



POLICY PAPER

RUSSIA'S HYBRID ATTACKS IN EUROPE

FROM DETERRENCE TO ATTRIBUTION TO RESPONSE

| HENRIK PRAKS |

APRIL 2025

Title: Russia's Hybrid Attacks in Europe: From Deterrence to Attribution to Response
Author: Praks, Henrik
Publication date: April 2025
Category: Policy Paper

Cover page photo: An Estonian naval ship on a NATO patrol in the Baltic Sea on 9 January 2025.
Hendrik Osula, AP Photo/Scanpix.

Keywords: attribution, critical infrastructure, cybersecurity, deterrence, hybrid warfare, intelligence, maritime law, resilience, sabotage, sanctions, terrorism, visa policy, Baltic states, European Union, NATO, Russia

Disclaimer: The views and opinions contained in this analysis are those of its authors only and do not necessarily represent the positions of the International Centre for Defence and Security or any other organisation.

ISSN 2228-2068

© International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee, www.icds.ee

CONTENTS

Acknowledgements	III
About the Author	III
Introduction	1
1. Deterrence	1
1.1. Deterrence by Denial	2
1.2. Deterrence by Punishment	2
2. Attribution	3
2.1. Technical Attribution	3
2.2. Political Attribution	4
2.3. Legal Attribution	5
2.4. Sabotage as State Terrorism?	5
3. Response	6
3.1. Principles	6
3.2. Multilateral Response	8
3.3. NATO	8
3.3.1. Article 5	9
3.3.2. Article 4	10
3.4. The European Union	10
3.4.1. Sanctions	11
3.4.2. Diplomacy & Visa Policy	13
3.5. Shadow Fleet	13
Conclusions and Recommendations	14

ACKNOWLEDGEMENTS

The author extends sincere gratitude to all the experts and officials who generously took the time to engage in discussions in Brussels and Tallinn. The author would also like to express his gratitude to Marek Kohv for his invaluable assistance in the research stage, Tomas Jermalavičius for his detailed observations and suggestions, and Tetiana Fedosiuk for her precise editorial work. Their contributions made this paper possible.

ABOUT THE AUTHOR

HENRIK PRAKS

Henrik Praks re-joined the ICDS in August 2024 as a research fellow with the Security & Resilience Programme. In 2020, he was seconded by the Estonian Government Office as a Senior Analyst to the European Centre of Excellence for Countering Hybrid Threats in Helsinki. Earlier in his career, he held various positions within the Estonian Ministry of Defence, focusing on defence and security policy, regional security, NATO, and EU defence issues. He was a lecturer in strategic studies at the Baltic Defence College (BALTDEFCOL). Mr Praks was a member of the ICDS research team between 2015 and 2018. During that period, he was also Director of the Annual Baltic Conference on Defence (ABCD). Mr Praks has an MA degree from Tartu University's Faculty of Law and an MA degree in East European Studies from Freie Universität Berlin. He is also a graduate of the International Training Course of the Geneva Centre for Security Policy.

INTRODUCTION

As Russia's war of aggression against Ukraine has entered its fourth year, its hybrid attacks have become a regular occurrence across Europe.¹ While the focus previously was on activities in the cyber and information domains, Russia now frequently employs kinetic attacks. Cyber operations, disinformation campaigns, and attempts to manipulate electoral processes are accompanied by sabotage against infrastructure, arson, and other physical attacks conducted by persons recruited by Russian intelligence services. Moreover, Russia and its vassal state of Belarus utilise migration pressure against neighbouring countries, while navigation systems in many areas are affected by electronic interference. Since late 2023, four commercial ships travelling to or from Russian ports in the Baltic Sea have been suspected of cutting data and electricity cables as well as the seabed gas pipeline.

Russia's actions now represent an escalating campaign of hybrid warfare, directly affecting the security and stability of European nations

These malign activities can no longer be dismissed as mere nuisance, given their rising frequency and intensity. Russia's aggressive actions now represent an escalating campaign of hybrid warfare, directly affecting the security and stability of European nations. As Russia is not unique in using hybrid methods, their

¹ The paper uses the phrase "hybrid attacks" as a general term to describe malicious activities undertaken by the Russian state, either directly through its intelligence services and other structures or by utilising proxy actors. While the use of the term "hybrid" in the context of these actions is frequently challenged, it does provide a general description to characterise a variety of attacks beyond the conventional military level.

effects and our response are closely followed by other actors, first and foremost China. Autocratic regimes favour hybrid warfare precisely because democratic states struggle with responding directly and proportionally while also being more open and much easier to penetrate for such subterfuge. The attacks are usually deliberately designed to complicate detection, evade accountability, and hinder decisive responses. Additionally, the targeted nations may lack the capability or the political will to respond effectively.

This policy paper aims to explore the most promising areas for international response to hybrid threats from Russia. With both NATO and the EU striving to strengthen their roles, this research draws from interviews with representatives of both institutions and an analysis of open-source materials. The paper studies the conceptual framework underpinning the response to hybrid threats; examines the actions taken within NATO and the EU in the fight against hybrid threats, as well as the opportunities to address them; and presents a set of policy recommendations for these organisations and their member states to enhance their efforts in tackling these challenges. This paper focuses on proactive measures to hamper Russia's ability to cause harm and impose costs for its hybrid aggression.

1. DETERRENCE

In responding to Russia's attacks, the policy goal should be to create conditions where such attacks can no longer occur. Achieving this requires establishing effective deterrence against hybrid threats. Deterrence is the practice of discouraging or restraining someone from taking unwanted actions. The literature distinguishes between two fundamental approaches to deterrence: deterrence by denial and deterrence by punishment.² Translating this into practice means that Russia's cost-benefit calculations must be changed so that the Kremlin either fails to achieve its objectives through attacks (deterrence by denial) or faces significant consequences (deterrence by punishment).

² Thomas C. Schelling, *Arms and Influence* (Yale University, 2008).

So far, Europe has failed to establish adequate defence mechanisms against hybrid attacks – much less deterrence. It thus remains unclear how Europe plans to effectively address Russia’s hybrid warfare. Consequently, Russia continues to hold the initiative and operational advantage, which keeps the costs of hybrid tactics low, allowing it to act with relative freedom and minimal repercussions. Meanwhile, Europe struggles to mount a robust and coordinated response.

Europe has failed to establish adequate defence mechanisms against hybrid attacks – much less deterrence

Unless Russia is adequately challenged, it sees no reason to change its behaviour. Remaining passive, accepting the repetition of such acts of subversion and sabotage, and dealing with the consequences emboldens Russia, meaning that not only will they continue but also lead to even more aggressive and risky actions. Failure to respond is not only costly in monetary terms but highly damaging to people’s sense of security.

