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 – What other NATO countries can learn from the Norwegian and Romanian experience?

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

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.

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.

Alina BÂRGĂOANU Senior Associate Expert, New Strategy Center and the 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 and an affiliate member of the European Center of Excellence for Countering Hybrid Threats, Helsinki.

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

Introduction: NATO's political warfare challenge

Before presenting a more detailed examination of how the preliminary findings of the FLANKS 2 project conducted jointly by the Norwegian Institute of International Affairs NUPI and the leading Romanian think tank the 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 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 presented also a brief discussion on the meaning of the concept of political warfare and other concepts that are currently used to describe a set of malign 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 collective West.

Here is summary of the discussion on these key concepts. 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 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

---

[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 defence. *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

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

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 assumed 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 Russia can play in this context.[7] A throughout 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 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 NATO decided to agree a strategy on NATO's role in Countering Hybrid Warfare, which was being implemented in coordination with the EU.[9] In the same document also the main objectives of the NATO Cyber Defence Pledge that was to enhance the cyber defences of national networks and infrastructures were outlined. They included the responsibility to improve its resilience and ability to respond quickly and effectively to cyber-attacks, including in hybrid contexts as well as the continuous adaptation of 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 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 to achieve their objectives. One

---

[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. 333. 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] 2014 Wales Summit Declaration at https://www.nato.int/cps/en/natohq/official_texts_112964.htm

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

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 to rest with 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 2018 Brussels Summit Declaration disinformation campaigns and malicious cyber activities were listed as elements of hybrid warfare the Alliance had to deal with. Russia was accused of challenging Euro-Atlantic security and stability through hybrid actions, such as attempted interference in the election processes, and the sovereignty of NATO countries, like in the case of Montenegro, and through widespread disinformation campaigns, and malicious cyber activities. Also, the use of a military-grade nerve agent in attack against Sergey Skripal in Salisbury was added to the list of hybrid challenges faced by NATO. The declaration also 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, as 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 supposed 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 the Alliance must address. The same document identified Russia as one of the countries that had intensified the use of hybrid instruments of power to influence policies of other countries. The document listed interference in Allied elections and democratic processes; political and economic pressure and intimidation; widespread disinformation campaigns; malicious cyber activities; and turning a blind eye to cyber criminals operating from its territory, including those who target and disrupt critical infrastructure in NATO countries as well as illegal and destructive activities by Russian Intelligence Services on Allied territory as malign 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 it had to address, including cyber, space, and hybrid as well as the malicious use of emerging and disruptive technologies that could pose a challenge to its security.[15]

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 in democratic processes, political and economic coercion, widespread disinformation campaigns, malicious cyber activities, and illegal and disruptive activities of Russian intelligence services. Also, other NATO's strategic competitors and

[10] Ibid.
[11] 2018 Brussels Summit Declaration at https://www.nato.int/cps/en/natohq/official_texts_156624.htm
[12] Ibid.
[13] 2021 Brussels Sumit Communiqué at https://www.nato.int/cps/en/natohq/news_185000.htm
[14] Ibid.
[15] 2022 Madrid Summit Declaration at https://www.nato.int/cps/en/natohq/official_texts_196951.htm

potential adversaries were identified as investing heavily in technologies that can be highly effective and can play a decisive part in conflict and help implement various malign hybrid activities. These hybrid activities targeted, according to the Declaration, 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. The Declaration also provided some clues on how NATO was to address these hybrid threats at the Alliance level and by providing support to member states exposed to this type of activities.

Finally, the Washington Sumit 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, instrumentalisation of irregular migration, malicious cyber activities, electronic interference, disinformation campaigns and malign political influence, as well as economic coercion as key Russian hybrid activities posing a threat to Allied security. The Alliance underlined that these Russian hybrid activities will not deter Allies' resolve and support to Ukraine and that the Alliance will also provide support to its partners most exposed to Russian destabilisation efforts.

