National Defence University
Department of Warfare
Series 2: Research Reports No. 37

Russia's war against Ukraine

Trends and lessons

Pentti Forsström (ed.)

MAANPUOLUSTUSKORKEAKOULU
SOTATAIDON LAITOS
JULKAISUSARJA 2: TUTKIMUSSELOSTEITA NRO 37

NATIONAL DEFENCE UNIVERSITY
DEPARTMENT OF WARFARE
SERIES 2: RESEARCH REPORTS NO. 37

RUSSIA'S WAR AGAINST UKRAINE

TRENDS AND LESSONS

PENTTI FORSSTRÖM (ED.)

NATIONAL DEFENCE UNIVERSITY
DEPARTMENT OF WARFARE
HELSINKI 2025

Pentti Forsström (ed.): *Russia's war against Ukraine – Trends and Lessons*
Maanpuolustuskorkeakoulu
Sotataidon laitos
Julkaisusarja 2: Tutkimusselosteita nro 37
National Defence University
Department of Warfare
Series 2: Research Reports No. 37

Editor:

Pentti Forsström

Authors (those not present in-person in brackets):

(Marina Miron) and Rod Thornton; Vadym Pakholchuk; Nina Andriianova and (Valerii Hordiichuk); Sergei Melkonian; Marzia Cimmino; Kristina Melin; Jussi Jalonen; Yevgenii Harkavyi; Hanna Mäkinen and (Kari Liuhto); Ksenia Piddubna; Oona-Maaria Hyppölä (separate research report); Margarete Klein; Tobias Kollakowski; Stepan Yakymiak.

Recent publications in PDF format: *http://www.doria.fi/handle/10024/73990*

Cover picture: FNDU

Pictures and illustrations: Authors

ISBN 978-951-25-3534-7 (Pbk.)
ISBN 978-951-25-3535-4 (PDF)
ISSN 2343-5275 (print)
ISSN 2343-5283 (web)

Maanpuolustuskorkeakoulu – Sotataidon laitos

National Defence University – Department of Warfare

PunaMusta Oy
Joensuu 2025
Finland

11

RUSSIA'S SHADOW WAR: THE MEDIA COVERAGE OF RUSSIA'S HYBRID WAR AGAINST THE EU IN THE 21ST CENTURY

Hanna Mäkinen and Kari Liuhto

Introduction

Since Russia's full-scale invasion of Ukraine in 2022, the European Union (EU) has faced an unprecedented wave of hybrid attacks[1]. Hybrid warfare, or hybrid threats, is a broad and multifaceted concept covering 'a range of destabilising and synchronised civil and military actions'[2]. In hybrid warfare, various tactics and tools are used in a flexible, creative and coordinated manner, and the aim is to achieve political objectives by exploiting the vulnerabilities of adversaries without triggering a full-scale conventional war[3]. Hybrid warfare often involves ambiguous actions that blur the lines between war and peace, making it difficult to attribute the actions to a specific actor or to counter them[4].

Russia's hybrid warfare against the EU has evolved over the 21st century, adapting to new technologies and geopolitical contexts. One of the first major instances of Russia's hybrid attacks were the 2007 cyberattacks and riots in Estonia. Following the relocation of the Bronze Soldier, a Soviet-era statue, in Tallinn in April 2007, and the increased tension between Estonia and Russia, Estonia faced a series of major cyberattacks targeting government, banking, and media websites, causing widespread disruption. The relocation of the statue also caused anger among Russian-speaking population of Estonia that was incited by Russian-language newspapers and propaganda, culminating in two nights of riots in Tallinn.[5] Hence, besides highlighting the vulnerability of digital infrastructure, this example showed how internal divisions within a society could be exploited by a hostile state by using hybrid tactics.

---

[1] Sophia McGrath, *Spotlight on the Shadow War: Inside Russia's attacks on NATO Territory* (U.S. Helsinki Commission, 2024), https://www.csce.gov/wp-content/uploads/2024/12/Spotlight-on-the-Shadow-War-Website.pdf; Benedicte Dobbinga, "Research: Europe increasingly targeted by Russian sabotage," *Leiden University*, January 20, 2025, https://www.universiteitleiden.nl/en/news/2025/01/research-europe-increasingly-targeted-by-russian-sabotage.

[2] Sandra Kalniete and Tomass Pildegovičs, "Strengthening the EU's resilience to hybrid threats," *European View*, 20, no. 1 (2021): 24, https://doi.org/10.1177/17816858211004648.

[3] Harri Mikkola et al., *Hybridivaikuttaminen ja demokratian resilienssi. Ulkoisen häirinnän mahdollisuudet ja torjuntakyky liberaaleissa demokratioissa* (The Finnish Institute of International Affairs, 2018), 23, https://www.fiia.fi/en/publication/hybridivaikuttaminen-ja-demokratian-resilienssi; Andrew Mumford and Pascal Carlucci, "Hybrid Warfare: The Continuation of Ambiguity by Other Means," *European Journal of International Security* 8, no. 2 (2023): 198–199, https://doi.org/10.1017/eis.2022.19.

[4] James K. Wither, "Making Sense of Hybrid Warfare," *Connections* 15, no. 2 (2016): 74. http://www.jstor.org/stable/26326441; Mumford and Carlucci, "Hybrid Warfare: The Continuation of Ambiguity by Other Means," 199.

[5] Damien McGuinness, "How a cyber attack transformed Estonia," *BBC*, April 27, 2017, https://www.bbc.com/news/39655415.

Since Russia's annexation of Crimea in 2014, both academic and public discussion on the concept of hybrid warfare have increased significantly. The term 'hybrid' seemed to describe well the combination of kinetic and non-kinetic means Russia used in Crimea and Eastern Ukraine, such as unmarked soldiers, cyberattacks, economic pressure, and a massive disinformation campaign to justify and legitimize the annexation. Since then, hybrid warfare has also become a central security concern in both the EU and NATO.[6] Russia's interference in the 2016 US presidential election demonstrated its ability to manipulate democratic processes with cyberattacks and disinformation campaigns[7]. Similar tactics were used in Europe to sow discord and undermine trust in democratic institutions[8].

In addition, economic pressure has been a significant tool in Russia's hybrid warfare arsenal. By leveraging its control over energy supplies, Russia has attempted to exert influence over EU member states, particularly those heavily dependent on Russian gas and oil[9]. Russian cyberattacks, in turn, have targeted critical infrastructure, government institutions, media, and private sector entities across the EU, aiming to disrupt operations and sow chaos[10]. Furthermore, there is always an information dimension connected to hybrid attacks because they are also part of information warfare[11].

Recent reports indicate that alongside conventional military operations in Ukraine, Russia has intensified its hybrid war against the West, attacking critical infrastructure, carrying out sabotage operations and orchestrating weaponised migration, election interference and disinformation campaigns[12]. At the same time, because several hundreds of Russian diplomatic spies have been expelled from Europe since February 2022, Russia has turned to other modes of operation, for instance recruiting 'disposable agents' in social media, that are much harder for counter-intelligence to trace and handle[13]. Since 2024, Russia's hybrid attacks on Europe have become even more

---

[6] Wither, "Making Sense of Hybrid Warfare," 73–77.

[7] Benjamin Jensen et al., "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist," *Journal of Strategic Studies* 42, no. 2 (2019): 219–223, https://doi.org/10.1080/01402390.2018.1559152.

[8] Kalniete and Pildegovičs, "Strengthening the EU's resilience to hybrid threats," 25–26; Helmi Pillai, *Protecting Europe's critical infrastructure from Russian hybrid threats* (Centre for European Reform, 2023), 3, https://www.cer.eu/sites/default/files/pb_HP_hybrid_threats_25.4.23.pdf.

[9] Mikkola et al., *Hybridivaikuttaminen ja demokratian resilienssi. Ulkoisen häirinnän mahdollisuudet ja torjuntakyky liberaaleissa demokratioissa*, 44-45.

[10] Pillai, *Protecting Europe's critical infrastructure from Russian hybrid threats*, 3–4.

[11] Minna Ålander, "Death by a Thousand Paper Cuts: Lessons from the Nordic-Baltic Region on Countering Russian Gray Zone Aggression," *Carnegie Endowment for International Peace*, November 14, 2024, https://carnegieendowment.org/research/2024/11/russia-gray-zone-aggression-baltic-nordic?lang=en.

