NEW STRATEGY CENTER

Norsk Utenrikspolitisk Institutt

JOINT WORKING PAPER II

FLANKS 2

Addressing the challenge of the Russian hybrid warfare the NATO way. The case of Norway and Romania

Dr. Jakub GODZIMIRSKI, Research Professor, Norwegian Institute Of International Affairs

Dr. Alina BÂRGĂOANU, Senior Associate Expert, New Strategy Center

Răzvan CEUCA, International Relations Expert, New Strategy Center

FLANKS 2 – Addressing the challenge of the Russian hybrid warfare the NATO way. The case of Norway and Romania

The findings of the research presented here are a result of the implementation of the bilateral initiative FLANKS II - Dealing with the challenge of political warfare in the COVID-19 and Ukraine war context, financed under the Fund for Bilateral Relations 2014-2021, copublished by New Strategy Center, Romania and the Norwegian Institute of International Affairs (NUPI).

July 2024

Iceland Liechtenstein Norway grants

Authors:

Jakub GODZIMIRSKI is a Research Professor at NUPI. He has been working on Russian foreign and security policy issues for more than 20 years, paying special attention to the role of energy resources in Russian grand strategy. In addition, he also has worked on European policy and its impact on developments in Central and Eastern Europe, including relations with Russia.

Alina BÂRGĂOANU Senior Associate Expert at New Strategy Center and Dean of the College of Communication and Public Relations, National University of Political Studies and Public Administration (Bucharest). She is currently a member of the Advisory Board of the European Digital Media Observatory. In 2018, she was a member of the High-Level Expert Group on Fake News and Online Disinformation.

Răzvan CEUCA is an external relations expert at the New Strategy Center, specializing in state-level cybersecurity and Russian hybrid warfare. His recent studies focus on Moscow's narratives about the Ukraine war and Ukraine's cyber defense efforts. He is also a PhD student at Babeș-Bolyai University, researching cybersecurity approaches of states in Eastern Europe.

Co-editors:

Dr. Ileana ROTARU is Senior Associate Expert at New Strategy Center and an Associate Professor of West University of Timisoara, Romania (Department of Philosophy and Communication Sciences) and PhD supervisor in Communication Sciences. Her research has been focusing on the trans-disciplinary fields of communication sciences.

Sergiu MITRESCU is the Program Director of the New Strategy Center in Bucharest. He holds a BA in International Relations and a MA in Security Studies from the University of Birmingham, United Kingdom. His research focuses on hybrid threats with a particular focus on Russian New Generation Warfare.

NEW STRATEGY CENTER

Norsk Utenrikspolitisk Institutt

Addressing the challenge of the Russian hybrid warfare the NATO way. The case of Norway and Romania

FLANKS 2

Dr. Jakub GODZIMIRSKI, Research Professor, Norwegian Institute of International Affairs

Dr. Alina BÂRGĂOANU, Senior Associate Expert, New Strategy Center

Răzvan CEUCA, International Relations Expert, New Strategy Center

Addressing the challenge of the Russian hybrid warfare the NATO way
The case of Norway and Romania

Introduction: NATO's political warfare challenge

Before presenting a more detailed analysis of how the preliminary findings of the FLANKS 2 project carried out jointly by the Norwegian Institute of International Affairs NUPI and the Romanian think tank "New Strategy Center" can be relevant for NATO, we must briefly present our operational understanding of the key concepts used in this examination.

The main objective of the FLANKS 2 project was to develop and further consolidate the understanding and knowledge of how societies and institutions in the Nordic and Black Sea Region must be prepared to meet and deal with the challenges posed by political warfare and the use of various instruments of power which fall short of kinetic warfare. By examining the use of various instruments of national power by actors challenging the existing rules-based order and international law, the project aimed to map what instruments of national power short of military one are at the disposal of revanchist states operating in the two regions and to provide policy-relevant support and advice for citizens and institutions dealing with the challenge of political warfare in the regions in question. The key findings of this project are presented in a report published in 2024 by the project team.[1] This report also presented a brief discussion on the meaning of the concept of political warfare and other concepts that are currently used to describe a set of hostile activities referred sometimes to as Foreign Information Manipulation and Interference (FIMI)[2] implemented by Russia and other revanchist regimes and targeting opinion and policy making circles in the Western, liberal world.

Here is a summary of the discussion on these key concepts. The RAND report presented a detailed examination of issues related to modern political warfare.[3] One of the first to use the concept was George Kennan, who defined it as "the employment of all the means of national power, short of war, to achieve national objectives". Paul Smith argued that political warfare could include elements of violence but "its chief aspect is the use of words, images, and ideas, commonly known, according to context, as propaganda and psychological warfare". United States Special Operations Command defined political warfare as "a spectrum of activities associated with diplomatic and economic engagement, Security Sector Assistance (SSA), novel forms of Unconventional Warfare (UW), and Information and Influence Activities (IIA)." RAND authors proposed the definition of political warfare as "a deliberate policy choice to undermine a

---

[1] Ionita, D., Cristea, I., Melnic, C., Stefureac, R., Godzimirski J.M., Blackburn, M. (2024). *Norway and Romania: Navigating Information Warfare.* New Strategy Center and Norwegian Institute of International Affair NUPI at https://newstrategycenter.ro/wp-content/uploads/2024/04/Norway-and-Romania-Navigating-Information-Warfare.pdf

[2] For more on this see EEAS (2024). 2nd EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defense. *Report on FIMI Threats* at https://euneighbourseast.eu/wp-content/uploads/2024/01/eeas-2nd-report-on-fimi-threats-january-2024_0-compressed.pdf. For the first edition of this report see https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf

[3] Robinson, L., Helmus, T. C., Cohen, R. S., Nader, A., Radin, A., Magnuson, M., & Migacheva, K. (2019). *Modern Political Warfare. Current Practices and Possible Responses*. Rand Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1772/RAND_RR1772.pdf

rival or achieve other explicitly political objectives by means other than routine diplomacy or all-out war".[4]

The term political warfare is not widely used in the Russian context, where these types of activities are most often referred to as New Generation Warfare (NGW). The NGW is most interested in Psychological and People-Centred Aspects and places greater emphasis on psychological and human factors over traditional military concerns. The main objective in the context of modern full-spectrum conflict is to influence minds and perceptions of targeted groups. The main NGW ideas were outlined in the text published in 2013 by Valeriy Gerasimov, the Chief of the Russian General Staff.[5]

Finally, there is also the concept of hybrid warfare that at least partly overlaps with the concept of political warfare and shares some features with what Russians describe as NGW. According to a recently published study[6], hybrid warfare should be understood as all kinds of aggression short of all-out warfare and includes, but is not limited to, disinformation, sabotage, subversion as well as cyber operations. The same study states that the use of information technologies makes grey zone aggression more effective as they expand the speed, scale, and intensity of grey zone conflict through cyber and social media influence operations.

NATO's understanding of the hybrid challenge

NATO is aware of the existence of this type of threats and the role that Russia can play in this context.[7] A thorough examination of official NATO statements reveals that the term "political warfare" is not used by the alliance, but this type of challenges is referred to in NATO's official statements as hybrid warfare. According to NATO official documents summing up discussions on the most important challenges that the Alliance must address, hybrid threats are understood as a wide range of overt and covert military, paramilitary, and civilian measures that are employed in a highly integrated design. There is also an understanding in the NATO decision-making circles that the Alliance must possess the necessary tools and procedures required to deter and respond effectively to hybrid warfare threats, and the capabilities to reinforce national forces. These capabilities include enhancing strategic communications, developing exercise scenarios in light of hybrid threats, and strengthening coordination between NATO and other organisations that must address similar challenges.[8] In response to these hybrid threats, the transatlantic alliance decided to agree a strategy on NATO's role in Countering Hybrid Warfare, which was implemented in coordination with the EU.[9] The same document outlined the main objectives of the NATO Cyber

---

[4] Robinson et al. 2019 p.6.

[5] Gerasimov, V. (2013) The Value of Science in Prediction. *Military-Industrial Kurier,* 27 February at https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html. See also Prudnikov, L. A., & Kuzmenko, A. V. (2023). Primeneniye nevoyennykh mer v interesakh obespecheniya voyennoy bezopasnosti Rossii (Application of non-military measures in the interests of ensuring military security of Russia). *Voyennaya Mysl*(1) and . https://vm.ric.mil.ru/Stati/item/461891/ and Fridman, O. (2018). *Russian Hybrid Warfare. Resurgence and Politicisation*. Hurst & Company for the Western reading of this phenomenon.

[6] Maschmeyer, L. (2023). Assessing Hybrid War: Separating Fact from Fiction. *CSS Analyses in Security Policy, no. 33.* https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse332-EN.pdf

[7] For more on this see NATO (2024). Countering hybrid threats at https://www.nato.int/cps/en/natohq/topics_156338.htm.

[8] NATO 2014 Wales Summit Declaration at https://www.nato.int/cps/en/natohq/official_texts_112964.htm

[9] NATO 2016 Warsaw Summit Communiqué at https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Defence Pledge, namely to enhance the cyber defences of national networks and infrastructures, to improve resilience and ability to respond quickly and effectively to cyber-attacks, including in hybrid contexts, as well as to continuously adapt NATO's cyber defence capabilities. NATO also decided to take steps to ensure its ability to effectively address the challenges posed by hybrid warfare that was understood, as we have already underlined, as a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures, employed in a highly integrated design by state and non-state actors alike. One of the steps was the adoption of a strategy and actionable implementation plans on NATO's role in countering hybrid warfare. Although the primary responsibility to respond to hybrid threats or attacks was of the targeted nation, NATO was prepared to assist an Ally at any stage of a hybrid campaign and these actions were described as a part of collective defence that was the main task of the Alliance.[10]

In the 2018 Brussels Summit Declaration, disinformation campaigns and malicious cyber activities were listed as elements of hybrid warfare with which the Alliance had to deal. Russia was accused of challenging Euro-Atlantic security, stability and sometimes even sovereignty of its member states through hybrid actions, such as attempted interference in the election processes, widespread disinformation campaigns, and malicious cyber activities. The use of a military-grade nerve agent in the attack against Sergey Skripal in Salisbury was also added to the list of hybrid challenges facing NATO. At the same time, the 2018 declaration mentioned that the Alliance was facing increasing challenge from both state and non-state actors who use hybrid activities that aim to create ambiguity and blur the lines between peace, crisis, and conflict, and warned that in cases of hybrid warfare, the Council could decide to invoke Article 5 of the Washington Treaty, just like in the case of an armed attack.[11] In addition, to deal with the challenges posed by hybrid warfare NATO decided to establish Counter Hybrid Support Teams, which are designed to provide tailored, targeted assistance to Allies, upon their request, in preparing for and responding to hybrid activities.[12]

In its Brussel Summit Communiqué issued in June 2021, NATO listed cyber, hybrid, and other asymmetric threats, including disinformation campaigns, and the malicious use of ever-more sophisticated emerging and disruptive technologies among the main threats that the Alliance must address. The same document identified Russia as one of the countries that had intensified the use of hybrid instruments of power in order to influence policies of other countries. The document listed interference in Allied countries' elections and democratic processes; political and economic pressure and intimidation; widespread disinformation campaigns; malicious cyber activities; turning a blind eye to cyber criminals operating from its territory, including those who target and disrupt critical infrastructure in NATO countries; illegal and destructive activities carried out by Russian Intelligence Services on Allied territory as hostile activities that could be attributed to Russia.[13] In response to these negative trends, the Alliance signalled its interest in and willingness to enhance its situational awareness and expand the tools at its disposal to counter hybrid threats, including disinformation campaigns, by developing comprehensive preventive and response options.[14] In the relatively brief NATO Madrid Summit Declaration issued in June 2022, the Alliance listed various asymmetric threats that it had to address, including cyber, space, and

[10] Ibid.
[11] NATO 2018 Brussels Summit Declaration at https://www.nato.int/cps/en/natohq/official_texts_156624.htm
[12] Ibid.
[13] NATO 2021 Brussels Sumit Communiqué at https://www.nato.int/cps/en/natohq/news_185000.htm
[14] Ibid.

hybrid as well as the malicious use of emerging and disruptive technologies that could pose a challenge to its security.[15]

The 2023 Vilnius Summit Declaration mentioned the term hybrid no less than 15 times and presented the most comprehensive examination of how the Alliance was to deal with this challenge. Russia was named as the country that had intensified its hybrid actions against NATO Allies and partners, including through proxies. Russia's actions included interference with democratic and electoral processes, political and economic coercion, widespread disinformation campaigns, malicious cyber activities, and illegal and disruptive activities of Russian intelligence services. Other NATO's strategic competitors and potential adversaries were also identified as investing heavily in technologies that can be highly effective, can play a decisive part in conflicts, and help implement various hostile hybrid activities. According to the 2023 Declaration, these hybrid activities targeted NATO's political institutions, its critical infrastructure, societies, democratic systems, economies and citizens. The Declaration repeated that hybrid activities could lead to the Alliance invoking Article 5 of the Washington Treaty and provided some clues as to how NATO was to address these hybrid threats at an Allied level and by providing support to member states most exposed to this type of activities.

