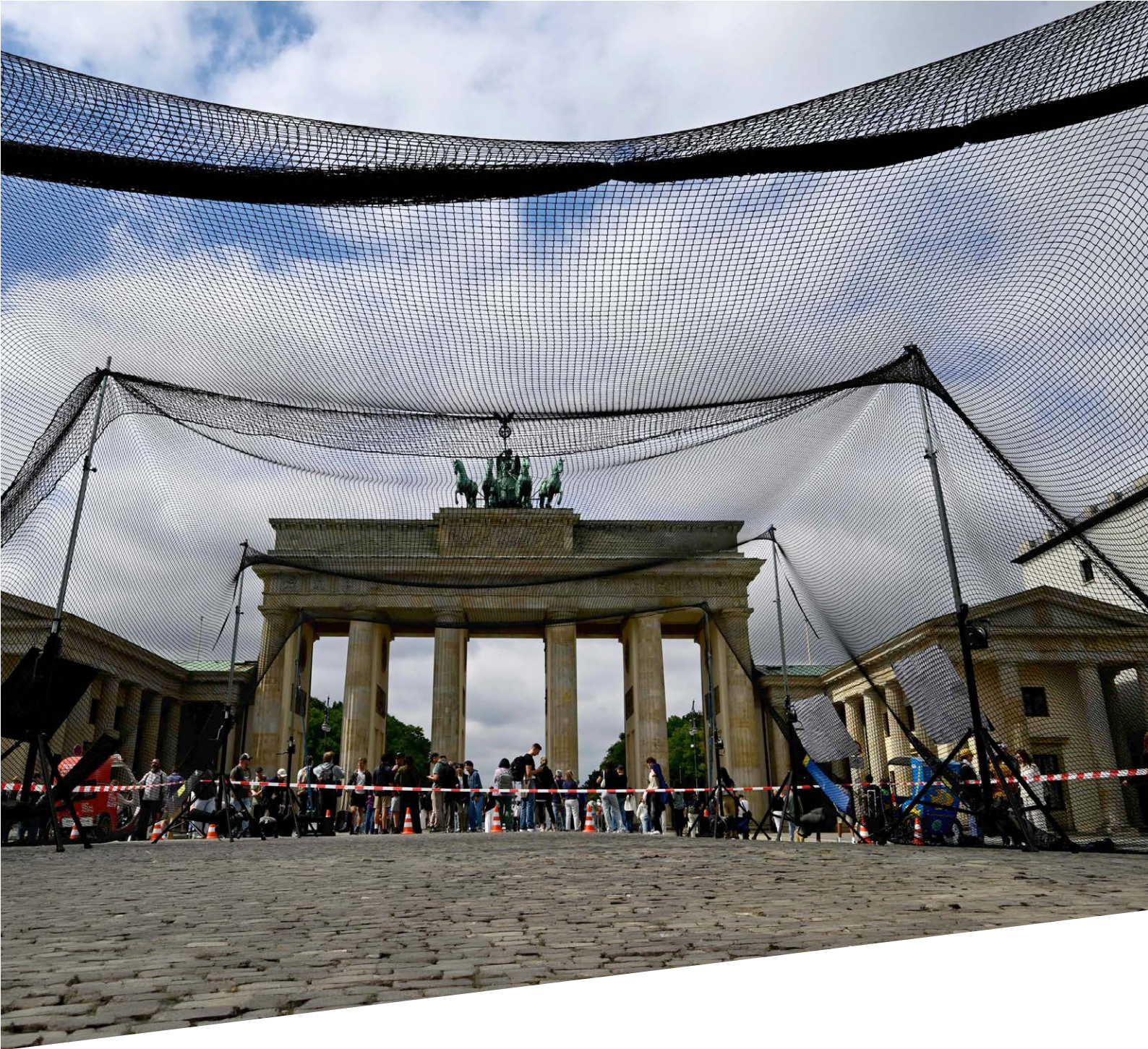




ANALYSIS

FIGHTING A WAR AT HOME

THE INSTITUTIONALISATION OF GERMANY'S RESPONSE
TO RUSSIAN HYBRID ATTACKS

| NAOMI BREUER |

SEPTEMBER 2026

RKK
ICDS

RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI - ESTONIA

Title: Fighting a War at Home: The Institutionalisation of Germany's Response
to Russian Hybrid Attacks

Author: Breuer, Naomi

Publication date: September 2026

Category: Analysis

Cover page photo: Berlin's Brandenburg Gate behind a symbolic protective netting against drones on 24 August 2026, marking Ukrainian Independence Day and calling attention to Russia's drone attacks against Ukraine. John MACDOUGALL / AFP / Scanpix.

Keywords: cyberattacks, deterrence, disinformation, drone incursions, espionage, Germany, hybrid warfare, resilience, Russia, sabotage

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 2228-2076

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

CONTENTS

List of Abbreviations	II
Acknowledgements	III
About the Author	III
Introduction	1
1. Phase I: Reactive and Defensive (2022–24)	2
1.1. APT28 Attack	2
1.2. Dieter S. Sabotage and Reconnaissance Operation	3
1.3. Arson at the Rheinmetall CEO Home	3
1.4. DHL Fire in Leipzig	4
2. Phase II: Institutionalisation of the Response (2024–26)	4
2.1. 2024 Cyberattacks	4
2.2. NoName057(16) hacktivist network	5
2.3. 2025 Federal Elections	5
2.4. 2026 Elections	6
2.5. Drone Flyovers	6
2.6. Assassination Plots	7
3. The Shift in Rhetoric and Law	8
4. Feeling the War at Home	9
Conclusion	9

