Policy Paper

A Better Balance

Imposing Costs on Hybrid Aggressors in the Baltic States

| Arelena Shala | Bradley Jackson | Johannes Hui | Dave Sprague |

November 2022

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

Title: A Better Balance. Imposing Costs on Hybrid Aggressors in the Baltic States
Authors: Shala, Arelena; Jackson, Bradley; Hui, Johannes; Sprague, Dave
Publication date: November 2022
Category: Policy Paper

Cover page photo: Gas bubbles from the Nord Stream 2 leak on the Baltic Sea (Danish Defence Command/Handout via Reuters/Scanpix)

Keywords: Hybrid warfare, Baltic states, NATO

ISSN 2228-2068

63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee, www.icds.ee

About the Authors

Arelena Shala, Bradley Jackson, Johannes Hui, and Dave Sprague were graduate students in the Freeman Spogli Institute's Master's in International Policy programme at Stanford University during 2021-2. This policy paper is based on the final capstone project for their master's programme, which dealt with deterrence of hybrid threats and was carried out in cooperation with the ICDS.

Acknowledgements

We are grateful to those who generously shared their time and ideas during our research interviews and our supervision at Stanford.

First, we would like to thank Professors Francis Fukuyama and Jeremy Weinstein for mentoring our capstone team over six months and providing the feedback and guidance necessary to produce a comprehensive policy proposal according to best practices taught at Stanford.

We also extend our special gratitude to other great personalities at Stanford who willingly offered their time and resources to help produce and promote our project. That includes Professor Rose Gottemoeller, Ambassador Michael McFaul, Secretary Condoleezza Rice, and LTG (Ret) H.R. McMaster.

Finally, we would like to thank all the regional experts from think tanks, government, and academia who were willing to share their unique perspectives and recommendations through interviews despite the time difference and their preoccupation with the 2022 Russian invasion of Ukraine, which occurred shortly after this research project began. We especially thank the Center for Geopolitical Studies in Riga, the Baltic Defence College in Tartu, and the Swedish Defence Research Agency in Stockholm, for hosting us during our field research in the region.

Introduction

During the Cold War, every Soviet KGB officer was required to dedicate roughly a quarter of their time to developing 'active measures' – creative, covert strategies aimed at the enemies of the Soviet Union, intended to advance Soviet political goals while avoiding the outbreak of war. Active measures included political operations, like disinformation campaigns and support to extremist parties in democratic countries, support for insurgencies and the installation of puppet regimes, assassinations, and sponsorship of political violence. These ideas, upon which KGB officers depended for satisfactory evaluations and promotions, were passed to Service A of the KGB's First Chief Directorate, where they were sorted, refined, and implemented. The importance of active measures in the Soviet context cannot be overstated. Directorate A was resourced with over 15 000 operatives – far more than the US State Department – and a multimillion-dollar budget.[1] While the Cold War ended three decades ago, the Kremlin's creativity in and penchant for subversive campaigns remain.

While the Cold War ended three decades ago, the Kremlin's creativity in and penchant for subversive campaigns remain

Russia's full-scale invasion of Ukraine was preceded by nearly eight years of intense hybrid aggression in the form of 'little green men', support to proxy forces in eastern Ukraine, cyber attacks, economic coercion, and so on. Russia has not achieved its political goals in Ukraine, but has suffered militarily, and severely damaged relations with the West. In this setting, the Baltic states can expect further Russian hybrid aggression.

The Baltic states are a principal target of the Kremlin's active measures. Putin's 2007 Munich address, when he decried the US led international order and the expansion of NATO, and his December 2021 demands to withdraw all NATO troops and equipment from the Baltic states and other eastern European members indicate that Russia seeks to challenge Baltic sovereignty with all means at its disposal.[2] Today, active measures are known by various names including 'hybrid war', 'subthreshold military activity', and 'grey zone warfare', but they are inherently similar in that they undermine security and sovereignty through clever applications of national power in ways that attempt to avoid escalation to conventional conflict or, sometimes, prepare the ground for it. Ukraine represents the most recent case study in which hybrid actions preceded a conventional invasion – an outcome that NATO cannot accept for its members.

Russia's 2007 hybrid attack on Estonia serves as an example of how a variety of subthreshold actions can be used to destabilise a vulnerable target state.[3] These aggressions followed the relocation of a Soviet World War II memorial, the Bronze Soldier, an action Russia perceived as an egregious insult. In response, Moscow engaged in cyberattacks that briefly disabled, among other public systems, banking services and the mobile phone network. This limited the authorities' and media's ability to communicate with the public. Kremlin-backed groups rioted in Tallinn and attacked the Estonian embassy in Moscow.

[1] The New York Times, "Meet the KGB Spies Who Invented Fake News | NYT Opinion," YouTube Video, 19 November 2018, 15:37.

[2] The Presidential Executive Office, "Speech and the Following Discussion at the Munich Conference on Security Policy," The President of Russia, 10 February 2007; Andrew Roth, "Russia Issues List of Demands It Says Must Be Met to Lower Tensions in Europe," *The Guardian*, 17 December 2021.

[3] Ivo Juurvee and Anna-Marita Mattiisen, *The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict* (Tallinn: ICDS, 2020).

Disinformation campaigns sought to inflame the Russian diaspora in Estonia, claiming the Bronze Soldier had been destroyed as part of the government's systematic persecution of the Russian minority. Suddenly announced Russian repairs of railway lines to Estonia disrupted transit and flows of oil and coal into the country. Russia and its allies engaged in diplomatic pressure for the dismissal of the Estonian prime minister and government. In retrospect, it is apparent that these activities were coordinated and executed by the Russian Federal Security Service (FSB) and Foreign Intelligence Service (SVR), using Russian covert military and intelligence operatives placed in Estonia on the authority of Vladimir Putin.[4]

Modern-day active measures and hybrid campaigns threaten both Baltic regional sovereignty and the credibility of NATO's Article 5 commitment. Although Russia's hybrid activities in the Baltic states vary – including spreading COVID-19 vaccine disinformation, energy blackmail, airspace violations, and the kidnapping of an Estonian security officer – hybrid actions involving Russian military capabilities, equipment, and personnel pose the greatest risks to the status quo and military escalation in the region. These actions carry the greatest danger of accidents and, as part of a larger strategy, the greatest potential to evolve into a scenario that challenges democratic governance and rule of law in the Baltic states.

This policy paper explores Russia's subthreshold military activities, and NATO's readiness to deter them. We recommend NATO to update its counter-hybrid policy to achieve a better balance of denial and punishment strategies, and to effectively signal to Russia that the continuance of its subthreshold campaigns is not worth the costs it will incur as a result. As Russia strives to foment instability and upend the rules-based international order, NATO and its partners must demonstrate their commitment to regional security in the Baltic states. They must thus seek consensus on a more robust, meaningful deterrence strategy in the hybrid space.