[12] McGrath, *Spotlight on the Shadow War: Inside Russia's attacks on NATO Territory*; Daniela Richterova et al., "Russian Sabotage in the Gig-Economy Era," *The RUSI Journal* 169, no. 5 (2024), https://doi.org/10.1080/03071847.2024.2401232; Bart Schuurman, *Russian operations against Europe since the 2022 invasion of Ukraine* (The Hague: Leiden University, 2025), https://www.universiteitleiden.nl/binaries/content/assets/governance-and-global-affairs/isga/infographic-russian-operations-against-europe.pdf; EBU Investigative Journalism Network, "Playing With Fire. Are Russia's hybrid attacks the new European war?" *Eurovision News,* March 12, 2025, https://investigations.news-exchange.ebu.ch/playing-with-fire-are-russias-hybrid-attacks-the-new-european-war/#group-section-The-Long-Game-h5jbSZtZX7.

[13] John Paul Rathbone et al., "Europe kicked out Vladimir Putin's spies. Now they're back," *Financial Times,* March 6, 2024, https://www.ft.com/content/f066d653-70e2-42e9-baac-c342417c8ef3; Laura Kayali et al., "Europe is under attack from Russia. Why isn't it fighting back?" *Politico,* November 25, 2024, https://www.politico.eu/article/europe-russia-hybrid-war-vladimir-putin-germany-cyberattacks-election-interference/.

common and severe. These actions are part of Russia's broader strategy to destabilize and undermine the EU and its allies, and erode their support for Ukraine.[14]

This article explores the various dimensions of Russia's hybrid war against the EU in the 21st century based on the news of suspected Russian hybrid operations, examining its aims and desired impacts, the actors involved and the tactics used in it. Through this analysis, this research contributes to a deeper understanding on the modus operandi of Russia's hybrid warfare, and sheds light on how some major cases of these hybrid operations have been reported for the general public by the European media. By understanding the full scope of Russia's hybrid war, the EU, its member states and their citizens can better prepare and respond to the ongoing challenges posed by hybrid threats.

Russia's hybrid war in the European media

The Western media has extensively covered Russia's hybrid warfare, informing the public about its multifaceted tactics, its impacts on European security, and the measures being taken to counter it. Investigative journalists have also played an important role in revealing and raising awareness of Russia's hybrid operations[15]. In this article, we focus on incidents that have been attributed to or suspected of Russia's hybrid warfare in the European media. This research applies an inductive and data-driven approach, analysing the content of news related to Russia's hybrid operations in the 27 EU member states in the 21st century. The news material has been collected by conducting a systematic search[16] in the Financial Times and complemented with material from other European[17] and national[18] media outlets.

The majority of suspected Russia's hybrid operations reported by the media have taken place after the annexation of Crimea in 2014, with a significant increase after the start of Russia's full-scale invasion of Ukraine in February 2022, and particularly since 2024. These incidents include attacks on critical infrastructure (e.g., sabotage and cyberattacks), espionage (e.g., collection and exploitation of confidential information), influence operations (e.g., disinformation campaigns and election interference), instrumentalization of migrants, intimidation (e.g., bomb threats), and violence (e.g., assassinations), among others. Cases of suspected Russia's hybrid operations have occurred in all EU member states. However, based on media reporting, especially Germany and Poland seem to have experienced a surge in suspected Russia's

---

[14] Charlie Edwards, "Russia's hybrid war in Europe enters a dangerous new phase," *IISS*, November 26, 2024, https://www.iiss.org/online-analysis/online-analysis/2024/11/russias-hybrid-war-in-europe-enters-a-dangerous-new-phase/; Schuurman, *Russian operations against Europe since the 2022 invasion of Ukraine*; "Hybrid threats," European Council and the Council of the European Union, last modified February 25, 2025, https://www.consilium.europa.eu/en/policies/hybrid-threats/.

[15] See e.g., Bellingcat Investigation Team, "How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine," *Bellingcat*, April 26, 2021, https://www.bellingcat.com/news/uk-and-europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/; Martin Laine and Anastasiia Morozova, "Leaked Files from Putin's Troll Factory: How Russia Manipulated European Elections," *VSquare*, September 16, 2024, https://vsquare.org/leaked-files-putin-troll-factory-russia-european-elections-factory-of-fakes/; EBU Investigative Journalism Network, "Playing With Fire. Are Russia's hybrid attacks the new European war?".

[16] Search terms: 1) Russia AND hybrid AND (war OR warfare OR attack OR operation), 2) Russia AND sabotage.

[17] EurActiv, Euronews, Politico.

[18] E.g., Delfi, DW, the Finnish Broadcasting Company Yle, Helsingin Sanomat, LeMonde, LRT.

hybrid attacks since February 2022, including disinformation campaigns and sabotage operations aiming to interfere elections, influence public opinion, weaken support for Ukraine and disrupt the functioning of the economy and society. In Poland, in particular, the political leadership has made outspoken statements about the hybrid threat from Russia[19], which has increased the media publicity of the issue. In Finland, as well, the media has extensively covered Russia's suspected hybrid operations during the recent years, and the topic has been widely discussed in public.

Based on the media material, we have outlined four main dimensions of Russia's hybrid war against the EU: political, social, economic and military. These dimensions are illustrated in Figure 1, with some examples of Russia's hybrid operations linked to these dimensions. The dimensions overlap as it is typical for Russia's hybrid operations to aim to cause multisectoral damage, exploiting vulnerabilities, undermining stability, causing disruption, and gaining strategic advantages.

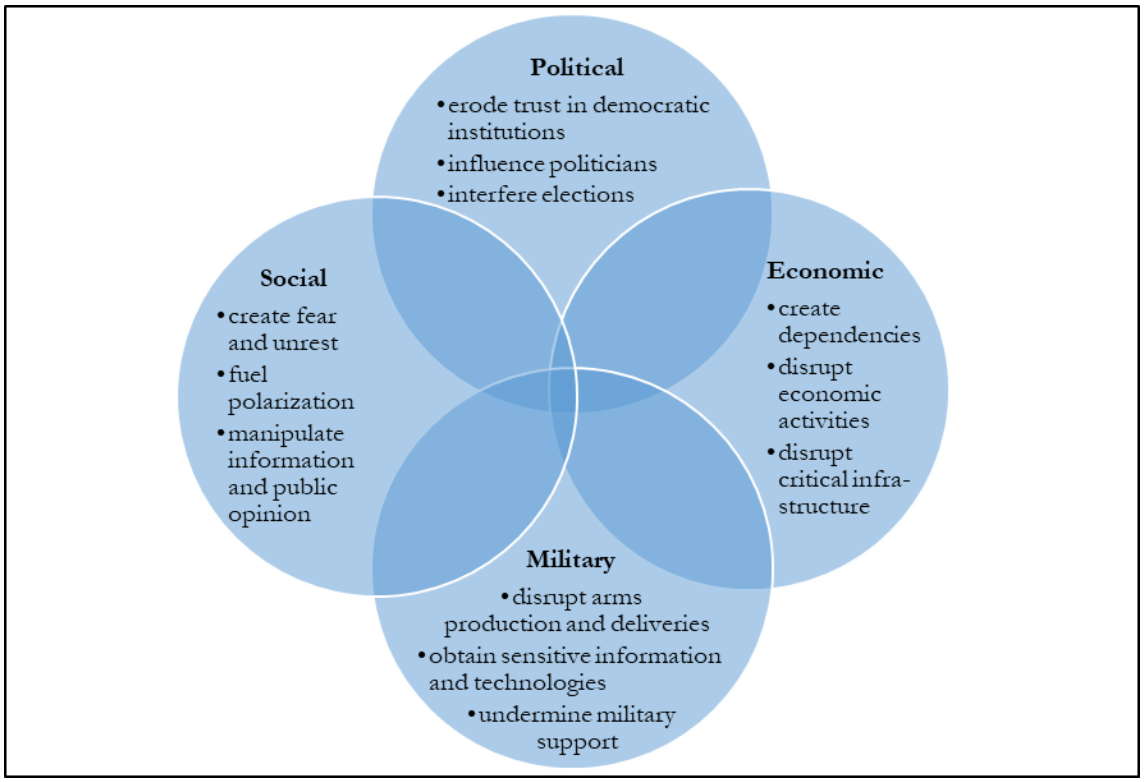

Figure 1. Dimensions of Russia's hybrid war against the EU with examples

For instance, these operations aim to impact politics by interfering elections, influencing politicians and eroding trust in democratic institutions and the EU. They also aim to weaken and destabilize society by creating fear and unrest, fuelling polarization and manipulating information and public opinion. They strive for economic impact by creating dependencies and by disrupting economic activities and critical infrastructure. In addition, they aim to gain military advantage by disrupting arms production and deliveries, and by obtaining sensitive information and technologies. Furthermore, they aim to undermine military support for Ukraine.

[19] See e.g., Alice Hancock and Raphael Minder, "Poland 'most attacked' online by Russia, says minister," *Financial Times,* January 16, 2025, https://www.ft.com/content/e0e1a016-e4e0-4628-a0ac-c4a6e9d15db6.