One of the aspects of hybrid warfare that NATO came to recognize as an important challenge relatively late was the question of the use of information space in this context. Terms 'disinformation' and 'misinformation' appeared relatively late in the official declarations and communiqués issued by the alliance. The issue of disinformation as a challenge appeared for the first time in the 2018 Brussels Summit Declaration and has been since addressed in all summit declarations and Communiqués while the concept of misinformation was mentioned only once in 2024 Washington Summit Declaration. Also, the question of the use of fabricated/false narratives to influence public opinion in NATO countries was recognized as a challenge to NATO security relatively late as it was mentioned for the first time in the 2022 Statement by Nato Heads of State issued the day after the launching by Russia of its full-scale war against 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 may testify of the alliance's concern about the impact operations in the cyberspace, including those launched as an element of anti-NATO hybrid campaigns can have on NATO's security. It is also obvious that Russia's illegal occupation of Crimea followed by various types of Russia's hybrid operations against the alliance mentioned in the official NATO statements as posing potentially a threat to its members have also made the alliance pay more attention to the question of how to increase the level of resilience in member states. All 76 mentions of the term 'resilience' in this set of NATO documents are made in documents issued after 2014, starting with the Wales Summit Declaration from 2014 and ending with the 2024 Washington Summit Declaration. Finally, NATO also has expressed growing interest in the two areas that can be exposed to hybrid threats and are at the same time crucial for national and societal resilience – questions related to energy and energy security have emerged in NATO official declarations 122 times, starting with the 2006 Riga Summit Declaration, while questions related to infrastructure (59 mentions) have been addressed occasionally in the declarations and communiqués between 1997 and 2012, but have been discussed more intensely at the alliance summits in the period after the outbreak of the conflict in Ukraine in 2014.

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

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**

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

NATO's Russia Challenge

NATO and Russian strategic narratives on each other

After the dissolution of the Soviet Union and the emergence of the Russian Federation as the legal heir of the defunct USSR and as evidenced in the Table 1 Russia has been an important factor on NATO's map of strategic interests. 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 for the impact of a greater NATO military presence near the Russian border for its national security[17] and Russian policymakers have often argued that during the discussion on the reunification of Germany in 1990 and 1991 NATO promised not to enlarge to the east.[18]

While the signing of the 1997 NATO–Russia Founding Act[19] where it was clearly stated that NATO and Russia do not consider each other as adversaries, Russia–NATO relations have had their ups and downs. Russia's military intervention in Ukraine and annexation of Crimea in 2014 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 24 February 2022 has resulted in the new set of measures being taken by NATO and in the alliance and other members of the Western community providing political, economic and military support to Ukraine facing the Russian aggression.

As witnessed 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. The official NATO Declaration from the Chicago Summit in 2012 described relations with Russia as being of strategic importance as they contributed to creating a common space of peace, stability and security. NATO also aimed at building a lasting and inclusive peace, together with Russia, in the Euro-Atlantic area, based upon the goals, principles and commitments of the NATO-Russia Founding Act and the Rome Declaration and wanted 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 and illegal military intervention in Ukraine and demanded that Russia stop and withdraw its forces from inside Ukraine and along the Ukrainian border. 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 in 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, as the challenge to the Alliance undermining Euro-Atlantic security and posing the threat to creation of a Europe that is whole, free,

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

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

and at peace. Russia's recent activities and policies had according to this Communiqué reduced stability and security, increased unpredictability, and changed the security environment because Russia had not only breached the values, principles and commitments which underpin the NATO-Russia relationship but also had broken 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 2018 Brussels Summit Declaration[23] but 2021 Brussels Summit Communiqué described Rusia'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' full scale war against Ukraine was described as the gravest threat to the Euro-Atlantic security in decades. NATO called on Russia to immediately cease its military assault, to withdraw all its forces from Ukraine and to turn back from the path of aggression. Rusia 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 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 an all-domain threat to NATO that will persist into the long term. 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 the post-Cold war Russian approach towards NATO has to a certain extent mirrored NATO's approach to Russia. After a relatively short period of what is sometimes referred to as a romantic Atlanticist period of Russian foreign policymaking associated with Andrey Kozyrev at the helm of the Russian MFA 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 Vladimir Putin,

---

[22] 2016 Warsaw Summit Communiqué https://www.nato.int/cps/en/natohq/official_texts_133169.htm
[23] 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.

have even aired the idea of Russia joining the alliance[30], the same alliance has been increasingly presented in the Russian official debate as a possible source of strategic threat.[31] NATO has been regularly mentioned in Russian documents of doctrinal character as shown in Table 2.