A weak response to hybrid attacks, likewise, reflects the overall lack of a clear European policy towards aggressive and expansionist Russia. At the political level, European nations need to recognise that Russia is waging war not only against Ukraine. The large-scale kinetic campaign of aggression in Ukraine is accompanied by hybrid warfare against the “collective west,” as Russia views it.

The west is hindered in its response by a psychological barrier: the fear of escalation resulting in slow and cautious reactions. It presupposes that any bolder step could provoke Russia to (military or non-military) escalation. Thus, avoiding escalation often motivates a watered-down response that benefits the Kremlin.

1.1. DETERRENCE BY DENIAL

Strategies of this kind aim to deter an action by making it difficult or impossible for an adversary to achieve its objectives. Denying an attacker confidence in its ability to succeed

reduces the incentive to carry out a particular malign action. In practice, this involves taking defensive measures that make it harder for Russia to accomplish its goals.

Not all hybrid threats are fully deterrable due to their reliance on ambiguity, deniability, gradual escalation, and low-intensity tactics, with cyberattacks and information operations being particularly challenging in this regard.³ These incremental actions, having become a daily occurrence, may not provoke a strong response, allowing adversaries to avoid crossing red lines that would trigger a clear deterrent action. Therefore, in the case of hybrid threats, building resilience within societies and

systems can be more effective than trying to prevent the threat entirely. Mitigating the effects through resilience is a crucial part of the response. Countries must be as agile as possible in absorbing attacks and coping with the long-term threats from Russia. The aim is that if Russia sees it cannot cause any serious damage, it will eventually stop wasting its resources on futile attacks.

Not all hybrid threats are fully deterrable, so building resilience can be more effective than trying to prevent the threat

However, relying solely on resilience has proven to be ineffective in influencing Russia’s behaviour. As one interviewee put it, “It is not possible just to out-resilience Russia.” For example, in the context of attacks on critical infrastructure, it is not feasible to defend entire networks of cables and pipelines – whether on the seabed or land – along with energy facilities, data centres, and other key assets, from all potential threats at all times.

1.2. DETERRENCE BY PUNISHMENT

Deterrence by punishment seeks to prevent an adversary from taking unwanted actions by threatening severe retaliation if they proceed. The goal is to raise the costs of the adversary’s actions to a point where the risks outweigh the benefits, thereby forcing it to reconsider

³ Vytautas Keršanskas, “[Deterrence: Proposing a more strategic approach to countering hybrid threats](#),” *Hybrid Influence CoE Paper 2* (March 2020).

or avoid the action entirely. In practice, deterrence by punishment functions by making it clear that if the adversary engages in specific malign activities, it will face significant retaliation or punishment. To constrain and change Russia's behaviour, there is no alternative to employing proactive measures to impose costs to prevent future attacks. This necessitates a deterrence-by-punishment strategy, where Russia understands that continued aggression will result in severe consequences.

To constrain and change Russia's behaviour, there is no alternative to employing proactive measures

A vital role in deterrence belongs to signalling, which can be relayed either through public statements or non-public channels. For deterrence to be effective, the policy must be credible, and the aggressor must believe that the response can be carried out. Therefore, words must be backed by capability and resolve. A mere threat of a response may not be enough; in some cases, action is required. Fear of escalation is often the primary motive behind inaction. However, there is plenty of historical evidence that when pushed back by a strong reaction, Russia would back down.⁴

2. ATTRIBUTION

An essential part of a response to a hybrid attack and deterring further hostile actions is attribution, which consists of technical, political, and legal means pointing the finger at the culprit. Attribution sends a message to Russia that "we are aware of its methods"; plays an important part in strategic communications; provides a legal basis in international law for proportional response; and enables bringing Allies together to enact countermeasures. However, attribution is a complex issue, especially in multilateral contexts. The challenge lies not only in gathering sufficient evidence but, more importantly, in mustering the political will, which an adversary is also expected to attempt to influence and manipulate.

⁴ Keir Giles, [What deters Russia Enduring principles for responding to Moscow](#) (Chatham House, 2023).

In practice, it can be difficult to attribute attacks to specific state actors with a high degree of certainty. Hybrid attacks are often conducted

The attribution challenge lies not only in gathering sufficient evidence but mustering the political will

through proxies or in other ways that obscure the perpetrator's identity, making it difficult to publicly blame or sanction the responsible party. The attacker's ability to maintain at least some degree of plausible deniability dilutes the effectiveness of traditional deterrence models that depend on clear attribution and accountability. Key issues to be considered in the context of attribution are:

- **Demonstrating harm:** Physical damage is easier to attribute than cognitive attacks, and cases of physical damage often generate greater public pressure for attribution.
- **Identifying the perpetrator:** Establishing who conducted the attack.
- **Linking proxies:** Demonstrating the proxies' (criminals, commercial entities, etc) connection to the state or actor behind the attack.
- **Proving intent:** Establishing that the harm was intentional rather than accidental.

There are three levels of attribution:

- technical (identifying the tools and methods used);
- political (publicly naming the attacker);
- legal (criminal liability, indictment).

2.1. TECHNICAL ATTRIBUTION

Technical attribution is the essential first step. It addresses key questions such as: Who is involved? What tools, tactics, and procedures were used? In this context, intelligence and investigative agencies play a central role by gathering evidence that can be shared with Allies and preferably with the public. In parallel, the work of investigative journalism networks and open-source intelligence (OSINT)

volunteer groups have become additional means of uncovering the attacker's methods.

Russia's recent operations often involve incidents that, in isolation, may seem like ordinary criminal activities but when connected, reveal a broader pattern

Russia's hybrid campaigns must be detected, identified, and countered as early as possible. The first step requires cross-border situational awareness and intelligence sharing to 'connect the dots.' Russia's recent operations often involve incidents in different countries that, when viewed in isolation, may seem like ordinary criminal activities. However, when connected, these events can reveal a broader pattern of sabotage or other hostile actions. As Europe ramps up its defence spending in response to the rapidly deteriorating security environment, investments in counterintelligence should also be prioritised.⁵ Improved detection capabilities could lead to more frequent attribution and accurate countermeasures against Russia.

2.2. POLITICAL ATTRIBUTION

Technical attribution can – but does not need to – be followed by political attribution, which involves publicly labelling the attacker. Damaging the aggressor's image and imposing political costs enhances deterrence. However, in the case of Russia, mere naming and shaming through public disclosure has lost its effect, as Moscow is now largely indifferent to its reputation in the west. The standard Russian response to being caught is to deny everything and accuse the other party of "Russophobia" – a one-size-fits-all explanation for almost any western allegation.⁶

Responding to hybrid attacks does not always require public disclosure, and not all attacks need to be publicly attributed. It may, in

⁵ The term "counterintelligence" here means information gathered and activities conducted to protect against espionage, sabotage, assassinations, and other activities by hostile foreign intelligence services.