In the following, we discuss the dimensions of Russia's hybrid war against the EU through four case examples based on their media reporting. In these cases, covered by the European media, Russia has been suspected or proven to have sought to influence and destabilize the EU and individual member states through a combination of various means.

Political influencing through disinformation campaigns

One of the key components of Russia's hybrid warfare strategy has been disinformation campaigns, with Russian state-sponsored media and social media trolls and bots spreading false narratives to influence political decision-makers, undermine public trust in democratic institutions and create societal divisions. Russia's propaganda model has been characterised as 'the firehose of falsehood', its typical features being the abundance of communication channels and messages, and the ruthless dissemination of partial truths and false information[20]. While sanctions imposed by the EU on Russian state-sponsored media outlets[21] have restricted Russia's possibilities to spread disinformation through traditional media in the EU countries, social media has become an important instrument of Russian propaganda and information manipulation campaigns, facilitated by the use of digital tools such as artificial intelligence.

Aiming to justify its war of aggression, undermine support for Ukraine and divide the EU, Russia has intensified its efforts to influence politics and manipulate public opinion both at the EU-level and in individual member states[22]. Russia's recent disinformation operations reported by the media range from creating panic about the bed bug epidemic in France and connecting it with the arrival of Ukrainian refugees[23] to amplifying the Arabic-language disinformation campaign related to Quran burnings in Sweden that complicated Sweden's accession to NATO[24]. A particularly massive wave of disinformation was directed towards the EU, and particularly France, Germany and Poland, before the 2024 European Parliament election, which Russia saw as central in defining the EU's future stance towards itself and Ukraine[25]. Besides spreading disinformation designed to manipulate public opinion on Ukraine, Russia also aimed to increase support for far-right parties especially in France and Germany, and hence their weight in the European Parliament, hoping that the parties would promote the reduction of aid to Ukraine and the easing of sanctions against Russia[26].

---

[20] Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model," *RAND,* July 11, 2016, https://www.rand.org/pubs/perspectives/PE198.html.
[21] "EU sanctions against Russia explained," European Council and the Council of the European Union, last modified March 19, 2025, https://www.consilium.europa.eu/en/policies/sanctions-against-russia-explained/#media.
[22] "Split the EU: a constant priority of the Kremlin," EUvsDisinfo, last modified February 26, 2025, https://euvsdisinfo.eu/split-the-eu-a-constant-priority-of-the-kremlin/.
[23] Kayali et al., "Europe is under attack from Russia. Why isn't it fighting back?"
[24] Elisabeth Braw, "How Sweden Became Public Enemy No. 1," *Foreign Policy*, July 28, 2023, https://foreignpolicy.com/2023/07/28/sweden-quran-nato-iran-iraq-russia/.
[25] Leila Abboud et al., "Europe battles 'avalanche of disinformation' from Russia," *Financial Times*, March 21, 2024, https://www.ft.com/content/2ffe8b64-f9bc-46d4-bf40-eefbbc6fac77; EurActiv, "France, Germany, Poland facing 'permanent' Russian disinformation attacks: EU," June 5, 2024, https://www.euractiv.com/section/elections/news/france-germany-poland-facing-permanent-russian-disinformation-attacks-eu/; Simo Ortamo, "Uusi tietovuoto paljasti Venäjän häikäilemättömän vaikutusoperaation, asiantuntijalta tyly huomio," *Yle,* September 23, 2024, https://yle.fi/a/74-20112682.
[26] Laine and Morozova, "Leaked Files from Putin's Troll Factory: How Russia Manipulated European Elections."

In addition, Russia was accused of paying to pro-Russian politicians, including members of the European parliament, to promote Russian propaganda in the EU[27].

As an example of actors implementing these influence operations, leaked documents obtained by Estonian and German media outlets revealed how Russian troll factory 'Social Design Agency' (SDA) carried out a massive disinformation campaign in social media just before the 2024 EU Parliament election[28]. SDA operated as a kind of information warfare unit, conducting information influence operations in different countries, producing comments and spreading propaganda memes, cartoons and videos in different social media platforms. The leaked documents also exposed that SDA's operations were coordinated by the Kremlin: the representatives of Russian presidential administration were present in meetings with SDA and giving it orders. In the narratives spread by SDA in social media, the EU's support for Ukraine was presented as waste of money, causing rising living costs and economic suffering in the EU. Narratives aiming to increase support for far-right parties, in turn, focused on accusing 'liberal globalists' of fomenting panic about the Russian threat, climate disaster and pandemics, and undermining traditional values, for instance.[29]

Regarding the success of Russia's disinformation campaign, it is unclear what kind of impact – if any – it had on the election results. Far-right parties were able to increase their support in the elections but they might have done it even without Russia's interference.[30] However, the flood of Russian propaganda has led the EU to adopt measures to counter it, such as a sanctions framework against individuals and entities engaged in, for instance, information manipulation and interference, and undermining electoral processes and democratic institutions[31].

Migration as an instrument of exerting political pressure and exploiting social divisions

Instrumentalised migration, also known as weaponised migration, can be used as a hybrid warfare tactic by states or non-state actors that deliberately create or manipulate migration flows to achieve geopolitical objectives. By creating large-scale migration crises, adversaries can strain the resources and infrastructure of target countries which can lead to social unrest, political instability, and economic challenges.[32] In the last ten years, this tactic has been used by the leaders of Russia and Belarus on several

---

[27] Andy Bounds, "Russia paid pro-Kremlin lawmakers to influence EU elections, says Belgium," *Financial Times,* April 12, 2024, https://www.ft.com/content/8bb921fa-57b3-44aa-80d6-b35794a523db; Javier Espinoza et al., "Brussels seeks to ban Russian funding of European politicians," *Financial Times,* May 6, 2024, https://www.ft.com/content/ab480869-684e-4180-bfa6-70266beeca24.

[28] See e.g., Martin Laine, "Dokumendid otse Kremli trollivabrikust: kuidas Venemaa taas europarlamendi valimisi mõjutas," *Delfi*, September 16, 2024, https://www.delfi.ee/artikkel/120321674/dokumendid-otse-kremli-trollivabrikust-kuidas-venemaa-taas-europarlamendi-valimisi-mojutas; Laine and Morozova, "Leaked Files from Putin's Troll Factory: How Russia Manipulated European Elections."; Ortamo, "Uusi tietovuoto paljasti Venäjän häikäilemättömän vaikutusoperaation, asiantuntijalta tyly huomio."

[29] Laine and Morozova, "Leaked Files from Putin's Troll Factory: How Russia Manipulated European Elections."

[30] Ortamo, "Uusi tietovuoto paljasti Venäjän häikäilemättömän vaikutusoperaation, asiantuntijalta tyly huomio."

[31] European Council and the Council of the European Union, "Hybrid threats."

[32] George Scutaru and Andrei Pavel, "Weaponization of Migration: A Powerful Instrument in Russia's Hybrid Toolbox," *The Caravan*, September 17, 2024, https://www.hoover.org/research/weaponization-migration-powerful-instrument-russias-hybrid-toolbox.

occasions when waves of refugees from third countries have been sent especially to their borders with Finland, Latvia, Lithuania and Poland[33]. Russia's military presence and intervening in conflicts in several Asian and African countries not only aims to create an image of it as a global superpower, but also serves its interests in causing refugee flows to Europe. Furthermore, in Ukraine, Russia has been continuously targeting civilian infrastructure, causing the displacement of hundreds of thousands of Ukrainians.[34] The aim of the instrumentalised migration is to put pressure on the EU's external borders and individual member states that share a border with Russia and Belarus, their political decision-makers and asylum-seeking systems, as well as create and exploit national and EU-level divisions.

