Norwegian Institute of International Affairs

POLICY BRIEF – 9 / 2024

Differentiating Hybrid Threats against the High North and Baltic Sea regions

Per Erik Solli

Brief Summary

Russia's grey-zone threats and actions are a major concern for bordering countries who are on the receiving end of such actions, both physical and cyber.

NATOs policy is that the member nations are responsible for building resilience and responding to hybrid threats or attacks.

To avoid invalid interpretations or paralysis in assessment and response to such complex and diverse threats, they should be differentiated and dealt with separately rather than boxed into a wide cognitive basket.

In the High North, relations with Russia have significantly deteriorated since 2014 as a spillover effect of the Russian interventions and the war against Ukraine and the Western states' collective responses to these aggressions. So-called hybrid threats and actions have also contributed to these strained relations. In the western world, international and national institutions and academia normally assess and describe hybrid concepts either as disruptive and orchestrated actions by state and/or non-state actors with a wide range of agendas or as a category of threats between uneventful peace and full-fledged war. The two main categories of hybrid concepts in the western sphere are hybrid warfare and hybrid threats, although there are no set definitions for either term.

The Russian framing of national political and societal turbulence includes a narrative on how western states facilitate so-called 'color-revolutions'. According to official Russian rhetoric these movements are allegedly sparked by deliberate

western multi-faceted campaigns rather than internal domestic discourses and initiatives. Russian officials regularly accuse NATO states of being dominated and influenced by the USA and under centralized control by NATO. In reality, NATO has a decentralized strategy of countering hybrid threats and their impact on societal security. Countries impacted by hybrid threats are responsible for countermeasures. Also, hybrid treats are almost absent in official U.S. strategies and priorities.

This policy brief elaborates on western definitions of hybrid concepts, presenting how these concepts are articulated by NATO and the USA. It documents how hybrid threats impact some of the states bordering Russia in the High North and the Baltic Sea region, and assesses ambiguities related to counterstrategies and operational responses.

Western Hybrid Concepts

Hybrid warfare as a theory and term in military strategy was coined by Frank Hoffman in 2007. At the time, several analysists were attempting to explain the success of Hezbollah in the battle with Israeli military forces in Lebanon in 2006. Hoffman pointed out that Hezbollah gained a superior position through a simultaneous and mixed application of regular and irregular warfare combined with an effective international information campaign. The term hybrid warfare was new, but historians pointed out that this combination of warfare methods had occurred many times before. While there is no universally agreed definition, understanding hybrid warfare is crucial for addressing contemporary and future security challenges. Hybrid warfare involves an interplay or fusion of conventional and unconventional instruments of power and tools of subversion. These elements are blended in a synchronized manner to exploit the vulnerabilities of an adversary and achieve synergistic effects, both at the strategic and operational levels.

Hybrid threats is a more contemporary term and is normally framed in grey zone scenarios, situations short of regular warfare, and are applicable if an adversary does not want to trigger NATO's article 5 and a collective defense response. The anonymous "green men" and the multifaced Russian swift takeover of the Crimea peninsula in 2014 was a trigger to put so-called hybrid threats on the agenda in NATO, the EU and western states. According to the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), hybrid threats refer to actions conducted by state or non-state actors who combine overt and covert military and non-military means to undermine hybrid threats or harm a target. The goal is to achieve specific political objectives. NATO defines hybrid threats as "harmful activities planned and carried out with malign intent". These threats aim to undermine a target, such as a state or an institution, through a variety of combined means.

Hybrid threats and actions include disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and the use of regular forces. The goal is to blur the lines between war and peace, destabilize societies, and sow doubt in the minds of target populations. In addition, there are maritime hybrid threats and actions that include sabotage against gas pipelines and communications cables on the seabed.

NATO's decentralized approach to hybrid warfare and threats

NATO's Strategic Concept of 2010 did not mention any type of hybrid concepts, but in the 2022 version various hybrid tactics are depicted seven times in relations to the activities of Russia and China. NATO clearly points out that "the primary responsibility to respond to hybrid threats or attacks rests with the targeted country". Thus, an important part of the approach is to strengthen national resilience in NATO member states, and if requested NATO can offer additional assistance, for example with counter-hybrid support teams.