Finally, the Washington Summit Declaration issued in July 2024 also paid some attention to hybrid threats posing a challenge to the Alliance. The term hybrid is mentioned 10 times and Russia is again accused of launching various types of hybrid operations against NATO members. The Declaration listed sabotage, acts of violence, provocations at Allied borders, weaponization of irregular migration, malicious cyber activities, electronic interference, disinformation campaigns and hostile political influence, as well as economic coercion as key Russian hybrid activities posing a threat to Allied security. The Summit Declaration underlined that these Russian hybrid activities will not deter Allies' resolve and support to Ukraine and that the Alliance will provide support to its partners most exposed to Russian destabilisation efforts.

One of the aspects of hybrid warfare that NATO came to recognize relatively late as an important challenge was the question of the weaponization of the information space in this context. The terms "disinformation" and "misinformation" appeared relatively late in the Alliance official declarations and communiqués. The issue of disinformation as a challenge appeared for the first time in the 2018 Brussels Summit Declaration and has been addressed in all summit declarations and Communiqués ever since, while the concept of misinformation was mentioned only once in 2024 Washington Summit Declaration. At the same time, the use of fabricated/ false narratives to influence public opinion in NATO countries was recognized as a challenge to NATO security relatively late. It was mentioned for the first time in the 2022 Statement by NATO Heads of State issued the day after Russia launched its full-scale invasion of Ukraine and was repeated in the 2023 Vilnius Summit Declaration.

An issue that attracted even more attention than hybrid warfare in this official set of NATO summit declarations and communiqués is the question of cyber-related threats and challenges. While the term "hybrid" is mentioned 83 times, the term "cyber" occurs 176 times, which is an indication of the Alliance's concern with the impact of such operations in the cyberspace. Russia's illegal occupation of Crimea followed by various types of hybrid anti-NATO operations, as mentioned in the official NATO statements, made the alliance pay more attention to the question of how to increase the level of resilience in member states. 76 mentions of the term "resilience" are made in NATO documents issued after 2014, starting with the 2014 Wales Summit Declaration and ending

[15] NATO 2022 Madrid Summit Declaration at https://www.nato.int/cps/en/natohq/official_texts_196951.htm

with the 2024 Washington Summit Declaration. Finally, NATO has also expressed a growing interest in two additional areas that can be exposed to hybrid threats and that are crucial for national and societal resilience, namely energy and energy security. These have emerged in NATO official declarations 122 times, starting with the 2006 Riga Summit Declaration. Questions related to infrastructure (59 mentions) were occasionally addressed in the declarations and communiqués between 1997 and 2012, but have been discussed more intensely during NATO summits ever since the outbreak of the conflict in Ukraine in 2014.

NATO Declaration and Communique	Russia	hybrid	cyber	information	energy	infrastructure	resilience
1991 **NATO Declaration on Peace and Cooperation**	3			1			
1994 **NATO Brussels Summit Declaration**	3						
1997 **NATO Founding Act**	73					2	
1997 **Madrid Declaration**	10			2			
1999 **Washington Summit Communiqué**	11			5		1	
2002 **NATO Russia Relations**	33			3		1	
2002 **Prague Summit Declaration**	6		1			1	
2004 **Istanbul Summit Communiqué**	5			1		1	
2005 **NATO Statement**	2						
2006 **Riga Summit Declaration**	10	1	1	4	4	3	
2008 **Bucharest Summit Declaration**	22		5	7	6	2	
2009 **Strasburg Kehl Summit Declaration**	28		8	3	11	2	
2010 **Lisbon Summit Declaration**	15		11	4	10		
2012 **Chicago Summit Declaration**	33		10	3	14	1	
2014 **Wales Summit Declaration**	40	5	19	6	14	2	2
2016 **Warsaw Summit Communiqué**	56	12	23	11	17	8	15
2018 **Brussels Summit Declaration**	51	17	25	4	15	3	8
2021 **Brussels Summit Communiqué**	59	17	25	11	13	9	20
2022 **02 25 NATO Statement**	27						
2022 **03 24 NATO Statement**	16		3	2		2	3
2022 **Madrid Summit Declaration**	10	2	7		3		4
2023 **Vilnius Summit Communiqué**	61	19	28	7	10	15	17
2024 **Washington Summit Declaration**	41	10	10	6	5	6	7
Total 1991-2024	**615**	**83**	**176**	**80**	**122**	**59**	**76**

Table 1. Occurrences of various hybrid warfare related concepts in official NATO Summit Declarations and Communiqués between 1991-2024[16]

[16] The set of official NATO texts from https://www.nato.int/cps/en/natohq/topics_50115.htm

NATO's Russia Challenge

NATO and Russia mutual strategic narratives

After the dissolution of the Soviet Union and the emergence of the Russian Federation as the legal heir of the defunct USSR, Russia has been an important factor on NATO's map of strategic interests, as evidenced in Table 1. At the same time, the process of NATO enlargement has been met by Russia with a very high dose of scepticism and has obviously soured relations between NATO and Moscow. Russia has voiced concerns over the impact on its national security of a greater NATO military presence near its border[17] and Russian policymakers have often argued that, during the 1990 and 1991 discussions on the reunification of Germany, NATO promised not to enlarge to the east.[18]

While the 1997 NATO–Russia Founding Act[19] clearly stated that NATO and Russia do not consider each other as adversaries, Russia–NATO relations have had their ups and downs ever since. Russia's military intervention in Ukraine and its annexation of Crimea in 2014 have led NATO to adopt various countermeasures aimed at improving the security of the alliance, including deployment of NATO troops to areas deemed, for geographical reasons, most exposed to potential Russian aggression. The launching of the full-scale Russian war against Ukraine on February 24, 2022 has resulted in the new set of measures that NATO and other members of the Western community have taken in order to provide political, economic and military support to Ukraine.

As indicated by several political declarations presented by the Alliance over the past decades, Russia's policies have not always been viewed as the main source of threat to the member states and to the Alliance as a whole. The official NATO Declaration of the 2012 Chicago Summit described relations with Russia as being of strategic importance as they contributed to creating a common space of peace, stability and security. NATO also stated the aim to build a lasting and inclusive peace in the Euro-Atlantic area together with Russia, based upon the goals, principles and commitments of the NATO-Russia Founding Act and the Rome Declaration, underlining its wish to see a true strategic partnership between NATO and Russia.[20]

After Russia's annexation of Crimea in 2014, the official NATO tone changed. Wales Summit Declaration described Russia's aggressive actions against Ukraine as having challenged NATO vision of a Europe whole, free, and at peace. The Alliance condemned Russia's escalating military interventions in Ukraine and demanded that Russia stop and withdraw its forces from Ukraine and along the Russian-Ukrainian border. According to NATO's documents, the Russian actions represented the violation of Ukraine's sovereignty and territorial integrity and represented a serious breach of international law and a major challenge to Euro-Atlantic security.[21]

Warsaw Summit Communiqué described Russia's aggressive actions, including provocative military activities at the periphery of NATO territory and its demonstrated willingness to attain political goals by the threat and use of force as a source of regional instability and as a challenge

[17] For a brief account on this debate see Godzimirski, J.M. (2019). Explaining Russian reactions to increased NATO military presence. *NUPI Policy Brief* 16/2019 at https://www.jstor.org/stable/resrep25738

[18] For the best account on this issue see Sarotte, M. E. (2021). *Not One Inch: America, Russia, and the Making of Post-Cold War Stalemate*. Yale University Press.

[19] NATO-Russia Founding Act at https://www.nato.int/cps/en/natohq/official_texts_25468.htm.

[20] NATO 2012 Chicago Summit Declaration at https://www.nato.int/cps/en/natohq/official_texts_87593.htm

[21] NATO 2014 Wales Summit Declaration https://www.nato.int/cps/en/natohq/official_texts_112964.htm

to the Euro-Atlantic security. According to the Warsaw Communiqué, Russia's recent activities and policies reduced stability and security, increased unpredictability, and changed the security environment because they breached the values, principles and commitments which underpin the NATO-Russia relationship, broke the trust at the core of cooperation, and challenged the fundamental principles of the global and Euro-Atlantic security architecture.[22] Similar wording on Russia was repeated in the 2018 Brussels Summit Declaration[23], while the 2021 Brussels Summit Communiqué described Russia's actions as constituting a threat to Euro-Atlantic security.[24]

In a Statement by NATO Heads of State and Government on Russia's attack on Ukraine issued on 25 February 2022, Russia's full-scale invasion of Ukraine was described as the gravest threat to the Euro-Atlantic security in decades. NATO called on Russia to immediately cease its military assault, withdraw all its forces from Ukraine and turn back from the path of aggression. Russia was accused of rejecting the path of diplomacy and dialogue repeatedly offered to it by NATO and Allies and of violating international law, including the UN Charter.[25]

NATO's Madrid Summit Declaration from June 2022 described Russia's war of aggression against Ukraine as gravely undermining international security and stability and as a blatant violation of international law. Russia itself was named as the most significant and direct threat to the Allies' security and to peace and stability in the Euro-Atlantic area.[26]

Vilnius Summit Communiqué issued in July 2023 identified Russia as the most significant and direct threat to Allies' security and to peace and stability in the Euro-Atlantic area.[27] Similar wording can be found in the Washington Summit Declaration issued in July 2024, where Russia is described as the most significant and direct threat to Allies' security and as a country that seeks to fundamentally reconfigure the Euro-Atlantic security architecture, posing a long-term, all-domain threat to NATO. Russia is also described as a country rebuilding and expanding its military capabilities and continuing its airspace violations and provocative activities.[28]

The evolution of Russian approach towards NATO during the post-Cold War period has, to a certain extent, mirrored NATO's approach to Russia. After a relatively short period which is sometimes referred to as a romantic Atlanticist period of Russian foreign policymaking, and which is associated with Andrey Kozyrev at the helm of the Russian Ministry of Foreign Affairs, a more sceptical and interest-based approach to partnership with NATO has become the hallmark of Russian foreign and security policy.[29] Although discussions about Russia's closer and mutually beneficial cooperation with NATO in addressing some of the common challenges have emerged regularly in the Russian debate and some Russian politicians, including President Vladimir Putin, have even aired the idea of Russia joining the alliance[30], the same alliance has been increasingly

[22] NATO 2016 Warsaw Summit Communiqué https://www.nato.int/cps/en/natohq/official_texts_133169.htm
[23] NATO 2018 Brussels Summit Declaration https://www.nato.int/cps/en/natohq/official_texts_156624.htm
[24] 2021 Brussels Summit Communiqué https://www.nato.int/cps/en/natohq/news_185000.htm
[25] Statement by NATO Heads of State and Government on Russia's attack on Ukraine https://www.nato.int/cps/en/natohq/official_texts_192489.htm
[26] 2022 Madrid Summit Declaration at https://www.nato.int/cps/en/natohq/official_texts_196951.htm
[27] 2023 Vilnius Summit Declaration at https://www.nato.int/cps/en/natohq/official_texts_217320.htm
[28] 2024 Washington Summit Declaration at https://www.nato.int/cps/en/natohq/official_texts_227678.htm
[29] For more on this evolution see Rahr, A., & Krause, J. (1995). *Russia's New Foreign Policy* (Vol. 91). Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik, Godzimirski, J. M. (2005). Russia and NATO. Community of values or community of interests? In J. Hedenskog, V. Konnander, B. Nygren, I. Oldberg, & C. Pursiainen (Eds.), *Russia as a Great Power. Dimensions of Russian Security* (pp. 57–80). Routledge, Averre, D. (2006). Russia and NATO since 1991: from Cold War through cold peace to partnership? *International Affairs*, *82*(4), 814–815.
[30] Baker, J. A. (2002). Russia in NATO? *Washington Quarterly*, *25*(1), 95–103. https://doi.org/10.1162/016366002753358348

presented in the Russian official debate as a possible source of strategic threat.[31] NATO has been regularly mentioned in Russian doctrinal documents as shown in Table 2.