[4] Juurvee and Mattiisen, *The Bronze Soldier Crisis of 2007*, 17; "Estonian Ex-PM: Bronze Night Riots in Tallinn Coordinated by Russian Officers on Site," *Baltic News Network*, 26 April 2017.

1. Background

1.1. The Russian Context

To understand hybrid deterrence in the Baltic region, we first explore Russia's geopolitical threat perceptions and its doctrine of using hybrid warfare to achieve strategic goals. Of note, Western and Russian security concepts and language are different.

The Russian leadership genuinely perceives Russia to be operating under a long-lasting encirclement by the West

The Russian leadership genuinely perceives Russia to be operating under a long-lasting encirclement by the West and NATO, which aims to undermine and ultimately destroy the Russian state and values.[5] Russia views its current behaviour as a defensive response to Western aggression across various domains, including the political, economic, military, and cultural.

Russian thinking about and execution of warfare differs in some regards from the West's views. Russia does not use the term 'hybrid warfare' to define its subthreshold actions and subversion campaigns. In Russian strategic literature, it is used to describe the West's way of waging war against Russia; Russian campaigns below the threshold are a defensive response to this perceived aggression.[6] The essence of what Russia calls 'New Generation Warfare' is reflected in the statements of Valeriy Gerasimov, the Russian Chief of the General Staff, and in Russian military doctrine. Essentially, Russian New Generation Warfare exercises a mix of hard and soft power across various domains, using military, diplomatic, informational, and economic levers in a coordinated fashion. According to Gerasimov, "The very 'rules of war' have changed. The significance of nonmilitary means to achieve political and strategic goals has grown, and, in many cases, nonmilitary means have exceeded the power of force of weapons in their effectiveness." Further highlighting the role of

[5] Dmitry Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," *French Institute of International Relations (Ifri) Proliferation Papers*, no. 54 (November 2015): 19.

[6] Adamsky, "Cross-Domain Coercion," 21.

nonmilitary measures alongside conventional military force, Gerasimov observes:

> "The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures – applied in coordination with the protest potential of the population.
>
> All of this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special-operations forces. The open use of forces, often under the guise of peacekeeping and crisis regulation, is resorted to only at a certain stage, primarily for the achievement of final success in the conflict."[7]

Gerasimov recommends that the optimal ratio of non-military to military measures should be four to one, with both forms being supervised by military officials.[8]

1.2. The Baltic Context

Hybrid campaigns in the Baltic region carry escalatory risks not felt elsewhere in the Alliance. Estonia, Latvia, and Lithuania are geographically isolated from the rest of NATO by Russia, Belarus, Russia's Kaliningrad exclave, and the Baltic Sea. Strategically, Russia wants to regain its Soviet-era influence over the Baltic states, to maintain its access to the Baltic Sea, and to reduce the risks of isolation facing the Kaliningrad exclave.

As a result of Soviet era forced migration policies, the Baltic states also host sizable ethnic Russian minority populations. According to 2021 census data, ethnic Russians make up 23.7% of the population in Estonia, 24.2% in Latvia (2022), and 6.5% in Lithuania.[9] The size of these populations and their tendency to consume mostly Russian state media make the Baltic states potential targets for Russian disinformation and political campaigns intended to sow domestic civil unrest. Russia's 'compatriot' policy allows it to cite (fabricated) threats to Russian speakers outside its borders as a pretext for military intervention.

The Baltic states face a strategic challenge due to their geographic isolation from the rest of NATO and a conventional military asymmetry at the regional level that favours Russia.[10] The potential for hybrid acts using military capabilities to escalate rapidly – either accidentally or deliberately – into larger political outcomes like regime collapse and invasion appears high; for example if Russian hybrid campaigns result in the collapse of Baltic governance or the obfuscated annexation of Baltic territory similar to Russian campaigns in Ukraine and Georgia. Compounding this, other Allies face challenges in coming to the aid of the Baltic nations. In a series of conventional wargames conducted by RAND, Russian conventional forces were able to defeat regional NATO forces (at 2014 force levels) and reach the capitals of Estonia and Latvia in under sixty hours, before NATO reinforcements could arrive through the Suwałki corridor or Baltic Sea.[11] This means the Alliance potentially faces a task of liberating the Baltic states, instead of defending them, if hybrid and conventional deterrence fails. In recognition of these circumstances, NATO heads of state and government agreed on further measures to enhance deterrence on the Alliance's eastern flank at their 2022 summit in Madrid.[12]

NATO potentially faces a task of liberating the Baltic states, instead of defending them, if hybrid and conventional deterrence fails

To evaluate the suitability of current hybrid deterrence policies, we next explore the breadth of hybrid military threats and the risks they pose.

[7] Valeriy Gerasimov, "Ценность науки в предвидении [The Value of Science in Foresight]," *VPK (Военно-Промышленный Курьер* [Military-Industrial Courier]) no. 8 (February 2013): 476.

[8] Adamsky, "*Cross-Domain Coercion*," 23.

[9] Statistics Estonia, "Population figure," accessed 11 October 2022; Official Statistics Portal (Latvia), "Population by ethnicity at the beginning of year – Ethnicity and Time period," accessed 11 October 2022; Official Statistics Portal (Lithuania), "Population and Housing Census," accessed 11 October 2022.

[10] Edward Lucas, Ben Hodges, and Carsten Schmiedl, "Close to the Wind: Baltic Sea Regional Security," *CEPA*, 9 September 2021.

[11] David A. Shlapak and Michael Johnson, *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltic states* (Santa Monica: The RAND Corporation, 2016), 1.

[12] NATO, "Madrid Summit Declaration. Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022," Press Release (2022) 095, 29 June 2022, para 8.

2. Military Hybrid Threats Explored

This policy paper focuses specifically on Russian military hybrid threats, meaning subthreshold actions that use military forces to achieve political goals (we thus exclude, for example, cyber and disinformation campaigns – while these may include military instruments, they are generally broader based). Often, military hybrid threats are intended to discredit governments and undermine NATO credibility. We describe below the types of Russian military subthreshold activities threatening the Baltic states that have either already occurred in the region or elsewhere or have the potential to occur.

2.1. Airspace violations

In 2020, Russian military planes were involved in 228 violations of international aviation norms near or in Estonian airspace. These include aircraft that neglected to transmit transponder codes, file a flight plan, or communicate with air traffic controllers. Such ambiguous military provocations threaten Baltic security and pose flight hazards for civilian aviation. They serve both a military and political purpose: to attrit the readiness of NATO air forces and remind the target state of its inability to enforce sovereign control over its own territory.[13] Given the small size of the Baltic states and their proximity to Russia, they have little time to react to these incursions. A Russian military aircraft flying at 500 knots can reach Tallinn in eleven minutes, while it takes roughly fifteen minutes to muster NATO aircraft from the Baltic Air Policing mission at Ämari airfield in Estonia.[14] Continued airspace incursions allow the aggressor to probe responses for input into future military planning, serve to answer Russian intelligence requirements, and use up flight hours of Allied aircraft.