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

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

To start 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 (not collided) cooperation with NATO was deemed important and vital (FPC 1993, FPC 2000). These areas were listed in detail in FPC 2008 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 for expanding 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 that Russia also expressed concern about was NATO's out-of-area operations, which according to Russian interpretation have contributed to worsening security, to undermining the

[30] Baker, J. A. (2002). Russia in NATO? *Washington Quarterly*, *25*(1), 95–103. https://doi.org/10.1162/016366002753358348

[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

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 concern also was voiced in this set of doctrines about the potential presence of NATO military bases and infrastructure close to 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 details in other official statements. In their 2022 article mapping Russian official approaches to NATO Wilhelmsen and Hjermann examined how NATO had been 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 from the period before the outbreak of the full-scale war in Ukraine was that Russian discourse entrenched an understanding of NATO as hostile, deceptive and constantly engaged in waging hybrid warfare against Russia. In a shorter version of their article they identified six ways of NATO framing in the collection of 156 documents produced between 2014 and 2022 by the Russian Ministry of Defence and Ministry of Foreign Affairs.[33] The collective West – and NATO is the most important Western institutional actor the official Russia identifies as the source of strategic threat – was presented as: 1) being completely controlled by the Washington D.C. 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 context. 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 prevent the outbreak of an open conflict. What Russia wanted to achieve by presenting these documents was the effective rollback of NATO to situation from before 1997 when NATO-Russia Founding Act was signed as well as 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 21 February 2022 Russia recognized the two Donbas 'republics', signed agreements on mutual help with them and three days later, on 24 February 2022 launched a full-scale war against Ukraine. This action shook the fundaments of the European security architecture and opened a new chapter in Russia's relations with NATO and the rest of the collective West.

Russia's strategic and operational objectives and instruments of power

We should assume that when relating to NATO in this new strategic situation caused by the decision to launch a full-scale war on Ukraine Russia will seek to achieve its long-term strategic objectives as well as some mid-term operational objectives. The use of various instruments of power from the Russian power toolbox will be determined by what objectives are sought achieved and how various

[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

instruments of power can facilitate achievement of these specific long-term strategic and mid-term operational objectives when dealing with NATO.

Based on a throughout examination of various studies on Russian foreign and security policy[34] we assume that the list of long-term strategic goals to be achieved by the current regime includes: survival and stability of the current regime; Russia's participation as a recognized great power in alliance systems and international institutions; the idea of replacing the Western global rules-based order with a new one; stabilization of the country's frontiers s defined by the current regime; unification of territories that the current regime defines as belonging to the Russian world (russkiy mir); assurance of favourable conditions for economic growth of the country, preferably through a closer cooperation with some friendly regimes.

However, to be able to achieve these strategic objectives Russia must be able to achieve what could be understood as mid-term operational objectives in the current circumstances shaped by its decision to go to war. In our opinion, these 2024 operational NATO-relevant objectives include: winning the war in Ukraine; splitting the West to stop its support to Ukraine; to intimidate the West; to weaken trust among members of the Western community; to undermine trust between people and political elites in Western societies.

Russia has various instruments of power at its disposal when trying to achieve these objectives. These instruments of power can be used not only when Russia pursues its interests in a legitimate manner, but also when Russia launches various types of hybrid operations against those who are defined by the current regime as 'unfriendly actors'. Military instruments of power are for instance employed in illegitimate kinetic operations in Ukraine that are to help Russia achieve some of its strategic objectives, but Russia uses also other instruments of power from its toolbox in the context of the war in Ukraine. These include diplomatic and political, information related instruments of power, the already mentioned military instruments of power as well as economic and financial instruments of power. These instruments of power 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 to advance 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, which will almost automatically strengthen Russia's hand in this strategically important region. A good example of how diplomacy can be used in Russian hybrid warfare to sow discord are various statements on NATO policy in the context of the war in Ukraine made by Maria Zakharova, the head of the information department of the Russian MFA, or the role played in the context of the war in

[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.

