong emphasis on societal resilience against hybrid and systemic threats. As part of this agenda, Allies committed to strengthening national resilience objectives and integrating them into defence planning, a process further advanced at the 2024 Washington Summit through the formal inclusion of civilian preparedness in national and collective defence frameworks (NATO, 2024). The NATO 2030 framework also identifies a range of strategic risks to Alliance stability, including Emerging and Disruptive Technologies and hybrid warfare, which are increasingly central to the threat landscape (NATO, 2030).

5.1.1 Protecting Essential Civilian Services: Safeguarding the Backbone of Society

The resilience of civilian services - such as communication networks, transportation systems, and energy grids - is fundamental to mitigating hybrid threats. Many of these services rely on

satellite and GPS infrastructure, which has increasingly been targeted by electronic warfare and cyber operations across Europe. Recent GPS jamming incidents have demonstrated how such disruptions can affect not only military systems but also civilian aviation, maritime navigation, and logistics chains.

To counter these vulnerabilities, European states have prioritised strengthening satellite-dependent infrastructure through redundancy systems, encrypted communications, and diversification of navigation technologies. The European Union's broader resilience approach, particularly under its critical infrastructure protection framework, emphasises reducing single points of failure across interconnected systems (EEAS, 2022).

The energy sector has also become a focal point for resilience efforts due to its exposure to sabotage and hybrid disruption risks. Past incidents affecting infrastructure in parts of Southern France have illustrated the potential for cascading failures across dependent systems. Similarly, railway networks, critical for both civilian mobility and military logistics, have seen increased investment in monitoring systems and rapid response capabilities. These measures aim to ensure continuity of essential services even under conditions of disruption or attack.

5.1.2 Enhancing Interoperability: A Networked Approach to Resilience

Resilience depends not only on the robustness of individual systems but also on the interoperability of institutions, providers, and infrastructures. Hybrid threats often exploit systemic interdependencies between energy, transport, and digital networks. In response, European initiatives have focused on improving coordination mechanisms across public and private stakeholders.

The European Union Agency for the Space Programme (EUSPA) plays a key role in this context by supporting standardised protocols for responding to disruptions in satellite navigation systems, in cooperation with national authorities and private operators. This reflects the EU's broader approach to resilience-building through institutional coordination and shared standards (EEAS, 2023).

Interoperability is further reinforced through civil-military cooperation frameworks, including exercises under the EU Civil Protection Mechanism. These exercises test coordination between emergency services, infrastructure operators, and defence structures, identifying bottlenecks and improving crisis response capacity. The objective is to ensure that failures in one domain do not cascade into systemic breakdown, but instead trigger coordinated adaptive responses across institutions.

5.1.3 Crisis Preparedness and Public Awareness: Empowering Citizens as First Responders

Public awareness and preparedness are central to resilience against hybrid threats, which often directly affect civilian populations through service disruptions or information manipulation. As such, several European states have developed national preparedness strategies aimed at strengthening individual and household readiness.

Sweden's *Om krisen eller kriget kommer* ("If Crisis or War Comes"), originally published in 2018 and updated in 2023, is widely cited as a leading model. It encourages citizens to maintain emergency supplies, develop contingency plans, and prepare for prolonged

disruptions such as power outages or communication failures. The 2023 update explicitly incorporates hybrid threats, reflecting the evolving security environment. Similar approaches have been adopted in Finland (*Varautumisopas*) and Norway (*Beredt på det uforutsette*), both of which integrate cyber threats, disinformation, and infrastructure disruption into civilian preparedness guidance.

France has also introduced its own preparedness framework through *Se préparer aux situations d'urgence* (SGDSN, 2023; updated 2024), reinforcing the importance of resilience planning at the household and community level. These initiatives collectively aim to foster a culture of preparedness and situational awareness among citizens.

Local communities further strengthen this resilience architecture. Grassroots initiatives, including neighbourhood preparedness schemes and local reporting networks, enhance situational awareness and reduce response times to potential sabotage or disruption. This bottom-up dimension contributes to social cohesion and reduces the effectiveness of hybrid tactics aimed at exploiting societal fragmentation.

5.1.4 Empowering Local Actors: Combating Information Manipulation at the Grassroots Level

Information manipulation represents one of the most persistent dimensions of hybrid warfare, targeting trust in institutions and amplifying societal polarisation. Local actors, including journalists, educators, and municipal authorities, play a critical role in identifying and countering disinformation.

Capacity-building programmes, often developed in cooperation with fact-checking organisations and media literacy initiatives, equip local stakeholders with tools to detect false narratives and verify information sources. In France, collaboration between public broadcasters and Viginum, the national agency against foreign information manipulation, supports real-time monitoring and response to disinformation campaigns. In Germany, public broadcasting institutions cooperate with security agencies to analyse and expose coordinated influence operations.

During electoral periods, several European states have developed specialised coordination mechanisms. Estonia, for example, integrates electoral authorities with cybersecurity institutions and NATO-linked centres of expertise to monitor and counter foreign interference attempts. These frameworks reflect a broader trend toward institutionalised, cross-sectoral resilience against hybrid information threats.