The countries targeted by instrumentalised migration from Russia and Belarus have reacted by taking strong counter-measures against it. The border infrastructure has been reinforced in Finland, Poland, Latvia and Lithuania, and the countries have adopted legislative measures to prevent the influx of migrants[35]. Finland has closed its border crossing points on its land border with Russia in 2023 and restricted the reception of applications for international protection to other border crossing points[36]. Latvia, Lithuania and Poland have adopted similar measures allowing them to turn back migrants already in 2021[37]. However, weaponised migration is a complicated question for Western democracies to deal with because it challenges the countries' interests on one hand in protecting national security, and on the other hand in protecting human rights and the rules-based international order. If a country decides to combat waves of migration by closing its borders, it may suffer reputational damage because of violating international human rights conventions. Criticism can result especially if countermeasures lead to human suffering.[38]

Instrumentalised migration can also be used to shift public opinion, influence electoral outcomes and facilitate both internal and EU-level polarization. Increased migration can incite anti-immigrant sentiments and bolster far-right political movements, a development which Russia considers serving its interests. Russia has fuelled this polarization further by spreading disinformation.[39] For instance, in 2016, Russian media and politicians seized an opportunity to stir up anti-immigrant sentiments in

---

[33] Sergei Kuznetsov, "Lithuania slams shut the door to the EU for irregular migrants,"*Politico,* September 1, 2021, https://www.politico.eu/article/lithuania-migrants-eu-asylum-belarus-alexander-lukashenko/; Sari Taussi and Elina Ervasti, " Valko-Venäjän ja Puolan rajalla on Euroopan uusin siirtolaiskriisi – keitä ovat ihmiset rajalla ja miksi he ovat siellä? Katso ja lue vastaukset," *Yle,* November 9, 2021, https://yle.fi/a/3-12180959; Cory Bennett, "Belarus sends de-escalation signals on migrant crisis," *Politico*, November 15, 2021, https://www.politico.eu/article/belarus-de-escalation-signals-migrant-crisis/; Eero Mäntymaa, "Venäjä päästi kahdeksan vuotta sitten 1700 turvapaikanhakijaa itärajalle – Yle selvitti, moniko heistä sai jäädä Suomeen," *Yle,* December 2, 2023, https://yle.fi/a/74-20063227.

[34] Scutaru and Pavel, "Weaponization of Migration: A Powerful Instrument in Russia's Hybrid Toolbox."; Monika Wohlfeld et al., "NATO and Instrumentalized Migration," *Center for Strategic and International Studies*, July 12, 2024, https://www.csis.org/analysis/nato-and-instrumentalized-migration.

[35] Kuznetsov, "Lithuania slams shut the door to the EU for irregular migrants."; Žygintas Abromaitis, "'All friendships are over': Lithuania fortifies border with Russia's Kaliningrad," *LRT,* September 6, 2024, https://www.lrt.lt/en/news-in-english/19/2354296/all-friendships-are-over-lithuania-fortifies-border-with-russia-s-kaliningrad.

[36] "Situation at Finland's eastern border," Finnish Government, accessed March 21, 2025, https://valtioneuvosto.fi/en/situation-at-finlands-eastern-border.

[37] Kuznetsov, "Lithuania slams shut the door to the EU for irregular migrants."

[38] Ålander, "Death by a Thousand Paper Cuts: Lessons from the Nordic-Baltic Region on Countering Russian Gray Zone Aggression."

[39] Scutaru and Pavel, "Weaponization of Migration: A Powerful Instrument in Russia's Hybrid Toolbox."

Germany by spreading a story, originally published in social media and later proved as invented, of immigrants having abducted and raped a 13-year-old ethnic Russian girl in Berlin[40].

Furthermore, managing a migration crisis can divert attention and resources away from other critical issues, weakening a country's ability to respond to other hybrid threats[41]. For instance, intensified border surveillance causes additional expenses and necessitates reallocation of border guard resources. Adversaries may also use the threat of creating or exacerbating a migration crisis as leverage in negotiations or to coerce target countries into making concessions[42]. Hence, as is typical of hybrid warfare, instrumentalised migration serves many purposes. Moreover, it is an efficient hybrid weapon because the target states are forced to respond to it in some way but often must compromise between national security and human rights.

Disrupting critical infrastructure to destabilize the economy and society

Since the start of full-scale war in Ukraine in 2022, Russia has intensified its attempts to disrupt critical infrastructure in the EU with hybrid tactics, such as cyberattacks, sabotage, and surveillance[43]. According to the media, Russia has been suspected of targeting energy grids, communication networks, water supply and other vital systems with cyberattacks and sabotage operations[44]. Russian spy ships have also been observed near critical energy and telecommunication infrastructure[45]. News of suspicious incidents, such as the disruption of railways in France[46] and Germany[47], sabotage of communication cables in France[48], cyberattacks on water facilities in France

---

[40] Stefan Wagstyl, "German politics: Russia's next target?" *Financial Times*, January 29, 2017, https://www.ft.com/content/31a5758c-e3d8-11e6-9645-c9357a75844a.
[41] Wohlfeld et al., "NATO and Instrumentalized Migration."
[42] Sari Aurel, *Instrumentalized migration and the Belarus crisis: Strategies of legal coercion* (The European Centre of Excellence for Countering Hybrid Threats, 2023), 30, 20230425-Hybrid-CoE-Paper-17-Instrumentalized-migration-and-Belarus-WEB.pdf.
[43] Pillai, *Protecting Europe's critical infrastructure from Russian hybrid threats.*
[44] Simo Ortamo, "Venäjä näyttää nyt tekevän kyberiskuja länsimaiden vesilaitoksiin – Mikko Hyppönen: 'Aikamoinen uutinen'," *Yle,* April 21, 2024, https://yle.fi/a/74-20084689; Kayali et al., "Europe is under attack from Russia. Why isn't it fighting back?"; Arno Van Rensbergen, "Hybrid threats: Russia's shadow war escalates across Europe," *The Parliament Magazine*, January 21, 2025, https://www.theparliamentmagazine.eu/news/article/hybrid-threats-russias-shadow-war-escalates-across-europe; EBU Investigative Journalism Network, "Playing With Fire. Are Russia's hybrid attacks the new European war?"
[45] Jean-Pierre Stroobants, "In the North Sea, Russia conceals espionage activities with commercial ships," *LeMonde,* June 22, 2024, https://www.lemonde.fr/en/international/article/2024/06/22/in-the-north-sea-russia-conceals-espionage-activities-with-commercial-ships_6675426_4.html; Kayali et al., "Europe is under attack from Russia. Why isn't it fighting back?".
[46] Victor Goury-Laffont and Clea Caulcutt, "'Coordinated arson attack' brings French trains to a halt hours before Olympics opening ceremony," *Politico,* July 26, 2024, https://www.politico.eu/article/coordinated-attack-brings-french-train-system-to-a-halt-on-opening-olympics-weekend/.
[47] France24, "Rail traffic in northern Germany disrupted by 'sabotage'," October 8, 2022, https://www.france24.com/en/europe/20221008-rail-traffic-in-northern-germany-disrupted-by-sabotage.
[48] Victor Goury-Laffont, "French fiber optic cables hit by 'major sabotage' in second Olympics attack," *Politico,* July 29, 2024, https://www.politico.eu/article/french-fiber-optic-cable-hit-with-alleged-acts-of-sabotage/; Polly Thompson, "French infrastructure was targeted for a 2nd time during the Olympics, with internet and phone cables cut across the country," *Business Insider,* July 29, 2024, https://www.businessinsider.com/french-fiber-optic-cables-cut-phone-internet-services-infrastructure-attack-2024-7.

and Poland[49] and on hospitals in the Netherlands, Germany, and Poland[50], and GPS interference in Finland[51] have become frequent in the media.

As an example of tactics to disrupt critical infrastructure, GPS interference suspected of being of Russian origin has intensified since 2022. As for Russia, GPS interference may serve both offensive and defensive goals: it causes harm to other countries and at the same time enables Russia to protect itself from possible missile and drone attacks. It is also a cheap and rather easy way to create confusion.[52] GPS disturbances have been widely covered by the Finnish media, experts often stressing that GPS interference is annoying rather than dangerous because alternative navigation systems are available[53]. So far, GPS interference has mainly disturbed air navigation in Finland and across the Baltic Sea, and also caused some harm to marine traffic[54]. For instance, the Finnish airline Finnair had to suspend its flights to Tartu, Estonia for a month due to GPS disturbances, and several airports in eastern Finland have reverted to radio navigation systems enabling flights to land when facing GPS interference[55]. GPS interference also ruined the 2024 aerial photography and laser scanning flights of the National Land Survey of Finland (NLS). The information collected with these flights is critical to many functions of society and used, for instance, by the Finnish Defence Forces.[56]

So far, the impacts of disruptions of critical infrastructure in the EU have remained limited and temporary. However, attacks on critical infrastructure can lead to significant harm and disarray, affecting economic activities, social stability, and even national security, depending on their type, purpose, and level of success.[57] For instance, by disrupting satellite navigation, it would be possible to paralyse different parts of