LIST OF ABBREVIATIONS

AfD	Alternative for Germany (<i>Alternative für Deutschland</i>)
BfV	Federal Office for the Protection of the Constitution (<i>Bundesamt für Verfassungsschutz</i>)
BA	Federal Criminal Police Office (<i>Bundeskriminalamt</i>)
BMI	Federal Ministry of the Interior (<i>Bundesministerium des Innern</i>)
BND	Federal Intelligence Service (<i>Bundesnachrichtendienst</i>)
CDU	Christian Democratic Union (<i>Christlich Demokratische Union Deutschlands</i>)
DdoS	distributed denial-of-service
FDP	Free Democratic Party (<i>Freie Demokratische Partei</i>)
GBA	Federal Public Prosecutor's Office (Generalbundesanwalt beim Bundesgerichtshof)
GDAZ	Joint Drone Defence Centre (<i>Gemeinsames Drohnenabwehrzentrum</i>)
GDP	gross domestic product
IT	information technology
SPD	Social Democratic Party (<i>Sozialdemokratische Partei Deutschlands</i>)
ZEAM	Central Office for the Detection of Foreign Information Manipulation (<i>Zentrale Stelle zur Erkennung ausländischer Informationsmanipulation</i>)

ACKNOWLEDGEMENTS

The author is grateful to Marek Kohv, Head of the Security and Resilience Programme at the ICDS, and Tomas Jermalavičius, ICDS Head of Studies, whose insights and comments greatly strengthened this analysis.

ABOUT THE AUTHOR

NAOMI BREUER

Naomi Breuer is a third-year economics and international relations student at Stanford University. Her research interests include European security, democratic resilience, and transatlantic relations, with a particular focus on Germany. Her work also explores Russia, information security, and the intersection of political and economic developments. She has experience in journalism and policy research. In summer 2026, she was an intern at the ICDS under the security and resilience programme, where she contributed to research on German defence and security issues.

As one of Russia's primary targets, Germany has faced hybrid attacks that have taken the form of disinformation campaigns, cyberattacks, drone flyovers, and acts of sabotage. They exploit concerns about a perceived lack of sovereignty, overreliance on the EU, fears of the war spreading, threats to security and territorial integrity, corruption, and the

Germany is particularly vulnerable because of limits on its surveillance measures and a strict separation between intelligence services and law enforcement

INTRODUCTION

Germany's response to Russian hybrid threats has become institutionalised since 2022 due to emergent evidence revealing a sustained campaign against German society and democracy. Officials now treat the issue more seriously and consider offensive countermeasures.

Since Russia's invasion of Ukraine, Moscow has targeted western nations through hybrid warfare to undermine their democratic institutions, justify its war of aggression, and impede the international response and public support to Ukraine. Germany has been experiencing some of Europe's most sustained campaigns due to its pivotal role in the EU, its growing weight in NATO, and its status as the world's third-largest economy. Berlin is also the second-largest bilateral donor to Ukraine, having provided nearly €100 bn since the start of the full-scale invasion through the beginning of 2026.¹ Germany has trained more than 24 000 Ukrainian troops, provided around €55 bn in military aid and €1.2 bn in support for the energy sector, and supplied humanitarian aid.² It leads European rearmament and, as a logistical hub, NATO's support for Ukraine. It plans to increase its defence budget to €162 bn by 2029, more than any other European country.³

declining trust in government.⁴ Germany tied with Estonia for having the third most hybrid attacks between 2022 and mid-2025, with 11 episodes recorded, and incidents generally more severe than average: 2 assassination attempts, 5 attempted arsons or attacks with explosives, and drone flyovers at military bases.⁵ The country is particularly vulnerable because of limits on its surveillance measures and a strict separation between intelligence services and law enforcement.⁶

German authorities now see the campaigns as a coordinated Russian strategy, prompting a shift from reactive crisis management to a more institutionalised, anticipatory approach. "The goal of these Russian cyber and disinformation attacks is clear: It is to divide society, stir up mistrust, provoke rejection, and weaken confidence in democratic institutions," German Foreign Ministry spokesperson Martin Giese said.⁷ This analysis traces the evolution by studying major hybrid incidents since 2022 and assessing how each helped shape responses and rhetoric.

¹ Christoph Hasselbach and Bernd Riegert, "[Germany to Maintain Ukraine Aid despite Political Headwinds](#)," *Deutsche Welle*, 14 April 2026.

² Hasselbach and Riegert, "Germany to Maintain Ukraine Aid."

³ Liana Fix, "[Europe Rearms](#)," *Council on Foreign Relations*, n.d., accessed in August 2026.

⁴ Anastasia Pociumban and Ricarda Nierhaus, [Countering Hybrid Threats](#), Report No. 1 (German Council on Foreign Relations, February 2026).

⁵ Kacper Rekawek, Julian Lanchès, Maria Zotova, and Donald Bowser, [Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare](#) (International Center for Counter-Terrorism, 30 September 2025).

⁶ Stephanie Baker and Aaron Kirchfeld, "[Russia's Secret War and the Plot to Kill a German CEO](#)," *Bloomberg*, 5 August 2025.

⁷ Richard Connor, "[Germany Summons Russian Ambassador over 'Hybrid' Attacks](#)," *Deutsche Welle*, 12 December 2025.

1. PHASE I: REACTIVE AND DEFENSIVE (2022–24)

During the first two years of the full-scale invasion, Germany's response to hybrid campaigns was primarily reactive and defensive. Lacking information on the scale and extent, Berlin focused on reacting to individual episodes rather than developing a structured response.

1.1. APT28 ATTACK

One episode marked a shift in Germany's understanding of Russian cyber threats. A year-long investigation revealed that Russia's interference was far longer-running and more severe than previously known. The government issued a statement in May 2024 attributing the campaign to APT28, a group tied to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (*Главное управление Генерального штаба Вооружённых Сил Российской Федерации*,

Russia's interference was far longer-running and more severe than previously known

GRU), and thus assigning responsibility to the Russian state.⁸ This attribution led Germany to adopt a more explicit approach incorporating deterrence measures and diplomatic consequences for Russia.

An investigation was triggered when, in January 2023, email accounts of the Executive Committee of the Social Democratic Party (*Sozialdemokratische Partei Deutschlands*, SPD) were compromised.⁹ Around the same time, several government websites went offline – after Berlin had made the decision to send tanks to Ukraine. After the breach, then-Federal Minister of the Interior Nancy Faeser promised to strengthen protective measures, prepare for further attacks, and increase efforts against manipulation and

disinformation ahead of that year's European elections.¹⁰ The initial response focused primarily on prevention and resilience rather than retaliation and deterrence.