Ukraine by Permanent Representative of Russia to the United Nations Ambassador Vasily Nebenzia. Also Russia's overt and covert political support to various fringe political groups, corrupting political processes, and exploiting societal divisions canlead to undermine political cohesion and the functioning of and trust in the political systems in targeted countries, which would in turn help Russia achieve some of its stated and not-stated operational and strategic objectives, also in relations with NATO.

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 and in addition traditional propaganda and disinformation operations Russia has been engaging in other types of information related actions, such as Influence operations, elections and political interference, attempts at weaponization of history, as for instance exemlified by an article written aparently by Putin in 2021 that presented a completely false version of the history of Russian-Ukrainian relations. Also issues related to advertising intelligence, malvertising, alghoritmic warfare in information space, data and information harvesting belong to this hybrid information-related Russian repertoire. It is also important to underline that Russian hybrid operations in the information space can benefit from weaponization of the hyper connectivity of the 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 infrastructure, such as RT or Sputnik, that is actively used to spread pro-Russian narratives and counter what the official Russia labels as the Western Russophobia. These 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 space to promote Russia's official narratives, such as 'the peaceful Russia vs the war mongering West'; 'malfunctioning Western world order', 'the rigged international system dominated by the West and NATO'; 'the West against the rest'; as well as 'Russia as the leading force in the fight for a multipolar system' in which Russia is to 'help other countries liberate from neo-colonial and unfair rule'.

A separate and important issue related at least partly to Russian hybrid warfare in the broadly understood information and digital space and attracting a lot of attention in NATO are Russia's cyber operations targeting critical infrastructure, government systems, and key industries with the purpose of creating disruption and chaos. This could serve an important operational Russian objective, namely the undermining of the trust between political class that may face some problems with delivering important public goods, and population deprived of access to 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 emergence 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 in NATO countries are the murder of Aleksander Litvinenko in London, the use of Novichok against Sergei Skripal in Salisbury or the killing in Berlin of one of the former leaders of the Chechen resistance. These acts of political violence below 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 destabilization of regions in which also the West has some 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 collective West.

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 to result not only in limiting the 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 expected also that the very high level of energy dependence on Russia in the key NATO countries, like Germany, could make them more reluctant to provide support to Ukraine or support 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 the 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 collective West, paying special 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.[35]

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 also focused on 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

[35] 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

relationship with Moscow and were willing to use the veto to block EU negotiations on various issues with Russia.[36]

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 collective West examining 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 Crime and four years before the Russian full-scale invasion of Ukraine in February 2022.[37] 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 Russia 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.[38] 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 most 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.[39] In both surveys the citizens in all NATO countries and in Sweden were asked the question 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 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 the most reluctant to providing support to Ukraine and this reluctance is on rise. Since winning the war in Ukraine is undoubtedly the most important operational objective pursued currently by the Russian regime and the Western support to Ukraine is one of the main reasons why Russia has not been able to achieve this objective, we must 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 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.

---

[36] Leonard and Popescu 2007.

[37] 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

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

[39] These surveys can be accessed here: 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

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 malign 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 interviewed citizens were sceptical towards providing support to Ukraine, but also in Germany the level of scepticism was relatively high 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.

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

NATO Member 2024	2007 Category ECFR Power Audit	2018 Russia treats as relatively friendly	2018 Russia 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
Czechia	FrostyPragmatist					x	42	51	9
Hungary	FriendlyPragmatist	x				x	37	50	13
Bulgaria	FriendlyPragmatist			x		x	57	50	-7
Greece	TrojanHorse		x			x	47	48	1
North Macedonia	?					x	39	47	8
Slovenia	FriendlyPragmatist					x	40	46	6
Slovakia	FriendlyPragmatist		x			x	48	45	-3
Montenegro	?					x	57	44	-13
Germany	StrategicPartners					x	34	39	5
Belgium	FriendlyPragmatist			x		x	30	32	2
Romania	FrostyPragmatist				x	x	36	32	-4
Italy	StrategicPartners	x				x	33	31	-2
Turkiye	?					x	19	30	11
Croatia	?					x	23	29	6
France	StrategicPartners		x			x	28	29	1
NATO Whole	New Cold Warrior?				x	x	26	28	2