Doctrine	NATO mentions (N)
1993 Military Doctrine	0
1993 Foreign Policy Concept	5
1997 National Security Concept	2
2000 National Security Concept	2
2000 Foreign Policy Concept	6
2008 Foreign Policy Concept	6
2009 National Security Strategy until 2020	5
2013 Foreign Policy Concept	6
2014 Military Doctrine	4
2015 National Security Strategy	4
2016 Foreign Policy Concept	4
2021 National Security Strategy	1
2023 Foreign Policy Concept	1

Table 2. NATO mentions in the official Russian doctrines 1993–2016

To begin with, NATO was seen as an important partner in solving security-relevant issues of mutual interest through greater interaction and cooperation (FPC 1993, FPC 2000, FPC 2008). However, Russia made this strategic cooperation dependent on NATO compliance with key clauses of the 1997 Founding Act, particularly those concerning "non-use or threat of force, and non-deployment of conventional armed forces groupings, nuclear weapons and their delivery vehicles in the territories of the new members" (FPC 2000).

Especially in areas where Russian and NATO security interests overlapped and did not collide, cooperation with NATO was deemed important and vital (FPC 1993, FPC 2000). These areas were listed in detail in 2008 FPC, where terrorism, the proliferation of weapons of mass destruction, regional crises, drug trafficking, natural and man-made disasters were defined as common threats to be addressed through political dialogue and practical cooperation. The 2013 FPC added maintaining peace and stability, countering common security threats, such as international terrorism, WMD proliferation, maritime piracy, drug trafficking, and natural and man-made disasters as areas of mutually beneficial cooperation. It also mentioned cooperation between Russia and NATO on solving security problems in Afghanistan as another important area of cooperation.

These doctrinal documents also revealed that Russia remained critical to NATO's plans to expand its area of responsibility, and how this could be detrimental to Russian security and national interests (NSC 1997, NSC 2000, FPC 2000, FPC 2008). FPC 2008 specifically noted deep concern about plans for admitting Georgia and Ukraine as new NATO members.

Another issue about which Russia expressed its concerns was NATO's out-of-area operations, which, according to the Russian interpretation, have contributed to worsening security,

[31] Davydov, Y. (2002). Razshirenie zony otvetstvennosti atlanticheskogo mira. In T. Shakleina (Ed.), *Vneshnaya politika i bezopasnost sovremennoy Rossii 1991-2002* (Vol. 2, pp. 124–141). MGIMO

undermining the existing international order (2000 FPC, 2000 NSC, 2009 NSS, 2021 NSS, 2023 FPC) and to the emergence of new splits and dividing lines in Europe (1997 NSC, 2008 FPC, 2013 FPC, 2016 FPC, 2021 NSS, 2023 FPC) that contradict the idea of indivisible security (2016 FPC). Deep concerns were also voiced in this set of doctrinal documents about the potential presence of NATO military bases and infrastructure close to the Russian borders, especially on the territory of new members (2000 NSC, 2008 FPC, 2009 NSS, 2013 FPC, 2014 MD, 2015 NSS, 2016 FPC).

Similar NATO-related issues are also discussed in more detail in other official statements. In their 2022 article mapping Russian official approaches to NATO, Wilhelmsen and Hjermann examined how NATO was framed in the official Russian discourse between 2014 and 2022. [32] The main conclusion drawn from this examination of the official Russian discourse on NATO during the period preceding the launch of the full-scale invasion of Ukraine was that the Russian discourse is dominated by an understanding of NATO as hostile, deceptive and constantly engaged in waging hybrid warfare against Russia. In a shorter version of their article, the two authors identified six ways in which NATO was framed in a collection of 156 documents produced by the Russian Ministry of Defence and Ministry of Foreign Affairs between 2014 and 2022.[33] The Western world, with NATO as the most important Western institutional actor identified by the official Russian discourse as the source of strategic threat – was presented as: 1) being completely controlled by the Washington DC, whose policies 2) created a world of instability and insecurity, because of 3) the hostile and deceptive nature of the West, that has 4) an extensive toolkit for its hybrid war on Russia in which key role is played by the West's overarching strategy of instigating "colour revolutions". In addition, it was noticed that 5) NATO became increasingly dangerous after 2014 and that 6) NATO's hostile actions were spreading to previously 'cooperative' spaces, for instance to the Arctic.

The evolving patterns of NATO-Russia amity/enmity examined above have been an important factor shaping security space in Europe and in the broader international space. In December 2021, Russia presented two proposals to the USA and NATO on how to address the growing tensions in relations between Russia, the West and Ukraine and how to prevent the outbreak of an open conflict. What Russia sought to achieve by presenting these documents was the effective rollback of NATO to a pre-1997 situation, when NATO-Russia Founding Act was signed, together with legally binding guarantees against any future NATO enlargements. Russia's Western counterparts were willing to discuss various measures to increase the level of trust and security, but rejected what was viewed as Russia's unacceptable ultimatums. On February 21, 2022, Russia recognized the two Donbas "republics", signed agreements on mutual help with them and three days later, on February 24, 2022 launched a full-scale invasion of Ukraine. This action has shaken the fundamentals of the European security architecture and has opened a new chapter in Russia's relations with NATO and the rest of the Western, liberal world.

Russia's strategic and operational objectives and instruments of power

It is our understanding that, when dealing with NATO in the new strategic situation caused by the decision to launch a full-scale invasion of Ukraine, Russia will seek to achieve its long-term

[32] Wilhelmsen, J., & Hjermann, A. R. (2022). Russian Certainty of NATO Hostility: Repercussions in the Arctic. *Arctic Review on Law and Politics*, *13*(0), 114-142. https://doi.org/10.23865/arctic.v13.3378

[33] Wilhelmsen, J., & Hjermann, A. R. (2023). Misplaced Certainty: NATO Hostility as Collective Common Sense Within Russia's Leadership. https://www.e-ir.info/pdf/102878

strategic objectives, as well as some mid-term operational objectives. These long-term strategic and mid-term operational objectives will most likely determine which instruments of power from the Russian power toolbox will be used.

Based on a thorough examination of various studies on Russian foreign and security policy[34], we premise that the long-term strategic goals that the current Kremlin leadership seeks to achieve include: survival and stability of the current regime; Russia's participation as a recognized great power in various systems of alliances and international institutions; replacement of the Western global rules-based order with a new one; stabilization of the country's frontiers as defined by the current regime; unification of territories that the current regime defines as belonging to the Russian world ("russkiy mir"); creation of favourable conditions for economic growth of the country, preferably through a closer cooperation with some friendly regimes.

However, in order to be able to achieve these strategic objectives, Russia must be able to achieve what could be understood as mid-term operational objectives. In our understanding, these 2024 and possibly 2025 operational NATO-relevant objectives include: winning the war in Ukraine; splitting the West so as to stop its support to Ukraine; intimidating the West; weakening trust among members of the Western community; undermining trust between people and political elites in Western societies.

Russia has various instruments of power at its disposal when trying to achieve such objectives. These instruments of power can be used not only when Russia pursues its interests in a legitimate manner, but also when it launches various types of hybrid operations against those defined by the current regime as "unfriendly actors". For instance, military instruments of power are employed in kinetic operations in Ukraine, but other non-kinetic instruments of power are used, too. These include diplomatic, political, and informational instruments of power, together with economic and financial ones. They can be combined and bundled together to achieve strategic and operational objectives without engaging in open warfare, which is the main feature of hybrid and political warfare.

Diplomatic instruments can be used in various ways in international and bilateral relations not only to advance the Russian interests in legitimate ways, but also to undermine international norms and agreements. In the case of Russia's relations with NATO, these instruments can be used to undermine transatlantic cooperation, sow discord among the members of the alliance and strengthen isolationist trends in the USA, hoping that this could result in the US withdrawal from Europe, and hence in the automatic strengthening of Russia's hand in this strategically important region. Some examples of how diplomacy is be used in Russian hybrid warfare to sow discord are various statements on NATO policy made by Maria Zakharova, the head of the information department of the Russian MFA, or the role played by Permanent Representative of Russia to the United Nations Ambassador Vasily Nebenzia. Russia's overt and covert political support for various fringe political groups, the attempt to influence and interfere with political processes, the

[34] Black, C. C. (1962). The Pattern of Russian Objectives. In I. Lederer (Ed.), *Russian Foreign Policy. Essays in Historical Perspective* (pp. 3–38). Yale University Press, Light, M. (2015). Russian Foreign Policy Themes in Official Documents and Speeches: Tracing Continuity and Change. In D. Cadier & M. Light (Eds.), *Russia's Foreign Policy Ideas, Domestic Politics and External Relations* (pp. 13–29). Palgrave Macmillan, Radin, A., & Reach, C. B. (2017). *Russian Views of the International Order* RAND Corporation, Stent, A. (2018). What Drives Russian Foreign Policy? In J. R. Deni (Ed.), *Current Russia Military Affairs: Assessing and Countering Russian Strategy, Operational Planning, and Modernization* (pp. 6-9). U.S. Army War College.

exploitation of societal divisions can undermine social and political cohesion, public trust and the functioning of institutions in targeted countries, which would in turn help Russia achieve some of its stated and not-stated operational and strategic objectives in relation to NATO and to the world at large.

Hybrid information warfare includes the spread of propaganda and disinformation to undermine the social cohesion of targeted nations, influence public opinion and political outcomes. These efforts are mentioned in official NATO statements as posing a direct threat to the security of the Allies. In addition to traditional propaganda and disinformation operations, Russia has been engaging in other types of information-related actions, such as hostile Influence operations, electoral and political interference, weaponization of history, as exemplified by an article authored by President Vladimir Putin in 2021[35] that presented a false, misleading version of the history of Russian-Ukrainian relations. The hybrid information-related repertoire has been updated to include advertising intelligence, malvertising, algorithmic warfare, data and information harvesting. It is important to underline that Russian hybrid operations in the information space benefit from the weaponization of a hyper-connected transnational information ecosystem in which various types of Russian and pro-Russian actors can freely operate. Russia has also put in place its own information and media infrastructure (with pillars such as RT or Sputnik), that is actively used to spread pro-Russian and anti-Western narratives, and to counter what the official Russian discourse labels as the West's Russophobia. Such media channels are often used to fuel anti-American, anti-NATO and anti-Ukrainian sentiments in the targeted NATO countries, which can help Russia achieve several of its strategic and operational objectives simultaneously. A potent instrument in Russia's hybrid information warfare is the use of the information technologies and media ecosystem to promote Russia's official narratives, such as "the peaceful Russia vs the war-mongering West'; "the malfunctioning Western world order"; "the rigged international system dominated by the West and NATO"; "the West against the rest"; "Russia as the leading force in the fight for a multipolar system, helping other countries to liberate from neo-colonial and unfair rule", "the victimhood play card against minorities of all kind and migrants".