The initial response focused primarily on prevention and resilience rather than retaliation and deterrence

The investigation – conducted by the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*, BfV), Germany's federal domestic intelligence agency, along with foreign partners and other German institutions – revealed some of the most important evidence to date.¹¹ In particular, the campaign was sponsored by the Russian state, which Foreign Minister Annalena Baerbock called "intolerable and unacceptable."¹² The investigation revealed that the campaign had begun in March 2022 and that the group was also behind the attacks on other government agencies, as well as logistics, defence, aerospace, and IT companies;¹³ the same group was responsible for a cyberattack on the Bundestag in 2025.¹⁴

The investigation has helped Germany better understand the reach of Russia's hybrid warfare and triggered a harsher response. Interior Minister Faeser said Germany would act in coordination with the EU and NATO to respond to the attacks that are a threat to democracy.¹⁵ The Foreign Ministry summoned the Russian ambassador in May and December 2024, a strong diplomatic tool that underscored the gravity of Germany's concern, and alluded to further measures.¹⁶ Consequently, the approach shifted from prevention to deterrence and security measures, adopting

⁸ "Germany Summons Russian Envoy over Cyberattack," *Deutsche Welle*, 5 March 2024.

⁹ Bundesregierung, *Attribution of a Russian Cyber Campaign* (Bundesregierung, 2024).

¹⁰ "Germany Summons Russian Envoy over 2023 Cyber-Attacks," *The Guardian*, 3 May 2024.

¹¹ Bundesamt für Verfassungsschutz, *APT28 verantwortlich für großangelegte Cyberkampagne* [APT28 Responsible for Large-Scale Cyber Campaign] (Bundesamt für Verfassungsschutz, 2024).

¹² "Germany Summons Russian Envoy over Cyberattack," *DW*.

¹³ Bundesamt für Verfassungsschutz, *APT28 verantwortlich für großangelegte Cyberkampagne*.

¹⁴ Bundesregierung, *Attribution of a Russian Cyber Campaign*.

¹⁵ "Germany Summons Russian Envoy over 2023 Cyber-Attacks," *The Guardian*, 3 May 2024.

¹⁶ Connor, "Germany Summons Russian Ambassador."

a firmer tone against Russia. The government also became more anticipatory, as the Federal Ministry of the Interior (*Bundesministerium des Innern*, BMI) started coordinating cross-departmental measures to protect the upcoming European elections.¹⁷

1.2. DIETER S. SABOTAGE AND RECONNAISSANCE OPERATION

Dieter S., the group leader, and his two accomplices were arrested in April 2024 for spying on behalf of Russia and planning attacks on German industry and military infrastructure, which led the German government to take a tougher stance on espionage.¹⁸

Berlin summoned the Russian ambassador, and then-Chancellor Olaf Scholz emphasised the need to counter the Russian threat.

The three German-Russian dual citizens collected confidential information about an oil refinery in Bavaria and a US military training area, Grafenwöhr, discovered the codewords for military goods, and planned bomb attacks on buildings and infrastructure used to supply aid to Ukraine.¹⁹ In particular, Dieter S. spent six months mapping military infrastructure since the end of 2023.²⁰ In October 2025, he was convicted of spying, preparing arson attacks on military installations and railways, and participating in a foreign terrorist organisation. He was sentenced to six years in prison, while the others received twelve and six months. The court found that the operation aimed to incite fear in the population and depress political support for Ukraine.²¹

In response, Foreign Minister Baerbock said the government would not allow Russia to bring its terror onto German soil.²² Justice

Minister Marco Buschmann confirmed that the country was indeed a target.²³ The high-profile statements indicate Germany's growing concern about hybrid threats and willingness to take a firmer stance against Russia. Notably, the perpetrators had been arrested before any attacks could take place, showing that Germany's proactiveness helped prevent significant destruction.

The high-profile statements indicate Germany's growing concern about hybrid threats and willingness to take a firmer stance against Russia

This incident also helped Germany realise the severity of the internal threat Russia posed – not only of espionage but also of active terrorists on the ground. It also exposed the threat of 'disposable agents,' i.e., low-level operatives recruited online who may not even know who they work for.²⁴ In response, Green Party member and member of the parliamentary committee overseeing German intelligence agencies Konstantin von Notz said the counterintelligence services need to be reorganised.²⁵

1.3. ARSON AT THE RHEINMETALL CEO HOME

In April 2024, Russia-linked arsonists set fire to the residence of Armin Papperger, the CEO of Rheinmetall, Germany's largest defence company. The plot drew attention to the growing number of Russia's kinetic attacks.²⁶ However, the perpetrators were never caught. Prior to the attack, US intelligence services had alerted the German officials to the plot, but the case was dropped due to a lack of evidence

¹⁷ Bundesministerium des Innern, [Cyberangriffe stammen von russischem Militärgeheimdienst](#) [Cyberattacks Originated from Russian Military Intelligence] (Bundesministerium des Innern, 2024).

¹⁸ Kate Connolly, "Three Men on Trial in Germany Accused of Russian Sabotage Plot," *The Guardian*, 20 May 2025.

¹⁹ Connolly, "Three Men on Trial in Germany."

²⁰ Louisa Off, "German Courts Convict Russian Spy, Start Trial of Three Other Suspects," *Reuters*, 30 October 2025.

²¹ Off, "German Courts Convict Russian Spy."

²² "Germany Charges 3 over Alleged Russia Spying Plot," *Deutsche Welle*, 30 December 2024.

²³ Carlo Angerer and Patrick Smith, "Germany Arrests 3 Suspected of Plotting Russian Sabotage against U.S. Military Sites and Ukraine Aid," *NBC News*, 21 April 2025.

²⁴ Ray Furlong and Iryna Sysak, "A Munich Courtroom Casts a Spotlight on Russia's Amateur Saboteurs," *Radio Free Europe/Radio Liberty*, 24 May 2025.

