Troubled Waters: Can Civil-Military Cooperation Prevent Hybrid Conflict in the Baltic Sea States?

31 OCTOBER 2026

Harriet Lannerö



Photo by Ant Rozetsky on Unsplash

Introduction

Since the 1990s, the importance of Civil Military Cooperation (CIMIC) has become increasingly clear. We need only consider the examples of Kosovo, Bosnia and East Timor (Rehse, 2004) that have highlighted time and again how cooperation and coordination between the military and civilian organisation has significant potential to reduce harm to civilians and support long-term stability (CCOE). During any conflict, above or below an Article 5 threshold, combat and fighting only contribute to around 7% of activity, with the other 93% delivered by CIMIC (Roberts, 2025). With war once again on Europe's doorstep, CIMIC must receive the same level of attention

as rearmament itself, especially since the conflict landscape has changed so drastically.

Hybrid Threats

Hybrid threats represent a new type of warfare that combines both military and non-military methods. They can originate from both state and non-state actors who target political institutions, influence public opinion and undermine the security of NATO citizens (NATO, 2026). This is problematic because hybrid threats tend to target societies, not combatants, hence why a policy of 'Total Defence' is required to combat them. Epitomised by deception and sabotage, hybrid threats facilitate the use of new tools, such as social media or targeting digitalised infrastructure (Nilsson et al., 2021). From cutting undersea cables vital to our power sources and communication, to sowing disinformation designed to erode trust in our institutions, these chaos attacks point to a deliberate hybrid campaign with Russia as the prime suspect (Lawrence, 2025). The 'complexity landscape', where power is shifted from state institutions to commercial ownership, is a symptom of the lack of trust and breakdown of the relationship between state and society (Lawrence, 2025). Critically at risk is the Baltic Sea region, which has emerged as one of the world's most contested maritime spaces following Russia's invasion of Ukraine. With the accession of Finland and Sweden to NATO, an unprecedented situation has emerged where the Baltic Sea is now almost entirely surrounded by Alliance members, creating a 'NATO lake' as it has been affectionately dubbed. Securing the Baltic region means securing Europe's northern flank, protecting critical trade routes, and demonstrating the collective resolve of democratic nations against authoritarian aggression (Pribyl, 2026). Today, it is essential that the Baltics Sea States employ CIMIC as tool of deterrence and preparedness, ultimately to mitigate the risk of escalation, as seen with the Total Defence policy Sweden has demonstrated where all sectors of civil and military society collaborate to maintain sovereign security of herself and her allies (Government Offices of Sweden).

Threats to Undersea Cables

Firstly, undersea cables have repeatedly been targeted in Russian attacks such as the "Balticconnector" between Finland and Estonia on the 8th of October 2023 (Loik, 2024). At a similar time, undersea communication cables between Sweden-Estonia and Finland-Estonia were also damaged (Loik, 2024). Such attacks have thus far not been especially consequential in and of themselves, however they do pose a critical risk if submarines or other maritime vessels of the Russian Federation would be prepared to conduct a coordinated attack on undersea cables in the event of an escalation of conflict. The UK Ministry of Defence estimates that approximately 99% of global internet traffic operates through undersea cables, making it

a lucrative target for anyone seeking to do Europe harm (Loik, 2024). It is likely that the war in Ukraine is going to keep Russia's conventional forces tied up for some further years, meaning that the exploitation of asymmetric advantages will remain a lucrative doctrine (Muuga et al., 2024). Furthermore, undersea infrastructure provides the cover of plausible deniability as surveillance is near impossible, not to mention hugely expensive to repair. Undersea infrastructure is also not a feature of Russian global data transmission, meaning the risk of a mirrored Western counterattack is low. While all of the cases of undersea tampering have so far been alleged, high-ranking Russian officials, including Dmitry Medvedev himself, have emphasised that should Europe continue involvement in the Russia-Ukraine conflict, Russia could retaliate by targeting Western undersea communication cables (Runde et al., 2024). This, combined with other physical evidence, means that we cannot simply wait for these risks to go away by themselves; greater preparedness for such threats is vital towards ensuring long-term peace in Western society.