⁶ Peter Dickinson, "[Reluctant Russophobes: The Underwhelming International Response to Putin's Hybrid War](#)," *Atlantic Council*, 3 April 2028.

certain instances, also be avoided to prevent revealing to the attacker that its methods have been exposed. In some cases, national authorities may choose not to attribute attacks to Russia to avoid alarming their populations, especially when viable response options are lacking. Thus, deniability often benefits risk-averse European leaders, but ignoring attacks typically invites further aggression.

Political attribution remains a sovereign prerogative of a state. However, the impact of purely national attribution is limited, and attribution in multilateral frameworks can significantly bolster the legitimacy and effectiveness of the process. Public statements and diplomatic demarches by international bodies can serve as tools for joint attribution:

- **NATO:** In May 2024, the Alliance issued two Council statements attributing hybrid attacks to Russia.⁷ It can also be communicated by the Secretary-General, although these declarations similarly require consensus among Allies.
- **The EU:** The EU itself does not typically perform attribution directly but provides support to national efforts through collective political and legal actions. The first statement by the High Representative for Foreign Affairs calling out Russia publicly for hybrid attacks occurred only in October 2024.⁸
- **Groups of countries:** Attribution can also be carried out by coalitions. This practice is widespread in cyber-attack-related cases. Globally, the most significant attributions are made by the Five Eyes intelligence alliance members in collaboration.

However, at the multilateral level, the process of attribution remains incoherent and

⁷ North Atlantic Council, "[Statement by the North Atlantic Council on recent Russian hybrid activities](#)," NATO, 2 May 2024; North Atlantic Council, "[Statement by the North Atlantic Council concerning malicious cyber activities against Germany and Czechia](#)," NATO, 3 May 2024.

⁸ Council of Europe, "[Hybrid threats/Russia: Statement by the High Representative on behalf of the EU on Russia's continued hybrid activity against the EU and its Member States](#)," European Council, Council of the European Union, 8 October 2024.

sporadic. The role of organisations like the EU and NATO is primarily to facilitate intelligence sharing among member states and coordinate responses, while the attribution largely remains a national decision.

The role of the EU and NATO is primarily to facilitate intelligence sharing and coordinate responses, while the attribution largely remains a national decision

2.3. LEGAL ATTRIBUTION

The third category is legal attribution, which seeks to use legal means to hold perpetrators and organisers accountable. Legal processes are often time-consuming, with criminal investigations taking months or even years to complete. However, attribution must happen within a reasonable timeline: when attribution is delayed, it loses much of its value.⁹

When attribution is delayed, it loses much of its value

International politics is not a court of law, where establishing legal guilt is the priority. Instead, decisions are often ‘judgment calls’ based on probabilities rather than definitive proof. Russians do not always leave a ‘smoking gun’; instead, they often maintain plausible deniability, making it difficult for investigators to provide conclusive evidence. Therefore, political and legal attribution should be separate, as much as possible. For political attribution, it is not always necessary to invest significant resources into prosecution and prove every detail, especially since perpetrators are unlikely to be apprehended.

2.4. SABOTAGE AS STATE TERRORISM?

Attribution must be accompanied by a proactive communications strategy, which, in turn, requires clear definitions. While the EU has so far labelled such attacks as “hybrid,”

⁹ In September 2024, Estonia attributed the 2020 cyberattacks against Estonian state authorities to the GRU, Russian military intelligence service, see: “[A GRU military unit launched cyberattacks against Estonian authorities](#),” Republic of Estonia Prosecutor’s Office, 5 May 2024.

NATO has referred to them as “Russia’s escalating campaign of hostile actions in NATO countries,”¹⁰ and Secretary General Mark Rutte indicated his preference for the term “destabilisation campaign.”¹¹ The intensification of Russia’s hybrid warfare raises the question of whether it would be prudent to start calling at least more severe acts or attempts of sabotage “state terrorism.”

The term “terrorism” is traditionally reserved for acts of violence carried out by non-state actors, although states have also been labelled as “state sponsors of terrorism.” The United States has designated four countries – Cuba, North Korea, Iran, and Syria – as “state sponsors of terrorism.” In November 2022, the European Parliament made a political non-binding declaration recognising Russia as a “state sponsor of terrorism and a state that uses the means of terrorism” for its atrocities against Ukrainian civilians.¹²

Terrorist activities are generally characterised as an attempt to create an atmosphere of fear within the targeted society.

According to EU law, terrorist offences are acts committed with the aim of:

- 1) seriously intimidating a population;
- 2) unduly compelling a government or international organisation to perform or abstain from performing any act;
- 3) seriously destabilising or destroying the fundamental political, constitutional, economic, or social structures of a country or an international organisation.¹³

¹⁰ “[NATO Foreign Ministers chart way forward in addressing Russian sabotage](#),” NATO, 4 December 2024.

¹¹ Mark Rutte, “[Remarks by NATO Secretary General Mark Rutte at the European Parliament’s Committee on Foreign Affairs and Subcommittee on Security and Defence](#),” NATO, 13 January 2025.

¹² “[European Parliament declares Russia to be a state sponsor of terrorism](#),” European Parliament, 23 November 2022.

¹³ The European Parliament and of the Council, [Directive \(EU\) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA](#) (OJ L 88, 2017), 6-21.

Rather than focusing on narrow operational objectives or immediate victims, terrorist acts target society as a whole by using violence or intimidation against civilians for political purposes. State terrorism is committed by agents of the state or by proxies who operate with the resources of the state.¹⁴

The term “terrorism” could be used more frequently in strategic communications to describe Russia’s actions

While the formal international legal designation of the Russian Federation as a state sponsor of terrorism is politically unrealistic at this point, the term “terrorism” could be used more frequently in strategic communications to describe Russia’s actions. A sustained Russian campaign of sabotage acts, even if they do not result in casualties, should be seen not as mere criminal acts but as a sinister attempt to terrorise populations. The exposed Russian plot to target cargo planes in Europe and on the transatlantic routes has already been labelled as “air terror” by the Polish prime minister.¹⁵ It is rather fortunate that such attacks on the transport sector, as well as arson, have not resulted in casualties. In this light, nations should consider starting to refer to Russian sabotage as state terrorism. This would send a strong political signal and help raise public awareness of the seriousness of the Russian attacks. Although Russia has long abused the term “act of terror,” this should not discourage us from describing certain Russian actions as terrorism if they meet that definition.

Moreover, the US and the EU have mechanisms to blacklist organisations or individuals suspected of terrorism. These tools could be employed to target specific Russian entities involved in the planning and execution of assassinations and sabotage acts. The Iranian Revolutionary Guard Corps, for instance, has been designated as a terrorist organisation by the US and several other countries. Unit 29155 of Russia’s military

intelligence agency (the GRU), which has a long history of conducting both physical and cyber-attacks against foreign targets, should be treated in a similar manner.