Ambiguous military provocations attrit the readiness of NATO air forces and remind the target state of its inability to enforce sovereign control over its own territory

In January 2022, Swedish authorities reported multiple overflights of its nuclear power plants by drones that were "widely described as military-style and as having large wings," or high-altitude long-endurance drones comparable to US MQ-series Predators.[15] These kinds of actions are coercive in nature, presenting the targeted nation with difficult choices in response.

2.2. Obfuscated Territorial Grabs

Russia's annexation of Crimea in 2014 presents a playbook for military hybrid activities to change the territorial status quo that could be replicated in the Baltic context. In Crimea, 'little green men', achieved a *fait accompli* by simply removing their insignia and occupying critical government infrastructure. Though territorial grabs by overt means are clearly an act of war, Russia has shown creativity in pursuing such ends using covert tactics in combination with other efforts to obfuscate its actions and disrupt any international response.

Russia's annexation of Crimea in 2014 presents a playbook that could be replicated in the Baltic context

Russia already sows disinformation questioning the legitimacy of certain Baltic territory, for example campaigns claiming Klaipėda never belonged to Lithuania or that Vilnius should not be Lithuanian because it was occupied by Poland between the first and second world wars.[16] The Crimean model applied in these areas would allow Russia to

[13] Matus Halas, "NATO's Sub-Conventional Deterrence: The Case of Russian Violations of the Estonian Airspace," *Contemporary Security Policy* 43, no. 2 (2022): 12.

[14] Halas, "NATO's Sub-Conventional Deterrence," 13.

[15] "Sweden Drones: Sightings Reported over Nuclear Plants and Palace," *BBC News*, 18 January 2022.

[16] Emma Graham-Harrison and Daniel Boffey, "Lithuania fears Russian propaganda is prelude to eventual invasion," *The Guardian*, 3 April 2017.

challenge the status quo with a thin veil of deniability, exacerbating escalatory tensions and threatening national sovereignty and NATO credibility.[17]

2.3. Maritime Threats

Russian military transits and naval exercises in the Baltic Sea, often announced with little lead time, raise tensions and disrupt economic activity. In 2015, Russia declared an exercise zone in Lithuania's exclusive economic zone (EEZ), ordering a ship laying the NordBalt power cable to leave, delaying the project. In another incident in 2018, Russian live-fire exercises took place right outside Latvia's territorial waters and within its EEZ, forcing a partial shutdown of Latvian civilian airspace.[18] These provocations came immediately after Baltic leaders met with US President Donald Trump and days following the expulsion of Russian diplomats in response to the poisoning of former Russian intelligence officer Sergei Skripal in Salisbury, UK. Moscow has reduced its aggressive exercises more recently but remains capable of engaging in such hostilities to send political messages and demonstrate its military capability.

Unexploded ordnance, undersea mines, and chemical weapons from World War II allow conducting hybrid attacks with kinetic means concealed as an accident

Additionally, despite clearance operations along main transit routes, the Baltic Sea hosts vast quantities of unexploded ordnance, undersea mines, and chemical weapons dumped during the two world wars.[19] These offer the hybrid attacker a unique opportunity to conduct covert military activities at sea, targeting civilian or military infrastructure with kinetic means concealed as a mine-related accident.[20]

Lastly, the use of naval capabilities to disrupt or damage undersea lines of communication is another hybrid military threat in the Baltic region. As early as 2018, NATO commanders voiced concern about Russia's capability to sever undersea digital infrastructure.[21] Early in 2022, a Norwegian fibre optic cable running through a strategic waterway in the Barents Sea to Norway's Arctic satellite station on the Svalbard archipelago was mysteriously severed. Russia remains the primary suspect.[22] Similar acts could disrupt Baltic digital information flows on both civilian and military networks. Such acts require military technology and capabilities, and as such threaten regional security.

2.4. Energy and Critical Infrastructure

Russia has used energy blackmail in the past attempting to coerce targeted nations, including the Baltic states, to align with its goals.[23] The Baltic states have taken measures to diversify their dependence on Russian energy and the BRELL agreements, which define the terms and conditions for the continued operation of the Baltic grids as part of the IPS/UPS synchronous frequency grid. One of these measures was the establishment of the Klaipėda liquefied natural gas (LNG) platform in Lithuania. Latvia and Estonia have also announced plans to establish their own import terminals, and efforts are underway to increase the capacity of the Klaipėda terminal, meaning that the Baltic states are likely to achieve independence from Russian gas supply soon.[24]

Russia's covert activities targeting infrastructure abroad, like the sabotage of ammunition depots in Czechia in 2014, indicate the opportunities offered by such high payoff targets to the hybrid attacker.[25] If shrouded with a degree of

[17] Matus Halas, "Proving a Negative: Why Deterrence Does Not Work in the Baltic states," *European Security* 28, no. 4 (2019): 441.

[18] Heinrich Lange, Bill Combes, Tomas Jermalavičius, and Tony Lawrence, *To the Seas Again: Maritime Defence and Deterrence in the Baltic Region* (Tallinn: ICDS, 2019), 15.

[19] Lange et al., *To the Seas Again,* 9.

[20] Lange et al., *To the Seas Again,* A-2.

[21] Magnus Nordenman, "Russian Subs Are Sniffing around Transatlantic Cables. Here's What to Do about It," *Defense One*, 17 January 2018.

[22] Thomas Newdick, "Undersea Cable Connecting Norway with Arctic Satellite Station Has Been Mysteriously Severed," *The Drive*, 10 January 2022.

[23] Lange et al., *To the Seas Again*, 3.

[24] Mateusz Kubiak, "Baltic States Bet on New LNG Regasification Capacities," *The Jamestown Foundation*, 26 April 2022.

[25] Christo Grozev, Pieter van Huis, and Yordan Tsalov, "How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine," *Bellingcat*, 26 April 2021.

uncertainty and executed concurrently with other political and disinformation campaigns, Russia could threaten energy independence in the Baltic region while mitigating the risk of escalation to conventional conflict.

Russia could threaten energy independence in the Baltic region while mitigating the risk of escalation to conventional conflict

2.5. Political Destabilisation Campaigns

The Kremlin relies on covert operatives in its military intelligence service (GRU), SVR, and FSB to challenge the sovereignty of its targets and advance its global political goals. The list of Russian military and state security force involvement in its hybrid campaigns is long and well documented.[26] These include GRU-led assassination missions in the UK and Bulgaria, the kidnapping of an Estonian intelligence official in Estonia, destabilisation campaigns in North Macedonia, Moldova, Montenegro, Estonia, Poland, and Czechia, and the sabotage of ammunition depots in Czechia. Whether deployed to conduct industrial sabotage, recruit and handle sources, carry out assassinations, or facilitate political unrest and riots, Russia's covert military forces constitute the human dimension of Russian hybrid threats in the Baltic region and present a substantial threat to Baltic stability and sovereignty. This threat is particularly acute given the large Russian-speaking population in the Baltic region.