²⁵ Furlong and Sysak, "A Munich Courtroom Casts a Spotlight."

²⁶ Stephanie Baker and Aaron Kirchfeld, "Russia's Secret War and the Plot to Kill a German CEO," *Bloomberg*, 5 August 2025.

or firm leads.²⁷ This incident exemplifies the potentially deadly consequences of failing to take the Russian threat seriously, as well as a broader trend of failing to detect threats without US assistance. “The Americans rightly perceive themselves as a source of information for us on everything from child pornography to terrorism and are not happy with the fact that if it weren’t for them, we would be blind,” a German security advisor said.²⁸ Minister Baerbock echoed the sentiment, adding that the assassination plot proved that the Russian government was conducting hybrid warfare and that Europe must be wary of the issue and protect itself. The German government declined to further comment on the reports, and no specific measures to deter similar threats were announced.²⁹

1.4. DHL FIRE IN LEIPZIG

In contrast, Germany’s response to a fire at a DHL logistics centre at Leipzig airport in July 2024 reflected that authorities began to realise that Russia was targeting all sectors of the German economy and society. The incident involved a package with an incendiary device and a timer inside a shipping container at the logistics centre.³⁰ BfV head Thomas Haldenwang stated at the Bundestag that German intelligence services had determined Russia was responsible for this act of sabotage.³¹ The Federal Prosecutor’s Office (*Generalbundesanwalt beim Bundesgerichtshof*, GBA), which investigates crimes committed against Germany, was involved.³² Arrests were made in Lithuania and Poland.³³

²⁷ Baker and Kirchfeld, “Russia’s Secret War.”

²⁸ Greg Miller, Souad Mekhennet, and Ellen Francis, “Europe Worries about Its Dependence on U.S. Intelligence under Trump,” *The Washington Post*, 5 June 2025.

²⁹ “Bericht über russischen Anschlagplan auf Rheinmetall-Chef [Report on Russian Assassination Plot against Rheinmetall Chief],” *Tagesschau*, 11 July 2024.

³⁰ “Was soll das neue Abwehrzentrum bringen? [What Is the New Defence Centre Supposed to Achieve?],” *Tagesschau*, 16 June 2026.

³¹ Bart Noëth, “German Intelligence Accuses Russia of Sabotage That Nearly Caused an Air Disaster,” *Aviation24*, 14 October 2024.

³² “Bundesanwaltschaft ermittelt nach Brand eines DHL-Luftfrachtpakets [Federal Prosecutor Investigates after Fire on DHL Air-Freight Package],” *Die Zeit*, 15 October 2024.

³³ Noëth, “German Intelligence Accuses Russia of Sabotage.”

2. PHASE II: INSTITUTIONALISATION OF THE RESPONSE (2024–26)

Since then, Germany has come to better anticipate attacks and has implemented deterrence and protection measures. Berlin has also established more systematised methods for investigation and response, such as teams and centres dedicated to countering hybrid attacks. Although the country has not yet fully mastered how to keep Russia at bay, it is now working on new approaches, including active countermeasures.

2.1. 2024 CYBERATTACKS

One week before the European elections in June 2024, the Christian Democratic Union of Germany (*Christlich Demokratische Union Deutschlands*, CDU) party network was hacked. Several agencies were called in to repel the attack, investigate it, and prevent further damage; the BfV issued a subsequent warning to all Bundestag parties. However, no new legislation followed – only an investigation and mitigation measures. The approach was primarily reactive and defensive.³⁴

That same month, though, the BMI established an interministerial Central Office for the Detection of Foreign Information Manipulation (*Zentrale Stelle zur Erkennung ausländischer Informationsmanipulation*, PG ZEAM) to examine hybrid-warfare methods and detect and understand them early. As a joint initiative of several federal ministries, with a mandate to counter hybrid threats and protect democracy and a proposed budget of €7.8 mn in 2025, it provides the government with stronger response capabilities.³⁵ While ZEAM took time to develop, its establishment reflected a more institutionalised approach

³⁴ “Schwerer Cyberangriff auf die CDU [Serious Cyberattack against the CDU],” *Tagesschau*, 1 June 2024.

³⁵ “Zentrale Stelle zur Erkennung ausländischer Informationsmanipulation (ZEAM) [Central Office for the Detection of Foreign Information Manipulation (ZEAM)],” Bundesministerium des Innern, n.d., accessed in August 2026; Mina Trpkovic, “Germany’s Fragmented Approach to Disinformation in 2025 Elections,” *PRIF Blog*, 3 February 2025.

to countering hybrid threats in Germany and a growing desire for better coordination and action.

2.2. NONAME057(16) HACKTIVIST NETWORK

The NoName057(16) episode led to another evolution in Germany's response to hybrid threats. NoName057(16) is a pro-Russian hacktivist network known for disruptive distributed denial-of-service (DDoS) attacks. Germany's response was proactive, especially through law enforcement measures and coordination with international actors. Eastwood, a joint international operation coordinated by Europol and Eurojust, moved against the group in July 2026 and dismantled some of its infrastructure.

Germany issued six arrest warrants for the offenders residing in Russia; all suspects were placed on the international wanted list, and five were added to the EU Most Wanted website.³⁶ Twenty-four properties belonging to individuals affiliated with the group were searched, and more than a thousand suspected supporters were informed via Telegram that such actions are punishable under German law.³⁷

It was later revealed that several members of the network had been implicated in cyberattacks in 2023 and 2024: 14 waves of attacks targeting over 250 companies and institutions have been recorded since investigations began in November 2023.³⁸ The targets included arms manufacturers, power suppliers, transport companies, public institutions, and government agencies – i.e., organisations supporting Ukraine. According to the Federal Criminal Police Office (*Bundeskriminalamt*, BKA), the main objective was to gain media attention and influence political decisions.³⁹