At the EU level, preparedness and resilience policy has been further reinforced through initiatives promoted by Commissioner Hadja Lahbib, who outlined six strategic priorities: strengthening crisis management, improving infrastructure resilience, developing resilient communities, enhancing digital resilience, increasing cooperation on hybrid threats, and fostering a culture of preparedness (EPRS, 2025).

5.2 Civilian Resistance on an EU level

As shown in recent EU survey data, approximately 65% of EU citizens report feeling unaware of the steps to take in the event of a crisis. This highlights a structural gap in civilian preparedness and reinforces the need for coordinated EU-level planning to strengthen resilience and crisis response capacity (Eurobarometer, 2024). One might argue that

addressing this awareness gap is essential for ensuring that preparedness strategies are not limited to institutional frameworks but extend to the level of citizens and households.

Already in October 2024, the EU President of the Commission, Ursula Von der Leyen, requested a report on how to enhance Europe's civilian and defence preparedness, to the former Finnish President Sauli Niinistö, her special advisor at the time. The report, today known as Niinistö's report "Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness" is considered the precursor of the Preparedness Union Strategy, presented at the EU Parliament in April 2025.

In addition, the EU has also implemented during the years some protection mechanisms to hybrid attacks, highlighting they represent a threat to democracy. Showing an increasing effort throughout the years, in 2022 the EU had approved a "EU hybrid toolbox" aiming to help identify complex and multifaceted hybrid campaigns and to coordinate tailor-made and cross-sectoral responses, while in 2024 the Council approved an EU hybrid response team, and later on, also Integrated Political Crisis Response (IPCR) arrangements in case of a major response to a complex crisis.

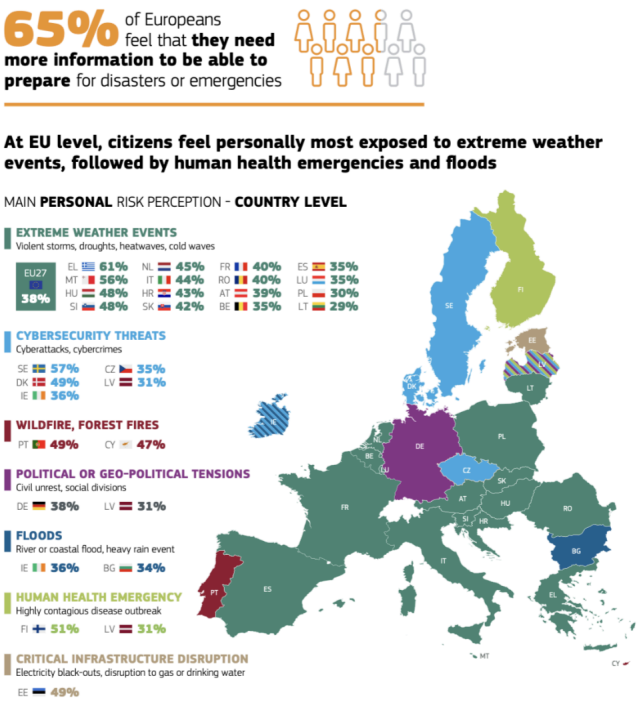

Figure 9. *Personal risk perception of disaster types at the EU and country level.*
Source: European Commission (2024, p. 2).

In the meantime, the civilian resilience has been improved by enhancing several steps, such as: fighting disinformation in light of protecting democratic elections while not censoring democratic debate, reduce vulnerabilities of the critical infrastructures, security of network and information systems with a new directive called "NIS2" to improve the resilience of both the private and public sector with regards to hybrid attacks, working with strategic partners such as NATO and finally supporting partners in fighting hybrid attacks.

5.3 Case-study: Estonia

In contemporary security environments, NATO Article 3 obligations, to maintain and develop individual and collective capacity to resist armed attack, extend beyond traditional military capabilities to include civilian resilience, encompassing continuity of government, protection of critical infrastructure, cyber defence, economic endurance, and societal preparedness (NATO, 2022).

Estonia, a small Baltic state in Northern Europe with a population of approximately 1.37 million, regained independence from the Soviet Union in 1991 and joined both NATO and the European Union in 2004 (Ministry of Foreign Affairs of Estonia, 2025). It represents one of the most illustrative examples of how NATO Article 3 can be operationalised through a legally grounded, whole-of-government and whole-of-society approach to civilian resilience.

5.3.1 Legal and Institutional Foundations of Civilian Resilience

Estonia's civilian resilience framework is anchored in the Emergency Act (*Hädaolukorra seadus*), which establishes the legal basis for crisis prevention, emergency management, and continuity of vital services (Government of Estonia, Emergency Act). The Act assigns clear responsibilities across ministries, municipalities, and private operators of essential services, reflecting NATO baseline requirements for civil preparedness.

Estonia is currently strengthening this framework through the draft Civil Crisis and National Defence Act, which aims to further integrate civilian crisis management with national defence planning. This reflects an understanding of resilience as a continuum spanning peacetime, crisis, and armed conflict, consistent with NATO's comprehensive approach to security (NATO, 2022).