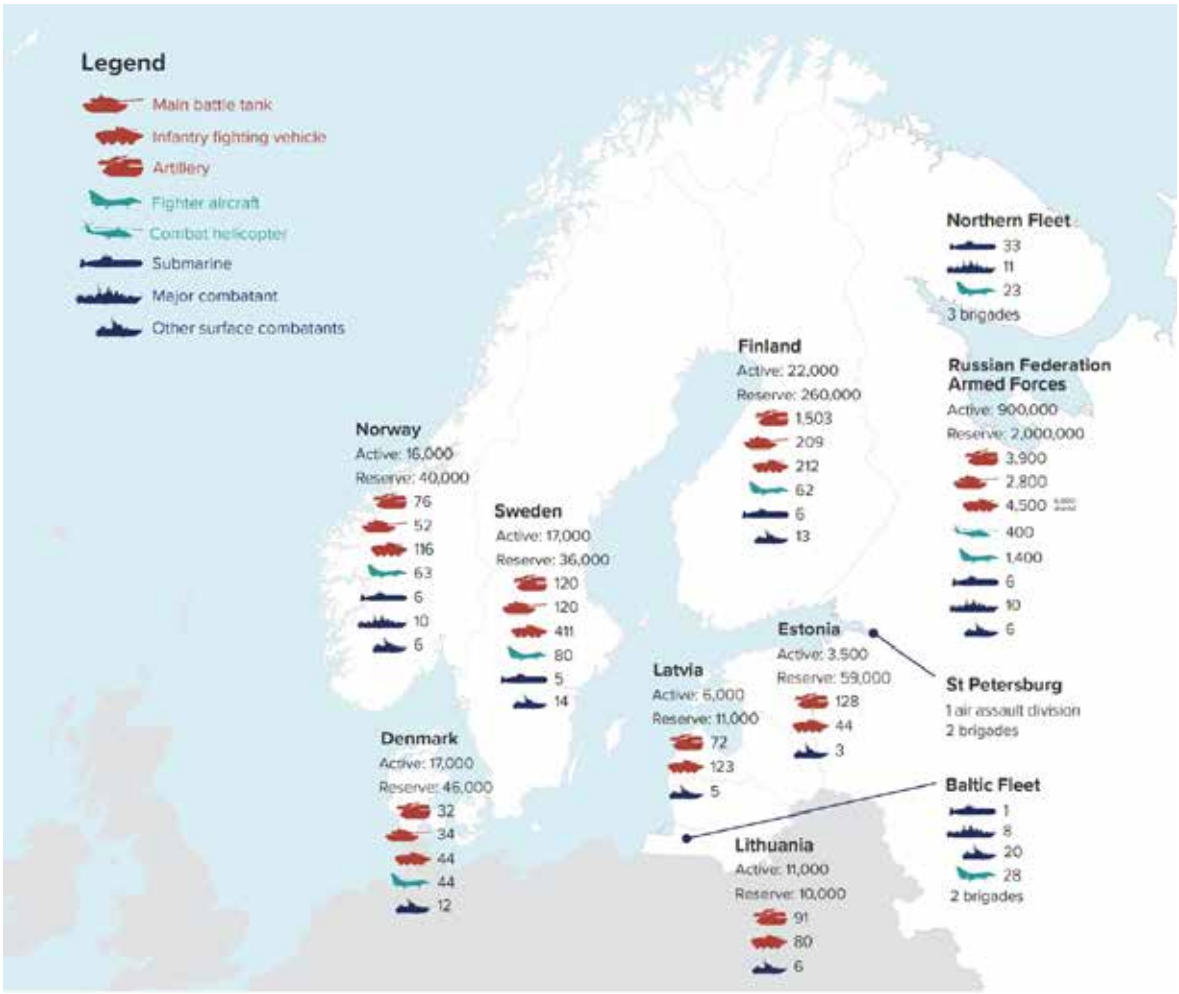

Figure 1. Military power in north-eastern Europe (before Russia's full-scale war in Ukraine). Graphic: CEPA, reproduced with kind permission[27]

[26] Grozev et al., "How GRU Sabotage and Assassination Operations."

[27] Ben Hodges et al., "Close to the Wind."

2.6. Hybrid Threats as a Regional and NATO Challenge

These military hybrid threats present a challenge to NATO. The Baltic states are drastically outnumbered by Russian military capabilities and effectively lack air and naval forces (see Figure 3), thus NATO deploys forces to bolster its defence and deterrence posture on the eastern flank. The flagships of this policy are the Baltic Air Policing (BAP) mission and the enhanced forward presence (eFP) deployments (multinational battle groups in Bulgaria, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, and Slovakia).[28] Any broader regional counter-hybrid policy will thus inevitably involve NATO forces and the Alliance itself.

2.7. Implications of Hybrid Threats

In a militarily unbalanced region, fear of escalation can create a sense of insecurity. A series of airspace violations or increased covert activity could be either routine harassment or a prelude to invasion. The situation in Ukraine illustrates how hybrid action in the form of historic troop build-ups, provocative military exercises, and campaigns intended to sow corruption and erode trust in institutions and government can foreshadow a conventional attack. In the Baltic region, uncertainty about Russia's intentions with regard to individual hybrid actions incites fear that they could quickly expand to something much more serious.

Subthreshold campaigns do not reflect a state of peace between countries, but a state of undeclared war

Beyond the potential risk of overwhelming escalation, hybrid threats also disrupt civilian activity and increase the risk of accidents, especially in the air and at sea. Subthreshold campaigns do not reflect a state of peace between countries, but a state of undeclared war. Although NATO acknowledges the magnitude of these threats, it has largely left responsibility for countering them to the Allies themselves. But the Baltic states (and others) lack the capabilities to counter some continuously disruptive and potentially dangerous military hybrid threats.

3. Towards a More Robust NATO Hybrid Strategy

Countering hybrid threats is regarded as primarily a national responsibility, but there are strong arguments concerning unity and the availability of capabilities that favour a more collective response. Possible multilateral security structures for countering hybrid campaigns in the Baltic region include NATO, the EU, and regional arrangements like Nordic Defence Cooperation and the Nordic Baltic Eight. Of these, the EU has made efforts to curb hybrid attacks and disinformation campaigns using economic and legislative levers, for example in its Joint Framework on Countering Hybrid Threats, its affiliation with the Helsinki-based Center of Excellence for Countering Hybrid Threats, and its creation of the East StratCom Task Force and *EU vs. Disinfo* platform to target disinformation and political interference campaigns.[29] At the national level, countries employ a mix of whole-of-society 'total defence' resilience strategies, denial strategies like territorial defence force generation and training, and prior to Russia's invasion of Ukraine, interdependence strategies, particularly in the energy sector.[30] NATO is best equipped to deal with military hybrid threats, due to the nature of its capabilities and mission.