NATO Member 2024									
Czechia	FrostyPragmatist					x	42	51	9
Hungary	FriendlyPragmatist	x				x	37	50	13
Bulgaria	FriendlyPragmatist			x		x	57	50	-7
Greece	TrojanHorse		x			x	47	48	1
North Macedonia	?					x	39	47	8
Estonia	FrostyPragmatist				x	x	19	26	7
Latvia	FrostyPragmatist			x		x	21	26	5
Netherlands	FrostyPragmatist				x	x	23	26	3
Poland	NewColdWarrior				x	x	23	26	3
Luxembourg	FriendlyPragmatist		x			x	19	23	4
Canada	?					x	18	22	4
United States	?					x	25	19	-6
Lithuania	NewColdWarrior				x	x	16	18	2
Denmark	FrostyPragmatist					x	16	17	1
Spain	StrategicPartners		x			x	18	17	-1
Sweden	FrostyPragmatist				x	x	17	15	-2
Norway	FriendlyPragmatist					x	16	14	-2
Portugal	FriendlyPragmatist		x			x	11	13	2
United Kingdom	FrostyPragmatist				x	x	15	13	-2
Finland	FriendlyPragmatist		x			x	9	12	3
Iceland	?					x	7	9	2
Albania	?					x	18	9	-9

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

Faced with this not only potential but also very real challenge of the Russian hybrid activity NATO has over the past years 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 this 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.[40] 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 of **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 digitilized sectors. For instance, Estonia has been at the forefront of cyber defence since the 2007 cyber-attacks 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 are committed to enhancing their cyber defence capabilities. This includes sharing best practices, improving cyber incident response, and conducting cyber defence exercises.

---

[40] 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 .

By increasing the level of protection of critical digital infrastructure against any malign hybrid operations the authorities in NATO countries aim also at **strengthening national economic and societal resilience**. These resilience related measures were to reduce their vulnerability to economic coercion by diversifying energy sources, implementing anti-corruption measures, enhancing the resilience of their financial systems and by 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 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 **enhancing 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 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, media literacy campaigns, and fact-checking services to ensure the public has access to accurate information. Finland has for instance introduced various measures to combat 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 combat 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 required also 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 malign operations. Some legal measures related to money laundering, political lobbying by foreign entities, and the spread of fake news have been introduced in response to increased levels of malign activities. For instance, the UK has enacted the 'Magnitsky Amendment', allowing the government to impose sanctions on individuals involved in gross human rights abuses, which includes those using hybrid warfare tactics. Also various types of bans on sending Russian propaganda through Russian channels in several NATO countries were introduced to limit Russia's ability to influence public opinion. When 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 borders of Lithuania, Poland and Finland to try to cross them on their way to the EU, the authorities in these countries introduced special laws and regulations to seal of the borders and also decided to build new infrastructure ta make 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.

Also questions related to increasing the level of **public awareness and civil society engagement** in dealing with the hybrid warfare have been introduced to increase the level of national resilience in this new situation. One element of this approach is increased level of collaboration between the government and private sector, particularly in critical infrastructure sectors, to protect against cyber attacks 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 Geneve in June 2021 when he gave 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. [41]

Diplomatic channels are also used to address hybrid threats, with introduction of various types of sanctions against actors involved in this type of activity, combined with diplomatic isolation, and efforts to uphold international law as some of the introduced measures. 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 likeminded 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 in this context.[42] The key measures were development of joint strategies, conducting exercises, and providing support to member states targeted by hybrid tactics, and all of them have been mentioned in official NATO statements issued after 2014. The European Union Agency for Law Enforcement Cooperation (Europol) also 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.[43]

Finally, when all these above-mentioned measures are not sufficient to address hybrid warfare related challenges, there is also a role for **military instruments** to be introduced to deal with this threat. This has amongst others led to restructuring of armed forces with introduction of special units or ecene a new branch to deal with this challenge, introducing 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 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

[41] 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/

[42] For more 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 .