5.3.2 Cyber Resilience – a Core National Security Function

Cyber resilience is a central pillar of Estonia's national security strategy. Following the 2007 cyberattacks, Estonia institutionalised cybersecurity as a core state function. The Cybersecurity Act and the Cybersecurity Strategy 2024–2030 provide a structured framework based on prevention, preparedness, response, and recovery (Ministry of Economic Affairs and Communications, 2024).

Implementation is coordinated by the Estonian Information System Authority (RIA), responsible for protecting critical information infrastructure and managing national cyber incident response. Estonia also hosts the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), reinforcing the link between national cyber resilience and NATO collective defence.

Cyber resilience is reinforced through education and societal preparedness. Cybersecurity education is integrated into school curricula, while national tools such as Cybertest assess digital competencies across populations (Estonian Information System Authority). Public awareness campaigns on cyber hygiene further support resilience by improving citizen-level preparedness (Government of Estonia).

Public–private cooperation is a defining feature of Estonia's model, particularly given that much critical infrastructure is privately operated. Structured information-sharing mechanisms and joint cyber exercises enhance coordination between state and industry actors. Trust in digital governance is further reinforced through the X-Road system, which enables citizens to monitor access to their personal data by public institutions, strengthening transparency and accountability.

5.3.3 Civil Defence, Infrastructure, Exercises, and Climate Resilience

Estonia is also strengthening its physical civil defence infrastructure. The Estonian Rescue Board has begun marking public shelters, while legal reforms require shelters in new large public buildings (Estonian Rescue Board). In addition, resilience centres equipped with backup power and essential supplies are being developed to support communities during prolonged disruptions.

A key institutional actor is the Estonian Stockpiling Agency, established in 2021, which manages national reserves of critical goods such as fuel, food, and medical supplies to ensure continuity during crises (Estonian Stockpiling Agency).

These systems are tested through large-scale civil crisis exercises, most notably CREVEX. The 2023 iteration simulated cascading crises involving energy disruptions, cyber incidents, and information operations, involving ministries, municipalities, and private operators (Government Office of Estonia, 2023). Such exercises operationalise the Emergency Act and ensure interoperability across sectors.

Climate change is also integrated into Estonia's resilience planning as a risk multiplier. Flood warning systems and continuous monitoring frameworks are embedded within national emergency preparedness structures, particularly in high-risk regions such as Pärnu (Environmental Portal, 2026).

Conclusion

Hybrid warfare has become a defining characteristic of the contemporary European security environment. As this publication has shown, it is not a discrete category of conflict, but a strategic approach that integrates multiple tools - informational, economic, cyber, and physical - designed to exploit vulnerabilities while remaining below the threshold of conventional war. The deliberate blurring of boundaries between peace and conflict, civilian and military domains, and state and non-state actors is not incidental; it is fundamental to the effectiveness of hybrid strategies. Across Europe, the period between 2014 and 2025 illustrates both the scale and persistence of these threats. From the weaponisation of migration and election interference to cyberattacks, infrastructure sabotage, and coordinated disinformation campaigns, hybrid activities have generated continuous, multi-domain pressure on European states and societies. Their impact is often cumulative rather than immediate, gradually eroding institutional trust, social cohesion, and the ability of states to respond effectively.

A central conclusion of this analysis is that hybrid warfare is inherently strategic and long-term. It is not simply a tool of disruption, but a means of reshaping the broader security environment. In this context, actors such as Russia have demonstrated a systematic integration of hybrid methods into their strategic planning, leveraging ambiguity and deniability to pursue geopolitical objectives while avoiding direct confrontation. Hybrid warfare, therefore, reflects deeper structural tensions within the international system and is likely to remain a persistent feature of European security.

At the same time, this publication highlights both the progress made and the limitations that remain in Europe's response. Efforts to strengthen cyber resilience, protect critical infrastructure, counter disinformation, and enhance EU–NATO cooperation demonstrate a growing recognition of the challenge. However, these responses are often fragmented, unevenly implemented, and, in many cases, reactive rather than anticipatory. This fragmentation itself constitutes a vulnerability, one that hybrid actors are well positioned to exploit.

Addressing hybrid warfare effectively will therefore require more than incremental adaptation. It calls for a more coherent and integrated European approach to defence and security, one that moves beyond national silos and reflects the interconnected nature of the threats faced. Strengthening coordination between member states, improving information-sharing mechanisms, and aligning strategic priorities across institutions will be essential. Equally important is the need to invest in societal resilience, as hybrid operations ultimately target the internal cohesion of democratic systems.

In this regard, the role of networks such as the European Defence Network is not peripheral, but increasingly relevant. By fostering cross-border dialogue, producing independent analysis, and connecting a new generation of professionals across Europe, EDN seeks to contribute to the development of a more coherent and forward-looking European defence ecosystem. Its emphasis on cooperation, analytical rigor, and a shared strategic culture reflects a broader necessity: that Europe's security challenges can no longer be addressed within purely national frameworks.

Looking ahead, the evolution of emerging technologies, particularly artificial intelligence, will likely increase both the scale and sophistication of hybrid operations, further

complicating attribution and response. This underscores the need for continuous adaptation, as well as for policy frameworks capable of keeping pace with technological change while preserving democratic principles.