In the aftermath of the illegal annexation of Crimea, the alliance stated in 2016 that "hybrid actions against one or more Allies could lead to a decision to invoke Article 5 of the North Atlantic Treaty". NATO has developed a strategy to counter hybrid warfare with three main elements: prepare, deter, defend.

However, NATO member nations for the most part face non-military hybrid threats far short of the Article 5 threshold. Thus, collaboration with other organizations with a wider mandate and role has become important, such as the EU and various civilian institutions. Finland established an international, autonomous network-based organization promoting a whole-of-government and whole-of-society approach to countering hybrid threats. The Hybrid Threats Centre of Excellence (Hybrid CoE) in Helsinki was inaugurated in October 2017 by NATO Secretary General Jens Stoltenberg and EU High Representative for Foreign Affairs and Security Policy/Vice-President of the European Commission Federica Mogherini. The Centre is an

initiative of the Government of Finland, and a Joint EU/NATO Declaration in 2016 explicitly stated that both EU and NATO member states would be encouraged to support the center. Currently 35 nations are participating states in the Hybrid CoE.

Hybrid warfare and threats in U.S. documents and programs

The USA is a member of the Hybrid CoE, but the topic has not been high on the agenda in NATO's most powerful state. Hybrid warfare or threats are not mentioned in the 2015, 2017 and 2022 versions of the U.S. National Security Strategy, nor in the National Military Strategy documents of 2015/2018/2022. In the U.S. National Defense Strategy of 2022 "hybrid" is mentioned only once related to strengthening resilience in states on Europe's eastern flank. The White House published a National Strategy for the Arctic Region in 2022, and the Department of Defense and several of the military services have recently published their own strategy documents for the Arctic. Hybrid threats and warfare are not mentioned in any of the American strategy documents related to the Arctic/ High North.

The Multinational Capability Development Campaign (MCDC) is an international military program lead by the U.S. Joint Staff with a partnership of 24 countries and international organizations (IGOs). Most of the partners are from Europe and some from the Asia-Pacific region. The program runs a series of two-year development projects to address urgent needs. From 2013 to 2024 a total of 51 projects were approved by the multinational board, and only three of them were related to hybrid warfare and threats (in the 2015-2020 period). Hybrid warfare and threats are thus not high on the agenda in this multinational forum with a large number for NATO-members. While other topics are higher on the agenda, nations neighboring Russia still face challenges every year related to hybrid threats.

Russian hybrid threats and actions in bordering states

All NATO and EU states are vulnerable to digital/ cyber hybrid threats, but geography matters regarding physical hybrid threats and actions. Estonia, Finland, Latvia and Norway are among the border states to Russia, and all encounter various hybrid threats and actions on a regular basis. In addition, Lithuania and Poland have borders to the Kaliningrad Oblast, a highly militarized Russian enclave by the Baltic Sea. The mix of challenges in the hybrid format targeting the border states include ad hoc forward deployments of offensive weapons and occasional episodes of Russian military aircraft harassing western military aircraft operating in international airspace. The states in the High North and Baltic regions also face frequent cyber-attacks, the staged outflow of migrant asylum seekers across the border from Russia, GPS-jamming in the border areas, war memorial campaigns, and so-called troll-factories conducting disruptive campaigns of disinformation and propaganda in social media channels. In the Baltic Sea region there have been instances of harassment of western naval ships and, and a few border violations by Russian military aircraft.

Norway and Finland have occasionally experienced large groups of non-Russian refugees massing in the area across the border stations to Russia. In the fall of 2015 over 5000 refugees, many without papers, massed in Russian towns near Norway and subsequently appeared at the Storskog border station. The large flow of asylum seekers saturated local and regional institutions, and the federal government had to assist with additional resources. Russia denied accusations of a deliberate campaign, but interviews of refugees revealed an organized operation on the Russian side. Due to a similar massing of refugees close to their border, Finland closed all border crossings to Russia late 2023 to prevent a similar situation as Norway experienced eight years earlier. Storskog in Norway is currently the only entry point of Russians into the Schengen area, but several restrictions are in place. The challenge of flocks of asylum-seeking refuge has not reoccurred at Storskog.