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

reassure allies. This and other measures such as creation of the Very High Readiness Joint Task Force (VJTF) has enhanced NATOæs military capabilities making the alliance more able 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 NATO may consider invoking Article 5, which states that an attack on one member is an attack on all, in response to hybrid operations if they reach a certain threshold. This demonstrates the alliance's readiness to collectively address hybrid threats as serious as conventional attacks 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 hybrid attacks. 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 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

Like most of 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 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 that provides national professional guidelines for media activity.[44]

Improving and adjusting national governance

In response to changes in the international environment, technology and the need to improve national governance in the field of security Norway also introduced 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 cyber attacks and sabotage. Especially after the sabotage against NordStream pipelines in September 2022 the question of protection of 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 protection of critical infrastructure in the region.[45] Norway has also implemented almost all EU regulations on protection of critical infrastructure which makes it easier to work together with other EU and NATO member states on finding common solutions to a common challenge of Russian hybrid warfare. Implementation of EU regulations on protection of critical infrastructure creates a common regulatory space and facilitates designing and implementation of common solutions increasing national economic and societal resilience, which is crucial when dealing with various aspects of hybrid warfare.

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 several times reminded citizens about what they need to be able to cope with a manmade 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.[46] A special website with information in both Norwegian and English was made available to providing information on practical aspects of civil preparedness.[47]

Strengthening international cooperation

Confronted with an increasingly provocative and aggressive Russian policy Norway has also decided to pay more attention to deterrence related solutions and less to questions related to assurance-related aspects of 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, amongst other by contributing to NATO's Enhanced Forward Presence (EFP) and participating in joint exercises designed to improve interoperability and readiness against hybrid

[44] See https://presse.no/pfu/etiske-regler/vaer-varsom-plakaten/vvpl-engelsk/
[45] https://www.nrk.no/rogaland/signerer-sikkerheitspakt-for-nordsjoen_-_-saman-er-me-sterkare-1.16836118
[46] DSB. (2024). Du er en del av Norges beredskap at https://www.dsb.no/globalassets/dokumenter/egenberedskap/dsb_beredskap_brosjyre_original.pdf
[47] For more on that in English see https://www.sikkerhverdag.no/en/ .

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 the Norwegian society and the country' relatively high level of exposure to Russian hybrid operations it was also important to generate new knowledge policy relevant on how Norway should prepare to deal with the hybrid challenge. In 2018 Norwegian Defence Research Establishment (FFI) published a report summing up the findings of a project on the role of hybrid operations in the future conflict.[48]

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 assumed 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 the development of information and communication technology over the past 20 years has had for 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[49] dealt with the question of how hybrid operations may challenge our ability to have a good situation 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 policy relevant suggestions and recommendations on how to improve the ability to obtain situation awareness facing 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.[50] The main idea behind this study was to consider what Norway can learn from Finland, Sweden, Estonia, the United Kingdom, the Netherlands and 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 approached the issue. Based on the suggested best practices and the states' approaches, recommendations regarding what Norway can learn to strengthen the ability to counter hybrid threats provided in this interesting and extensive study.

There were five key recommendations and the study concluded that 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. Also questions of how to strengthen and organize the Norwegian government's

[48] 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

[49] 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

[50] 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

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. The report also considered how to strengthen resilience in the Norwegian democracy, in critical infrastructure and in the population and how to organize modern psychological defence in the country. Also questions related to changes in the legal framework were given attention in the proposal on how to improve Norway's ability to cope with hybrid challenges. Finally, the authors of the report proposed a cautious approach to the idea of giving the Norwegian Armed Forces responsibility related to countering hybrid threats, because their most important task is to maintain 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. What also needs to be factored in in the Norwegian strategic calculations, also regarding how to deal with the hybrid challenges, is the fact the international environment in which the Norwegian policy is shaped and implemented, has changed dramatically after the enlargement of NATO to Finland and Sweden.