Ultimately, hybrid warfare is not a temporary phenomenon, but a structural condition of modern conflict. It challenges traditional assumptions about deterrence, sovereignty, and the nature of war itself. For Europe, responding effectively will depend not only on capabilities, but on unity of purpose. A more coordinated, integrated, and strategically aligned European defence architecture is no longer a long-term ambition, it is an operational necessity. The extent to which Europe can achieve this will shape its resilience, credibility, and security in the years to come.

I would like to thank you very much for taking the time to read this publication, the first for the European Defence Network, and we hope you gained insight and value from it.

Bibliography

Adams, P. (2021, October 21). *Belarus accused of using migrants to pressure EU*. BBC News. https://www.bbc.com/news/world-58952867

AirCosmos. (2023, May 15). Sabotage sur le navire de guerre britannique HMS Glasgow: acte de vandalisme ou règlement de comptes? https://air-cosmos.com/article/sabotage-sur-le-navire-de-guerre-britannique-hms-glasgow-acte-de-vandalisme-ou-reglement-de-comptes-64991

Akhvlediani T. (01 October 2025) *In Moldova's election, the line held and a mandate was won – but the hard work is only just beginning.* CEPS Publication. https://www.ceps.eu/in-moldovas-election-the-line-held-and-a-mandate-was-won-but-the-hard-work-is-only-just-beginning/

Álvarez-Miranda, B., & Brey, E. (2025). Reframing coercive engineered migration theory: Ceuta and the Western Sahara. *Mediterranean Politics, 30*(2), 316–337. https://doi.org/10.1080/13629395.2023.2293417

Authority for European Political Parties and European Political Foundations (November 2023) *Foreign Electoral Interference Affecting EU Democratic Processes* https://www.appf.europa.eu/cmsdata/277388/Foreign%20electoral%20interference%20affecting%20EU%20democratic%20processes.pdf

Bachmann, S.-D. D., Putter, D., & Duczynski, G. (2023). *Hybrid warfare and disinformation: A Ukraine war perspective*. **Global Policy, 14**(5), 858–869. https://doi.org/10.1111/1758-5899.13257

Ball, J. (2018). *Hybrid and non-linear warfare systematically erases the divide between war and peace*. Global Security Review. https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/

Bargués, P., & Bourekba, M. (2022). *War by all means: The rise of hybrid warfare* (CIDOB Report No. 8). Barcelona Centre for International Affairs (CIDOB). https://www.cidob.org/en/publications/war-all-means-rise-hybrid-warfare

BBC News. (2021). *Belarus migrant crisis: Poland reports fresh border breach attempts*. https://www.bbc.com/news/world-europe-59231136

BBC News. (2025a). *Balloons from Belarus are causing chaos in Lithuania. Is it smugglers, or a hybrid attack?* https://www.bbc.com/news/articles/c8655gn84ego

BBC News. (2025b). EU chief von der Leyen's plane hit by suspected Russian GPS jamming. https://www.bbc.com/news/articles/c9d07z1439zo

BFM TV with AFP. (2025, May 12). "Une guerre hybride": la Pologne accuse la Russie d'avoir ordonné un grand incendie à Varsovie en 2024. https://www.bfmtv.com/international/europe/une-guerre-hybride-la-pologne-accuse-la-russie-d-avoir-ordonne-un-grand-incendie-a-varsovie-en-2024_AN-202505120250.htm

Burrows E. (2025) What to know about Russia's GPS jamming operation in Europe https://apnews.com/article/russia-europe-jamming-spoofing-gps-satellite-b6d48d7d515f7edb48c7241f13a22851

Capaul, I. (2024). *A taxonomy of hybrid threats* (CSS Analyses in Security Policy No. 352). Center for Security Studies (CSS), ETH Zürich. https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse352-EN.pdf

Chivvis, C. S. (2017). *Understanding Russian "hybrid warfare" and what can be done about it*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR1972.html

Clapson C. (2025) Belgian security services convinced Russia is behind the drone incidents https://www.vrt.be/vrtnws/en/2025/11/05/belgian-security-services-convinced-russia-is-behind-the-drone-i/

Clark, M. (2020). *Russian hybrid warfare*. Institute for the Study of War. https://www.understandingwar.org/report/russian-hybrid-warfare

Colomina, C. (2022). *Words as weapons: From disinformation to the global battle for the narrative* (CIDOB Report No. 08-2022). Barcelona Centre for International Affairs (CIDOB). https://www.cidob.org/en/publications/words-weapons-disinformation-global-battle-narrative

Council of the European Union (20 May 2025) *Hybrid Threats* https://www.consilium.europa.eu/en/policies/hybrid-threats/#response

CyberPeace Institute (2022) Case Study: Viasat https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

Davies J. (2021) *Foreign Election Interference and Hybrid Warfare Foreign Election Interference and Hybrid Warfare* https://openworks.wooster.edu/cgi/viewcontent.cgi?params=/context/independentstudy/article/12164/&path_info=Hybrid_Warfare_and_Election_Interference_.pdf

De Mello, A. (2021). Rescuing multilateralism. In H. H. S. Viswanathan & A. Mathur (Eds.), *The future of BRICS* (pp. 14–22). Observer Research Foundation.