In Norway, airlines and other agencies have since 2016 registered disruptions of GPS signals in Finnmark in the area close to Russia. Disturbances normally occurred in conjunction with military exercises in Russia and were detected only a few days a year up until 2021 (maximum 20 days a year). In 2022, GPS jamming occurred more frequently and was detected in 122 days of the year. In 2023 the disturbances occurred almost daily (294 days), and the frequency is very high in 2024. Finland and the Baltic States have also seen a sharp increase in GPS jamming since 2023, both in frequency and size of the affected areas.

However, the previous and ongoing jamming of navigational satellite signals are not necessarily

a part of a harassment strategy. GPS and other forms of electronic jamming are used daily for self-protection in zones of armed conflict such as the Middle East and Ukraine. Russia also regularly disturbs navigational satellite signals near their main military bases to obstruct drone and missile attack, also as far north as the Kola peninsula. Some experts have assessed GPS jamming as strategic political signaling, but it has previously also appeared in conjunction with unit training and exercises, and now almost regularly after 2022, as an air defense method at the tactical level.

However, when jamming is applied at Russian military base areas close to the border of other states, the side effects are a major problem for civilian users of GPS, including the emergency services. Norway and other states have for years addressed Russian authorities to explain the significant implications of cross border jamming for the civilian users, but without success. Thus, the only current fallback option for border states is to adapt and enhance resilience. For example, civilian airlines operating in Northern Norway and Finnmark county have implemented procedures and technical solutions to neutralized vulnerabilities related to GPS jamming.

Hybrid Ambiguity

While states bordering Russia face activities labelled 'hybrid threats' and are largely responsible for dealing with them themselves, they also face the challenge of interpreting such threats and crafting a suitable 'counter-hybrid response.' Attribution is often a challenge concerning several types of hybrid threats. Moreover, it can be difficult or impossible to determine if simultaneous events are staged by one actor or if several actors are involved. Even if diverse actions can be attributed to a singular state or non-state actor, a central question in the analysis remains; is this an orchestrated (hybrid) campaign or just several independent initiatives? A possible pitfall resulting from the high attention to hybrid concepts is that actors become cognitively preprogrammed with the notion of an orchestrated (Russian) hybrid threat campaign and thus assume that an emerging case is in this category. Even if it is probable, it might not be a correct conclusion in all cases.

Mindful of such a pitfall, a senior official in the NATO Headquarters has stated that we have to stop labeling phenomena we do not understand as hybrid threats. Instead of military or civil institutions using hybrid concepts as a collective cognitive basket for almost every type of challenge, an alternative strategy is to work piecemeal. Such a strategy would imply dealing separately with the issues at hand. In cases such as border violations attribution is plausible, the roles and responsibilities for crafting a response are clear, and a counter reaction is possible to determine. On the other hand, in cases such as influence operations in social media, attribution is a major challenge and building resilience may be the only reasonable response. A case-by-case strategy is also more suited to avoid invalid interpretations of attribution, intent and objectives. Thus, differentiating hybrid threats and employing a diversified strategy can be more valid than a holistic approach to threats and actions that are disparate and may or may not be interrelated.

Per Erik Solli is Senior Defence Analyst in NUPIs Research group on security and defence. Solli also has a position as Senior Adviser at Nord University.

This brief is part of the project 'Norway as an in-between for Russia: Ambivalent space, hybrid measures' financed by the Norwegian MoD. It has been edited by NUPI Research Professor Julie Wilhelmsen.

NUPI Norwegian Institute of International Affairs

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from shortterm applied research to more long-term basic research.

NUPI
PB 7024, Pilestredet Park 18, 0176 Oslo, Norway
post@nupi.no | nupi.no

Photo credit: NTB