The case of Romania (NSC)

Russian political warfare, observed in various European nations, typically encompasses a blend of cyber attacks, dissemination of false information, economic manoeuvring, and the cultivation of political and societal rifts. As delineated 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, fostering internal discord that obstructs cohesive reactions to Russian activities. In this context, Romania has encountered multiple aspects of this warfare, rendering its encounter notably enlightening in contrast to other nations.

Romania stands out in this particular scenario due to the persistent influence of Russia, despite the absence of historical, political, economic, or linguistic factors that render its neighboring countries susceptible. In the case of Bulgaria, 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. Moreover, the prevalence of corruption and the presence of oligarchs provide fertile soil for Russian interference. 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 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.

Nevertheless, Romania is distant from being significantly impacted by Russia's political warfare arsenal, as evidenced by a GLOBSEC Trends report for 2024. 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 negate Romania's susceptibility to the harmful 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 at Ukraine in 2024. This shift can be attributed to the dissemination of disinformation targeting pro-Western narratives and depicting Ukraine negatively, particularly in relation to its treatment of minorities. Additionally, 38% of respondents view far-right nationalism as a concern, a lower figure compared to most of Romania's CEE counterparts. This disparity is largely due to insufficient public education on the matter and the prevalence of narratives suggesting that Western countries regard Romanians as inferior, potentially fueling a desire for a stronger nationalist stance. Furthermore, 36% of Romanians expressed agreement with the notion that a totalitarian regime without elections could be advantageous for their country. Therefore, while Romania demonstrates considerable resilience against Russia's multifaceted political warfare in comparison to neighboring countries in the Black Sea region, this does not preclude it from being a target and necessitating effective strategies to counter such endeavors.

Strengthening cybersecurity

One of the main focal points of Russian political warfare involves cyber operations. Romania has encountered numerous cyber attacks directed at governmental entities and critical infrastructure, along with cyber-enabled disinformation campaigns. On the 29th of April, 2022, a multitude of websites linked to national authorities and financial-banking establishments were subjected to DDoS cyber attacks, rendering them inaccessible for a prolonged period. The attribution for this cyber assault was asserted by the pro-Russian group KILLNET. This particular group acknowledged responsibility for the targeting of governmental websites, the Ministry of Defence, the Border Police, CFR Călători, and other entities. More recently, in March 2024, several financial institutions such as Transylvania Bank (BT) and Romanian Commercial Bank (BCR) encountered DDoS attacks, resulting in disturbances in the online functionalities of their banking platforms. These attacks were linked to a Russian hacktivist faction recognized as NoName057. In reaction, 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 combat 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 falling 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 an exemplar of cyber diplomacy with neighboring nations. In its capacity as a NATO member, Romania undertook the principal responsibility in supervising the NATO-Ukraine Trust Fund on Cyber Defense, totaling 965,000 EUR. Following the initial implementation phase, this endeavor supplied Ukraine with an integrated system tailored to fortify defenses against cyber threats and assaults, encompassing incident management hubs and forensic laboratories. It also entailed arrangements for cyber defense training sessions and simulation drills, along with setting up a framework aimed at enhancing Ukraine's cyber defense capabilities through domestic initiatives.

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. An illustrative case in point is Romania, which has undertaken an initiative to exploit natural gas resources in its Black Sea Exclusive Economic Zone (EEZ). Notably, energy corporations Petrom and Romgaz disclosed intentions to develop the Neptun Deep offshore gas field in Romania last year. The advancement of this field signifies 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, the largest in the Romanian sector with an estimated volume of 100 bcm, is situated at water depths ranging from 100 to 1,700 meters. Infrastructure construction is slated to commence in 2024, with initial production anticipated in early 2027. The Neptun 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 satisfies approximately 80 percent of its gas demand through domestic production. The combined output from the Neptun Deep field and Ana (another field being developed by Black Sea Oil & Gas), when integrated with existing production, is expected to cover Romania's yearly consumption of around 12 billion cubic meters if all goes according to plan. Once Romania's Black Sea gas production becomes operational, the country could potentially export surplus gas to neighboring nations, thereby serving as a substitute for their Russian gas imports. Consequently, Romania emerges as a standout example in terms of mitigating the energy dimension of Russia's strategic maneuvers against NATO, underscoring the necessity for Western nations to continue endorsing regional allies and partners, exhibiting solidarity against Russian aggression, and fostering regional energy security through diversification of energy sources. [51]Achieving this objective hinges on bolstering both fossil fuel and renewable energy production within domestic borders.