While this specific group has been neutralised, cybercrime remains prevalent: around 334 000 cases targeting the internet, data networks, IT systems, or their data were recorded in 2025, with two-thirds originating outside Germany or from unknown locations. It has cost the German economy an estimated €202.4 bn in damage, around 4.5% of GDP.⁴⁰ "Cyber criminals continually adapt their methods, thus increasing pressure on the state, the economy and society. In light of this, it is critical that we also keep pace with developments," BKA Vice President Martina Link said.⁴¹

While not all of Germany's actions to protect itself in the cyber domain are part of its hybrid response, these measures have made the country more resilient

While not all cyberattacks are part of Russia's hybrid campaign, and not all of Germany's actions to protect itself in the cyber domain are part of its hybrid response, these measures have made the country more resilient. While ransomware attacks increased by over 10% in 2025, fewer victims paid ransom, suggesting many businesses have become more resistant. Germany is also exploring AI to enable faster responses and detect vulnerabilities.⁴²

2.3. 2025 FEDERAL ELECTIONS

Perhaps the most significant reflection of Germany's increasingly proactive and institutionalised response to hybrid threats was its preparation for the 2025 federal elections. The BfV publicly warned about the potential for foreign influence and manipulation, anticipating disinformation campaigns, cyberattacks, espionage, and sabotage by Russia, and set up a task force

³⁶ "Global Operation Targets NoName057(16) Pro-Russian Cybercrime Network: The Offenders Targeted Ukraine and Supporting Countries, Including Many EU Member States," Europol, 16 July 2025.

³⁷ "Behörden schalten Servernetz prorussischer Hacker ab [Authorities Shut Down Server Network of Pro-Russian Hackers]," *Tagesschau*, 16 July 2025.

³⁸ Europol, "Global Operation Targets NoName057(16)."

³⁹ *Tagesschau*, "Behörden schalten Servernetz prorussischer Hacker ab."

⁴⁰ Federal Ministry of the Interior, *2025 National Situation Report on Cyber Crime: Germany Is a Prime Target of Cyber Criminals* (Federal Ministry of the Interior, 2026).

⁴¹ Federal Ministry of the Interior, *2025 National Situation Report on Cyber Crime*.

⁴² "2025 National Situation Report on Cyber Crime: Germany Is a Prime Target of Cyber Criminals," Federal Ministry of the Interior, 12 May 2026.

for handling those.⁴³ The CDU, SPD, Free Democratic Party (*Freie Demokratische Partei*, FDP), Alliance 90/the Greens (*Bündnis 90/Die Grünen*), and the Left Party (*Die Linke*) signed the Fairness Agreement, mutually committing to refrain from disinformation, AI-generated content, and violence throughout the election campaign.⁴⁴ The BMI also introduced a procedure for attributing foreign manipulation and disinformation to state actors. This allowed the government to publicly link the online media outlet *Red* and the Storm-1516 campaign to Russia, and made attribution central to Germany's fight against hybrid warfare.⁴⁵ Together, these measures indicate a more proactive approach to anticipating attacks and taking appropriate measures to mitigate their effect.

The government's proactive, anticipatory approach meant the country was no longer caught off guard

After the elections, however, the BfV issued a report that found that the hybrid attacks were not as extensive as anticipated. Disinformation and misinformation (including AI-generated content), exploitation of far-right narratives, articles and videos designed to appear as news sites, and pro-Russia influencers and messages persisted, but the government's proactive, anticipatory approach meant the country was no longer caught off guard.⁴⁶

The lack of action shows that a strategy has not fully been developed and that Berlin is still hesitant to take sweeping measures

discredit candidates and portray the country as deeply divided.⁴⁷ The government has been monitoring the campaign but, because it has not yet had significant reach, has not taken active measures (e.g., deleting videos) to reduce its impact, the interior ministry says. Nor has the campaign been attributed to the Russian state but, according to security sources, German authorities are certain Moscow is behind it.⁴⁸

The campaign began on 24 June, and over 180 fake posts have already circulated on X, BlueSky, and TikTok. However, the overarching campaign was traced back to 2023 and previously targeted the 2025 federal elections. All parties have been affected – except the Alternative for Germany (*Alternative für Deutschland*, AfD), which aims to restore German-Russian relations.⁴⁹

Although Germany has become better at anticipating hybrid attacks, the lack of action, particularly in this case, shows that a strategy has not fully been developed and that Berlin is still hesitant to take sweeping measures that could deter Russia or limit the effect of their campaigns. The government should step in while the effect is still limited and the damage is easier to mitigate.

2.4. 2026 ELECTIONS

With several state, parliamentary, and local elections approaching in September, Germany recently identified a Russian influence operation, *Matryoshka* (also known as Overload), circulating fabricated stories to

2.5. DRONE FLYOVERS

Unidentified drone sightings over Germany have been prominent throughout the war – 1 000 incidents in 2025 alone. Despite initial struggles to respond, Germany opened a third Joint Drone Defence Centre (*Gemeinsames Drohnenabwehrzentrum*, GDAZ) in December 2025 and the fourth Joint Centre for the

⁴³ [“Gefährdung der Bundestagswahl durch unzulässige ausländische Einflussnahme](#) [Threat to the Bundestag Election from Unlawful Foreign Influence],” Bundesamt für Verfassungsschutz, n.d., accessed in August 2026.

⁴⁴ Trpkovic, “Germany's Fragmented Approach to Disinformation.”

⁴⁵ [“Disinformation as Hybrid Threat,”](#) Federal Ministry of the Interior, n.d., accessed in August 2026.

⁴⁶ Bundesamt für Verfassungsschutz, “Gefährdung der Bundestagswahl durch unzulässige ausländische Einflussnahme.”

⁴⁷ Joscha Weber, [“Faktencheck: Deutsche Wahlen im Fokus russischer Fakes](#) [Fact Check: German Elections in the Focus of Russian Fakes],” *Deutsche Welle*, 3 August 2026.

⁴⁸ [“Russia Steps Up Disinformation before German Elections, Security Sources Say,”](#) *Reuters*, 5 August 2026.

⁴⁹ Joscha Weber, “Faktencheck.”