3. RESPONSE

Attribution should not be viewed as an end in itself. Hybrid attacks against Europe must be followed by a response. If a country attributes an attack to another state but fails to respond adequately, it creates the impression of powerlessness. This, in turn, allows the hostile actor to achieve its objectives in the information space by instilling fear and a sense of weakness in the target nation’s population.

This does not mean that each instance of attribution must always be followed by specific immediate countermeasures. Instead, a general signal of intent must be sent, indicating that aggression will have consequences while maintaining strategic ambiguity by leaving Russia uncertain about the nature of the response.

3.1. PRINCIPLES

Under the UN Charter, countries have the right to take self-defence measures. Even if a hostile action does not reach the threshold of an armed attack justifying the use of force, international law allows for countermeasures. Those are intended to induce the offender to comply with its international obligations while holding it accountable for its violation.

Countermeasures must adhere to the principle of proportionality but can be asymmetric

Countermeasures must adhere to the principle of proportionality but do not need to be symmetrical; asymmetric methods can be employed. Symmetrical responses are often difficult for liberal democracies due to ethical and legal constraints. This is why Russia favours hybrid warfare – it is challenging to respond directly and proportionally. As a result, an asymmetrical response is usually necessary.

¹⁴ Kacper Rekawek, [“Russian State Terrorism and State Sponsorship of Terrorism”](#) (International Centre for Counter-Terrorism, September 2024).

¹⁵ Michael Schwartz, [“Poland’s Leader Suggests Russian Hand in Plot to Attack Western Cargo Planes,”](#) *The New York Times*, 15 January 2025.

For western nations, the bar for covert offensive actions inside Russia in a situation short of war is extremely high. Some states, however, have reportedly engaged in reciprocal cyber operations targeting capabilities of Russian actors. The most publicised case was the US Cyber Command's blocking of internet access to the notorious Internet Research Agency troll farm to prevent interference in the 2018 mid-term election – i.e., an offensive cyber operation that signalled the US's capabilities and willingness to target foreign interference networks.¹⁶ Such covert activities must be discreet and undertaken by a small group of the most capable nations.

Russia tends to hide behind the proxies. International legal frameworks, such as the International Law Commission's Articles on the Responsibility of States, provide a legal basis for addressing state-sponsored hybrid threats.¹⁷ To hold a state accountable for actions carried out by proxies, it must be demonstrated that the state controls or sponsors the perpetrators. Even if individuals within state institutions acted beyond their authority, the state remains accountable.

The challenge is finding an adequate response option that sends a message of resolve by targeting Russia where it hurts and inflicts sufficiently high costs for it to stop its hostile actions while considering undesired consequences. In this context, military responses to hybrid attacks are often seen as too escalatory, yet inaction allows the aggression to continue unchecked.

Successful deterrence must be tailored to a specific adversary

Deterrence is not merely a straightforward rational decision-making process; psychological and cognitive factors also play a significant role. Successful deterrence must be tailored

¹⁶ Ellen Nakashima, "[U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms](#)," *The Washington Post*, 26 February 2019; Andy Greenberg, "[US Hackers' Strike on Russian Trolls Sends a Message—but What Kind?](#)," *Wired*, 27 February 2019.

¹⁷ International Law Commission, "[Responsibility of States for Internationally Wrongful Acts](#)" in *Yearbook of the International Law Commission* Vol. II, Part Two (General Assembly, 2001).

to a specific adversary – in this case, Russia and its leadership. Responses to hybrid attacks should be based on an assessment of how they affect Russia's cost-benefit calculation, requiring an understanding of what motivates the Russian regime and what harms it the most. Countermeasures can target both those involved in hostile activities and the aggressor's general weaknesses; they should hold a credible promise of higher costs to follow in case of non-compliance.

A reasonable approach would be a combination of public and covert responses across various fields. Some of the countermeasures could be signalled in advance; others could be held in reserve, as an unpleasant surprise for Russia.

Ideally, there should be a matrix in place where specific Russian hybrid attacks correspond to targeted countermeasures

Ideally, there should be a matrix in place where specific Russian hybrid attacks correspond to targeted countermeasures. However, as hybrid threats are constantly evolving, creating such a matrix is a complicated task.

Possible targets of response measures include:¹⁸

- **Counterforce targets:** specific units and technical capabilities involved in conducting the attacks (e.g., individuals and units within Russian intelligence services). The goal is to degrade Russia's operational capability to cause harm.
- **Countervalue targets:** key elements of the Russian regime and economy, targeting which would have a broader economic and societal impact. This includes sectoral economic and financial sanctions.
- **Counterpolitical targets:** individuals and entities with significant political value (i.e., members of Russia's elite, including both formal leadership and members of informal power networks).

¹⁸ For conceptual principles, see: Mattia Bertolini, Raffaele Minicozzi, and Tim Sweijts, "[Ten Guidelines for Dealing with Hybrid Threats A Policy Response Framework](#)" (The Hague Centre for Strategic Studies, April 2023).

3.2. MULTILATERAL RESPONSE

The response to Russia's hybrid attacks can be:

- national;
- multilateral involving a unified response within the EU or NATO or a (regional) group of countries;

Effective deterrence by punishment requires international cooperation

Countering begins at the national level: both the EU and NATO have stated that, in the case of hybrid threats, the primary responsibility lies with individual states. However, effective deterrence by punishment requires international cooperation; therefore, NATO and the EU acknowledge that hybrid attacks also warrant a collective response. By treating a hybrid attack against one member state as an attack against the EU or NATO rather than an isolated event, a collective response demonstrates solidarity, which is especially crucial for smaller countries.

Building international coalitions to punish and deter an aggressor is a delicate task that considers nations' interests and broader geopolitical consequences. A small state like Estonia must be confident that if a specific action seems reasonable from its standpoint, the Allies will support it. The other dilemma is that if Russia were to conduct a hybrid attack that EU and NATO members would assess differently, it could deepen political divisions within these organisations, weakening their ability to respond as a unified bloc.

The aim should be a fast and coherent multilateral response, but political sensitivities related to national interests and priorities make it challenging to formulate one. States may have varying perspectives on how to handle hybrid threats, including fear of escalation and unintended consequences. Large consensus-based organisations like the EU are often slow due to the need for every member state to agree, resulting in lengthy internal decision-making processes. It can be further delayed by bureaucratic inefficiencies, leading to slow or insufficient response.