Conclusions: challenges ahead

In his 2015 examination of Russian strategy Dima Adamsky[52] underlined the importance of indirect approach in Russian dealing with its enemies. Since NATO and NATO members are in the current Russian narrative defined as the main source of strategic threat to Russia and NATO is also viewed as a stronger actor than Russia the use of indirect approach to dealing with NATO and its member states could, according to Russian decisionmakers, yield some positive strategic results. However, Russia ability to inflict serious damage or impose its political will by employing asymmetrical means has so far not resulted in any substantial weakening of the West's will to support Ukraine to prevent Russian victory on the battleground 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 defending itself against Russian aggression. The other one is the apparent lack of a skilful orchestration of military and non-military (political, psychological, ideological, informational) means in operations aimed at the collective West that could secure the success of such a combined operation. The third possible explanation is that the measures adopted by the collective West, including NATO and the EU, to counter Russian hybrid activity have resulted in a higher level of public awareness and resilience that make Russian hybrid operations less effective.

[51] Scutaru, G. (2024). Black Sea's Offshore Energy Potential and its Strategic Role at a Regional and Continental Level. New Strategy Center.

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

In his recent study on hybrid warfare Maschmeyer[53] concluded that there is no clear evidence of the effectiveness of the Russian hybrid strategy and the use of political warfare against its enemies in the collective West but there is mounting evidence of the limitations of the Russian approach. To what extent this limited impact is due to implementation of various countermeasures by the collective West that we have examined in this brief study is an open question, but it is important to present some of the challenges faced by the policymaking community at national and international levels that must adjust policies towards hybrid warfare in years to come.

These challenges include:

- Attribution difficulties, which has to do with the fact that hybrid campaigns leave little traceable evidence;
- Legal and normative constraints, which has to do with the fact that there are no clear legal regulations to address the grey areas exploited by hybrid warfare;
- Coordination and consensus building can be difficult when dealing with unclear situations from the grey zone between cooperation and full-scale conflict;
- Technological advancements as countermeasures must continually evolve to keep pace with the advancements in offensive capabilities;
- Information warfare, since information spreads quickly across digital platforms countering disinformation, misinformation and propaganda is very time and effort consuming;

- Economic dependencies can make it difficult to implement measures harming interests of potential adversaries;
- Increasing public awareness and resilience are demanding tasks involving fostering of critical thinking, which can pose various challenges especially in polarized societies;
- Maintaining democratic values can also pose a challenge as introduction of various types of countermeasures can infringe on freedom of speech and other basic human rights;
- Strategic communication which involves producing countering adversary narratives but also effectively communicating national policies and responses to the public;
- Resource allocation and burden sharing is always a problem, especially if the hybrid threats are not so evident;
- Adaptability and flexibility has to do with the fact that potential adversaries can develop new ways of hybrid warfare that can demand more flexibility and innovative thinking on our side;
- Unity of effort has to do with the fact that to maintain unity of effort over a longer period is demanding, especially when dealing with threats that are not necessarily considered very evident or existential.

NATO, the EU, member states and partners who share the basic democratic and liberal values and norms will have to find ways of dealing with the old and new challenges posed by the use of hybrid tactics by its key geopolitical and normative challengers in Europe and elsewhere. The challenges listed above will have to be dealt with in a balanced manner by both national and international policy- and decision-makers to avoid a situation when the medicine applied against the hybrid challenge could have side effects that will be worse than the 'hybrid disease' itself.

[53] Maschmeyer 2023, p.2.

Follow us on social media:


NSC_Romania


newstrategycenter


office@newstrategycenter.ro


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