The Threat of Disinformation

Secondly, there is an arguably greater hybrid threat in the form of deception and disinformation, aiming to dictate the nature of public debate or diminish the credibility of key social actors (Nilsson et al., 2021). In 2025, the World Economic Forum named disinformation as the leading global short-term threat and highlighted the need for greater cooperation to address shared crises (World Economic Forum, 2025). An increased availability of data on target audiences, easier access to specific target segments, the increasing speed of information dissemination, and the ability to remain anonymous or pretending to be someone else have all been enabling factors for these attacks. The EU's Disinformation Lab uncovered one of Russia's large-scale disinformation campaigns in 2024, known as "Doppel-Gänger" (Abrahamian, 2026). Russia had been producing fake websites which mimicked seventeen media outlets. A key example of this was a fake NATO website designed to spread disinformation on budget proposals and military deployments (ibid). It predominantly promoted Russia's influence in Ukraine, even denying the Bucha massacre in 2022 which resulted in 500 Ukrainian deaths (ibid). The Atlantic Council examined at the most popular social network in Eastern Europe, called Telegram, in 2025 and found that that from a pool of 2.9 million posted comments on information forums in Ukraine, at least 96 000 comments were flagged as originating from bots. The top three narratives being propagated were: criticism over a sovereign Ukraine, criticism of President Zelenskyy, and criticism over the global West (Dukach et al., 2025). The Baltics are susceptible to such forms of hybrid threats due to their proximity and demographics, where many Baltic countries have a significant Russian speaking population. With NATO, the EU, and Western society at large at Russia's arm's reach of

influence (in terms of language, population, norms and history), such disinformation could potentially destabilise institutional integrity (Abrahamian, 2026). Telegram has recently been used to spread disinformation regarding Ukrainian drones which crashed in Lithuania on the 23rd of March 2026, falsely claiming that the Baltic States had opened their airspace to Ukrainian drones. This disinformation made its way onto Russian State news channel *60 Minutes*, framing the narrative to seem as though the Baltics are an active participant in the conflict. In this way, by potentially legitimising hostile rhetoric or retaliatory measures, hybrid threats can actively contribute to an erosion of European security despite their non-military nature.

CIMIC Contribution

Having understood the threats looming over Europe, how can CIMIC support conflict prevention? Dissatisfaction, discord and dynamic destabilisation (Roberts, 2025) brought about by foreign disinformation campaigns introduces significant risk of conflict. If our liberal societies, overcome by disinformation, were to be convinced of the Russian narrative in Ukraine, military and financial support for Ukraine would fall and thereby increase the possibility of Russian victory. Putin's imperialistic dreams certainly do not end with Ukraine, and the Baltic states are at a higher risk of future invasion given their geography. Strong societal resilience is critically important to prevent this and can be fostered by CIMIC: 1. A strong democratic basis combined with high levels of trust in the government; 2. Well-informed and resilient citizens; 3. Increased critical thinking in order to not be vulnerable to political and economic pressure (CCOE, 2026). One way to mitigate these risks is through restrictions placed on Russian TV networks in the Baltics, and while banning of popular social networks in the Baltics is likely to provoke backlash regarding freedom of expression, workshops should be facilitated in public spheres to teach media literacy and in identifying disinformation (Abrahamian, 2026). A Whole-of-Society approach is much more effective than simply restricting access to information, which the Latvian Transatlantic Organisation (LATO) has pioneered in this regard (Abrahamian, 2026). Greater information sharing, active education, and a Total Defence framework are all essential to CIMIC and will reduce to the risk of total conflict if implemented efficiently.

Deterrence

Furthermore, as seen during the Cold War, deterrence is a vital part of de-escalation, peacekeeping, and global power communication. Should a Total Defence and Whole-of-Society approach be taken in the Baltic States, the disinformation approach, and critically the plausible deniability that Russia hides behind would be hindered. Critical undersea infrastructure is largely built by the private sector, which must take a CIMIC approach to the issue, including greater communication and information sharing with the

military. Coordination is especially important here; in 2022 the European Commission launched a new EU Cable Security Action Plan with a €1bn initiative for improved threat monitoring. Yet action at a NATO level has proved inefficient even though they have the decision-making status and command structures needed to enact change (Paukkunen, Black, 2026). Currently Russia believes that they can get away with their actions without reprisal – coordinating a national response alongside NATO is vital towards changing this perception, especially to strengthen the credibility of smaller allies who face the greatest risk. Only then will deterrence prevent action that would cross the Article 5 threshold (Paukkunen, Black, 2026).