Defence against Hybrid Threats (*Abwehr gegen hybride Bedrohungen*, GAZ Hybrid) in June 2026 to coordinate against Russian threats.⁵⁰ These developments reflect the institutionalisation of proactive actions as well as policies. For example, Interior Minister Alexander Dobrindt commissioned a drone defence unit to help airports and other sites respond to such incursions.⁵¹ In 2025, the Bundeswehr was authorised to shoot down drones, while previously, only the Federal Police had that authority.⁵²

The Munich Airport and the Berlin Brandenburg Airport have had to halt or suspend air traffic control operations due to drone sightings. In October 2025, four drones were spotted over Gnoien military base while Ukrainian soldiers were training.⁵³

On 5 August 2026, a drone with explosives was found at Leipzig Airport, a logistics hub for NATO and the Bundeswehr, next to an Antonov Airlines plane owned by the Ukrainian state.⁵⁴ Authorities removed the detonator and discovered 800g of explosives, which threatened significant damage to the aircraft.⁵⁵ The interior minister said the fact that the device carried explosives was “a new quality of danger”, and he called it a hybrid attack.⁵⁶ Federal prosecutors said the case “constitutes a serious attack on the transportation and logistics infrastructure in Germany” and undermined the country’s security. An investigation was launched, focusing on “foreign powers.”⁵⁷ Another

object hit a freight plane that same day,⁵⁸ and on 6 August, two drones were spotted over a German military base in Mechernich.⁵⁹

The interior minister recalled that a few months earlier he had told the public the threat level needed to be raised – moving from an abstract threat to a high-level one – and stressed that this was now evident: the assessment made months before, that Germany was facing a high-level threat, had become a reality.⁶⁰ The drone incursions are a major escalation in the hybrid domain for Germany and the rest of Europe. This is the first time a drone with explosives has been found far from the Ukrainian border, and deep into Europe.

The drone incursions are a major escalation in the hybrid domain for Germany and the rest of Europe

2.6. ASSASSINATION PLOTS

Threats against the leading German business figures remain high. In March 2026, disposable agents were detained for surveying Stefan Thumann, the head of Donau Stahl, a company supplying drones to Ukraine, and his family.⁶¹ A BfV report found that they were part of a planned assassination attempt. The government now faces the ever-pressing question of what to do should the Russians succeed in assassinating a German citizen. According to *Die Zeit*, Berlin now views Russia as capable of anything, and the interior minister is regularly briefed on cases like these.⁶²

The ongoing threats against private individuals demonstrate that, despite proactively disrupting such plots, Germany’s actions fail to deter Russia’s aggression. Berlin is mulling

⁵⁰ “German Conference of Interior Ministers Decides to Set Up a Joint Counter-Drone Centre,” Federal Ministry of the Interior, 5 December 2025; Tagesschau, “Was soll das neue Abwehrzentrum bringen?” Tagesschau.

⁵¹ Wesley Dockery, “Germany Registers over 1,000 Suspicious Drone Flights,” *Deutsche Welle*, 22 December 2025.

⁵² Hans Pfeifer, “Germany Bolsters Defenses amid Russian Hybrid Warfare,” *Deutsche Welle*, 21 November 2025.

⁵³ Dockery, “Germany Registers over 1,000 Suspicious Drone Flights.”

⁵⁴ Marcel Fürstenau, “Unconstitutional? German Intelligence to Receive More Powers,” *Deutsche Welle*, 12 August 2026.

⁵⁵ Dan Sabbagh, “The Leipzig drone bomb marks a dangerous escalation for Europe,” *The Guardian*, 6 August 2026.

⁵⁶ Geir Moulson, “Explosive Drone Found at Airport Alarms German Authorities,” *AP News*, 6 August 2026.

⁵⁷ Fürstenau, “Unconstitutional?”

⁵⁸ Moulson, “Explosive Drone Found.”

⁵⁹ Ruth Comerford, “Drones Spotted over German Base Days after Leipzig Bomb Incident,” *BBC*, 9 August 2026.

⁶⁰ Moulson, “Explosive Drone Found.”

⁶¹ “Russian Intelligence Services Were Preparing an Assassination Attempt against CEO of German Drone Manufacturer Donau Stahl, *Die Zeit* Reports,” *The Insider*, 6 August 2026.

⁶² Hannah Knuth and Holger Stark, “Nächste Stufe: Mord? [Next Stage: Murder?],” *Die Zeit*, 5 August 2026.

whether it must escalate its response to target Russian structures and authorities, rather than just the operatives carrying out attacks on the ground. Otherwise, such incidents will continue.

The ongoing threats against private individuals demonstrate that, despite proactively disrupting such plots, Germany's actions fail to deter Russia's aggression

3. THE SHIFT IN RHETORIC AND LAW

Following Russia's invasion of Ukraine in 2022, it was often unclear to German authorities where hybrid attacks were stemming from and whether they were part of a sustained campaign or isolated incidents – yet they still recognised the threat.

As early as November 2024, BfV officials were already saying that Russia was using its entire toolbox of attack mechanisms at a significant, unprecedented scale.⁶³ Since 2025, it has become an institutional understanding that Russia systemically targets German democracy and society, actively trying to destabilise both.⁶⁴ The BMI press release in February 2025 said that Russian hybrid warfare in the realms of interference, disinformation, cybersecurity, and critical infrastructure has severely affected Germany's security.⁶⁵ The Bundeswehr said German society as a whole must fight hybrid warfare for the country to remain resilient.⁶⁶ Friedrich Merz's words, as newly elected chancellor at that time, reflect a broader shift in German sentiment: "We are not at war, but we are no longer living in peace either."⁶⁷

⁶³ Laura Kayali, Dirk Banse, Wolfgang Büscher, Ulrich Kraetzer, Uwe Müller, and Christian Schweppe, "Europe Is under Attack from Russia. Why Isn't It Fighting Back?," *Politico*, 25 November 2024; Pfeifer, "Germany Bolsters Defenses."

⁶⁴ Tagesschau, "Was soll das neue Abwehrzentrum bringen?" *Tagesschau*.
"Three Years of Russia's War of Aggression: 1.25 Million Refugees from Ukraine in Germany," Federal Ministry of the Interior, 21 February 2025.