Therefore, especially in cases where states are affected by specific and geographically limited types of hybrid attacks, smaller regional groups of like-minded nations can prove more efficient. For example, the Baltic Sea states can collaborate on maritime security issues, while EU and NATO eastern-flank countries can address matters of border control and border security. This type of multilateral response has already been applied. In January 2025, damage to undersea critical infrastructure in the Baltic Sea and the corresponding responses were discussed in the novel format of the Baltic Sea NATO Allies Summit in Helsinki.¹⁹ The six nations bordering Russia – from Norway in the north to Poland in the south – have been coordinating on issues such as detecting and repelling drones.²⁰

Smaller regional groups of like-minded nations can prove more efficient

3.3. NATO

NATO, as a political-military Alliance with a clear focus on military matters, has struggled to define its role in countering hybrid attacks. They increasingly require a broader, multi-domain response, which NATO is unable to provide on its own. Therefore, already at its Warsaw Summit in July 2016, the Alliance emphasised the importance of enhanced cooperation with the European Union to address common security challenges, including the hybrid domain. At the Summit, the first NATO-EU declaration established a Joint Framework on Countering Hybrid Threats. In it, the two organisations committed to working closely together to strengthen their ability to detect, prevent, and respond.²¹

NATO's primary role in countering hybrid threats is related to the military domain and is framed within the broader context of

¹⁹ President of the Republic of Finland, "[Joint Statement of the Baltic Sea NATO Allies Summit](#)," Tasavallan Presidentti, 14 January 2025.

²⁰ "[Baltics, Poland, Finland, Norway to set up drone walls with Russia](#)," ERR, 25 May 2024.

²¹ President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, "[Joint declaration](#)" (NATO, 8 July 2016).

collective defence and deterrence. Hybrid warfare is not a standalone phenomenon: as observed in Ukraine, it can serve as a precursor to conventional war. In such situations,

Hybrid warfare can serve as a precursor to conventional war

military responses can include adjusting force posture, reactions, and readiness levels, as well as pre-emptive deployments of military capabilities in the face of escalating hybrid attacks. Such moves demonstrate capabilities and readiness to respond to a hybrid campaign with military means or specialised units, like special operations forces. NATO can coordinate the offensive use of cyber capabilities. These actions signal to potential aggressors that the Alliance will respond collectively to further escalation threatening to cross the threshold of military conflict.

A recent shift in NATO's strategic priorities is related to the protection of undersea energy and communication infrastructure, a critical vulnerability in the face of hybrid threats. Since 2022, to monitor and protect it, several dedicated coordination bodies have been established.²² In January 2025, following recent cable-cutting incidents in the Baltic Sea, NATO decided to enhance its maritime and surveillance presence by launching a Baltic Sentry mission. It is primarily aimed at deterring attempts for further sabotage. However, the problem is that it does not have the legal authority to intervene in ship movements – this authority lies with national law enforcement agencies.

At the 2024 Washington Summit, NATO leaders agreed on the need for additional countermeasures to hybrid attacks and a review of NATO's policies. The Alliance plans to adopt an overarching Russia policy at its upcoming summit in The Hague. Given the unprecedented turbulence and uncertainty caused by the Trump administration, the direction of this document remains unclear.

²² These include NATO's Critical Undersea Infrastructure Coordination Cell (CUICC), the Critical Undersea Infrastructure Network, the joint NATO-EU Task Force on Resilience of Critical Infrastructure, and the Maritime Centre for the Security of Critical Undersea Infrastructure.

3.3.1. ARTICLE 5

Since 2016, NATO has declared that hybrid actions against Allies could lead to invoking Article 5 of the Washington Treaty. So far, no attack has been deemed sufficient to meet the threshold of the collective defence clause. Activation itself requires consensus in the North Atlantic Council (NAC), which might be hard to achieve due to political decision-making. The conditions for a hybrid attack to be considered as meriting Article 5 activation can be assumed to include:

- attribution to an external actor (e.g., Al-Qaeda in the case of the 9/11 attacks), which may not be easy to determine;
- classification as an intentional action, not an accident;
- sufficient scale and impact (an attack resulting in casualties and/or massive damage).

Article 5 does not require a single catastrophic act to be activated; the cumulative effects of a series of coordinated attacks could trigger it. Thus, Article 5 focuses on the effects and magnitude of an attack rather than the means by which it is carried out.

The next question concerns the consequences of a hypothetical activation. The activation itself would send a clear signal that NATO considers itself at war. In the case of a conventional military attack, this triggers relevant military response plans. However, it remains unclear what NATO's response would be to a massive and costly hybrid attack where traditional military means may seem inappropriate.

NATO has not publicly communicated the level or extent of damage that would trigger Article 5. This ambiguity is deliberate and meant to deter, forcing the aggressor to exercise self-restraint and avoid large-scale attacks. While intentional, it also creates an opportunity for an aggressor to exploit: Russia's actions may, by design, stay below the threshold of collective defence provisions.

Although the only invocation of Article 5 took place in response to the 9/11 terrorist attacks

against the US, the commitment has been traditionally understood in the context of a conventional military attack. The invocation of Article 5 to respond to a covert hybrid attack is less straightforward, as the collective commitment is less suited for it.

3.3.2. ARTICLE 4

The connected question is whether Article 4 – triggered when an Ally believes its territorial integrity, political independence, or security is under threat – could be used. While Article 4 does not impose any obligation beyond consultation, its use is generally expected to lead to a joint decision and/or action. However, those can take place within NATO without formally activating Article 4.

Article 4 will be reserved for when a hybrid attack is perceived as severely undermining national security and a potential precursor to more overt actions

The added value of Article 4 lies primarily in situations where there is a clear risk of significant deterioration of the security situation: the activation itself signals that Article 5 could be triggered. Therefore, the Article 4 provisions will likely be reserved for when a hybrid attack is perceived as severely undermining national security and a potential precursor to more overt actions, including military force. There is a concern within the Alliance that the misuse of this clause for consultations in situations where there is no such real threat could undermine the deterrent power of both articles.

3.4. THE EUROPEAN UNION

The EU has a range of diplomatic, political, and legal measures at its disposal, which member states can collectively impose to address hybrid threats. It has established several tools, frameworks, and mechanisms to tackle this phenomenon. The EU's regulatory power allows it to address legal gaps, and as a political entity, it is often seen as a more suitable framework than NATO.

A lot of focus has been on building the resilience of EU member states. This involves reinforcing the security of critical infrastructure, increasing cybersecurity capabilities, and improving the EU's ability to respond to disruptions caused by hybrid attacks.

The EU's regulatory power allows it to address legal gaps, and as a political entity, it is often seen as a more suitable framework than NATO

- The EU's Critical Entities Resilience Directive (CER Directive) aims to strengthen the resilience of critical infrastructure across 11 key sectors, including energy, transport, health, and telecommunications, ensuring that essential services can withstand both cyber and physical disruptions.²³ It is now crucial for EU countries to prioritise adapting their national legislation and implementing these updated rules.

- In the field of cybersecurity, the key steps undertaken by the EU include the EU's Network and Information Security Directive (NIS2) aimed at bolstering cybersecurity resilience across essential services and critical infrastructure.²⁴ Meanwhile, the EU Agency for Cybersecurity (ENISA) is tasked with supporting member states in building up their cyber resilience.