---

[49] Ortamo, "Venäjä näyttää nyt tekevän kyberiskuja länsimaiden vesilaitoksiin – Mikko Hyppönen: 'Aikamoinen uutinen'."
[50] Euronews, "European hospitals targeted by 'pro-Russian' hackers," February 1, 2023, https://www.euronews.com/2023/02/01/european-hospitals-targeted-by-pro-russian-hackers.
[51] Antti Parviala, "Suomen gps-häiriökartta punaisena – onko paikannus maalla, merellä ja ilmassa uhattuna?" *Yle,* March 18, 2024, https://yle.fi/a/74-20079337.
[52] Parviala, "Suomen gps-häiriökartta punaisena – onko paikannus maalla, merellä ja ilmassa uhattuna?"; Teemu Juhola, "Venäjän GPS-häirintä kasvoi rajusti Virossa vain vuodessa – asiantuntijalta karu arvio tilanteesta," *Yle,* May 21, 2024, https://yle.fi/a/74-20088861.
[53] Jari Tanskanen, "Finnair keskeyttää Viron Tarton lennot kuukaudeksi – kentälle rakennetaan GPS-häirinnästä riippumaton lähestymisjärjestelmä," *Yle,* April 29, 2024, https://yle.fi/a/74-20086197; Juhola, " Venäjän GPS-häirintä kasvoi rajusti Virossa vain vuodessa – asiantuntijalta karu arvio tilanteesta."
[54] Anne Kauranen et al., "Explainer: What is GPS jamming and why is it a problem for aviation?" *Reuters,* May 1, 2024, https://www.reuters.com/business/aerospace-defense/what-is-gps-jamming-why-it-is-problem-aviation-2024-04-30/; Jyri Tynkkynen, "Perinteinen GPS-häirintä on edelleen ykkösongelma satelliittinavigoinnille uudesta spoofing-häirinnästä huolimatta," *Yle,* January 31, 2025, https://yle.fi/a/74-20140362.
[55] Tanskanen, "Finnair keskeyttää Viron Tarton lennot kuukaudeksi – kentälle rakennetaan GPS-häirinnästä riippumaton lähestymisjärjestelmä"; Topias Peltonen and Elisa Paljakka, "Itä-Suomen lentoasemat ottivat uudelleen käyttöön radionavigaatiojärjestelmän GPS-häirinnän takia," *Yle,* November 7, 2024, https://yle.fi/a/74-20123095.
[56] "Interference spoiled aerial photography in southeastern Finland, potentially resulting in damage of millions of euros – the National Land Survey of Finland has solutions for preparing for GNSS disturbances," National Land Survey of Finland, last modified October 2, 2024, https://www.maanmittauslaitos.fi/en/topical_issues/interference-spoiled-aerial-photography-southeastern-finland-potentially-resulting.
[57] Pillai, *Protecting Europe's critical infrastructure from Russian hybrid threats*, 2, 4.

society that use satellite navigation and time, such as logistics, money traffic, data networks and the actions of various authorities[58].

Attacks on energy infrastructure could also have wide-ranging effects on the functioning of societies. In December 2015, a cyberattack on the power grid in Ukraine left more than 230 000 residents without electricity for several hours[59]. The cyberattack was attributed to Sandworm, a hacker group linked to Russian intelligence, that attacked the Ukrainian power grid also in 2023. Experts have also raised concerns about Russia-linked hackers targeting European energy infrastructure.[60] Furthermore, as the EU has disengaged from Russian energy, the risk of Russia disrupting the energy infrastructure of Norway, the EU's major natural gas and crude oil supplier, has increased[61]. Consequently, the growing risk of severe hybrid attacks has heightened concerns about the vulnerability of Europe's critical infrastructure and led to increased cooperation between the EU and NATO to counter hybrid threats[62]. NATO has also increased its military presence in the Baltic Sea to supervise and protect critical undersea infrastructure[63].

Proving that Russia is behind the attacks on the EU's critical infrastructure is often difficult, not least because there are various actors involved in hybrid operations. In addition to carrying out sabotage operations with its intelligence agencies, Russia has been using proxies, that might not even know they are working for Russia, to avoid attribution[64]. For instance, Russia has been 'outsourcing' sabotage operations to 'gig workers' recruited in social media, which is a low-cost and flexible way to carry out hybrid attacks[65]. Similar mode of operation has been used in cyberattacks. Although cyber operations are usually orchestrated by pro-Russian hackers that may be directly led and financed by the Russian state, or at least operating under its auspices, ordinary people who sympathize with Russia can also be encouraged to participate in them from their own computers[66]. In addition, organised crime groups, Russians living abroad and citizens of third countries, among others, have been used to carry out hybrid operations[67]. In general, the difficulty of assigning blame is characteristic of

---

[58] Juhola, " Venäjän GPS-häirintä kasvoi rajusti Virossa vain vuodessa – asiantuntijalta karu arvio tilanteesta."; Jyri Tynkkynen, "Norjassa havahduttu uudenlaiseen GPS-häirintään – Suomessakin jo tutkittu asiaa," *Yle,* January 30, 2025, https://yle.fi/a/74-20139819.

[59] "Compromise of a power grid in eastern Ukraine," Council on Foreign Relations, accessed March 23, 2025, https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine.

[60] Sam Clark, "Winter is coming. So are Russia's elite hackers," *Politico,* November 22, 2024, https://www.politico.eu/article/russia-hackers-europe-winter-energy-infrastructure-moscow-gas-hike-digital/.

[61] Nerijus Adomaitis, "Norway's spy chief sees Russia more likely to attempt sabotage," *Reuters,* September 11, 2024, https://www.reuters.com/world/europe/norways-spy-chief-sees-russia-more-likely-attempt-sabotage-2024-09-10/.

[62] Pillai, *Protecting Europe's critical infrastructure from Russian hybrid threats*; European Council and the Council of the European Union, "Hybrid threats."

[63] "NATO launches 'Baltic Sentry' to increase critical infrastructure security," NATO, last modified January 14, 2025, https://www.nato.int/cps/en/natohq/news_232122.htm.

[64] Rathbone et al., "Europe kicked out Vladimir Putin's spies. Now they're back."

[65] Richterova et al., "Russian Sabotage in the Gig-Economy Era," 14–15.

[66] EBU Investigative Journalism Network, "Playing With Fire. Are Russia's hybrid attacks the new European war?"

[67] Rathbone et al., "Europe kicked out Vladimir Putin's spies. Now they're back."; Sam Jones et al., "Russia plotting sabotage across Europe, intelligence agencies warn," *Financial Times,* May 5, 2024, https://www.ft.com/content/c88509f9-c9bd-46f4-8a5c-9b2bdd3c3dd3; Richard Milne, "Russia behind Ikea arson attack in Lithuania, prosecutors say," *Financial Times,* March 17, 2025, https://www.ft.com/content/756a948b-e48d-480e-88e4-c0d52b361b35; Lisa O'Carroll, "Russia using criminal networks to drive

hybrid warfare. In addition, if a 'natural' cause is found for an incident which has been suspected to be Russia's hybrid attack, it can further increase the ambiguity related to this activity, and thus play into Russia's pocket.[68]

Undermining the EU's military support for Ukraine with hybrid tactics

Since the annexation of Crimea, Russia has aimed to disrupt the military supplies to Ukraine by using hybrid tactics. To reach this aim, Russia has employed covert operations to carry out assassinations and acts of sabotage in several EU member states. These tactics have been complemented with disinformation campaigns targeted at EU politicians and citizens, such as threats that providing military aid for Ukraine could escalate a 'third world war', and claims that providing aid to Ukraine will lead to EU-wide economic deprivation[69].

Russia has carried out hybrid operations aiming to prevent delivery of weapons and ammunition to the areas in which it is military active already in 2010s. In October and December 2014, two explosions took place in ammunition depots in Czech Republic, causing the death of two people and the evacuation of the surrounding areas. In 2021, the Czech prime minister publicly announced that the explosions were carried out by Russia's foreign military intelligence agency GRU, and in 2024, this was confirmed in a police investigation.[70]

Although it happened already in 2014, this incident became a subject of wider media attention only in 2021 when the involvement of the GRU was made public. According to Bellingcat's investigations, the explosions in Czechia were part of Russia's longer-term operation that aimed to disrupt Ukraine's capabilities to procure weapons for its fight against Russia[71]. Explosions in four ammunition warehouses in Bulgaria between 2011 and 2020 and two poisoning attempts of a Bulgarian arms dealer are suspected to be part of the same operation[72]. Bellingcat has also revealed that the same two GRU agents that were accused of poisoning Sergei and Julia Skripal in the UK in 2018 were responsible of the sabotage[73]. As a response to the sabotage operation, several

---

increase in sabotage acts, says Europol," *The Guardian,* March 18, 2025, https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol.

[68] Van Rensbergen, "Hybrid threats: Russia's shadow war escalates across Europe."

[69] "The Kremlin's futile disinfo trash catapult," EUvsDisinfo, last modified September 5, 2024, https://euvsdisinfo.eu/the-kremlins-futile-disinfo-trash-catapult/; "Split the EU: a constant priority of the Kremlin," EUvsDisinfo.