⁶⁶ Pfeifer, "Germany Bolsters Defenses."

⁶⁷ Friedrich Merz, "Für ein souveränes, handlungsfähiges, starkes Europa [For a Sovereign, Capable, Strong Europe]," speech, *Der Bundeskanzler*, 26 September 2025.

In 2026, hybrid warfare remains a central topic, and the narrative has shifted to Germany's lack of preparedness and countermeasures. "Germany is in a clear foreign policy and identity crisis in which tried-and-tested frameworks for understanding and action are reaching their limits," the 2025 report from the Munich Security Conference concluded.⁶⁸ In June 2026, Col. Sönke Marahrens, a director at the European Centre of Excellence for Countering Hybrid Threats in Helsinki, said Germany was late to realise it was being attacked and that its response remains too slow.⁶⁹

The narrative has shifted to Germany's lack of preparedness and countermeasures

As Germany confronts its lack of preparedness, offensive measures are being considered. "All of this shows: our deterrence does not work. Russia does not feel real consequences. The west reacts only reactively – by increasing resilience, cyber defence, or exposure. But most experts, including myself, are convinced that a combination of reactive and active measures, defensive and offensive actions, is necessary to deter and truly influence Russia's behaviour," Arndt Freytag von Loringhoven, former vice president of the Federal Intelligence Service (*Bundesnachrichtendienst*, BND), said.⁷⁰ Martin Jäger, the service's current chief, said that deterrence is not working and that Germany should consider active countermeasures: "We should much more often prove that we would be able to do very similar things to make the other side also feel the pain."⁷¹

The government has begun to experiment with active measures. Berlin recently supported new sanctions targeting individuals believed to

⁶⁸ Tobias Bunde and Valentin Daur, *After the End of Certainties: A Snapshot of Public Opinion on the Zeitenwende* (Munich Security Conference, December 2025).

⁶⁹ Daniel Thomas, "Germany Was Late to Grasp Russian Hybrid Attacks, Bundeswehr Colonel Tells Defence Forum," *Euromaidan Press*, 10 June 2026.

⁷⁰ "Germany Increasingly Aware of Russia's Hybrid Threats, Response Insufficient – Ex-Intelligence Official," *Ukrinform*, 24 March 2026.

⁷¹ "Germany Spy Chief Says Russia Must Feel 'Pain' to Deter Hybrid Attacks," *Türkiye Today*, 14 February 2026.

be responsible for hybrid attacks.⁷² Germany's intelligence services have historically had limited powers since WWII, impacting their ability to respond to hybrid threats. However, that too has been changing: the cabinet recently approved a draft bill that would grant the BfV and the BND more powers. If parliament approves the bill, the intelligence services will be authorised to neutralise enemy IT systems, conduct acts of sabotage abroad, and manipulate or delete data during times of tension. The BMI's restructuring is essential, according to its own leadership, given the new hybrid threat landscape.⁷³ The bill thus marks a major step for Germany's response to hybrid warfare.

4. FEELING THE WAR AT HOME

The shift in official rhetoric reflects the shift in the public's perception of the issue. The Munich Security Index 2025 shows that

The shift in official rhetoric reflects the shift in the public's perception

Germans perceive the risk Russia poses to their country as greater than in any other country surveyed.⁷⁴ The share of the population who view the military threat from Russia as 'very high' rose from 39% in 2024 to 47% in 2025, while 54% expressed concern about Russian attempts to influence public opinion.⁷⁵ 73% of Germans now view Russia as Europe's biggest threat, up from 51% in 2021.⁷⁶ Russia had an index score of 78 in 2025, up from 67 in 2024 – the second-highest overall risk perceived by the public and the largest increase in index points. In 2023, it tied for the 'risk' with the greatest 'concern', and in 2022 it ranked 18th. Cyberattacks went from having an index score of 74 in 2023 to 70 in 2024 and to 76 in 2025.⁷⁷

⁷² Connor, "Germany Summons Russian Ambassador."

⁷³ Fürstenau, "Unconstitutional?"

⁷⁴ Bunde and Daur, *After the End of Certainties*.

⁷⁵ Körber-Stiftung, *The Berlin Pulse 2025/26: Adapting to the End of Certainties* (Körber-Stiftung, 2025).

⁷⁶ Friedrich-Ebert-Stiftung, *Germany Security Radar 2025: Europe – Lost in Geopolitics* (Friedrich-Ebert-Stiftung, 2025).

⁷⁷ Munich Security Conference, *Munich Security Index 2025* (Munich Security Conference, 2025).

The data also show that Germans feel a broader sense of insecurity. Friedrich Ebert Stiftung's Security Radar 2025 found that Germans' top concern is wars and conflict (82%), and international terrorism is the third-highest concern (76%), while concern about being personally affected by war rose from 47% in 2021 to 75% in 2024.⁷⁸ In spring 2025, only 38% of respondents rated the national security situation as 'safe' or 'very safe', down from 65% in August 2020.⁷⁹ The future outlook is also grim: 71% expect more crises and conflicts in the coming years, and 48% consider a large-scale military attack by Russia on a NATO or European country within the next five years 'somewhat' or 'very' likely.⁸⁰

By December 2025, many Germans saw the need to reorient security policy, with 42% believing it did not go far enough and 71% saying the country was not doing enough to adapt to the changed situation. Many were nervous about the new threat environment and thought the country was unprepared for the associated risks.⁸¹

Assessed together, these surveys suggest Germans increasingly view Russia as a direct domestic security threat and fear for their own safety and future, thus raising the stakes for German society.

Germans increasingly view Russia as a direct domestic security threat

CONCLUSION

Over time, Germany's response to hybrid warfare has become more coordinated and institutionalised. Only after a series of incidents, and the thorough investigations those incidents triggered, did officials fully realise the extent of Russia's war of hybrid aggression. Now, however, Berlin takes the issue very seriously and has begun pursuing enhanced security measures to proactively counter hybrid threats.