The EU has developed several toolboxes that provide mechanisms for collective action. These toolboxes, designed to integrate responses from various sectors, equip the EU and its member states with a range of instruments to detect, respond, and counter hybrid threats.

- **Hybrid Toolbox**, formalised in December 2022, is the central element of the EU's response. It aims to pool resources with the key goal of ensuring coherence among the different instruments for an informed,

²³ [“Critical Entities Resilience Directive \(CER\) | Updates, Compliance,”](#) Cyber Rusk GmbH, accessed in March 2025.

²⁴ [“NIS2 Directive: new rules on cybersecurity of network and information systems,”](#) European Commission, 15 January 2025.

targeted, and coordinated response.²⁵ However, progress in implementing practical steps can be slow due to structural challenges within the EU, as legal and administrative frameworks must be respected. It remains uncertain whether the Hybrid Toolbox can effectively integrate efforts across various EU sectors.

- **Cyber Diplomacy Toolbox** is designed to provide the EU with a range of options for collectively addressing significant malicious cyber activities.²⁶
- **FIMI Toolbox** is a framework designed to counter foreign information manipulation and interference in the EU and member states, including monitoring and analysis of foreign interference campaigns and implementation of countermeasures.²⁷ One of its key objectives is to identify and expose foreign actors behind information manipulation efforts, thus enabling the attribution and sanctioning of those responsible.

Success often depends on political will, effective coordination, swift attribution, and continuous adaptation to Russian tactics

While the toolboxes provide frameworks for action, implementing them is not always easy or politically feasible. Hence, success often depends on political will, effective coordination, swift attribution, and continuous adaptation to Russian tactics. Reaching consensus among the 27 member states on the use of measures like sanctions can take time, while hybrid attacks often evolve rapidly.

Similar to NATO's Washington Treaty, the Treaty on European Union (TEU) contains clauses – Article 42.7 (mutual assistance clause) and Article 222 (solidarity clause) – that could be activated in response to hybrid attacks.

²⁵ Council of the EU, "[Council conclusions on a Framework for a coordinated EU response to hybrid campaigns](#)," European Council, Council of the European Union, 21 June 2021.

²⁶ "[The Cyber Diplomacy Toolbox](#)," Cyber Rusk GmbH, accessed in March 2025.

²⁷ "[Information Integrity and Countering Foreign Information Manipulation & Interference \(FIMI\)](#)," European Union External Action, 14 March 2025.

- **Article 42.7** obligates EU member states to provide "aid and assistance by all the means in their power" to a member state; it can be triggered in response to a hybrid attack if it rises to the level of armed aggression, although this has not been explicitly acknowledged by the EU. For instance, France invoked it in November 2015 following the terrorist attacks in Paris. Unlike Article 5, it does not require unanimity among member states and can be activated unilaterally. However, given NATO's central role in Europe's military defence, Article 5 remains more appropriate when an attack meets the threshold of armed aggression.

- **Article 222** establishes a framework for EU member states to assist one another in a crisis; it is more likely to be applied in response to a large-scale hybrid crisis or attack. It allows a nation in distress to request assistance and enables the EU to respond in solidarity, even if the attack has not yet been formally attributed. While Article 222 specifically addresses assistance in the case of natural disasters and terrorism, its potential application to hybrid attacks has been explored in exercises. The broader scope of the solidarity clause offers a more flexible framework in a wide range of scenarios. The European Commission plays a central role in coordinating the EU's response. Although not an immediate issue, Article 222 remains a viable option to consider further.

3.4.1. SANCTIONS

The key tool at the EU's disposal for targeting the initiators, enablers, and executors of hybrid attacks is sanctions. Targeted restrictive measures comprise freezing of assets, travel bans, and the prohibition on providing financial or technological support to individuals, groups or entities involved in attacks. The EU's framework contains the new Hybrid Sanctions Regime and sector-specific Cyber Sanctions Regime, as well as sanctions imposed on Russia in response to its aggression against Ukraine.²⁸

As of March 2025, over 2 400 Russian individuals and entities have been sanctioned under the 16 EU packages adopted in response

²⁸ "[EU Sanctions Map](#)," last updated 25 February 2025.

to the full-scale invasion.²⁹ While the formal criterion is their support of the war, many – such as agents of the Kremlin’s propaganda – have been implicated in Russian FIMI, and disinformation in particular, well beyond Ukraine.

- Under the horizontal **Cyber Sanctions Regime** established in 2019, the EU has targeted 17 individuals and 4 entities, with 15 and 2, respectively, linked to Russia’s intelligence services and cybercrime networks (others were of Chinese and North Korean origin).³⁰ The latest listing occurred in January 2025 when three individuals from GRU Unit 29155 were sanctioned for the 2020 cyberattacks against Estonia. Amidst the high number of cyberattacks, the relatively limited number of actors targeted by the cyber sanctions regime so far may indicate the difficulty of conclusively determining the exact perpetrators.³¹
- In October 2024, the EU established the **Hybrid Sanctions Regime** – the first Russia-specific tool to target individuals and entities involved in a broad range of hybrid threat activities. Its mandate is rather expansive, covering not only Russian citizens but also foreign nationals working on behalf of Russia. Additionally, it can be applied to address actions taken not only within the EU but globally, reflecting the wide-reaching nature of the Russian threat. The criteria encompass both non-kinetic and kinetic attacks, including the spread of propaganda and disinformation, political influence campaigns, interference activities, acts of violence, targeting of critical infrastructure, and the instrumentalisation of migration.³²

²⁹ “[EU sanctions against Russia explained](#),” European Council, Council of the European Union, last updated 19 March 2025.

³⁰ “[Cyber-attacks: three individuals added to EU sanctions list for malicious cyber activities against Estonia](#),” European Council, Council of the European Union, 27 January 2025.

³¹ Annegret Bendiek Matthias Schulze, “[Attribution: A Major Challenge for EU Cyber Sanctions An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW](#),” *SWP Research Paper* 2021/RP 11 (16 December 2021): 42; Stefan Soesanto, “[Europe Has No Strategy on Cyber Sanctions](#),” *Lawfare*, 20 November 2020.

³² The Council of the European Union, [Council Decision \(CFSP\) 2024/2643 of 8 October 2024 concerning restrictive measures in view of Russia’s destabilising activities](#) (European Union Law, 9 October 2024).

Targets are proposed by member states and the European External Action Service (EEAS), with the final selection based on political and legal relevance. The first package, adopted in December 2024, sanctioned 16 individuals and 3 entities (including GRU unit 29155) linked to Russia’s destabilising actions abroad.³³

The application of sanctions at the EU’s disposal is limited by the evidence requirements

The application of sanctions at the EU’s disposal is limited by the evidence requirements. The EU Council Legal Service reviews the lists to ensure that sufficient evidence is provided, maintaining a very high threshold of legal proof to withstand potential court challenges. However, hybrid threat actors typically operate in secrecy, while national intelligence services are often hesitant to release too much evidence publicly. Investigative journalism, therefore, plays a significant role in producing materials. In this approach, the EU contrasts with the US and the UK, where classified intelligence can be routinely used to impose sanctions. As a result, there are often discrepancies whereby the EU is unable to acquire sufficient evidence against a certain target whom others have sanctioned. While intelligence and investigative agencies should strive to release as much information as possible, the EU should also explore options to make its criteria more flexible.