However, NATO's instruments to deter Russian hybrid campaigns are incomplete. The 2021 Brussels Communique states that hybrid warfare could involve Article 5 of the Washington Treaty, but the definition of 'armed attack' in this context remains vague.[31] Additionally, the 2016 Warsaw Communique

[28] NATO, "NATO's military presence in the east of the Alliance," 8 July 2022.

[29] Lauren Speranza, *A Strategic Concept for Countering Russian and Chinese Hybrid Threats* (Washington, D.C.: The Atlantic Council, July 2020), 9.

[30] Dalia Bankauskaitė, "Lithuanian Total Defense," CEPA, 27 February 2020.

[31] NATO, "Brussels Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 14 June 2021," Press Release (2021) 086, 14 June 2021, para 31.

places responsibility for countering hybrid threats on the nations themselves.[32] Building on the Warsaw statement, NATO's 2021 Brussels Communique repeats the risks associated with hybrid warfare and offers assistance, with NAC approval, in the form of Counter Hybrid Support Team (CHST) deployments to requesting nations.[33] The CHST concept is novel, but leaves room for improvement. The CHSTs consist mostly of policy advisors assembled on an ad-hoc basis, such as when Lithuania was under pressure from the migration flows engineered by Belarus during summer 2021; they are not fully resourced or mandated for planning and response actions.[34] NATO acknowledges the need to "send a message that hybrid activities come at a price that attackers may not be willing to pay," but what activities warrant a response and what price will be imposed remain unclear.[35] Russia employs hybrid warfare precisely because it takes advantage of these seams in NATO policy while avoiding the collective military strength of Alliance members.

Deterrence theory argues that to influence behaviour, your policy must be credible, you must have the capability to implement it, and your target must believe you.[36] Although deterrence by denial strategies are prudent and politically palatable in terms of managing escalatory risks, on their own, they appear insufficient to modify Russian hybrid behaviour which, in the Baltic region, continues undiminished. Deterrence by punishment strategies to mitigate subthreshold military activities are additionally required and would be far more effective.[37] The costs that target states choose to impose for hybrid actions must be communicated to the attacker and must be implemented quickly in the event the action occurs.[38] Unlike traditional nuclear deterrence, where the tolerance for failure is zero, an effective hybrid deterrence policy should take a cumulative approach, seeking to draw down hybrid attacks closer to zero over time.[39] Developing a policy to this effect is a challenging task for a 30-veto player system like NATO, considering the variance in member threat-perceptions and proximity to the problem.

An effective hybrid deterrence policy should take a cumulative approach, seeking to draw down hybrid attacks closer to zero over time

4. A Proposed Hybrid Response Model

This chapter proposes a model to achieve a better balance in hybrid deterrence in the Baltic context. It comprises a framework of potential threat scenarios, and corresponding preventive denial measures and reactive punishment approaches.[40]

4.1. Objectives

The overall aim is to modify Russian behaviour by signalling NATO's commitment to prompt cost imposition in response to hybrid provocations. NATO will need to determine and signal the types of costs it might impose for these provocations and codify them in a more assertive counter-hybrid strategy that incorporates appropriate NATO, bilateral, and national level responses of both preventive denial and reactive punishment.

The model thus includes: a decision-making support framework that organises hybrid

[32] NATO, "Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016," Press Release (2016) 100, 9 July 2016.

[33] NATO, "Brussels Summit Communiqué," para 31.

[34] Franklin Kramer, Hans Binnendijk, and Lauren Speranza, *NATO Priorities after the Brussels Summit* (Washington, D.C.: The Atlantic Council, November 2018).

[35] Michael Rühle and Clare Roberts, "Enlarging NATO's Toolbox to Counter Hybrid Threats," NATO Review, 19 March 2021; Michael J. Mazarr, Arthur Chan, Alyssa Demus, Bryan Frederick, Alireza Nader, Stephanie Pezard, Julia A. Thompson, and Elina Treyger, *What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression* (Santa Monica: The RAND Corporation, 2018), 73.

[36] Michel R. Matheny, "Employing Military Force in the 21st Century," *Parameters* 47, no. 2 (2017): 33.

[37] Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression below the Threshold of Major War* (Santa Monica: The RAND Corporation, 2019), 130, xvii.

[38] Halas, "NATO's Sub-Conventional Deterrence," 5.

[39] Halas, "NATO's Sub-Conventional Deterrence," 4.

[40] Kramer et al., "NATO Priorities after the Brussels Summit."

military provocations by their intensity; and a policy framework that provides both preventive denial strategies and reactive cross-domain punishments for potential hybrid attacks.

NATO will need to determine and signal the costs and codify them in a more assertive counter-hybrid strategy

4.2. Deterrence Framework

First, we classify hybrid attacks by level of intensity. Figure 2 displays the space between wartime and peacetime activities in which hybrid attacks occur. As a simple example, a Russian aircraft flying with its transponder off in violation of airspace norms might be considered a low intensity hybrid activity, while a significant troop build-up along the Latvian border might be considered a high intensity activity.

By adopting a deterrence by punishment strategy, NATO will create a lower threshold for responding to hybrid challenges. In doing so, it will have a mechanism to signal clear costs to hybrid aggressors and deter and reduce the number of hybrid attacks, particularly high intensity activities for which there could be harsher retribution.

The second form of response (the bottom green arrow) depends on deterrence by denial and resilience building efforts. Here, NATO can support efforts to curb the effectiveness and impact of hybrid attacks, making them, particularly lower intensity attacks more manageable, limiting their damage on target states and deterring aggressor states who realise such efforts have minimal effectiveness.