[70] Gordon Corera, "Salisbury poisoning suspects 'linked to Czech blast'," *BBC*, April 18, 2021, https://www.bbc.com/news/uk-56790053; Keno Verseck, "Is Russia behind the 2014 Czech munition depot blasts?" *DW,* April 20, 2021, https://www.dw.com/en/is-russia-behind-the-2014-czech-munition-depot-blasts/a-57260551; Martin Fornusek, "Czech police conclude Russian agents behind deadly 2014 ammunition depot blasts," *The Kyiv Independent,* April 29, 2024, https://kyivindependent.com/czech-police-says-russian-agents-behind-deadly-2014-bombing/.

[71] Bellingcat Investigation Team, "How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine."

[72] Bellingcat Investigation Team, "How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine"; Marton Dunai, "Russian hitmen and saboteurs target Bulgaria's arms industry, magnate says," *Financial Times,* November 19 2023, https://www.ft.com/content/b1aa5696-6515-487d-ba4d-380c9c431c18.

[73] Bellingcat Investigation Team, "Senior GRU Leader Directly Involved With Czech Arms Depot Explosion," *Bellingat,*
April 20, 2021, https://www.bellingcat.com/news/2021/04/20/senior-gru-leader-directly-involved-with-czech-arms-depot-explosion/.

Russian diplomats were expelled from Czechia, as well as from other countries as an expression of solidarity. It also led to cooling down of the Czech relations with Russia.[74] However, the Czech police did not press any charges because the suspects were said to be under Russia's protection[75].

Russia's attempts to sabotage military aid to Ukraine have continued during the ongoing war of aggression. In 2024, the US intelligence and Germany's security service were able to prevent Russia's plan to assassinate the CEO of Rheinmetall, a German defence industry company that has been a significant weapons supplier to Ukraine[76]. In addition, two persons with German-Russian dual nationality and connections to the GRU were arrested on planning bomb attacks to industrial and military facilities in Germany, including an US military base where Ukrainian soldiers were trained[77]. According to the media, suspicions of Russia's involvement have also been raised in connection to two fires in 2024, one in a metal factory belonging to a defence manufacturer in Germany and the other in an ammunition factory in Czechia[78]. These kinds of hybrid tactics – sabotage operations, assassination attempts and disinformation campaigns – are all part of Russia's strategy to undermine the EU's support for Ukraine, weaken Ukraine's military capabilities and prolong the war.

Conclusions

Hybrid warfare, which blend conventional military actions and unconventional tactics, such as cyberattacks, disinformation campaigns, economic coercion, instrumentalised migration, and sabotage, has been strategically employed by Russia to destabilize and undermine the EU and its member states particularly since Russia's full-scale invasion of Ukraine. At the same time, the awareness of Russia's hybrid war against the EU has increased and it has become a matter of public knowledge. Russia's war of aggression has also led to a significant change in the EU's policies towards Russia that is now generally perceived as a security threat. Although Russia has generally tried to make it difficult to prove its involvement in hybrid attacks, the public statements of politicians and experts holding Russia responsible for these attacks have become common across the EU, drawing attention to this hostile action.

The media has played an important role in raising public awareness of Russia's hybrid war against the EU, although the incidents the media has found out are probably only a tip of the iceberg. Incidents suspected as Russia's hybrid operations often get a lot of media attention at the time of the event, naturally, because these kinds of headlines catch the interest of the public and sell newspapers. Therefore, it is also possible that

---

[74] Siegfried Mortkowitz, "Czechs pull back from Russia after bombing allegations," *Politico,* April 18, 2021, https://www.politico.eu/article/czechs-expel-russian-envoys-alleging-kremlin-role-in-deadly-2014-blast/.
[75] Fornusek, "Czech police conclude Russian agents behind deadly 2014 ammunition depot blasts."
[76] Katie Bo Lillis et al., "Exclusive: US and Germany foiled Russian plot to assassinate CEO of arms manufacturer sending weapons to Ukraine," *CNN,* July 11, 2024, https://edition.cnn.com/2024/07/11/politics/us-germany-foiled-russian-assassination-plot/index.html; Arjun Neil Alim et al., "Russia believed to be behind plot to assassinate European defence boss," *Financial Times,* July 11, 2024, https://www.ft.com/content/1b685d36-1981-4863-a868-b98d5f17cbe4.
[77] Sam Jones, "Germany arrests suspected Russian spies over bombing plot," *Financial Times,* April 18, 2024, https://www.ft.com/content/9ee73d65-9575-410c-acba-3bc8b0bc08ae.
[78] Sam Jones et al., "Russia plotting sabotage across Europe, intelligence agencies warn."; Paton Walsh et al., "From $7 graffiti to arson and a bomb plot: How Russia's 'shadow war' on NATO members has evolved," *CNN,* July 10, 2024, https://edition.cnn.com/2024/07/10/europe/russia-shadow-war-nato-intl-latam/index.html.

the media may in some cases exaggerate the Russian role in the incidents in order to increase the visibility of the news, and thereby their own sales. In addition, sometimes cases initially suspected to be Russian hybrid operations turn out to have other causes. This, together with extensive media coverage, can advance Russia's goals if it creates fear and confusion among the public.

In general, reporting on the consequences of the hybrid operations is harder to find in the media, which may partly be due to prolonged investigation and legal processes. Although Russia's involvement has often been evident, responses have varied and it has been difficult to hold someone accountable. Even if the case had progressed to the legal process, there are many examples in the media how suspects have defected to Russia or Belarus if allowed to wait for the trial on the loose, which is quite common. After that, the traces of them often disappear.

Based on the media material analysed in this study, Russia's hybrid war against the EU has evolved from a blend of tactics aimed at destabilizing adversaries to a more direct and aggressive approach with the full-scale invasion of Ukraine, posing significant challenges to European security. The selected four cases illustrate how political, social, economic and military aims and impacts intertwine in Russia's hybrid war against the EU, and how various means, such as disinformation campaigns, cyberattacks, sabotage, instrumentalized migration and even assassination attempts, are applied to reach the desired effects. They also show the variety of actors Russia has used in its hybrid operations, ranging from intelligence agencies, state-linked hacker groups and troll factories to criminals, Russian emigrants and citizens of third countries.

The evolution of Russia's hybrid war underscores the need for the EU to address various hybrid threats effectively. This requires, firstly, understanding the threat, and secondly, strengthening preparedness for and resilience to it. As a response to hybrid threats, the EU is increasingly focusing on cybersecurity, countering disinformation and electoral interference, and enhancing resilience against disruption of critical infrastructure. Recently, the EU has adopted a sanctions framework targeting individuals and entities engaged in destabilising activities against the EU and its member states, such as information manipulation, sabotage of critical infrastructure, malicious cyber activities, and instrumentalised migration.[79]

Because Russia aims to create divisions, increasing collaboration and information sharing both nationally and at the EU-level is important in order to foster unity. A comprehensive approach to security, in which the authorities, business community, and civil society collaborate in taking care of society's critical functions, improves resilience to hybrid threats. For instance, critical infrastructure is often owned and operated by the private sector, which thus plays an important role in strengthening its resilience. Citizens' resistance to disinformation, on the other hand, could be improve by building media literacy. At the moment, Russia is primarily trying to break up the EU's consensus on support for Ukraine by spreading disinformation, interfering elections and manipulating public opinion, to which the EU could best respond by demonstrating its unity and further increasing its support for Ukraine.

[79] European Council and the Council of the European Union, "Hybrid threats."

References

Abboud, Leila, Foy, Henry, and Paula Erizanu. "Europe battles 'avalanche of disinformation' from Russia." *Financial Times*, March 21, 2024. https://www.ft.com/content/2ffe8b64-f9bc-46d4-bf40-eefbbc6fac77.

Abromaitis, Žygintas. "'All friendships are over': Lithuania fortifies border with Russia's Kaliningrad." *LRT,* September 6, 2024. https://www.lrt.lt/en/news-in-english/19/2354296/all-friendships-are-over-lithuania-fortifies-border-with-russia-s-kaliningrad.

Adomaitis, Nerijus. "Norway's spy chief sees Russia more likely to attempt sabotage." *Reuters,* September 11, 2024. https://www.reuters.com/world/europe/norways-spy-chief-sees-russia-more-likely-attempt-sabotage-2024-09-10/.