A separate and important issue related at least partly to Russian hybrid and information warfare, which attracts a lot of attention from NATO are Russia's cyber operations targeting critical infrastructure, government systems, and key industries with the purpose to create disruption, panic and chaos. This may serve an important operational Russian objective, namely undermining the trust between citizens and a political leadership facing difficulties in delivering important public goods and basic societal services. Cyber-attacks can also reveal gaps and vulnerabilities in national resilience, which could also have negative impact on the societal cohesion in targeted countries.

Russia has also actively used what could be termed military instruments or political violence to achieve its objectives without having to resort to kinetic warfare. The appearance of "little green men" in Crimea in 2014 is a very good example of how military instruments of power can be used to achieve objectives. Also, the well documented attempts at lives of the prominent critics of the Russian regime, or other actors defined by the Russian regime as enemies of Russia in which violent means were used could fall under this category. The best-known examples of this type of operations conducted against actors on NATO countries' territories are the murder of Aleksander Litvinenko in London, the use of Novichok against Sergei Skripal in Salisbury or the killing of one of the former leaders of the Chechen resistance in Berlin. These acts of political violence below

[35] Putin, V. (2021). Meeting with permanent members of the Security Council. President of Russia. http://en.kremlin.ru/events/president/news/66181

the war threshold are good examples of Russia's use of violent means in the pursuit of its operational and strategic objectives. A specific and relatively innovative solution in Russian hybrid warfare in the current context is the use by Russia of various types of proxies. The use of the private security company Wagner, but also support provided to various non-state actors, insurgents, or paramilitary forces aiming at destabilizing regions in which Western countries has strategic interests is a good example of the use of these unconventional solutions. In one of his recent speeches, President Vladimir Putin warned the West, including NATO, that Russia could consider supplying some advanced weapons systems to actors and countries that could be interested in aiming these weapons at targets in the Western liberal world.

Finally, Russia demonstrated willingness and relatively limited ability to use some elements of economic pressure against NATO countries, even before the outbreak of the full-scale war in Ukraine in February 2022. For instance, Russia decided to cut its gas supplies to Europe before going to war in Ukraine to create and fuel economic and political tensions in Europe, including in the European NATO member states. This energy supply manipulation was meant not only to limit access to these crucial commodities in NATO and non-NATO Europe, but were also to generate extra revenues to the Russian state on the eve of the war. An additional strategic benefit was the creation of political, economic and social tensions in countries that were forced to pay very high energy bills or were expected to face energy shortages. Russia also expected that the very high level of energy dependence on Russia in the key NATO countries, such as Germany, could make them more reluctant to provide support to Ukraine or endorse various types of sanctions against Russia.

Mapping NATO members' Russia-related exposure: NATO-Russia power audit 2024

To understand how Russia can use various instruments of power from its political warfare repertoire towards NATO members, it is crucial to map how Russian perceptions of these countries have evolved over the past decades. To map this evolution of mutual perceptions we will now present some snapshot pictures of how these relations were viewed at various stages in the development of relations between Russia and the Western world, paying specific attention to Russia's relations with the growing number of NATO members. We will start by examining a 2007 ECFR study mapping relations between Russia and EU members states some years before the outbreak of the conflict in Ukraine and Russia's illegal annexation of Crimea.[36]

After having conducted a detailed examination of relations between EU member states and Russia the 2007 ECFR study divided EU member states into five categories. Cyprus and Greece were labelled **Trojan Horses**, as they often defended Russian interests in the EU system and were willing to veto common EU positions. France, Germany, Italy and Spain were labelled **Strategic Partners**, as they enjoyed a "special relationship" with Russia which, on various occasions, contributed to undermining common EU policies. Austria, Belgium, Bulgaria, Finland, Hungary, Luxembourg, Malta, Portugal, Slovakia and Slovenia were described as **Friendly Pragmatists**, as they maintained a close relationship with Russia and tended to put their business interests above political goals. Czech Republic, Denmark, Estonia, Ireland, Latvia, the Netherlands, Romania, Sweden and the United Kingdom were labelled **Frosty Pragmatists**, because they focused on

[36] Leonard, M., & Popescu, N. (2007). A Power Audit of EU-Russia Relations. In *ECFR Policy Paper*. European Council on Foreign Relations at https://ecfr.eu/wp-content/uploads/ECFR-02_A_POWER_AUDIT_OF_EU-RUSSIA_RELATIONS.pdf

business interests, but were less afraid than others to speak out against Russian behaviour on human rights or other issues. Finally, Lithuania and Poland were described as **New Cold Warriors**, because they had developed an overtly hostile relationship with Moscow and were willing to use the veto to block EU negotiations on various issues with Russia.[37]

Next, we present how the picture changed in the aftermath of the Russian incursion in Ukraine in 2014 and the growing tensions in relations between Russia and the Western world by examining the results of a study conducted in 2018 by Kadri Liik mapping the diverse perceptions of Russia in the EU member states four years after Russia's illegal annexation of Crimea and four years before the Russian full-scale invasion of Ukraine in February 2022.[38] Here we will pay special attention to where Russia placed various EU members states on the amity-enmity scale. This will be followed by a brief examination of how the official Russian discourse views NATO member states by looking at the list of unfriendly states published by the Russian authorities after the outbreak of the war in 2022.[39] All NATO countries are classified by Russia as unfriendly, no matter how relations between them and Russia had developed prior to the outbreak of the full-scale war in 2022. This means that in 2023 all NATO countries were most probably viewed by Moscow as belonging to the category of Cold Warriors, if we were to use the classification from the 2007 study, although some of them, like Hungary and, more recently Slovakia, could be viewed as being less "Russophobe" than others. Finally, we present some survey data on the willingness of population in all NATO countries to provide support to Ukraine as revealed in two surveys conducted by NATO in 2023 on the eve of the Vilnius Summit and towards the end of 2023.[40] In both surveys, the citizens in all NATO countries and in Sweden were asked whether their country should continue to provide support to Ukraine. In our overview we decided to aggregate negative answers of those who said that they somewhat disagree or strongly disagree with the idea of their country continuing to provide support to Ukraine as these represent what could be labelled a negative approach towards providing help to Ukraine, which would be in line with one of the key operational objectives pursued by Russia.

These survey data are used to measure the level of support for providing help to Ukraine in all NATO countries and map how this level of support has changed in this period. We argue that the results of these surveys can reveal some important vulnerabilities and can be used by the Russian policymakers to design and implement some hybrid operations in the information space targeting the countries where the population is most reluctant to providing support to Ukraine. Since winning the war in Ukraine is undoubtedly the most important operational objective currently pursued by the Russian regime and the Western support to Ukraine is one of the main reasons why Russia has not been able to achieve it, it is natural to assume that Russia is very interested in exploiting and strengthening existing gaps in NATO countries to make the Alliance stop its political, economic and military support to Ukraine. The results of this mapping exercise are presented in Table 3. The countries are listed in descending order, with those whose citizens were the most critical towards providing support to Ukraine at the top. In addition, we present the

[37] Leonard and Popescu N. (2007). A Power Audit of EU-Russia Relations. In *ECFR Policy Paper*. European Council on Foreign Relations at https://ecfr.eu/wp-content/uploads/ECFR-02_A_POWER_AUDIT_OF_EU-RUSSIA_RELATIONS.pdf

[38] Liik, K. (2018). Winning The Normative War With Russia An Eu-Russia Power Audit, *ECFR* at https://ecfr.eu/wp-content/uploads/EU-RUSSIA_POWER_AUDIT.pdf

[39] Ryumin,A. TASS. (2022). Kakiye strany vkhodyat v spisok nedruzhestvennykh Rossii stran at https://tass.ru/info/18435143

[40] The surveys can be accessed at: NATO Audience Research: pre-Summit polling results 2023 at https://www.nato.int/nato_static_fl2014/assets/pdf/2023/7/pdf/2300707-pre-summit-research-2023.pdf and NATO Annual Tracking Research 2023 at https://www.nato.int/nato_static_fl2014/assets/pdf/2024/3/pdf/240314-annual-tracking-2023-en.pdf

recent trends by mapping in the last column of the table how the opinion in the countries in question changed between the two NATO surveys conducted in 2023.

We argue that countries in which citizens are most critical to providing support to Ukraine as well as those in which there is a clear negative trend, meaning that the number of those who disagree with the idea of providing support to Ukraine has grown substantially in the period between the two surveys, are the most exposed to Russia's hostile operations aiming at disrupting the intra-NATO unity and the Allies support to Ukraine. Czechia, Hungary, Bulgaria, Greece, North Macedonia, Slovenia, Slovakia and Montenegro are the countries in which more than 40 percent of citizens surveyed were sceptical towards providing support to Ukraine. In Germany the level of scepticism was relatively high, too, as 39 percent of respondents expressed negative views on the idea of providing continued support to Ukraine. All in all, the level of scepticism was higher than the NATO average in 15 NATO countries.

NATO Member 2024	2007 Category ECFR Power Audit	2018 Russia treats as relatively friendly	2018 Russi treats as other EU but cultivates as possible friends	2018 Russia treats as unfriendly but cultivates	2018 Russia treats as unfriendly	2023 Official Russian list of unfriendly states	Share against support for Ukraine pre-Vilnius survey	Share against support for Ukraine 2023 NATO Tracking	Change 2023 pre vilnius vs NATO Tracker	Category 2024
Czechia	FrostyPragmatist					x	42	51	9	NewColdWarrior
Hungary	FriendlyPragmatist	x				x	37	50	13	TrojanHorse
Bulgaria	FriendlyPragmatist			x		x	57	50	-7	NewColdWarrior
Greece	TrojanHorse		x			x	47	48	1	NewColdWarrior
North Macedonia	?					x	39	47	8	NewColdWarrior
Slovenia	FriendlyPragmatist					x	40	46	6	NewColdWarrior
Slovakia	FriendlyPragmatist		x			x	48	45	-3	FriendlyPragmatist
Montenegro	?					x	57	44	-13	NewColdWarrior
Germany	StrategicPartners					x	34	39	5	NewColdWarrior
Belgium	FriendlyPragmatist			x		x	30	32	2	NewColdWarrior
Romania	FrostyPragmatist				x	x	36	32	-4	NewColdWarrior
Italy	StrategicPartners	x				x	33	31	-2	NewColdWarrior
Turkiye	?					x	19	30	11	NewColdWarrior
Croatia	?					x	23	29	6	NewColdWarrior
France	StrategicPartners		x			x	28	29	1	NewColdWarrior
NATO Whole	New Cold Warrior				x	x	26	28	2	NewColdWarrior
Estonia	FrostyPragmatist				x	x	19	26	7	NewColdWarrior
Latvia	FrostyPragmatist			x		x	21	26	5	NewColdWarrior
Netherlands	FrostyPragmatist				x	x	23	26	3	NewColdWarrior
Poland	NewColdWarrior				x	x	23	26	3	NewColdWarrior
Luxembourg	FriendlyPragmatist		x			x	19	23	4	NewColdWarrior
Canada	?					x	18	22	4	NewColdWarrior
United States						x	25	19	-6	NewColdWarrior
Lithuania	NewColdWarrior				x	x	16	18	2	NewColdWarrior
Denmark	FrostyPragmatist					x	16	17	1	NewColdWarrior
Spain	StrategicPartners		x			x	18	17	-1	NewColdWarrior
Sweden	FrostyPragmatist				x	x	17	15	-2	NewColdWarrior
Norway	FriendlyPragmatist					x	16	14	-2	NewColdWarrior
Portugal	FriendlyPragmatist		x			x	11	13	2	NewColdWarrior
United Kingdom	FrostyPragmatist				x	x	15	13	-2	NewColdWarrior
Finland	FriendlyPragmatist		x			x	9	12	3	NewColdWarrior
Iceland	?					x	7	9	2	NewColdWarrior
Albania	?					x	18	9	-9	NewColdWarrior

Table 3. Russia-NATO Power Audit. 2007-2024 evolution

What has NATO done to deal with the challenge of Russian hybrid warfare?