The maximisation of the effectiveness of the EU sanctions regime requires close cooperation with like-minded partner countries. Such coordination reduces the target’s ability to bypass restrictions, improves enforcement, amplifies the effect, demonstrates a unified front, and maintains pressure on Russia.

Sanctions – although a key countermeasure tool – are not a silver bullet capable of changing a hostile state’s behaviour. Albeit a significant economic impact, sanctions have not managed to force Russia into ending its aggression in Ukraine. Likewise, Russia has continued to launch hybrid attacks against the west. Therefore, sanctions should be viewed as part

³³ Council of the EU, “[Russian hybrid threats: EU agrees first listings in response to destabilising activities against the EU, its member states and partners](#),” European Council, Council of the European Union, 16 December 2024.

of a broader strategy, where they complement other measures.

3.4.2. DIPLOMACY & VISA POLICY

Whereas diplomatic demarches and public condemnations can still signal displeasure, Russia has become largely indifferent to such rhetorical measures.

The expulsions of Russian intelligence operatives embedded in diplomatic missions have significantly weakened these services' ability

The expulsions of Russian intelligence operatives embedded in diplomatic missions have significantly weakened these services' ability to operate in Europe. This has forced them to switch to online recruitment and contract amateurs with criminal backgrounds to conduct acts of sabotage and vandalism, but the latter are less effective and motivated than professionals. More challenges exist. First, the expulsions have been inconsistent across Europe. Some countries, such as the Baltic states, have reduced Russian diplomatic missions to a bare minimum; others, including those hosting large international organisations, have only expelled a small number of agents. Second, a person declared *persona non grata* (PNG) by one European country is not automatically considered PNG throughout the EU. The goal should be to establish a union-wide recognition.

Moreover, it bears reminding that there is no clear distinction between Russian spies and Russian diplomats – both groups perform intelligence services' tasks. Mitigating this threat requires coordination in restricting Russian diplomats' freedom of movement across the Schengen area. Czechia proposed to limit 3 000 Russian diplomatic passport holders in the EU to travelling only inside the country to which they were assigned; the initiative has so far failed to garner support at the EU level.³⁴ Meanwhile, the number of Schengen visas issued to Russian nationals, having declined sharply in 2022, started to

rise again in 2024.³⁵ Despite Russia's acts of sabotage and other hybrid attacks, some EU countries remain reluctant to tighten their visa policies. One option would be to issue country-specific tourist visas – called “limited territorial validity visas” under Schengen rules – to Russian applicants.³⁶ Another policy worth pursuing in order to scrutinise Russian travellers would be the introduction of the requirement for biometric documents to enter the EU, which several member states have nationally adopted.

3.5. SHADOW FLEET

Hybrid warfare often capitalises on legal grey areas where international law is unclear or open to interpretation. To counter this, it is essential to eliminate the ambiguities that allow states like Russia to operate with plausible deniability, thereby reducing their incentive to engage in such tactics.

The recent series of cable and pipeline cuts in the Baltic Sea caused by ships – typically associated with Russia's so-called “shadow fleet” – dragging their anchors raised questions about the rights of coastal states to intervene when they suspect misconduct or outright sabotage. Strict interpretations of the law of the sea offer limited protection to affected nations, creating opportunities for perpetrators to exploit legal vulnerabilities.

Coastal states need to jointly take a more flexible and proactive approach, as exemplified by Finland's intervention with the Eagle S oil tanker in December 2024. Holding vessels and their owners accountable is essential to ensuring that damage to subsea infrastructure is not left unpunished and will not be tolerated. Coastal states must aim at a unified legal interpretation allowing them to act decisively to protect themselves, even if it means setting court precedents.

The Baltic Sea is the largest exit point for Russia's seaborne oil, a crucial source of revenue that fuels its war of aggression in

³⁴ Teri Schultz, “EU divided over axing Russian diplomats' Schengen privileges,” *DW*, 29 August 2024.

³⁵ Arbërie Shabani, “Russians Show Increased Interest in Obtaining Schengen Visas Despite Sanctions Imposed,” *Schengen News*, 7 November 2024.

³⁶ “Schengen Visa Types & Validity,” Schengenvisa Info, accessed in March 2025.

Ukraine.³⁷ Targeting Russia's shadow fleet, which operates under flags of convenience in a legally ambiguous and environmentally hazardous manner, will undermine the aggressor's capacity to continue. Furthermore, these vessels are often poorly maintained and uninsured, thereby adding environmental and security risks.

The Kremlin understands the tactics it employs against others

Beyond imposing at the EU-level targeted sanctions on the shadow fleet – including measures against vessels as well as their owners, operators, and insurers – and putting diplomatic and, if necessary, economic pressure on the countries that provide flags of convenience, the coastal states could engage in sorts of 'legal harassment'. Frequent inspections, as well as security and environmental safety checks, could hinder operations, making them less profitable and more difficult to run. The Kremlin understands the tactics it employs against others.

CONCLUSIONS AND RECOMMENDATIONS

The increasing frequency and sophistication of Russia's hybrid attacks across Europe demand a comprehensive and multi-layered response. Their complexity – ranging from cyberattacks and disinformation to sabotage and kinetic attacks – challenges conventional defence and deterrence strategies.

Russia's hybrid attacks challenge conventional defence and deterrence strategies

Although response will remain primarily a national responsibility, the EU and NATO acknowledge the criticality of international cooperation. However, efforts so far have been hampered by fragmented national responses, slow decision-making, challenges in attribution, and lack of political will, driven by fears of escalation.

³⁷ ["Financing Putin's war: Fossil fuel imports from Russia during the invasion of Ukraine,"](#) Centre for Research on Energy and Clean Air, accessed in March 2025.

First and foremost, deterrence through denial must be strengthened. Rather than attempting to stop every attack, the focus should be on ensuring they are ineffective and costly for the aggressor. The response to Russia's hybrid operations cannot rely solely on resilience. An effective deterrence strategy should combine resilience-building and crisis response with the capacity to impose significant costs.

The swift and clear attribution of hybrid attacks is an essential step. European nations should ramp up counterintelligence and strategic communications activities to expose and counter Russian hybrid campaigns. Public attribution, combined with fact-based messaging about these malign activities, can weaken Moscow's ability to maintain plausible deniability and help win the information war.

An effective deterrence strategy should combine resilience-building and crisis response with the capacity to impose significant costs

As part of this effort, nations should more frequently refer to Russian sabotage attacks as acts of state terrorism.