⁷⁸ Friedrich-Ebert-Stiftung, *Germany Security Radar 2025*.

⁷⁹ Bunde and Daur, *After the End of Certainties*.

⁸⁰ Bunde and Daur, *After the End of Certainties*.

⁸¹ Bunde and Daur, *After the End of Certainties*.

As Germany considers how to approach the future of hybrid warfare, it must focus less on investigation and mitigation and more on active defence mechanisms – and even on offensive measures – so that Moscow understands that Berlin does not take its malign behaviour lightly and is willing to fight back. The government must therefore continue to adopt a framework that predetermines the response following the attribution of a Russian state-sponsored hybrid attack and depending on its severity. This would establish clear consequences and strengthen deterrence by demonstrating to Moscow the potential costs and the extent of further escalation, as well as a high degree of likelihood that Germany and its allies will inflict those costs on Russia.

Combating hybrid threats is a particularly serious concern for Germany, given its unique

strategic position in Europe. As a driving force behind European rearmament, Germany has become a high-value target for Russian efforts to undermine western coordination of aid and weaken the overall support for Ukraine.

Russia's attacks in Germany suggest its willingness to escalate beyond online influence campaigns to kinetic operations

Russia's attacks in Germany suggest its willingness to escalate beyond online influence campaigns to kinetic operations. Russia is unlikely to scale down its attacks, so Berlin must build a sustainable deterrence system that goes beyond responding to individual incidents. If it wants to remain a credible leader in the European security landscape, Germany's response to hybrid warfare must be swift and adaptable to evolving threats.

RECENT ICDS PUBLICATION

REPORTS

- Kohv, Marek; Henrik Praks, Shin Kawashima, and Keizo Kitagawa. *Connecting the Ends: A Baltic–Indo-Pacific Agenda for Undersea Infrastructure Security*. July 2026.
- Klyszcz, Ivan U.K., and Kristel Potsepp. *Spinning the Globe: Russian Information Warfare and Its Reach into the Global South*. June 2026.
- Klyszcz, Ivan U.K. *Agents of Decolonisation? The Chechen and Circassian Diasporas in Europe since 2022*. May 2026.
- Jermalavičius, Tomas (ed), Javad Keypour, François-Xavier Chevalleriau, Koen Claessen, Kristel Potsepp, Henrik Praks, Emil Sondaj Hansen, Nolan Theisen, Izabela Surwillo, Tomas Janeliūnas. *The Ties That Bind: Energy Connectivity in the Age of Geopolitical Turbulence*. April 2026.
- Hanso, Toomas, Urmas Hõbepappel. *Taiwani väina kriisistsenaariumid ja kriisi julgeolekumõjud Eestile*. March 2026.
- Tynkkynen. Veli-Pekka, *Draining Fuel from the Russian War Machine: Oil, Gas, and Sanctions Outlook*. March 2026.
- Hõbepappel, Urmas. *The Yin and Yang of Russia's Image in China: Netizen Discourse and Real-Life Implications*. March 2026.
- Gaens, Bart, Wrenn Yennie Lindgren, Jagannath Panda, Ville Sinkkonen, Prannavan Surendran. *Japan and Strategic Connectivity: Policies, Partners, and Possibilities*. February 2026.

POLICY PAPERS

- Eglit, Helena, Cattler, David. *"Trusted Autonomy in the AI Era: Safeguarding Democratic Decision Integrity."* July 2026
- Brünner, Finn-Niklas. *"Shielding the Skies: European Ballistic Missile Defence."* December 2025.
- Kallioniemi, Pekka. *"Beyond Defence: A Proactive Strategy for the West in the Information Domain."* November 2025.
- Hall, Eric. *"Europe's Forthcoming Sahel Strategy: A Limited Role in a Multipolar Region."* October 2025.

ANALYSES

- Giuashvili, Teona. *"Georgia's Foreign Policy Pivot."* July 2026.
- Tomio, Giulio. *"Under the Russian Flag: Reflagging and the Future of Shadow Fleet Enforcement."* July 2026.
- Hosaka, Sanshiro, and Elena Kim. *"Asia's Fallout from Russia's War Against Ukraine: North Korea's Rise in the Russia–China Balance."* April 2026.
- Koizumi, Yu. *"The Bear's Sharp Claw or a Soft Underbelly? Russian Armed Forces in the Far East."* April 2026.
- Akimenko, Valeriy, Keir Giles. *"The Russian Way of Ceasefires and the Traps It Sets for Europe."* March 2026.
- Blockmans, Steven, and Michael Emerson. *"The State of EU Enlargement at the Outset of 2026: On The Brink of Major Breakthroughs"*. February 2026.
- Claessen, Koen. *"Connectivity and Competition in the South Caucasus: Geography as a Source of Power."* January 2026.

BRIEFS

- Raik, Kristi (ed); Matti Pesu, Anders Wivel, Merili Arjakas, Helena Eglit, Margarita Šešelgyté. *"Small States Series."* August 2026.
- Le Grand, Pauline; Hainaut, Béatrice. *"EU Defence Series."* July 2026.
- Delval, Théa. *"The Special Tribunal for Ukraine: Turning the Wheels of International Justice."* June 2026.
- Delval, Théa, and Luca Rogers. *"Legality and Reality: The Eastern Flank and the Ottawa Convention"* Théa Delval Luca Rogers." June 2026.
- Rogers, Luca, and Felix Gasper. *"Germany's New Military Concept: Responsibility for Europe."* June 2026.
- Hainaut, Béatrice. *"EU Defence Series: European Autonomy in Orbit."* May 2026.
- Klyszcz, Ivan U.K. *"The Double Edge of Russian Sovereign AI: Isolation and Narrative Consistency."* May 2026.

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



ICDS.TALLINN



@ICDS-TALLINN.BSKY.SOCIAL



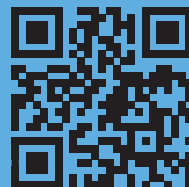
@ICDS _ TALLINN



ICDS-TALLINN



WWW.ICDS.EE



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

ISSN 2228-2076