Faced with the very real challenge of the Russian hybrid activity, NATO has been compelled to develop a set of measures to deal with this relatively new situation that emerged after the annexation of Crimea in 2014 and became even more critical after 2022. What NATO has been doing to cope with the new hybrid reality was to a very large extent in line with what other actors facing similar challenge have been doing over the past years.[41] This approach to hybrid warfare has been based on a combination of diplomatic, military, economic, and informational strategies.

NATO's approach to countering Russian hybrid warfare has been multidimensional and has involved a combination of strategic, operational, and tactical measures. At the strategic level, NATO emphasizes the importance of resilience and preparedness among its member states. This involves strengthening the defence capabilities of member nations, enhancing intelligence-sharing mechanisms, and promoting civil preparedness against a broad spectrum of threats. NATO also works on improving its cyber defence to protect against cyber-attacks and to counter disinformation campaigns effectively.

At the operational level, NATO has been adapting its military capabilities to be more agile and responsive to hybrid threats. This included the development of rapid deployment forces, such as the Very High Readiness Joint Task Force (VJTF) and regular exercises to simulate hybrid warfare scenarios, ensuring that Allies are trained to recognize and counter such threats.

At the tactical level, NATO employs a range of counter-hybrid support teams that can be dispatched to assist member states in the event of hybrid attacks. These teams are composed of experts in various fields, including cyber security, strategic communications, and counter-intelligence, providing targeted support where it is most needed.

As clearly demonstrated in our examination of the occurrences of the key hybrid warfare related concepts in NATO's key official statements, strengthening **cyber defences** has been the top priority. NATO and member states have introduced various types of measures to improve protection of their cyber infrastructure by investing in advanced cybersecurity measures, establishing rapid response teams, and promoting public-private partnerships to safeguard security of critical digitized sectors. For instance, Estonia has been at the forefront of cyber defence since the 2007 cyberattacks launched by Russia. The country established the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, which has become an important NATO hub for cyber defence research and training. Cyber defence is a critical component of NATO's response. The alliance has declared cyberspace as a domain of operations, and member states

[41] For more on this see Calha, J. M. (2015). *Hybrid Warfare: NATO's New Strategic Challenge?* NATO Parliamentary Assembly. https://www.nato-pa.int/sites/default/files/documents/2015%7C-%7C166%7CDSC%7C15%7CE%7CBIS%7C-%7CHYBRID%7CWARFARE%7C-%7CCALHA%7CREPORT.docx CIDOB. (2022). How democracies can overcome the challenges of hybrid warfare and disinformation? At https://www.cidob.org/en/publication/how-democracies-can-overcome-challenges-hybrid-warfare-and-disinformation. See also Rühle, M. (2021). NATO's Unified Response to Hybrid Threats at https://cepa.org/article/natos-unified-response-to-hybrid-threats/, Sweijs, T. (2022). Between War and Peace: 'Hybrid Threats' and NATO's Strategic Concept at https://hcss.nl/wp-content/uploads/2022/06/Between-War-and-Peace-HCSS-2022-V2.pdf and Lasconjarias, G., & Larsen, J. A. (2015). *NATO's response to hybrid threats*. NATO Defence College. http://www.ndc.nato.int/download/downloads.php?icode=471.

are committed to enhancing their cyber defence capabilities. This includes sharing best practices, improving cyber incident response, and conducting cyber defence exercises.

By increasing the level of protection of critical digital infrastructure against any hostile hybrid operations, authorities in NATO countries aim at **strengthening national economic and societal resilience**, too. These resilience-related measures are designed to reduce their vulnerability to economic coercion by diversifying energy sources, implementing anti-corruption measures, enhancing the resilience of their financial systems and reducing risks related to possible disruptions in value chains and access to crucial services. There are several examples of how NATO countries managed to cope with this type of challenges. Lithuania, Poland, Finland and Germany have reduced their energy dependence on Russia by constructing several LNG terminals, diversifying their energy sources, strengthening their energy security and increasing the level of economic and societal resilience. In response to the Russian war in Ukraine and Russian hybrid operations, the European Union has imposed economic sanctions on Russia, targeting its financial, energy, and defence sectors. In addition, NATO member states are encouraged to strengthen their national resilience as part of collective defence and to share their best national practices with other partners.

To be able to deal with the growing challenge of hybrid warfare originating from Russia, the Alliance and member states decided also to **enhance intelligence capabilities** that help them to detect and counter hybrid threats and identify the culprits, addressing the difficult question of attribution. The measures introduced in this area included intelligence sharing among allies and the establishment of dedicated units for analyzing hybrid warfare tactics and operations. All NATO members have bolstered their intelligence and counterintelligence operations to detect and disrupt Russian hybrid activities, including espionage and covert influence operations and get a better understanding of the key drivers of Russian aggressive policy.

Since information space is one of the main battlefields of the Russian hybrid war, it was also important to introduce various types of **information countermeasures**. These efforts included the creation of strategic communication units, implementation of media literacy campaigns and fact-checking initiatives to ensure that the public has access to accurate information. For instance, Finland has introduced various measures to tackle Russian disinformation campaigns through its comprehensive approach to strategic communication. The Finnish government has worked closely with media and educational institutions to enhance public awareness and resilience against disinformation. To tackle disinformation, NATO emphasizes the importance of strategic communication and works to expose and counter false narratives by providing timely and accurate information. Initiatives such as the NATO Strategic Communications Centre of Excellence (StratCom COE) play a crucial role in understanding and responding to disinformation campaigns.

This new situation also required some adjustments to be made in **the national and international legal and regulatory framework**, with new laws being introduced to cope with possible foreign interference and hostile operations. Some legal measures related to money laundering, political lobbying by foreign entities, and the spread of false information have been introduced in response to increased levels of hostile activities. For instance, the UK enacted the “Magnitsky Amendment”, allowing the government to impose sanctions on individuals involved in gross human rights abuses, including those using hybrid warfare tactics. At the same time, various types of bans on spreading and amplifying Russian messaging through Russian channels in several NATO countries were introduced in order to limit Russia’s ability to influence public opinion. Confronted with Russian and Belarusian hybrid operations at the borders when the two regimes allowed high

numbers of migrants from the Middle East to reach the borders of Lithuania, Poland and Finland, the authorities in these countries introduced special laws and regulations to seal the borders, while deciding at the same time to build new infrastructure that makes illegal border crossings more difficult. In addition, NATO seeks to strengthen legal and normative frameworks to address hybrid warfare and supports international efforts to develop norms of responsible state behaviour in cyberspace and other exposed domains.

Various measures related to increasing the level of **public awareness and civil society engagement** in dealing with hybrid warfare have been introduced to increase the level of national resilience under the new circumstances. One element of this approach is an increased level of collaboration between the government and the private sector, particularly in critical infrastructure sectors, to protect against cyberattacks and other hybrid threats.

Some countries have also adopted policies of **strategic deterrence**, signalling a willingness to respond to hybrid aggression with a range of punitive measures. Maybe the best known example of this type of signalling was President Joe Biden's message to his Russian counterpart during their meeting in Genève in June 2021, when the American President gave the Russian President Vladimir Putin a list of 16 critical infrastructure sectors, from energy to water, that should not be the subject of malicious cyber activity and warned that any action against these sectors will be met with a massive US punitive action in the cyberspace. [42]

Diplomatic channels are also used to address hybrid threats, with the introduction of various types of sanctions against actors involved in this type of activity, combined with diplomatic isolation. The same diplomatic channels are also used to uphold international law and norms, to build a consensus against the use of hybrid warfare tactics as well as to develop new forms of international cooperation better suited to address the hybrid challenge.

International cooperation among like-minded countries has also played a role in dealing with the Russian hybrid challenge. Cooperation within NATO and between NATO and the EU have played a crucial role in this context.[43] The key measures were developing joint strategies, conducting joint exercises, and providing support to member states targeted by hybrid tactics, all of them being mentioned in the official NATO statements issued after 2014. The European Union Agency for Law Enforcement Cooperation (Europol) has enhanced its efforts to combat hybrid threats, including cybercrime and terrorism, through increased collaboration with member states. In addition, the EU decided to establish The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki, a move that was welcomed by NATO as an important contribution to dealing with a common NATO and EU challenge.[44]

Finally, when all these above-mentioned measures are not sufficient to address hybrid warfare related challenges, **military instruments** can also play a role in order to deal with this threat. Among other things, this has led to the restructuring of armed forces, introducing special units or new branches to deal with the challenge, raising questions related to rapid deployment, special operations, and unconventional warfare capabilities. For instance, in response to the annexation of Crimea in 2014 and increased Russian use of hybrid instruments, NATO has increased its

[42] Cyberscoop. (2021). Biden says he gave Putin list of 16 sectors that should be off-limits to hacking at https://cyberscoop.com/biden-putin-summit-russia-geneva/

[43] For more of that, see European Parliament. (2017). Countering hybrid threats: EU-NATO cooperation at http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf.

[44] For more on this see EU and NATO welcome Hybrid CoE at https://www.hybridcoe.fi/news/eu-and-nato-welcome-hybrid-coe/

presence in Eastern Europe through the Enhanced Forward Presence, deploying multinational battle groups in the Baltic States and Poland to deter potential Russian aggression and reassure allies. This and other measures such as creation of the Very High Readiness Joint Task Force (VJTF) has enhanced NATO's military capabilities making the alliance more capable to respond to any signs of aggression, including hybrid threats. These forces conduct regular exercises to ensure that they are well-prepared to recognize and counter hybrid warfare tactics. Another element of NATO's strategy towards hybrid threats is the clear warning to potential hybrid wrongdoers that, in response to hybrid operations that reach a certain threshold, NATO may consider invoking Article 5, according to which an attack on one member is an attack on all. This demonstrates the Alliance's readiness to collectively address hybrid threats as seriously as conventional ones and creates, at the same time, a situation of strategic ambiguity for the potential attacker who will have to take this into consideration when planning to launch a hybrid attack on a NATO member.

NATO's response to Russian hybrid warfare can be therefore described as comprehensive, involving collective defence measures, enhanced readiness, and the integration of both military and non-military means to deter and defend against it. The alliance continues to evolve its strategies to address the dynamic nature of hybrid warfare, to ensure the security of its member states and to adapt its strategies to an ever changing environment.

How have Norway and Romania dealt with the hybrid challenge?

The case of Norway

Norway's strategy to counter Russian hybrid warfare is rooted in a combination of national defence measures, regional cooperation, and active participation in NATO initiatives. As a country with a strong Arctic identity and a strategic location in the High North, Norway has had to adapt its defence and security policy to address the evolving nature of threats, particularly following the increased tensions post-2014 and even more so post-2022.