De Spiegeleire, S., Sweijs, T., Zhao, T., Bekkers, F., Boone, G., van Kaathoven, K., Khalil, R., Khvan, N., Renkmane, L., Shambur, O., & Zelinska, O. (2011). *Russian language perspectives* (in S. De Spiegeleire, T. Sweijs, & T. Zhao, *Contours of conflict in the 21st century: A cross-language analysis of Arabic, Chinese, English and Russian perspectives on the future nature of conflict*). The Hague Centre for Strategic Studies. http://www.jstor.com/stable/resrep12573

Deutsche Welle. (2022, June 30). *Poland completes Belarus border wall to prevent migrant crossings*. https://www.dw.com/en/poland-completes-belarus-border-wall-to-prevent-migrant-crossings/a-62314260

DRSD. (2025). Sur la piste des ingérences : les agents de la DRSD en action. https://www.defense.gouv.fr/piste-ingerences-agents-drsd-action

DW. (2026, January 2). *Finnish police arrest 2 over undersea cable damage.* https://www.dw.com/en/finland-seizes-vessel-suspected-of-damaging-undersea-cable/a-75349419

Estonian Information System Authority. *Cybertest Programme* *https://www.ria.ee/en/cyber-security/cyberspace-analysis-and-prevention/kubertest*

Estonian Information System Authority (RIA). https://www.ria.ee

Estonian Rescue Board. *Civil protection and public shelters* *https://www.rescue.ee/en/instruction/public-shelters*

Estonian Stockpiling Agency. *Mandate and responsibilities*. https://varudekeskus.ee/en/estonian-stockpiling-agency/about-us/management

Euractiv. (2021, August 11). *Latvia, Lithuania take emergency action over Belarus border*. https://www.euractiv.com/news/latvia-lithuania-take-emergency-action-over-belarus-border/

European Centre of Excellence for civilian Crisis Management (30 November 2024) *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness* https://www.coe-civ.eu/kh/safer-together-strengthening-europes-civilian-and-military-preparedness-and-readiness

European Commission. (2025, August 22). Digital Markets Act. https://digital-markets-act.ec.europa.eu/index_en

European Commission. (2025, December 3). Cyber Resilience Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

European Commission. (2025, July 15). New European Digital Media Observatory hub fights disinformation in Ukraine and Moldova. https://enlargement.ec.europa.eu/news/new-european-digital-media-observatory-hub-fights-disinformation-ukraine-and-moldova-2025-07-15_en

European External Action Service (EEAS). (2022, July 25). CPX EU Integrated Resolve 22. https://www.eeas.europa.eu/node/416534_fr#:~\:text=CPX%20EU%20Integrated%20Resolve%2022,with%20internal%20and%20external%20dimensions

European Parliament (June 2025) *EU preparedness: From concept to strategy?* https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772898/EPRS_BRI%282025%29772898_EN.pdf

European Parliament News (09 October 2024) *Parliament condemns Russia's interference in Moldova* https://www.europarl.europa.eu/news/en/press-room/20241003IPR24421/parliament-condemns-russia-s-interference-in-moldova

European Union Agency for Asylum. (2022). *Situation at the eastern borders* (Section 4.1.1). In *EUAA asylum report 2022*. https://euaa.europa.eu/asylum-report-2022/411-situation-eastern-borders

France 24. (2024, July 17). PDG dans le viseur des opérations clandestines : des espions russes sans limites ? https://www.france24.com/fr/europe/20240712-pdg-dans-le-viseur-des-op%C3%A9rations-clandestines-des-espions-russes-sans-limites

France 24 with AFP. (2025, February 19). Un ex-shérif américain derrière une campagne de désinformation russe visant les élections allemandes. https://www.france24.com/fr/europe/20250219-un-ex-sh%C3%A9rif-am%C3%A9ricain-derri%C3%A8re-une-campagne-de-d%C3%A9sinformation-russe-visant-les-%C3%A9lections-allemandes

France 24 with AFP. (2025, September 19). Russian fighter jets enter NATO member Estonia's airspace in 'brazen' incursion. https://www.france24.com/en/europe/20250919-russian-fighter-jets-enter-nato-member-estonia-s-airspace-in-brazen-incursion

Fridman O. (2018). Russian Hybrid Warfare: Resurgence and Politicization. Oxford University Press.

Gabor, E. (2025). Hybrid warfare through interference in electoral processes: Using advanced technology and its impact on global security. Case study: The 2024 Romanian presidential election. *Politics in Central Europe.* Advance online publication. https://doi.org/10.2478/picbe-2025-0138

Gardner, H. (2015). *Hybrid warfare: Iranian and Russian versions of "Little green men" and contemporary conflict*(Research Paper No. 123). Research Division, NATO Defense College. https://www.ndc.nato.int/download/hybrid-warfare-iranian-and-russian-versions-of-little-green-men-and-contemporary-conflict/?wpdmdl=7275&refresh=693f437d498ea1765753725

Gaudiosi F. (January 2021) *NATO 2030: il rilancio dell'Alleanza Atlantica per il prossimo decennio.* SIOI Publication. https://www.osorin.it/uploads/model_4/.files/61_item_2.pdf?v=1612779103