Figure 2 shows how the approaches together push towards the expected result in which

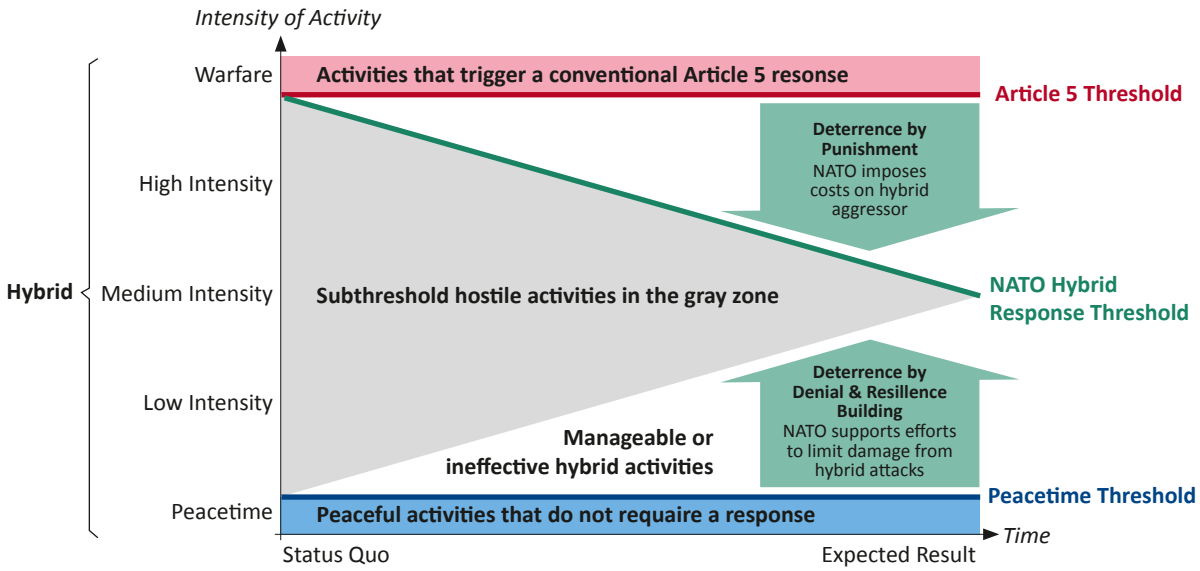

Figure 2. Deterrence Framework. *Source*: Hybrid CoE (adapted by the authors)[41]

We then propose two forms of deterrence response. The first (the upper green arrow) relies on NATO deterrence by punishment efforts to impose costs on aggressor states carrying out subthreshold actions. While NATO acknowledges that hybrid warfare could trigger an Article 5 response, below this threshold, it has few ways to respond to grey zone aggression.

a new NATO hybrid response threshold is established, and the number of grey zone activities is reduced through deterrence by punishment and deterrence by denial while resilience building steps render other hybrid attacks ineffective.

[41] Vytautas Keršanskas, "DETERRENCE: Proposing a more strategic approach to countering hybrid threats," *Hybrid CoE Paper* 2 (March 2020).

	Intensity Tier	Low	Medium	High
Legality	Sovereignty & Territorial Threat	Tests reponses to defending sovereignty and territorial integrity	Contests or threatens sovereignty and territorial integrity	Blatantly violates sovereignty or territorial integrity
	International Law	Does not clearly violate international law but may break various norms	Exists in international legal grey zone	Violates international law, even if in a manner that often does not cause consequences
Escalation Risk	Perceived Intent	Create minor increases in target states' threat perception	Causes instability in the target state or threaten further escalation or military action	Appear to be pretense for significant escalation or major military action
	Urgency	Ongoing pattern of activity that has not escalated	Escalatory behavior that warrants a prompt response, including behavior that escalates from previous patterns of hybrid action	Demands immediate, prompt response, particularly binary choices in response
Civilian Impact	Impact on Civilian/ Commercial Activity	Has minor impact on civilian and/or commercial activity	Briefly disrupts civilian and/ or commercial activity in the region	Created widespread disruptions of civilian and/or commercial activity
	Risk of Accidents	Poses no to minor risk of accidents with peacetime and/ or civilian activities	Creates plausible risk of accidents with peacetime and/ or civilian activities	Creates significant risk of accidents with peacetime and/ or civilian activities

Table 1. Intensity Classification

Intensity Tier	Aggression Examples	Denial/Resistance Options	Punishment/Reaction Options
Low	• Airspace: violate norms • Maritime: significant troop transits through the Baltic Sea • Energy: threaten to disrupt oil/gas flows • Telecomms: suspicious activity near undersea communications cables; interruptions of communication lines • Territorial: movement on the Curonian Spit on Lithuanian border, increased border crossings into Estonia, Latvia • Covert: intelligence gathering, surveillance and reconnaisance activity in NATO territory"	• Increase NATO eFP troop deployments • Expand mission of existing forces • Prioritize NATO ISR capabilities in the Baltics (could begin a contract bidding process w/ no commitment) • Deploy NATO SOF to train and advise security forces in counter-intelligence and interagency coordination	• Escort troops moving through Baltic Sea • Issue public statement condemning aggressor • Call in ambassador • Track, aggregate, and report hybrid attack incidents regularly at national and NATO level • Deny visas to Kaliningrad residents in Lithuania • Conduct information operations via billboard on rail route from Belarus to Kaliningrad • Offer support to partisan hacking groups in Russia and Belarus
Medium	• Airspace: ADIZ violations, GPS interference, drone crashes • Maritime: snap naval exercise • Energy: interrupt BRELL grid • Telecomms: cut internet cable w/ plausible deniability • Territorial: snap military exercise near border	• Purchase greater air defense and ISR capabilities • Invest in more robust telecommunications and energy infrastructure • Expand BAP to Baltic Air Defense which would loosen rules of engagement • Enhance NATO air-power presence and activity in Europe • Conduct Article 4 consultations to bolster air defense capabilities and national policy • Increase frequency of large-scale NATO and national military exercises	• Disclose intelligence reports or Russian violations • Deploy NATO naval forces to the Black Sea in line with the Montreux Convention • Deploy standing maritime groups to escort Russian naval units • Refuse to make payments to Russia for oil and gas • Expel diplomatic staff • Interdict Russian seaborne commerce • Disrupt Russian mining operations abroad • Disrupt Russian windfarm operations on the Kola peninsula • Expel family of Russian officials from Western institutions and universities
High	• Airspace: erritorial incursion, unpiloted or piloted overflights of critical infrastructure... • Maritime: submarine incursions • Energy: cyber and drone attack on energy infrastructure (LNG), block access to LNG terminals • Telecomm: large-scale disruption of national communications infrastructure • Territorial: significant border troop buildup	• Begin permanent basing of NATO forces in the Baltic states and increase deployments (upgrade from eFP) • Accelerate efforts towards energy independence	• Carry out offensive cyberattacks against adversary energy or telecommunications infrastructure • Run snap exercises using deployed NATO or national troops • Deploy NRF to assist targeted Allies • Publish firm air defense policies and shoot down drone/aircraft infringing on territorial airspace • Quarantine Russian rail movements to Kaliningrad

Table 2. Prototype Response Matrix

4.3. Prototype Response Matrix

We next propose a framework for categorising the intensity of an attack based on six different factors. The factors are grouped into three categories. The first category looks at legal challenges and the extent to which a hybrid attack threatens a state's sovereignty or territory and violates international law. The second looks at escalation risks based on the aggressor state's perceived intent and degree of urgency with which the target state must respond to the hybrid challenge. The third category examines civilian impact, specifically whether an attack disrupts civilian and commercial activity or raises the risk of accidents. Together, they provide a methodical approach for categorising any given grey zone activity as low, medium, or high intensity. This intensity classification provides a basis for determining appropriate responses, even against novel and unforeseen threats.