Russia's exploitation of legal grey areas, such as the maritime domain, should be addressed by clearer international regulations. Coastal states should unify their interpretations to allow for decisive action against damage to critical infrastructure, even if it means setting legal precedents. Challenges in consensus-building, with some countries adopting an overtly pro-Russian stance, may make small coalitions of the willing a more promising path to pursue. These often regional groups can act more swiftly than large international organisations, of which the Baltic littoral states' cooperation in maritime security and undersea infrastructure protection is a model to follow.

Hybrid attacks require multi-domain response measures: intelligence-sharing and situational awareness, as well as collective punitive actions, such as sanctions, diplomatic expulsions, and targeting Russian economic interests. European nations should adopt a unified approach to expulsions of Russian intelligence

operatives and tighten Schengen visa policies. Additionally, covert actions – such as offensive cyber operations aimed at degrading Russia’s capacity to conduct hybrid campaigns – should be an option in the response toolkit.

The Baltic littoral states’ cooperation in maritime security and undersea infrastructure protection is a model to follow.

The EU – with its existing institutional tools, especially sanctions regimes with a broad mandate – provides a viable legal and regulatory framework. Enhancing its flexibility may require lowering the evidentiary threshold and relying more on classified intelligence. NATO – with its focus on military matters – does not have a clearly defined role but remains a crucial part of the overall deterrence, sending a clear signal to the aggressor not to escalate from hybrid actions to full-scale military conflict.

While full deterrence may remain elusive, European nations can build a robust deterrence framework that not only defends against immediate threats but also signals a united front. To achieve that goal, like-minded states should consider the following recommendations:

- Strengthen national resilience to mitigate the impact and increase the cost;
- Improve attribution capabilities for swift and clear identification;
- Enhance intelligence-sharing and situational awareness, counterintelligence, and strategic communications to expose and counter malign activities;
- Label sabotage as state terrorism to increase the moral and legal weight of a response;
- Use sanctions more extensively, enforce sanctions regimes, encourage coordination, and increase flexibility;
- Unify legal interpretations, especially in maritime law;
- Standardise visa and expulsion policies;
- Foster smaller coalitions of willing nations and expand regional cooperation.

Ultimately, reinforcing European security requires a sustained, collective effort to hold Russia accountable and demonstrate that its hybrid tactics will not go unpunished.

RECENT ICDS PUBLICATIONS

REPORTS

- Arjakas, Merili, Kai Kaarelon, Solveig Niitra, Hille Hanso, Ivan U.K. Lyszcz. *Eesti roll muutuvast rahvusvahelise arengukoostöö arhitektuuris* [Estonia's Role In the Changing Architecture of International Development Cooperation]. March 2025.
- Klyszcz, Ivan U.K., Tony Lawrence, Eric Chan, Jyun-yi Lee. *Deterrence and Hybrid Warfare: Lessons from Russia's War in Ukraine for Taiwan and the Nordic-Baltic Region*. February 2025.
- Hosaka, Sanshiro. *A Mountain to Climb: Russia's Influence in the South Caucasus and EU Policy Options*. January 2025.
- Gretskiy, Igor. *New Russian Immigration to the EU: The Case of the Baltic States, Finland, Germany & Poland*. October 2024.
- Atanassova-Cornelis, Elena, Takuya Matsuda, Bart Gaens, and Nele Loorents. *Japan, NATO, and the Diversification of Security Partnerships*. September 2024.
- Klyszcz, Ivan U.K. (editor), Che-chuan Lee, and James Sherr. *China's and Russia's Aggressive Foreign Policies: Historical Legacy or Geopolitical Ambitions?* June 2024.

POLICY PAPERS

- Loorents, Nele, and Jun Nagashima. *"Bridging Two Oceans: The Evolving NATO-Japan Relationship."* July 2024.
- Akhvlediani, Tinatin, and Veronika Movchan. *"The Impact of Ukraine's Accession on the EU's Economy: The Value Added of Ukraine."* February 2024.
- Maigre, Merle. *"An E-Integration Marathon: The Potential Impact of Ukrainian Membership on the EU's Digitalisation and Cybersecurity."* January 2024.

ANALYSES

- Hanso, Toomas. *"Central Asia's New Railways: Russia's Pain, China's Gain."* March 2025.
- Alatalu, Siim. *"The EU's NIS2 Directive A Business Opportunity for the Defence Sector."* March 2025.
- Peterson, Annabel. *"The Enemy Within: Russians in Ukrainian Army Ranks and the Fracturing of Post-Soviet Identity."* February 2025.
- Idarand, Tõnis. *"For as Long as It Works: Russia's Nuclear Signalling During Its War in Ukraine."* January 2025
- Hanso, Toomas. *"China's New Information Support Force: Military Lessons from Ukraine."* December 2024.
- Sõukand, Kaspar. *"The Iron Leviathan: Russia's Rail Network in its War against Ukraine."* December 2024.
- Sundquist, Sara Matea. *"High Noon for the High North? Norway, Russia, and the Svalbard Stronghold."* November 2024.
- Leveque, Justin. *"Russian Malign Activities in France Since 2022: Stoking Tensions, Sowing Disorder, Disrupting Assistance to Ukraine."* September 2024.
- Vitiello, Alessandro. *"Shared Goals, Different Paths, and a Complex Outcome: A Deep Dive into Ukraine's 2024 Bilateral Security Agreements."* September 2024.

BRIEFS

- Tõhk, Tauno. *"More Than a Systemic Rival: China as a Security Challenge for the EU."* March 2025.
- Cordet, Maxime, and Marianne Paire. *EU Defence Series*. March 2025.
- Hosaka, Sanshiro. *"Why the 'Reverse Nixon' Strategy Will Fail: The Illusion of Decoupling."* March 2025.
- Claessen, Koen. *"The EU's Dilemmas in the Black Sea Region: Security and Enlargement."* March 2025.
- Klyszcz, Ivan U.K. *"Russia's Self-Serving Aid Policy: Influence, Opacity, and Propaganda."* March 2025.
- Blockmans, Steven. *"A New but Ambiguous Momentum in EU Enlargement."* February 2025.
- Nazarov, Mykola, Andriy Stavtyskyi, Leonid Polyakov, Stanislav Zhelikhovskiy, Maryna Vorotyntseva, Vitaliy Goncharuk, and Mykhailo Samus. *"Russia's War in Ukraine Series, Volume 2."* March 2024 / January 2025.

All ICDS publications are available from <https://icds.ee/category/publications/>.



ICDS.TALLINN



@ICDS _ TALLINN



@ICDS-TALLINN.BSKY.SOCIAL



ICDS-TALLINN



WWW.ICDS.EE



INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
63/4 NARVA RD., 10120 TALLINN, ESTONIA
INFO@ICDS.EE

ISSN 2228-2068