Lillis, Katie Bo, Bertrand, Natasha, and Frederik Pleitgen. "Exclusive: US and Germany foiled Russian plot to assassinate CEO of arms manufacturer sending weapons to Ukraine." *CNN,* July 11, 2024. https://edition.cnn.com/2024/07/11/politics/us-germany-foiled-russian-assassination-plot/index.html;

Alim, Arjun Neil, Foy, Henry, and Max Seddon. "Russia believed to be behind plot to assassinate European defence boss." *Financial Times,* July 11, 2024. https://www.ft.com/content/1b685d36-1981-4863-a868-b98d5f17cbe4.

Aurel, Sari. *Instrumentalized migration and the Belarus crisis: Strategies of legal coercion*. The European Centre of Excellence for Countering Hybrid Threats, 2023. 20230425-Hybrid-CoE-Paper-17-Instrumentalized-migration-and-Belarus-WEB.pdf.

Bellingcat Investigation Team. "Senior GRU Leader Directly Involved With Czech Arms Depot Explosion." *Bellingat,* April 20, 2021. https://www.bellingcat.com/news/2021/04/20/senior-gru-leader-directly-involved-with-czech-arms-depot-explosion/.

Bellingcat Investigation Team. "How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine." *Bellingcat*, April 26, 2021. https://www.bellingcat.com/news/uk-and-europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/.

Bennett, Cory. "Belarus sends de-escalation signals on migrant crisis." *Politico*, November 15, 2021. https://www.politico.eu/article/belarus-de-escalation-signals-migrant-crisis/.

Bounds, Andy. "Russia paid pro-Kremlin lawmakers to influence EU elections, says Belgium." *Financial Times,* April 12, 2024. https://www.ft.com/content/8bb921fa-57b3-44aa-80d6-b35794a523db.

Braw, Elisabeth Braw. "How Sweden Became Public Enemy No. 1." *Foreign Policy*, July 28, 2023. https://foreignpolicy.com/2023/07/28/sweden-quran-nato-iran-iraq-russia/.

Clark, Sam. "Winter is coming. So are Russia's elite hackers." *Politico,* November 22, 2024. https://www.politico.eu/article/russia-hackers-europe-winter-energy-infrastructure-moscow-gas-hike-digital/.

Corera, Gordon. "Salisbury poisoning suspects 'linked to Czech blast'." *BBC*, April 18, 2021. https://www.bbc.com/news/uk-56790053.

Council on Foreign Relations. "Compromise of a power grid in eastern Ukraine." Accessed March 23, 2025. https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine.

Dobbinga, Benedicte. "Research: Europe increasingly targeted by Russian sabotage." *Leiden University,* January 20, 2025. https://www.universiteitleiden.nl/en/news/2025/01/research-europe-increasingly-targeted-by-russian-sabotage.

Dunai, Marton. "Russian hitmen and saboteurs target Bulgaria's arms industry, magnate says." *Financial Times,* November 19 2023. https://www.ft.com/content/b1aa5696-6515-487d-ba4d-380c9c431c18.

EBU Investigative Journalism Network. "Playing With Fire. Are Russia's hybrid attacks the new European war?" *Eurovision News,* March 12, 2025. https://investigations.news-exchange.ebu.ch/playing-with-fire-are-russias-hybrid-attacks-the-new-european-war/#group-section-The-Long-Game-h5jbSZtZX7.

Edwards, Charlie. "Russia's hybrid war in Europe enters a dangerous new phase." *IISS*, November 26, 2024. https://www.iiss.org/online-analysis/online-analysis/2024/11/russias-hybrid-war-in-europe-enters-a-dangerous-new-phase/.

Espinoza, Javier, Hancock, Alice, and Tamma, Paola. "Brussels seeks to ban Russian funding of European politicians." *Financial Times,* May 6, 2024. https://www.ft.com/content/ab480869-684e-4180-bfa6-70266beeca24.

EurActiv. "France, Germany, Poland facing 'permanent' Russian disinformation attacks: EU." June 5, 2024. https://www.euractiv.com/section/elections/news/france-germany-poland-facing-permanent-russian-disinformation-attacks-eu/.

Euronews. "European hospitals targeted by 'pro-Russian' hackers." February 1, 2023. https://www.euronews.com/2023/02/01/european-hospitals-targeted-by-pro-russian-hackers.

European Council and the Council of the European Union. "Hybrid threats." Last modified February 25, 2025. https://www.consilium.europa.eu/en/policies/hybrid-threats/.

European Council and the Council of the European Union. "EU sanctions against Russia explained." Last modified March 19, 2025. https://www.consilium.europa.eu/en/policies/sanctions-against-russia-explained/#media.

EUvsDisinfo. "The Kremlin's futile disinfo trash catapult." Last modified September 5, 2024. https://euvsdisinfo.eu/the-kremlins-futile-disinfo-trash-catapult/.

EUvsDisinfo. "Split the EU: a constant priority of the Kremlin." Last modified February 26, 2025. https://euvsdisinfo.eu/split-the-eu-a-constant-priority-of-the-kremlin/.

Finnish Government. "Situation at Finland's eastern border." Accessed March 21, 2025. https://valtioneuvosto.fi/en/situation-at-finlands-eastern-border.

Fornusek, Martin. "Czech police conclude Russian agents behind deadly 2014 ammunition depot blasts." *The Kyiv Independent,* April 29, 2024. https://kyivindependent.com/czech-police-says-russian-agents-behind-deadly-2014-bombing/.

France24. "Rail traffic in northern Germany disrupted by 'sabotage'." October 8, 2022. https://www.france24.com/en/europe/20221008-rail-traffic-in-northern-germany-disrupted-by-sabotage.

Goury-Laffont, Victor and Clea Caulcutt. "'Coordinated arson attack' brings French trains to a halt hours before Olympics opening ceremony." *Politico,* July 26, 2024. https://www.politico.eu/article/coordinated-attack-brings-french-train-system-to-a-halt-on-opening-olympics-weekend/.

Goury-Laffont, Victor. "French fiber optic cables hit by 'major sabotage' in second Olympics attack." *Politico,* July 29, 2024. https://www.politico.eu/article/french-fiber-optic-cable-hit-with-alleged-acts-of-sabotage/.

Hancock, Alice and Raphael Minder. "Poland 'most attacked' online by Russia, says minister." *Financial Times,* January 16, 2025. https://www.ft.com/content/e0e1a016-e4e0-4628-a0ac-c4a6e9d15db6.

Jensen, Benjamin, Brandon Valeriano, and Ryan Maness. "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist." *Journal of Strategic Studies* 42, no. 2 (2019): 212–34. https://doi.org/10.1080/01402390.2018.1559152.

Jones, Sam. "Germany arrests suspected Russian spies over bombing plot." *Financial Times,* April 18, 2024. https://www.ft.com/content/9ee73d65-9575-410c-acba-3bc8b0bc08ae.

Jones, Sam, Rathbone, John Paul, and Richard Milne. "Russia plotting sabotage across Europe, intelligence agencies warn." *Financial Times,* May 5, 2024. https://www.ft.com/content/c88509f9-c9bd-46f4-8a5c-9b2bdd3c3dd3.

Juhola, Teemu. "Venäjän GPS-häirintä kasvoi rajusti Virossa vain vuodessa – asiantuntijalta karu arvio tilanteesta." *Yle,* May 21, 2024. https://yle.fi/a/74-20088861.

Kalniete, Sandra and Tomass Pildegovičs. "Strengthening the EU's resilience to hybrid threats." *European View*, 20, no. 1 (2021): 23-33. https://doi.org/10.1177/17816858211004648.

Kauranen, Anne, Plucinska Joanna, and James Pearson. "Explainer: What is GPS jamming and why is it a problem for aviation?" *Reuters,* May 1, 2024. https://www.reuters.com/business/aerospace-defense/what-is-gps-jamming-why-it-is-problem-aviation-2024-04-30/.

Kayali, Laura, Banse, Dirk, Büscher, Wolfgang, Kraetzer, Ulrich, Müller, Uwe, and Christian Schweppe. "Europe is under attack from Russia. Why isn't it fighting back?" *Politico,* November 25, 2024. https://www.politico.eu/article/europe-russia-hybrid-war-vladimir-putin-germany-cyberattacks-election-interference/.

Kuznetsov, Sergei. "Lithuania slams shut the door to the EU for irregular migrants." *Politico,* September 1, 2021. https://www.politico.eu/article/lithuania-migrants-eu-asylum-belarus-alexander-lukashenko/.

Laine, Martin. “Dokumendid otse Kremli trollivabrikust: kuidas Venemaa taas europarlamendi valimisi mõjutas.” *Delfi*, September 16, 2024. https://www.delfi.ee/artikkel/120321674/dokumendid-otse-kremli-trollivabrikust-kuidas-venemaa-taas-europarlamendi-valimisi-mojutas.