Strengthening national defence

At the national level, Norway has decided to invest in strengthening its military capabilities, particularly in the Arctic region. On 4 June 2024 a political consensus was reached in Oslo and a unanimous Storting voted in favour of the proposal on the long-term plan for the Armed Forces. The government presented its proposal for a long-term plan in April. They proposed spending a total of NOK 1,624 billion on Defence until 2036. Over the twelve-year period, there was an increase of NOK 600 billion extra, compared to last year's budget. The settlement on 4 June 2024 involves an increase of NOK 11 billion on top of this. An important decision was also made on the acquisition of one more long-range air defence system to protect Eastern Norway and the central capital area. It is also planned to increase the number of submarines to be delivered to the Norwegian Navy from five to six. The document also called for development of an overall drone strategy. This document signals also increased interest in enhancing surveillance and intelligence capabilities to detect and respond to hybrid threats promptly. Also questions related to protection of critical infrastructure, such as energy facilities, from potential hybrid attacks, including cyber threats and sabotage have received more attention in the official Norwegian policy.

Strengthening national cyber capabilities

Following most NATO countries and recognizing the significance of the cyber domain in hybrid warfare, Norway has bolstered its cyber defence systems and capabilities. It also works closely with NATO and other international partners to share intelligence and best practices in cyber security. The National Cyber Security Center is a department of the National Security Authority. Its main responsibility is to identify, develop and coordinate effective measures in the area of cybersecurity, prevent serious digital attacks and be a national hub for coordination of policies and measures related to cybersecurity. The NCSC was established in 2018 and opened on 1 November 2019. Additionally, Norway is involved in efforts to counter disinformation by promoting media literacy and supporting independent journalism and sharing its experience in this field with other NATO countries. An important role in this work is played by independent media that have developed a Code of Ethics of the Norwegian Press providing national professional guidelines for media activity.[45]

Improving and adjusting national governance

In response to changes in the international environment, changes in technology and the need to improve national governance in the field of security, Norway also introduced a new Law on Security on 1 January 2019. This new law makes Norway better prepared to address challenges related to possible hybrid operations against the country and aims at improving the effectiveness of the system of protection of critical infrastructure that could be exposed to cyberattacks and sabotage. Especially after the sabotage against Nord Stream pipelines in September 2022, the question of protection of the Norwegian and international energy infrastructure has received more attention. For instance, in April 2024 Norway and five other countries from the North Sea region signed an agreement on cooperation in the protection of the critical infrastructure in the region.[46] Norway has also implemented almost all EU regulations on the protection of critical infrastructure, which makes it easier to work together with other EU and NATO member states on finding common solutions to the common challenge of Russian hybrid warfare. Implementation of EU regulations on the protection of critical infrastructure creates a common regulatory framework and facilitates the design and implementation of common solutions increasing national economic and societal resilience.

Focus on national and societal preparedness and resilience

The Norwegian government also emphasizes the importance of civil preparedness and societal resilience. This includes educating the public about hybrid threats and ensuring that national infrastructure is resilient against a range of disruptions, from cyberattacks to misinformation. Since the outbreak of the full-scale war in Ukraine, and learning from the Ukrainian experience, Norwegian authorities have reminded citizens several times about what they need to be able to cope with a man-made or natural crisis. The Norwegian Directorate for Civil Protection (DSB) has launched several campaigns to increase the level of public awareness on how to deal with the resilience related issues and how to prepare to meet a possible crisis.[47] A special website with information in both Norwegian and English was made available and provides information on practical aspects of civil preparedness.[48]

---

[45] See https://presse.no/pfu/etiske-regler/vaer-varsom-plakaten/vvpl-engelsk/

[46] https://www.nrk.no/rogaland/signerer-sikkerheitspakt-for-nordsjoen_-_-saman-er-me-sterkare-1.16836118

[47] DSB. (2024). Du er en del av Norges beredskap at https://www.dsb.no/globalassets/dokumenter/egenberedskap/dsb_beredskap_brosjyre_original.pdf

[48] For more on that in English see https://www.sikkerhverdag.no/en/.

Strengthening international cooperation

Confronted with an increasingly provocative and aggressive Russian policy, Norway has decided to pay more attention to deterrence related solutions and less to questions related to assurance-related aspects in its policy towards Russia. There are still attempts at keeping at least some communication lines open with Russia to avoid accidental escalation, but there is much more focus on Norway's relations with NATO allies and on building strong relationship with the USA. As a NATO member, Norway actively participates in the alliance's collective defence measures against hybrid warfare, by contributing, among other things, to NATO's Enhanced Forward Presence (EFP) and participating in joint exercises designed to improve interoperability and readiness against hybrid tactics. Norway supports NATO's containment-plus policy, which involves a combination of military presence and diplomatic efforts to deter Russian aggression. This policy is evident in Norway's commitment to maintaining a robust defence posture in the Arctic.

Policy relevant research on hybrid warfare

Having in mind specific features of Norwegian society and the country' relatively high level of exposure to Russian hybrid operations, it was also important to generate new policy relevant knowledge on how Norway should prepare to deal with the hybrid challenge. In 2018, the Norwegian Defense Research Establishment (FFI) published a report summing up the findings of a project on the role of hybrid operations in the future conflict.[49] This report studied the possibility of hybrid warfare as a prelude to, or as an integrated part of, a future inter-state and low-intensity conflict in Europe. The reason for this is the increasing frequency of both kinetic and non-kinetic irregular means in armed conflicts everywhere, relative to conventional military force. The report was premised on the idea that that such means will be an important part of any future conflict between Norway and a foreign power. It paid special attention to the impact that the development of information and communication technology over the past 20 years has had on the non-kinetic hybrid warfare. It also examined how other factors contribute to changing the situation and what consequences this may have for the future hybrid operations against Norway.

Another FFI report published in 2021[50] dealt with the question of how hybrid operations may challenge our ability to have a good situational awareness, which is a precondition for making sound and timely decisions. This report presented an interesting operational definition of hybrid warfare as "the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects" and provided highly relevant policy suggestions and recommendations on how to improve the ability to obtain situational awareness when dealing with hybrid threats.

In 2022 FFI published a new report on what Norway can learn from other countries that must deal with the challenge posed by hybrid warfare.[51] The main idea behind this study was to consider what Norway can learn from Finland, Sweden, Estonia, the United Kingdom, the Netherlands and

---

[49] Diesen, S. (2018). Lavintensivt hybridangrep på Norge i en fremtidig konflikt (A low intensity hybrid attack on Norway ina future conflict). FFI Report 18000/80 at https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/2152/18-00080.pdf

[50] Malerud, A., Hennum, Ch., and Toverød, N. (2012). Situasjonsforståelse ved sammensatte trusler - et konseptgrunnlag (Situation awareness encountering hybrid threats – a conceptual basis)., *FFF Report* 21/00246 at https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/2833/00246.pdf

[51] Berghaust, J.C., Skjei, F. and Sellevåg, S.R. (2022). Hva kan Norge lære av andre lands tilnærming til sammensatte trusler? – rapport til Forsvarskommisjonen (What can Norway learn from other states' approach to hybrid threats? – A report to the Norwegian Defence Commission), *FFI Report* 22/02310 at https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3088/22-02310.pdf

Australia regarding how they work to deter, detect and respond to hybrid threats. The report shed light on suggested best practices in NATO and the EU, and how the different states have tackled the issue. Based on the suggested best practices and the states' approaches, five key recommendations regarding what Norway can learn to strengthen the ability to counter hybrid threats were formulated. The study concluded that, in order to have a good situational awareness, it was important to have a good understanding of concepts and terms. In addition, the study suggested that approaches to hybrid warfare should be synchronized, systematic and customized. Questions of how to strengthen and organize the Norwegian government's situational awareness, how the Norwegian intelligence and security services could be strengthened, and whether today's structure for domestic and foreign intelligence should be modified were considered important, too. The report considered how to strengthen resilience of the Norwegian democracy, of the critical infrastructure and of the population and how to organize modern psychological defense in the country. Questions related to changes in the legal framework were also considered. Finally, the report proposed a cautious approach to the idea of giving the Norwegian Armed Forces responsibilities related to countering hybrid threats, because their most important task is to maintain the military capacity for deterrence, contribute to situational awareness and assist civilian authorities with maintaining societal security.

Norway's approach to dealing with Russian hybrid warfare is characterized by a proactive stance in national defence, a commitment to regional stability through cooperation, and active engagement in NATO's development of a collective approach to this common challenge. Facing a rapidly changing and fluctuating situation, Norway continues to adjust its strategies, ensuring that it remains prepared to defend its sovereignty and contribute to regional and international security. Finally, what needs to be factored in in the Norwegian strategic calculations is that the international environment in which the Norwegian policy is shaped and implemented, has changed dramatically after Finland and Sweden joined NATO.

The case of Romania

As observed in various European nations, Russian political warfare typically involves a blend of cyberattacks, dissemination of false information, economic manoeuvring, and the creation and amplification of political and societal rifts. As emphasized by Peter Pomerantsev and Michael Weiss, the Kremlin is capable of employing diverse strategies in different states within what they term as a "non-linear internationale". The objective is to undermine opponents internally, thus fostering internal discord that obstructs cohesive reactions to Russian activities. From such a perspective, Romania has been exposed to various aspects of this new type of warfare.

Compared to some of its neighbours, Romania is less susceptible to some historical, political, economic, or linguistic factors. In the case of Bulgaria, for example, Moscow frequently exploits the common religious and cultural heritage to cultivate pro-Russian attitudes. Many Bulgarians express a sense of historical kinship with Russia owing to their shared Slavic origins and Orthodox Christian beliefs. This influence manifests itself in the Bulgarian media and political discussions, portraying pro-Russian narratives as defenders of traditional values in opposition to Western liberalism. Russian economic interests often intersect with local oligarchic networks. Notably, the Bulgarian energy sector, particularly the gas industry, has experienced substantial Russian investments and influence. Moving on to the Republic of Moldova, the separatist region of Transnistria, where Russian is predominantly spoken and which receives significant support from Russia, remains a pivotal source of tension. Moscow upholds a military presence in the region, backing separatist forces and utilizing it as a bargaining chip against Moldova's aspirations for closer integration with the EU and NATO. Additionally, Moldova grapples with deep divisions

between pro-European Union and pro-Russian factions, with corruption scandals further widening this rift.

Romania appears to be distant from being significantly impacted by Russia's political warfare arsenal, as evidenced by a GLOBSEC Trends report for 2024[52]. From a political standpoint, 83% of Romanians continue to endorse their nation's EU membership, 71% support the establishment of an EU Army to reduce reliance on the US military (the highest percentage among CEE states), 88% back Romania's NATO membership, and 78% believe that this affiliation decreases the likelihood of a foreign attack on Romania. A noteworthy observation is that although fewer respondents identify the US as a key strategic partner, acknowledgment of Germany, France, and the UK as strategic allies has risen. These Western European nations share a common feature of enhanced military collaboration with Romania. This favourable development, however, does not preclude Romania's susceptibility to the influence of the Kremlin. According to the same report, the percentage of respondents attributing responsibility for the war to Russia decreased from 65% in 2023 to 55% in 2024, with 22% pointing the blame to Ukraine in 2024. This shift can be attributed to the dissemination of disinformation amplifying anti-Western narratives and depicting Ukraine negatively, particularly in relation to its treatment of minorities. Additionally, 38% of survey participants view far-right nationalism as a concern, a lower figure compared to most of Romania's CEE counterparts. This disparity is due, among other things, to insufficient public awareness on the matter and to the prevalence of narratives suggesting that Western countries treat Romanians as inferior and Romania as a colony, thus fuelling a stronger nationalistic, sovereign stance. Furthermore, 36% of Romanians expressed agreement with the notion that a totalitarian regime without elections could be advantageous for their country. These findings are similar to another study conducted by New Strategy Center,[53] which underlined that possible explanations for these types of attitudes are consistent with specific political and social realities: "the case of Romania's accession to the Schengen area will determine the growth of Euro-sceptic political options, but also of war *fatigue* sentiment, which erodes public support for Ukraine, dilutes the blame for the war and, implicitly, serves Russia's objective to diminish the trust of the citizens of democratic states in their own institutions, but also in Euro-Atlantic ones." (2023, p.10) Therefore, while Romania still demonstrates considerable resilience in the face of Russia's multifaceted political warfare in comparison to neighbouring countries in the Black Sea region, this does not preclude it from falling to some of its tactics, which raises the question of coming up with effective strategies and countermeasures.