Gökalp Aras, N. E. (2019). *Coercive engineered Syrian mass migration in the EU-Turkey relations: A case analysis for future reference*. International Migration, 57(2), 186-199. *https://doi.org/10.1111/imig.12566*

Government of Estonia. *Emergency Act (Hädaolukorra seadus)*. https://www.riigiteataja.ee/en/

Government of Estonia. *National cyber hygiene initiatives*. https://e-estonia.com/estonias-cyber-security-model-for-europe/

Government Office of Estonia. *National civil crisis exercise CREVEX.* https://www.riigikantselei.ee/en/news/crevex-2023-largest-crisis-exercise-history-estonia-after-restoration-its-independence-begins

Greenhill, K. M. (2008). Strategic engineered migration as a weapon of war. *Civil Wars, 10*(1), 6–21. https://doi.org/10.1080/13698240701835425

Greenhill, K. M. (2010). *Weapons of mass migration: Forced displacement, coercion, and foreign policy*. Cornell University Press.

Grigalashvili V. (2020) *An ambiguous phenomenon of hybrid warfare. Theory and policy practice of Georgia.* https://neweurope.centre.ubbcluj.ro/wp-content/uploads/2020/04/6-article_GRIGALASHVILI.pdf

Hall, S., & Debre, M. (2025). Developing best practices "against terrorists who protest": Regional organizations as learning clubs for autocracies. *Contemporary Security Policy, 46*(4), 1225–1254. https://doi.org/10.1080/13523260.2025.2543625

International Committee of the Red Cross. (1977). *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I)*. https://ihl-databases.icrc.org/en/ihl-treaties/api-1977

Katagiri, N. (2024). Advanced persistent threats and the "big four": State-sponsored hackers in China, Iran, Russia, and North Korea in 2003–2021. *Comparative Strategy, 43*(3), 280–299. https://doi.org/10.1080/01495933.2024.2317251

Kerttunen M., Schuck K., Hemmelskamp J. (2023) Major Cyber Incident: KA-SAT 9A https://eurepoc.eu/publication/major-cyber-incident-ka-sat-9a/

Keskkonnaportaal, Flood Risk Prevention and Mitigation, Warning Systems https://keskkonnaportaal.ee/en/flood-risk-prevention-and-mitigation-warning-systems

Kozatskyi S. (2025) Poland to Construct Its Own "Drone Wall" to Counter Russian Attacks https://militarnyi.com/en/news/poland-to-construct-its-own-drone-wall-to-counter-russian-attacks/

La Libre Belgique with AFP. (2025, November 13). Survols de drones suspects: la Belgique craint de devenir une cible privilégiée. https://www.lalibre.be/belgique/2025/11/13/survols-de-drones-suspects-la-belgique-craint-de-devenir-une-cible-privilegiee-clone-PYRNUV2N3JE2JE4YPOJFP7EID4/

Le Figaro. (2025, February 5). Allemagne : enquête sur de mystérieux sabotages de voitures, la Russie soupçonnée. https://www.lefigaro.fr/international/allemagne-enquete-sur-de-mysterieux-sabotages-de-voitures-la-russie-soupconnee-20250205?msockid=0f21288f04c568e02d653c7e057c69fe

Le Figaro with AFP. (2025, December 5). Survol de drones en Bretagne : la base sous-marine de l'île Longue, sanctuaire de la dissuasion nucléaire française. https://www.lefigaro.fr/international/survol-de-drones-en-bretagne-la-base-sous-marine-de-l-ile-longue-sanctuaire-de-la-dissuasion-nucleaire-francaise-20251205

Le Marin (Ouest France). (2023, May 25). Actes de malveillance chez Naval group, une enquête ouverte. https://lemarin.ouest-france.fr/industries-navales/actes-de-malveillance-chez-naval-group-une-enquete-ouverte-f8bed559-dfa3-4643-b91f-c98e22e2795af

Le Monde. (2023, February 21). InfoDefense, les volontaires ordinaires de la propagande russe sur Telegram. https://www.lemonde.fr/pixels/article/2023/02/21/infodefense-les-volontaires-ordinaires-de-la-propagande-russe-sur-telegram_6162717_4408996.html

Le Monde. (2024, June 2). *Cinq cercueils découverts au pied de la tour Eiffel avec la mention « soldats français de l'Ukraine » : trois suspects en garde à vue.* https://www.lemonde.fr/societe/article/2024/06/02/cinq-cercueils-decouverts-au-pied-de-la-tour-eiffel-avec-la-mention-soldats-francais-de-l-ukraine-trois-suspects-en-garde-a-vue_6236923_3224.html

Le Monde. (2024, October 18). En Europe, des actes de sabotage à l'explosif attribués à la Russie. https://www.lemonde.fr/international/article/2024/10/18/en-europe-la-guerre-hybride-franchit-un-nouveau-seuil_6354760_3210.html

Le Monde. (2025, November 23). Face aux intrusions de drones, la France réfléchit à changer la loi pour pouvoir plus facilement les abattre. https://www.lemonde.fr/international/article/2025/11/23/face-aux-intrusions-de-drones-la-france-reflechit-a-changer-la-loi-pour-pouvoir-plus-facilement-les-abattre_6654487_3210.html