Laine, Martin and Anastasiia Morozova. “Leaked Files from Putin’s Troll Factory: How Russia Manipulated European Elections.” *VSquare*, September 16, 2024. https://vsquare.org/leaked-files-putin-troll-factory-russia-european-elections-factory-of-fakes/.

McGrath, Sophia. *Spotlight on the Shadow War: Inside Russia’s attacks on NATO Territory*. U.S. Helsinki Commission, 2024. https://www.csce.gov/wp-content/uploads/2024/12/Spotlight-on-the-Shadow-War-Website.pdf.

McGuinness, Damien. ”How a cyber attack transformed Estonia.” *BBC*, April 27, 2017. https://www.bbc.com/news/39655415.

Mikkola, Harri, Aaltola, Mika, Wigell, Mikael, Juntunen, Tapio, and Antto Vihma. *Hybridivaikuttaminen ja demokratian resilienssi. Ulkoisen häirinnän mahdollisuudet ja torjuntakyky liberaaleissa demokratioissa*. The Finnish Institute of International Affairs, 2018). https://www.fiia.fi/en/publication/hybridivaikuttaminen-ja-demokratian-resilienssi.

Milne, Richard. “Russia behind Ikea arson attack in Lithuania, prosecutors say.” *Financial Times,* March 17, 2025. https://www.ft.com/content/756a948b-e48d-480e-88e4-c0d52b361b35.

Mortkowitz, Siegfried. “Czechs pull back from Russia after bombing allegations.” *Politico,* April 18, 2021. https://www.politico.eu/article/czechs-expel-russian-envoys-alleging-kremlin-role-in-deadly-2014-blast/.

Mumford, Andrew, and Pascal Carlucci. “Hybrid Warfare: The Continuation of Ambiguity by Other Means.” *European Journal of International Security* 8, no. 2 (2023): 192–206. https://doi.org/10.1017/eis.2022.19.

Mäntymaa, Eero. ” Venäjä päästi kahdeksan vuotta sitten 1700 turvapaikanhakijaa itärajalle – Yle selvitti, moniko heistä sai jäädä Suomeen.” *Yle,* December 2, 2023. https://yle.fi/a/74-20063227.

National Land Survey of Finland. ”Interference spoiled aerial photography in southeastern Finland, potentially resulting in damage of millions of euros – the National Land Survey of Finland has solutions for preparing for GNSS disturbances.” Last modified October 2, 2024. https://www.maanmittauslaitos.fi/en/topical_issues/interference-spoiled-aerial-photography-southeastern-finland-potentially-resulting.

NATO. “NATO launches 'Baltic Sentry' to increase critical infrastructure security.” Last modified January 14, 2025. https://www.nato.int/cps/en/natohq/news_232122.htm.

O'Carroll, Lisa. “Russia using criminal networks to drive increase in sabotage acts, says Europol.” *The Guardian,* March 18, 2025. https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol.

Ortamo, Simo. “Venäjä näyttää nyt tekevän kyberiskuja länsimaiden vesilaitoksiin – Mikko Hyppönen: ’Aikamoinen uutinen’.” *Yle,* April 21, 2024. https://yle.fi/a/74-20084689.

Ortamo, Simo. "Uusi tietovuoto paljasti Venäjän häikäilemättömän vaikutusoperaation, asiantuntijalta tyly huomio." *Yle,* September 23, 2024. https://yle.fi/a/74-20112682.

Paul, Christopher and Miriam Matthews. "The Russian 'Firehose of Falsehood' Propaganda Model." *RAND,* July 11, 2016. https://www.rand.org/pubs/perspectives/PE198.html.

Parviala, Antti. "Suomen gps-häiriökartta punaisena – onko paikannus maalla, merellä ja ilmassa uhattuna?" *Yle,* March 18, 2024. https://yle.fi/a/74-20079337.

Paton Walsh, Nick, Dean, Sarah, and Karolina Jeznach. "From $7 graffiti to arson and a bomb plot: How Russia's 'shadow war' on NATO members has evolved." *CNN,* July 10, 2024. https://edition.cnn.com/2024/07/10/europe/russia-shadow-war-nato-intl-latam/index.html.

Peltonen, Topias and Elisa Paljakka. "Itä-Suomen lentoasemat ottivat uudelleen käyttöön radionavigaatiojärjestelmän GPS-häirinnän takia." *Yle,* November 7, 2024. https://yle.fi/a/74-20123095.

Pillai, Helmi. *Protecting Europe's critical infrastructure from Russian hybrid threats*. Centre for European Reform, 2023. https://www.cer.eu/sites/default/files/pb_HP_hybrid_threats_25.4.23.pdf.

Rathbone, John Paul, Jones, Sam, and Courtney Weaver. "Europe kicked out Vladimir Putin's spies. Now they're back." *Financial Times,* March 6, 2024. https://www.ft.com/content/f066d653-70e2-42e9-baac-c342417c8ef3.

Richterova, Daniela, Elena Grossfeld, Magda Long, and Patrick Bury. "Russian Sabotage in the Gig-Economy Era." *The RUSI Journal* 169, no. 5 (2024): 10–21. https://doi.org/10.1080/03071847.2024.2401232.

Schuurman, Bart. *Russian operations against Europe since the 2022 invasion of Ukraine*. The Hague: Leiden University, 2025. https://www.universiteitleiden.nl/binaries/content/assets/governance-and-global-affairs/isga/infographic-russian-operations-against-europe.pdf

Scutaru, George and Andrei Pavel. "Weaponization of Migration: A Powerful Instrument in Russia's Hybrid Toolbox," *The Caravan*, September 17, 2024. https://www.hoover.org/research/weaponization-migration-powerful-instrument-russias-hybrid-toolbox.

Stroobants, Jean-Pierre. "In the North Sea, Russia conceals espionage activities with commercial ships." *LeMonde,* June 22, 2024. https://www.lemonde.fr/en/international/article/2024/06/22/in-the-north-sea-russia-conceals-espionage-activities-with-commercial-ships_6675426_4.html.

Tanskanen, Jari. "Finnair keskeyttää Viron Tarton lennot kuukaudeksi – kentälle rakennetaan GPS-häirinnästä riippumaton lähestymisjärjestelmä." *Yle,* April 29, 2024. https://yle.fi/a/74-20086197.

Taussi, Sari and Elina Ervasti. " Valko-Venäjän ja Puolan rajalla on Euroopan uusin siirtolaiskriisi – keitä ovat ihmiset rajalla ja miksi he ovat siellä? Katso ja lue vastaukset." *Yle,* November 9, 2021. https://yle.fi/a/3-12180959.

Thompson, Polly. "French infrastructure was targeted for a 2nd time during the Olympics, with internet and phone cables cut across the country." *Business Insider,* July 29, 2024. https://www.businessinsider.com/french-fiber-optic-cables-cut-phone-internet-services-infrastructure-attack-2024-7.

Tynkkynen, Jyri. "Norjassa havahduttu uudenlaiseen GPS-häirintään – Suomessakin jo tutkittu asiaa." *Yle,* January 30, 2025. https://yle.fi/a/74-20139819.

Tynkkynen, Jyri. "Perinteinen GPS-häirintä on edelleen ykkösongelma satelliittinavigoinnille uudesta spoofing-häirinnästä huolimatta." *Yle,* January 31, 2025. https://yle.fi/a/74-20140362.

Van Rensbergen, Arno. "Hybrid threats: Russia's shadow war escalates across Europe." *The Parliament Magazine*, January 21, 2025. https://www.theparliamentmagazine.eu/news/article/hybrid-threats-russias-shadow-war-escalates-across-europe.

Wagstyl, Stefan. "German politics: Russia's next target?" *Financial Times*, January 29, 2017. https://www.ft.com/content/31a5758c-e3d8-11e6-9645-c9357a75844a.

Verseck, Keno. "Is Russia behind the 2014 Czech munition depot blasts?" *DW,* April 20, 2021. https://www.dw.com/en/is-russia-behind-the-2014-czech-munition-depot-blasts/a-57260551.

Wither, James K. "Making Sense of Hybrid Warfare." *Connections* 15, no. 2 (2016): 73–87. http://www.jstor.org/stable/26326441.

Wohlfeld, Monica, Nickels, Benjamin P., and Benjamin Jensen. "NATO and Instrumentalized Migration." *Center for Strategic and International Studies*, July 12, 2024. https://www.csis.org/analysis/nato-and-instrumentalized-migration.

Ålander, Minna. "Death by a Thousand Paper Cuts: Lessons from the Nordic-Baltic Region on Countering Russian Gray Zone Aggression." *Carnegie Endowment for International Peace*, November 14, 2024. https://carnegieendowment.org/research/2024/11/russia-gray-zone-aggression-baltic-nordic?lang=en.