Institutional and regulatory responses

The Romanian Ministry of National Defence (MApN) has implemented several initiatives to counter political warfare, focusing on hybrid threats like disinformation and cyber operations. A key component of these efforts is Romania's 2021-2024 Military Strategy, which emphasizes the need to strengthen national defense capabilities to address such evolving challenges. This strategy prioritizes resilience, intelligence sharing, and rapid response mechanisms to effectively counter hybrid warfare tactics. A practical tool supporting this strategy is the Inforadar portal (https://inforadar.mapn.ro/), launched in 2020. The platform plays a critical role in disseminating accurate information and combating disinformation, serving as a key element in the MApN's broader strategic communication efforts aimed at enhancing public awareness and resilience against hybrid threats

[52] GLOBSEC. (2024). GLOBSEC Trends 2024. GLOBSEC at https://www.globsec.org/what-we-do/publications/globsec-trends-2024-cee-brave-new-region

[53] New Strategy Center (2023), A year of War – National Attitudes in Romania and Norway policy Available at: https://newstrategycenter.ro/project/a-year-of-war-national-attitudes-in-romania-and-norway-policy/

The Romanian Ministry of Foreign Affairs has been actively engaged in countering political warfare, particularly in the realm of disinformation, through various initiatives. A key recent effort is the signing of a Memorandum of Understanding (MoU) with the United States in June 2024. This agreement focuses on enhancing cooperation to counter foreign state information manipulation. The MoU outlines several areas of collaboration, including information sharing, capacity building, and policy alignment, aimed at strengthening the resilience of both countries against disinformation and other hybrid threats. One significant initiative is Romania's involvement in the European Centre of Excellence for Countering Hybrid Threats, which focuses on building resilience against hybrid threats, including disinformation, across Europe.

The Euro-Atlantic Resilience Center (E-ARC) in Romania is a key institution dedicated to enhancing the country's ability to counter disinformation and other hybrid threats. E-ARC focuses on strengthening the resilience of both public and private sectors against information manipulation, particularly from foreign actors. The center's activities include research, strategic partnerships, and training programs designed to increase awareness and improve the capabilities of Romanian institutions in addressing these challenges.

Strengthening cybersecurity

One of the main focal points of Russian political warfare involves cyber operations. Romania has encountered numerous cyberattacks directed at governmental entities and critical infrastructure, along with cyber-enabled disinformation campaigns. On April 29, 2022, a multitude of websites linked to national authorities and finance and banking establishments were subjected to DDoS cyberattacks, rendering them inaccessible for a prolonged period. The pro-Russian group KILLNET claimed responsibility for this cyber assault. This particular group acknowledged responsibility for the targeting of governmental websites belonging to the Ministry of Defence, the Border Police, National Railway System, and other entities. More recently, in March 2024, several financial institutions such as Transylvania Bank and Romanian Commercial Bank encountered DDoS attacks, resulting in disruptions of the online functionalities of their banking platforms. These attacks were linked to a Russian hacktivist faction recognized as NoName057. As a response, Romania has significantly reinforced its cybersecurity capabilities. The establishment of the National Cyber Security Directorate (formerly known as CERT-RO) and cooperation with NATO's Cooperative Cyber Defence Centre of Excellence stand out as noteworthy measures. These endeavours are concentrated on enhancing the identification, reaction, and resilience to cyber threats. Additionally, investments in cultivating a skilled IT workforce play a critical role in crafting both strategies and subsequent software solutions to tackle Russian cyber operations. Statistical evidence from Eurostat reveals that as of August 2023, there were 240,800 IT&C professionals in Romania, with 82% of them below the age of 34. Consequently, Romania ranks second in Europe in terms of the quantity of IT specialists. Lastly, Romania could be seen as a good example of cyber diplomacy with neighbouring nations. In its capacity as a NATO member, in 2015 Romania undertook the main responsibility in supervising the NATO-Ukraine Trust Fund on Cyber Defence, totaling 965,000 EUR.[54] Following the initial implementation phase, this initiative supplied Ukraine with an integrated system tailored to fortify its defence against cyber threats and assaults, encompassing incident management hubs and forensic laboratories. It also entailed arrangements for cyber defence training sessions and simulation drills, along with setting up a framework aimed at enhancing Ukraine's cyber defence capabilities through domestic initiatives.

[54] Cocolan, M. (2018.). International cooperation for Critical Information Infrastructure Protection: NATO-UKRAINE Trust Fund on Cyber Defence. Rasirom. https://www.cipre-expo.com/wp-content/uploads/2018/10/Cocolan%20M%20NATO-UKRAINE%20Trust%20Fund%20on%20Cyber%20Defence.pdf

Soft containment

Soft containment is a strategy that aims to minimize interactions with Russia to restrict its influence within NATO. Several policy measures have been proposed, such as establishing an “Energy NATO” and decreasing reliance on Russian energy. A case in point is Romania, which has undertaken an initiative to exploit natural gas resources in its Black Sea Exclusive Economic Zone (EEZ). Notably, in 2023, energy corporations Petrom and Romgaz expressed their decisions to develop the Neptun Deep offshore gas field in Romania. Advancements of this field point to a positive development for energy security in the broader Black Sea region, with potential geopolitical and economic implications, particularly in offering an alternative to Russian gas and thereby diminishing Moscow's sway. The Neptun Deep field is the largest in the Romanian sector, with an estimated volume of 100 billion cubic metres (bmc). It is situated at water depths ranging from 100 to 1,700 metres. Infrastructure construction is slated to commence by the end of 2024, with initial production estimated to start production at the beginning of 2027. The Neptune Deep field is projected to yield between 7 bcm and 8 bcm annually. While numerous countries bordering the Black Sea rely on Russian gas imports, Romania covers approximately 80 percent of its gas demand through domestic production. When integrated with the existing production, the combined output from the Neptun Deep field and Ana (another field that is developed by Black Sea Oil & Gas, a Romanian-based independent energy company) is expected to cover Romania's yearly consumption of around 12 bmc. Once Romania's Black Sea gas production becomes operational, the country could potentially export surplus gas to neighbouring nations, thereby serving as a substitute for their Russian gas imports. Consequently, Romania emerges as a good example in terms of mitigating the energy dimension of Russia's strategic manoeuvres against NATO, underscoring the necessity for Western nations to endorse regional alliances and partnerships, exhibiting solidarity against Russian aggression, and fostering regional energy security through diversification of energy sources.

The project has been targeted by a dominant narrative that echoes a long-standing post-communist, isolationist sentiment. Following the Fall of the Iron Curtain, the privatization of the Romanian state-owned industrial complex significantly lagged behind those in Poland and Hungary. This hesitation was partly driven by a widely popular belief at the time that these assets belonged to Romania, are a matter of exclusive sovereignty and should not be sold to foreign investors seen as completely at odds with the interests of the Romanian state. This narrative, which presents a twisted, over-simplified version of the resource patriotism larger trend, has been revisited multiple times by ultra-nationalist groups, particularly concerning natural resources. In recent years, it has been employed against the Neptune Deep Project by far-right parties in Romania, aligning with the Kremlin’s objective to undermine both existing and future alternative energy sources for countries in the region.

For example, in May 2022, during the adoption of the Offshore Law which laid down the legal framework for the exploitation of offshore energy resources from the Black Sea, accusations were formulated, both in the political and public arena at large, that “the Minister of Energy is selling the gas for free”, despite the fact that the law which clearly stated that 60% of the profits will be collected by the Romanian state, with the remaining 40% by the companies involved in the exploitation of the process. In the case of Neptune Deep, the Romanian state is the majority shareholder in the consortium. The arguments against this energy project have often been infused with overtly pro-Russian stances and conspiracy theories (“foreigners seeking to steal Romanian resources”). Moreover, in the context of the upcoming 2024 parliamentary elections in Romania, such rhetorical arguments derived from the narrative that there is a completely antagonistic, zero sum, relationship between the Romanian state and the foreign companies involved in the

extraction of natural resources are even translated into policy proposals, seeking to the reverse the ownership of private energy companies.

Challenges ahead

In his 2015 examination of Russian strategy, Dima Adamsky[55] underlined the importance of indirect approach in Russian dealings with its enemies. Since in the current official Russian narrative, NATO and NATO members are defined as the main source of strategic threat to Russia, and NATO is viewed as a stronger actor than Russia, the use of indirect approach to dealing with NATO and its member states could yield some positive strategic results, according to Russian decision-makers. However, until now, Russia's ability to inflict serious damage or impose its political will by employing asymmetrical means has not resulted in any substantial weakening of the West's will to support Ukraine in preventing a Russian victory on the battleground. The impact of asymmetrical means has turned out to be limited due to several factors. One of these factors is most probably the Russian misreading of the West's resolve to stay together and provide help to Ukraine in defending itself against Russian aggression. Another one is the apparent lack of a skilful orchestration of military and non-military (political, psychological, ideological, informational) means in operations aimed at the Western world that could secure the success of such a combined operation. The third possible explanation is that the measures adopted at both NATO and EU level for countering Russian hybrid operations activity have resulted in a higher level of public awareness and resilience, which, in turn, rendered such operations less effective.

In his recent study on hybrid warfare, Maschmeyer[56] concluded that there is no clear evidence of the effectiveness of the Russian hybrid strategy and the use of political warfare against its perceived enemies in the Western world, but there is mounting evidence of the limitations of the Russian approach. The extent to which this apparent limited impact is due to the implementation of various countermeasures by the Western countries that we have examined in this brief study is an open question. Even so, it is important to summarize some of the challenges that the national and international policymaking community faces when trying to adjust policies towards hybrid warfare in the years to come.

These challenges include:

- **Attribution difficulties**, having to do with the fact that, most of the time, hybrid campaigns leave little traceable evidence; and even when technical attribution is possible, which is increasingly the case with both cyberattacks and disinformation, there is the extra challenge of political attribution;
- **Legal and normative constraints**, having to do with the fact that, most of the time, there are no clear legal regulations to address the grey areas exploited by hybrid warfare;
- **Coordination and consensus building**, which can be difficult when dealing with unclear situations from the grey zone ranging from cooperation to full-scale conflict;
- **Resource allocation and burden sharing**, especially when hybrid threats are not so evident or are not perceived so at an Allied level or the level of different members;

[55] Adamsky, D. (2015). Cross-domain coercion: the current Russian art of strategy. *Proliferation Papers* 54. IFRI, here p. 34.

[56] Maschmeyer, L. (2023). Assessing Hybrid War: Separating Fact from Fiction. *CSS Analyses in Security Policy, no. 33.* https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse332-EN.pdf

- **Unity of effort**, having to do with the fact that maintain unity of effort over a long period is demanding, especially when dealing with threats that are not necessarily and not always perceived as evident or existential;
- **The pace of technological evolution,** meaning that countermeasures must continually evolve to keep pace with the technological advancements, which are immediately incorporated in ever evolving offensive capabilities; potential adversaries can develop new ways of hybrid warfare, which requires a lot of adaptability, flexibility and innovative thinking on the Allied side;
- **Global economic interdependencies**, which can make it difficult to implement sanctions and other measures meant to harm the interests of potential adversaries and can have a boomerang effect on the initiators themselves;
- **The ever evolving features of the information environment**, meaning that countering disinformation and hostile influence campaigns, which is already time and energy consuming, must take into account the fact that content and information spread across the entire transnational information ecosystem (social and mainstream media alike) with unprecedented velocity, volume and variety;
- **Challenges related to strategic communications**, which involve not only countering hostile narratives, but also coming up with own narratives, effectively communicating national and trans-national policies and responses to the public;
- **Possible exploitation of democratic and digital affordances**, meaning that fostering critical thinking, encouraging media literacy or fact-checking initiatives can be weaponized especially in polarized and hyper-connected societies; upholding democratic values can also pose a challenge as introduction of various types of countermeasures can infringe or can be portrayed as infringing upon freedom of speech and other fundamental rights.