Conclusion

To conclude, CIMIC is an essential link between military forces and civilian infrastructure. It can enhance operational effectiveness, while also reducing harm to civilians and supporting long-term stability by limiting disinformation and strengthening the credibility of deterrence. A Whole-of-Society and Total Defence approach are vital to increase societal resilience and military preparedness. The Baltic Sea states, which are a flashpoint for hybrid threats due to their proximity, strategic importance, and Western influence, have already made a significant contribution to European security with the accession of Sweden and Finland to NATO; however, hybrid threats are far from having been adequately mitigated. Information sharing, multi-sector collaboration, and societal preparation in a CIMIC framework has the ability to prevent conflict and reduce risk to civilians, as the of development hybrid threats are likely to continue on an upward trajectory.

References:

Abrahamian, V., 2026. Russia's Disinformation Campaign in the Baltics. *Joint Baltic American National Committee*. Available at: https://www.jbanc.org/baltic-insights/russias-disinformation-campaign-in-the-baltics

Dukach, Yuliia, Adam, Iryna, Furbish, Meredith. *Digital occupation: Pro-Russian bot networks target Ukraine's occupied territories on Telegram.* The Atlantic Council. 2025.

Government Offices of Sweden. Total Defence. Available at: https://www.government.se/government-policy/total-defence/

Lawrence, T., 2025. The Baltic Sea in Peace and War. International Centre for Defence and Security.

Loik, R., 2024. Undersea Hybrid Threats in Strategic Competition: The Emerging Domain of NATO–EU Defense Cooperation, Journal on Baltic Security. 10(2), pp. 1-25.

Muuga, Emilia, Loik, Ramon, Kaup, Georg-Henri; Savimaa, Raul, Koort, Erkki. (2024) *Julgeolekuohud Balti riikide merealuste ühendustega seotud kriitilisele taristule [Security Threats to the Undersea Connections Related Critical Infrastructure of the Baltic States]*. Tallinn: Sisekaitseakadeemia (Estonian Academy of Security Sciences

NATO, 2026. Countering Hybrid Threats. Available at:

NATO CIMIC Centre of Excellence, 2026. CIMIC Handbook. Available at: https://www.cimic-coe.org/wp-content/uploads/2026/06/CIMIC-Handbook-2026.pdf

Nilsson, Niklas, Mikael Weissmann, Björn Palmertz, Per Thunholm, and Henrik Häggström. "Security challenges in the grey zone: Hybrid threats and hybrid warfare." Hybrid Warfare: Security and Asymmetric Conflict in International Relations. By Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm . London: I.B. Tauris, 2021. 1–18. Bloomsbury Collections. Web. 23 Apr. 2021

Paukkunen, S., Black, J., 2026. Deterring Russia Beneath the Waves: Securing NATO's Critical Undersea Infrastructure. *War on the Rocks*. Available at: https://warontherocks.com/deterring-russia-beneath-the-waves-securing-natos-critical-undersea-infrastructure/

Pribyl, S., 2026. Securing the Baltic: The Strategic Imperative for a Comprehensive Maritime Security Strategy. Center for Maritime Security. Available at: https://centerformaritimestrategy.org/publications/securing-the-baltic-the-strategic-imperative-for-a-comprehensive-maritime-security-strategy/

Rehse, P., 2004. CIMIC: Concepts, Definitions and Practice. Heft 136. Hamburg.

Roberts, P., 2025. CIMIC and C2: Fit for the Future?. Aurelius Lab.

Runde, Daniel F., Murphy, Erin L., and Bryja, Thomas. (2024) 'Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition', *Center for Strategic and International Studies CSIS*. [Online] 16 August 2024. https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

World Economic Forum, 2025. Global Risks Report 2025: Conflict, Environment and Disinformation Top Threats. Available at: https://www.weforum.org/press/2025/01/global-risks-report-2025-conflict-environment-and-disinformation-top-threats/