Table 2 is a prototype response matrix. It provides examples of actions that would fall into each intensity level, derived from interviews and literature.[42] These examples are drawn from several major risk areas (airspace and maritime threats, telecommunications isolation, maritime disruption and isolation, territorial incursions, and covert action) that are neither mutually exclusive nor collectively exhaustive.

The third and fourth columns provide a menu of appropriate deterrence by denial and deterrence by punishment options. These options should be implemented in concert with continued efforts at diplomatic dialogue aimed at reducing the threat of hybrid activity – such efforts fall outside the scope of this prototype.

4.4. Addressing the Risk of Escalation

Kokoshin et al. add to the growing body of analysis detailing how Russian military experts think about modern warfare and conflict escalation and de-escalation. Table 3 below illustrates the 17 rungs of Kokoshin's escalation ladder. According to this, information confrontation, grey zone activities in competition and crisis, and hybrid methods in war are relevant at the lower rungs prior to the employment of military force. So-called hybrid war, the fourth rung, has long been a topic of discussion in Russian military discourse as a way of describing US and Western actions to weaken and undermine unfriendly countries.

The deterrence-by-punishment options proposed in our counter-hybrid model aim to maintain escalation below the 6th rung, or the conventional threshold. Some options involve kinetic action, which may appear to cross this threshold, but the literature on deterrence theory offers some clarity in this regard: Morgan et al. argue that deliberate escalation can be used as a deterrent while making every effort to avoid inadvertent or accidental escalation. In some cases, deliberately escalatory actions are taken not because of the direct results expected from them but, rather, to send a signal to the opponent (or to a third party) about what further escalation might occur in the future.[43] The essence of this approach, known as suggestive escalation, is to communicate to the opponent that costly escalation will occur in the future in response to the behaviour to be deterred or in the event that the adversary does not comply with certain demands. Sometimes, merely issuing an explicit threat is escalatory; in other cases, suggestive escalation involves taking physical action, which may include using armed force.[44]

Cost imposition does not automatically lead to conflict escalation

Several past confrontations with Russia have reached the 5th rung of escalation without crossing the threshold into conventional war. In 2015, a Russian Su-24 violated Turkish airspace and was hit by air-to-air missiles fired by Turkish F-16s.[45] And in February 2018, US troops in Syria engaged in a four-hour-long

[42] Halas, "Proving a Negative," 431–48; Piotr Szymański, "Towards Resilience in 2030: NATO Allies and Partners in the North-East of Europe," in *Towards #NATO2030: The Regional Perspective of the Baltic States and Poland* ed. Māris Andžāns and Mārtiņš Vargulis (Riga: Latvian Institute of International Affairs, 2020), 140; Justin Sherman, "Cord-Cutting, Russian Style: Could the Kremlin Sever Global Internet Cables?" *The Atlantic Council*, 31 January 2022; Lange et al., *To the Seas Again*, 14-17; Halas, "NATO's Sub-Conventional Deterrence," 1–32.

[43] Forrest E. Morgan, Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica: The RAND Corporation, 2008), 42.

[44] Forrest et al., *Dangerous Thresholds*, 42.

[45] "Turkey Shoots Down Russian Warplane on Syria Border," *BBC News*, 24 November 2015.

Diplomatic	1	Aggrevation of the situation, including information confrontation or operations, economic sanctions
	2	Exchange of threatening statements about the possible use of military force
Grey Zone	3	Political crisis with an increased intensity of information confrontation, demonstrations of military force in the grey zone without combat use
	4	Hybrid war, limited combat use of military force along with the large-scale use of political, informational, economic, and other means
	5	Intentional or unintentional provocation (incident) in the interaction of great powers, which caused deaths and serious damage to military equipment
Conventional	6	Local conventional warfare with limited political goals of the opposing sides and limited use of military force in time and place
	7	Regional war with combat operations on land, air, sea without destroying spacecraft, with combat cyber operations
	8	Limited conventional warfare with defeat on one scale or another of spacecraft without destroying satellites of the missile attack warning system
	9	Large-scale conventional war without destroying large urban centers, chemical industries, nuclear power plants, etc.
	10	Large-scale conventional war with combat cyber operations to disrupt the state administration system and destroying important civilian infrastructure
	11	Conventional war with the disruption of large urban centers, with the destruction of chemical industries and nuclear power plants
Nuclear	12	Nuclear conflict, use of nuclear weapons as an instrument of direct political and military pressure
	13	Destruction of SSBNs of one of the great powers
	14	Demonstration use of nuclear weapons in a desert area
	15	War with the limited use of nuclear weapons against military facilities
	16	War with the use of strategic nuclear forces in a counterforce operation
	17	War with the massive use of nuclear weapons and other types of weapons of mass destruction

Table 3. Russian Escalation Ladder[47]

battle with Russian mercenaries from the Wagner Group which resulted in substantial personnel and equipment loss for the Kremlin-backed forces.[46] While these incidents are not prime examples of deliberate escalation, they do support the argument that cost imposition does not automatically lead to conflict escalation. In both cases, Russian behaviour changed as increasing the costs was likely directly linked to decreasing risk appetite.

4.5. Evaluation

Given the breadth of hybrid means and their targets, measuring the progress of a new NATO counter-hybrid strategy would require additional information sharing and coordination between Allied governments, the EU, private enterprise, and academia. This would be best accomplished in an opt-in coalition-style fusion cell that could be co-located with the Hybrid Centre of Excellence in Helsinki, or in Brussels. Torossian et al. offer a simple set of system-level metrics that span the elements of national power and offer a model that a future hybrid fusion cell could emulate.

To arrive at their assessment of hybrid trends, Torossian compiled data from a series of open sources, including the Uppsala Conflict Data Program, aviation and maritime tracking sites, the Integrated Crisis Early Warning System dataverse, national ministries of foreign affairs, NATO releases, and think tanks. These include metrics on the number of actors involved in proxy conflicts, military exercises and troops involved near international borders, numbers of reported air and sea incursions, and cyber attacks on critical infrastructure. They also assessed compliance with international rules and norms.[48]

An expanded hybrid fusion cell could replicate these methods. With a physical space for opt-in information sharing, these methods could

[46] Thomas Gibbons-Neff, "How a 4-Hour Battle between Russian Mercenaries and U.S. Commandos Unfolded in Syria," *The New York Times*, 24 May 2018.

[47] Clint Reach, "*Review of Escalation and Deescalation of Crises, Armed Conflicts, and Wars*," *NATO Defense College Russian Studies* (March 2022).