Conclusion

Hybrid political warfare poses significant challenges to NATO, the EU, and their member states taken individually. This form of warfare, which blends military, cyber, economic, and informational strategies, requires multifaceted and adaptive responses. The key to countering it lies in continuous adaptation, innovation, the ability to anticipate and respond to new forms of conflict and aggression, coupled with massive investments in resilience and measures that seek to address the dysfunctionalities exploited by political warfare.

The cases of Norway and Romania provide valuable insights into how different nations within the alliance are responding to these threats, highlighting both commonalities and differences in their approaches. Political warfare in the two countries takes different forms as it adapts to specific conditions following the following pillars: societal dispositions; geopolitical circumstances; historical path-dependencies; media and information landscape; regulatory environment; information and media literacy. Both countries showcase the importance of national resilience and the need for strong, adaptable defense strategies. Equally important, our study highlights that these strategies should be tailored to the specific geopolitical and societal contexts of each country.

At an allied level, NATO and the EU have made significant progress in addressing hybrid threats and political warfare. The integration of military and non-military measures, the emphasis on resilience, and the development of rapid response forces like the Very High Readiness Joint Task Force (VJTF) are critical components of the collective defense strategy. At the same time, our study also points out the challenges in maintaining unity and coherence across the alliance, particularly when dealing with the ambiguous nature of hybrid political warfare.

Finally, NATO and the EU must balance their responses, ensuring that measures taken in response to hybrid threats do not erode the democratic values they aim to protect. This delicate balance is essential to maintaining the legitimacy, relevance and effectiveness of the alliance in the face of evolving threats. NATO, the EU, and their partners sharing the basic democratic values and norms will have to find ways to deal with the old and new challenges posed by the use of hybrid warfare by their key geopolitical and normative challengers, competitors or adversaries. The challenges analysed in our study will have to be dealt with in a balanced manner by both national and international policy- and decision-makers so as to avoid a situation when the medicine applied against the hybrid challenge could have side effects that are worse than the “hybrid disease” itself.

Bibliography

- Adamsky, D. (2015). Cross-domain coercion: the current Russian art of strategy. Proliferation Papers 54. IFRI.
- Averre, D. (2006). Russia and NATO since 1991: from Cold War through cold peace to partnership? *International Affairs*, 82(4), pp. 814–815.
- Baker, J. A. (2002). Russia in NATO? *Washington Quarterly*, 25(1), pp. 95–103. https://doi.org/10.1162/016366002753358348
- Berghaust, J.C., Skjei, F., and Sellevåg, S.R. (2022). Hva kan Norge lære av andre lands tilnærming til sammensatte trusler? – rapport til Forsvarskommisjonen (What can Norway learn from other states' approach to hybrid threats? – A report to the Norwegian Defence Commission), FFI Report 22/02310. Available at: https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3088/22-02310.pdf
- Black, C. C. (1962). The Pattern of Russian Objectives. In I. Lederer (Ed.), *Russian Foreign Policy. Essays in Historical Perspective* (pp. 3–38). Yale University Press.
- Calha, J. M. (2015). Hybrid Warfare: NATO's New Strategic Challenge? NATO Parliamentary Assembly. Available at: https://www.nato-pa.int/sites/default/files/documents/2015%7C-%7C166%7CDSC%7C15%7CE%7CBIS%7C-%7CHYBRID%7CWARFARE%7C-%7CCALHA%7CREPORT.docx
- CIDOB. (2022). How democracies can overcome the challenges of hybrid warfare and disinformation? Available at: https://www.cidob.org/en/publication/how-democracies-can-overcome-challenges-hybrid-warfare-and-disinformation
- Cocolan, M. (2018). International cooperation for Critical Information Infrastructure Protection: NATO-UKRAINE Trust Fund on Cyber Defence. Rasirom. Available at: https://www.cipre-expo.com/wp-content/uploads/2018/10/Cocolan%20M%20NATO-UKRAINE%20Trust%20Fund%20on%20Cyber%20Defence.pdf
- Cyberscoop. (2021). Biden says he gave Putin list of 16 sectors that should be off-limits to hacking. Available at: https://cyberscoop.com/biden-putin-summit-russia-geneva/
- Davydov, Y. (2002). Razshirenie zony otvetstvennosti atlanticheskogo mira. In T. Shakleina (Ed.), *Vneshnaya politika i bezopasnost sovremennoy Rossii 1991-2002* (Vol. 2, pp. 124–141). MGIMO.
- Diesen, S. (2018). Lavintensivt hybridangrep på Norge i en fremtidig konflikt (A low-intensity hybrid attack on Norway in a future conflict). FFI Report 18000/80. Available at: https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/2152/18-00080.pdf
- DSB. (2024). Du er en del av Norges beredskap. Available at: https://www.dsb.no/globalassets/dokumenter/egenberedskap/dsb_beredskap_brosjyre_original.pdf
- EEAS. (2024). 2nd EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defense. Available at: https://euneighbourseast.eu/wp-content/uploads/2024/01/eeas-2nd-report-on-fimi-threats-january-2024_0-compressed.pdf
- European Parliament. (2017). Countering hybrid threats: EU-NATO cooperation. Available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf
- Gerasimov, V. (2013). The Value of Science in Prediction. *Military-Industrial Kurier*, 27 February. Available at: https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html
- GLOBSEC. (2024). GLOBSEC Trends 2024. GLOBSEC. Available at: https://www.globsec.org/what-we-do/publications/globsec-trends-2024-cee-brave-new-region
- Godzimirski, J. M. (2005). Russia and NATO. Community of values or community of interests? In J. Hedenskog, V. Konnander, B. Nygren, I. Oldberg, & C. Pursiainen (Eds.), *Russia as a Great Power. Dimensions of Russian Security* (pp. 57–80). Routledge.

- Godzimirski, J.M. (2019). Explaining Russian reactions to increased NATO military presence. *NUPI Policy Brief* 16/2019. Available at: https://www.jstor.org/stable/resrep25738
- Ionita, D., Cristea, I., Melnic, C., Stefureac, R., Godzimirski, J.M., Blackburn, M. (2024). Norway and Romania: Navigating Information Warfare. New Strategy Center and Norwegian Institute of International Affairs NUPI. Available at: https://newstrategycenter.ro/wp-content/uploads/2024/04/Norway-and-Romania-Navigating-Information-Warfare.pdf
- Lasconjarias, G., & Larsen, J. A. (2015). NATO's response to hybrid threats. NATO Defence College. Available at: http://www.ndc.nato.int/download/downloads.php?icode=471
- Leonard, M., & Popescu, N. (2007). A Power Audit of EU-Russia Relations. *ECFR Policy Paper*. European Council on Foreign Relations. Available at: https://ecfr.eu/wp-content/uploads/ECFR-02_A_POWER_AUDIT_OF_EU-RUSSIA_RELATIONS.pdf
- Liik, K. (2018). Winning The Normative War With Russia An Eu-Russia Power Audit. ECFR. Available at: https://ecfr.eu/wp-content/uploads/EU-RUSSIA_POWER_AUDIT.pdf
- Light, M. (2015). Russian Foreign Policy Themes in Official Documents and Speeches: Tracing Continuity and Change. In D. Cadier & M. Light (Eds.), *Russia's Foreign Policy Ideas, Domestic Politics and External Relations* (pp. 13–29). Palgrave Macmillan.
- Malerud, A., Hennum, Ch., and Toverød, N. (2012). Situasjonsforståelse ved sammensatte trusler - et konseptgrunnlag (Situation awareness encountering hybrid threats – a conceptual basis), FFI Report 21/00246. Available at: https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/2833/00246.pdf
- Maschmeyer, L. (2023). Assessing Hybrid War: Separating Fact from Fiction. *CSS Analyses in Security Policy*, no. 33. Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse332-EN.pdf
- M. E. (2021). Not One Inch: America, Russia, and the Making of Post-Cold War Stalemate. Yale University Press.
- NATO. (2014). Wales Summit Declaration. Available at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm
- NATO. (2016). Warsaw Summit Communiqué. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm
- NATO. (2018). Brussels Summit Declaration. Available at: https://www.nato.int/cps/en/natohq/official_texts_156624.htm
- NATO. (2021). Brussels Summit Communiqué. Available at: https://www.nato.int/cps/en/natohq/news_185000.htm
- NATO. (2022). Madrid Summit Declaration. Available at: https://www.nato.int/cps/en/natohq/official_texts_196951.htm
- NATO. (2023). Annual Tracking Research 2023. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/3/pdf/240314-annual-tracking-2023-en.pdf
- NATO. (2024). Countering hybrid threats. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm
- NATO. (2024). Washington Summit Declaration. Available at: https://www.nato.int/cps/en/natohq/official_texts_227678.htm
- NATO-Russia Founding Act. Available at: https://www.nato.int/cps/en/natohq/official_texts_25468.htm
- New Strategy Center. (2023). A year of War – National Attitudes in Romania and Norway policy. Available at: https://newstrategycenter.ro/project/a-year-of-war-national-attitudes-in-romania-and-norway-policy/
- Prudnikov, L. A., & Kuzmenko, A. V. (2023). Primeneniye nevoyennykh mer v interesakh obespecheniya voyennoy bezopasnosti Rossii (Application of non-military measures in the interests

of ensuring military security of Russia). *Voyennaya Mysl*(1). Available at: https://vm.ric.mil.ru/Stati/item/461891/
- Putin, V. (2021). Meeting with permanent members of the Security Council. President of Russia. Available at: http://en.kremlin.ru/events/president/news/66181
- Rahr, A., & Krause, J. (1995). Russia's New Foreign Policy (Vol. 91). Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik.
- Radin, A., & Reach, C. B. (2017). Russian Views of the International Order. RAND Corporation.
- Robinson, L., Helmus, T. C., Cohen, R. S., Nader, A., Radin, A., Magnuson, M., & Migacheva, K. (2019). Modern Political Warfare. Current Practices and Possible Responses. Rand Corporation. Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1772/RAND_RR1772.pdf
- Rühle, M. (2021). NATO's Unified Response to Hybrid Threats. Available at: https://cepa.org/article/natos-unified-response-to-hybrid-threats/
- Ryumin, A. (2022). Kakiye strany vkhodyat v spisok nedruzhestvennykh Rossii stran. *TASS*. Available at: https://tass.ru/info/18435143
- Sweijs, T. (2022). Between War and Peace: 'Hybrid Threats' and NATO's Strategic Concept. Available at: https://hcss.nl/wp-content/uploads/2022/06/Between-War-and-Peace-HCSS-2022-V2.pdf
- Stent, A. (2018). What Drives Russian Foreign Policy? In J. R. Deni (Ed.), *Current Russia Military Affairs: Assessing and Countering Russian Strategy, Operational Planning, and Modernization* (pp. 6-9). U.S. Army War College.
- Wilhelmsen, J., & Hjermann, A. R. (2022). Russian Certainty of NATO Hostility: Repercussions in the Arctic. *Arctic Review on Law and Politics*, 13(0), pp. 114-142. https://doi.org/10.23865/arctic.v13.3378
- Wilhelmsen, J., & Hjermann, A. R. (2023). Misplaced Certainty: NATO Hostility as Collective Common Sense Within Russia's Leadership. Available at: https://www.e-ir.info/pdf/102878

Follow us on social media:


NSC_Romania


newstrategycenter


office@newstrategycenter.ro


https://newstrategycenter.ro/en/home/