Lendon B., Yee I. (2025) NATO shoots down Russian drones in Polish airspace, accusing Moscow of being 'absolutely reckless' https://edition.cnn.com/2025/09/09/europe/poland-scramble-jets-russian-drone-reports-intl-hnk-ml

Le Parisien with AFP. (2022, September 12). Hôpital de Corbeil-Essonnes : le groupe russophone Lockbit 3.0 revendique la cyberattaque et lance un chantage aux données. https://www.leparisien.fr/high-tech/hopital-de-corbeil-essonnes-le-groupe-russophone-lockbit-30-revendique-la-cyberattaque-et-lance-le-chantage-aux-donnees-12-09-2022-7IM7PZYIYNFPVBIJXYVUNXZPOI.php

Le Parisien with AFP. (2025, June 27). Une attaque contre notre démocratie : l'Allemagne soupçonne la Russie de sabotage après l'incendie des camions de son armée. https://www.leparisien.fr/international/une-attaque-contre-notre-democratie-lallemagne-soupconne-la-russie-de-sabotage-apres-lincendie-des-camions-de-son-armee-27-06-2025-5EBI27XL6JHTJMXS32LYMHU7ZI.php

Lewis, S. (2018). Salisbury, Novichok and international law on the use of force. *The RUSI Journal, 163*(4), 10–19. https://doi.org/10.1080/03071847.2018.1529889

Lundgren, M. [@MagnusLLundgren]. (2025, May 29). Vetoes in the UN Security Council, 1946–2025 [Post]. X. https://x.com/MagnusLLundgren/status/1928253707872808963

Martisiute M. (14 January 2025) *Civil preparedness is a right* https://www.epc.eu/publication/Civil-preparedness-is-a-right-60949c/

Mediapart. (2024, June 27). *L'argent russe du Rassemblement national* [Russian money of the National Rally]. https://www.mediapart.fr/journal/france/dossier/largent-russe-du-rassemblement-national

Medina Llinàs, M. (2022). *Hybrid attacks on critical infrastructure* (CIDOB Report No. 8). Barcelona Centre for International Affairs (CIDOB). https://www.cidob.org/en/publications/hybrid-attacks-critical-infrastructure

Ministry of Economic Affairs and Communications. (2024). *Cybersecurity Strategy 2024–2030*. https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf

Ministry of the Interior of Estonia. *Civil Crisis and National Defence Act (draft)*. https://riigikantselei.ee/en/news/draft-version-civil-crisis-and-national-defence-act-submitted-approval

Moulier Boutang, Y. (2023). *Ukraine, Taïwan, le moment chinois. Vraiment ?* Multitudes, 91(2), 9–18. https://doi.org/10.3917/mult.091.0009

NATO. (2020). *NATO 2030: United for a new era—Analysis and recommendations of the reflection group appointed by the NATO Secretary General*. North Atlantic Treaty Organization. https://fpa.org/wp-content/uploads/2025/03/201201-Reflection-Group-Final-Report-Uni.pdf

NATO. (2023). *Resilience and Article 3*. https://www.nato.int/cps/en/natohq/topics_132722.htm

NATO (Updated 2024) *Resilience, civil preparedness and Article 3* https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3

NATO (Updated October 2022) *Resilience Committee* https://www.nato.int/en/about-us/organization/nato-structure/resilience-committee

NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org

Niinistö S. (2024) *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness* https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf

NewsGuard. (2025, September 18). *Russian influence campaign CopyCop expands to more than 300 fake media websites targeting Western countries*. NewsGuard. https://www.newsguardtech.com/special-reports/

Politico. (2025, April 7). Europe's new war with Russia: Deep sea sabotage. https://www.politico.eu/article/russia-sabotage-undersea-cables-baltic-sea-europe-war/

Publication Office of the European Union (2024) *Disaster risk awareness and preparedness of the EU population* https://op.europa.eu/en/publication-detail/-/publication/9012958d-ad3a-11ef-acb1-01aa75ed71a1/language-en

Radio France. (2025, November 26). Quatre personnes mises en examen pour ingérence et espionnage en faveur de la Russie. https://www.radiofrance.fr/franceinfo/podcasts/les-documents-franceinfo/quatre-personnes-mises-en-examen-pour-ingerence-et-espionnage-en-faveur-de-la-russie-8425992

Raufer, X. (2025). Guerre hybride, « anticolonialisme » : le retour du Komintern ? Sécurité globale, 42(2), 7-20. https://shs.cairn.info/revue-securite-globale-2025-2-page-7?lang=fr.