[48] Bianca Torossian, Lucas Fagliano, and Tara Görder, "Hybrid Conflict Neither war, nor peace," *Clingendael Strategic Monitor 2010-2020,* (January 2020).

Outcome	Indicator	Target	Means of Verification
Decreased airspace violations with deactivated transponders	Number of reported airspace incursions over period of time following implementation	Reduce by 25%	Estonian Air Navigation Services
Decreased number of troops involved in provocative border exercises	Number of military forces involved in coercive military exercises	Reduce by 25%	Commercial satellite imagery, NATO member intelligence sharing
Decrease number of GRU operatives in NATO countries	Number of espionage convictions increases	Increase convictions by 10%	NATO member justice ministries statements, media reports
Increase predictability of snap naval exercises	Lead time in announcements of naval exercises increases	Increase lead time by 7 days	Russian media, foreign affairs ministerial statements

Table 4. Campaign evaluation plan

also be enhanced to capture real-time data to guide decision making at the national and NATO levels.

NATO could also conduct a campaign-perspective approach to evaluation. Using a combination of process tracing, case study analysis, and expert judgment, NATO leaders could evaluate the extent to which its counter-hybrid deterrence strategy is affecting opponent behaviour. An example of this approach is offered in Table 4.

Conclusions and Recommendations

Russia's full-scale invasion of Ukraine demonstrates that hybrid warfare is not just a substitute for conventional war but may also be a precursor to it. However the war ends, Russia will endeavour to regain lost credibility and demonstrate that other critical targets have not lost its attention. The EU and NATO should expect both more and more innovative Russian hybrid activities, especially against vulnerable members, such as the Baltic states. To make more efficient use of existing and future capabilities and to show resolve in the face of these threats, we recommend a more collective western response; and specifically that NATO begin developing a counter-hybrid strategy.

Russia will endeavour to regain lost credibility and demonstrate that other critical targets have not lost its attention

We further recommend that NATO should use a flexible model to assess the intensity of hybrid actions and develop appropriate deterrence by punishment strategies and proactive denial measures. We propose such a model above. This approach would both ensure credibility and aid in maintaining the strategic ambiguity that some concerned Allies will likely desire. Signalling to Russia that it will face concrete consequences if its destabilising behaviour is unchanged would allow NATO to mitigate the risks associated with Russia's hybrid campaigns against the Baltic states and elsewhere. This should lead to a change in Russian behaviour in NATO's favour.

RECENT ICDS PUBLICATIONS

REPORTS

Teperik, Dmitri, Solvita Denisa-Liepniece, Dalia Bankauskaitė, and Kaarel Kullamaa. ***Resilience Against Disinformation: A New Baltic Way to Follow?***. October 2022.

Jermalavičius, Tomas, Max Bergmann, Peter Crail, Thomas O'Donnell, Tomas Janeliūnas, and Tõnis Idarand. ***Developing Nuclear Energy in Estonia: An Amplifier of Strategic Partnership with the United States?***. September 2022.

Arjakas, Merili, Hille Hanso, Kristi Raik, Peeter Raudsik, and Vladimir Sazonov. ***Estonia's Co-operation with the EU's Southern Neighbourhood: Strategic Objectives and Focus***. August 2022.

Jermalavičius, Tomas, Tomas Janeliūnas, Andrian Prokip, Iliya Kusa, Alan Riley, Pier Paolo Raimondi, Andrei Beliy, and Miguel Sainz de Vicuña. ***Geopolitics of Europe's Hydrogen Aspirations: Creating Sustainable Equilibrium or a Combustible Mix?***. May 2022.

Haugevik, Kristin, Piret Kuusik, Kristi Raik, and Niels Nagelhus Schia. ***Small States, Different Approaches: Estonia and Norway on the UN Security Council***. November 2021.

Teperik, Dmitri, Grigori Senkiv, Dmytro Dubov, Oleh Pokalchuk, Illia Miroshkin, Oksana Iliuk, Anastasiia Apetyk, and Larysa Snihur. ***Resilient Ukraine – A Delicate Mosaic? Society, Media, Security, and Future Prospects.*** November 2021.

Stoicescu, Kalev, with contributions from Tatiana Kastouéva-Jean, Liana Fix, Artūrs Bikovs, Agnieszka Legucka, and Keir Giles. ***Dialogue with Russia. Russia Needs to Reset Relations with the West.*** June 2021.

BOOKS

Raik, Kristi, Frank Jüris, and Bart Gaens, eds. ***Nordic-Baltic Connectivity with Asia via the Arctic: Assessing Opportunities and Risks***. Tallinn: ICDS Estonian Foreign Policy Institute, 2021.

POLICY PAPERS

Klyszcz, Ivan U. K. "**Russia's Federal Subjects at War: Background and Implications**." October 2022.

Blockmans, Steven, and Kristi Raik. "**Ukraine's Path to EU Membership: How to Turn a Geopolitical Necessity into a Viable Process**." June 2022.

Shestopalova, Alona. "**Forgotten and Potentially Vulnerable: Why the Online Activity of Middle-Aged Women Matters During Global Information Warfare**." April 2022.

Denisa-Liepniece, Solvita, and Dmitri Teperik. "**Local Russian-language Journalism in the Baltics: Challenges and Perspectives for Building Resilient Communities of Media Professionals**." March 2022.

Raik, Kristi, Frank Jüris, Aimar Ventsel, and Tõnis Idarand. "**Estonia's Interests and Opportunities in the Arctic.**" June 2021.

ANALYSES

Juurvee, Ivo. "**Civil Defence in Ukraine: Preliminary Lessons From the First Months of War**." November 2022.

Värk, René. "**Russia's Conduct of Hostilities in Ukraine**." November 2022.

Värk, René. "**Russia's Legal Arguments to Justify its Aggression against Ukraine**." November 2022.

Heins, Jonas. "**Putin and Assad, Partners in Crime: Why Russian Forces Steal Wheat from Ukraine**." November 2022.

Gretskiy, Igor. "**A War of the Final Soviet Generation: Russia's Demography, Society, and Aggression Against Ukraine**." August 2022.

Crippa, Lorenzo. "**From Rome to Kyiv, Passing Through Moscow: Russian Strategic Narratives in the Italian Public Discourse on Ukraine**." April 2022.

Gowan, Richard. "**Estonia in the Security Council: A History in Three Crises**." March 2022.

Weitz, Richard. "**NATO's Hypersonic Challenge**." February 2022.

Lawrence, Tony. "**Command and Control for the CSDP: A Permanent Operation Headquarters for the EU?**" ICDS Analysis, January 2022.

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


ICDS.Tallinn


@ICDS _ Tallinn


ICDS-Tallinn


www.icds.ee

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

ISSN 2228-2068