Recorded Future. (2025, September 17). Annex C, page 26 of the PDF titled "CopyCop French Websites". https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-ru-2025-0917.pdf

Reuters. (2021a, August 10). *Lithuania – Belarus diplomatic spat leaves migrants stranded*. BBC News. https://www.bbc.com/news/world-europe-58121577

Reuters. (2021b, September 2). *Polish president imposes state of emergency on Belarus border*. https://www.reuters.com/world/europe/polish-president-imposes-state-emergency-belarus-border-2021-09-02/

Rodenas I. (08 July 2025) *Election Interference in the Age of Hybrid Warfare.* CYIS Publication. https://www.cyis.org/post/election-interference-in-the-age-of-hybrid-warfare

Rodriguez-Triocci, E. (2024). What about the BRICS? Examining power politics in a changing world order. *Journal of Political Power, 17*(1), 21–41. https://doi.org/10.1080/2158379X.2024.2341018

Sandu S. (25 September 2025) *Moldova's 2025 Elections: A Test Case for Russia's Hybrid Warfare* https://www.stimson.org/2025/moldovas-2025-elections-a-test-case-for-russias-hybrid-warfare/

Satter R. (2022) Satellite outage caused 'huge loss in communications' at war's outset -Ukrainian official https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/

Schmitt O. (2021) *Ideology and Influence in the Debate over Russian Election Interference* https://www.researchgate.net/publication/345004565_Ideology_and_Influence_in_the_Debate_over_Russian_Election_Interference

SGDSN. (2024, February 12). French Government (SGDSN), Annual Report on Foreign Digital Interference. https://www.sgdsn.gouv.fr/publications/portal-kombat-un-reseau-structure-et-coordonne-de-propagande-prorusse

SGDSN. (2025, February 7). Challenges and opportunities of artificial intelligence in the fight against information manipulation.

https://www.sgdsn.gouv.fr/files/files/Publications/20250207_NP_SGDSN_VIGINUM_Rapport%20menace%20informationnelle%20IA_EN_0.pdf

SGDSN (VIGINUM). (2025). Analyse du mode opératoire informationnel russe Storm-1516. https://www.sgdsn.gouv.fr/publications/analyse-du-mode-operatoire-informationnel-russe-storm-1516

Stephen, M. D. (2025). Beyond multilateralism: China's international order building through transnational policy forums. *The Pacific Review*. Advance online publication. https://doi.org/10.1080/09512748.2025.2590512

Sud-Ouest with AFP. (2025, June 13). Sabotage de câbles en mer Baltique : fin de l'enquête en Finlande, trois marins du navire fantôme russe soupçonnés. https://www.sudouest.fr/enquetes/sabotage-de-cables-en-mer-baltique-fin-de-l-enquete-en-finlande-trois-marins-du-navire-fantome-russe-soupconnes-24837055.php

Swinhoe D. (2022) Viasat: Our network was hit by a "multifaceted and deliberate" cyberattack https://www.datacenterdynamics.com/en/news/viasat-our-network-was-hit-by-a-multifaceted-and-deliberate-cyberattack/

Szeptycki, A. (2017). La guerre d'information russe contre l'Occident: Le cas de l'Ukraine. In J. Holeindre & J. Fernandez (Eds.), *Annuaire français de relations internationales: 2017* (Vol. XVIII, pp. 233–246). Éditions Panthéon-Assas. https://doi.org/10.3917/epas.batch.2017.01.0233

Talik, M. (2024). *Between security and human rights: Addressing state-sponsored instrumentalization of migration by Belarus and Russia*. Pulaski Policy Papers / Pulaski Foreign Affairs Commentary. Warsaw: Kazimierz Pulaski Foundation. https://pulaski.pl/en/pulaski-policy-papers-between-security-and-human-rights-addressing-state-sponsored-instrumentalization-of-migration-by-belarus-and-russia/

The Guardian. (2024, November 4). Incendiary device plot targeting UK may have been dry run for US and Canada. https://www.theguardian.com/uk-news/2024/nov/04/incendiary-device-plot-targeting-uk-may-have-been-dry-run-for-us-canada-russia-dhl

The Guardian. (2025, September 9). At least nine pigs' heads found outside mosques in Paris region. https://www.theguardian.com/world/2025/sep/09/pigs-heads-found-mosques-paris-region

Weiss, J. C., & Wallace, J. L. (2021). Domestic politics, China's rise, and the future of the liberal international order. *International Organization, 75*(2), 635–664. https://doi.org/10.1017/S002081832000048X

Wojnowski, M. (2022). *The genesis, theory, and practice of Russian coercive migration engineering: A contribution to the study of the migration crisis on NATO's eastern flank*. Internal Security Review, 26(14). *https://doi.org/10.4467/20801335PBW.21.042.15702*

Wojnowski, M. (2022). *The genesis, theory, and practice of Russian coercive migration engineering: A contribution to the study of the migration crisis on NATO's eastern flank*. Przegląd Bezpieczeństwa Wewnętrznego, 14(26), 263–300. https://doi.org/10.4467/20801335PBW.21.042.15702

Wolff S. (29 September 2025) *Russian interference has failed in Moldova, to Europe's relief* https://www.birmingham.ac.uk/news/2025/russian-interference-has-failed-in-moldova-to-europes-relief

Yang, F. W. (2025). Rare earth and resource nationalism: What happened before and after China's embargo on Japan? *Journal of Contemporary China, 34*(153), 383–400. https://doi.org/10.1080/10670564.2024.2335547

European Defence Network

NextGen Inspiring Europe's Defence

Shaping
Thinking
Connecting
Building

Hybrid threats operate in ambiguity.
Europe cannot afford to do the same.