# From Tanks to TikTok: Adapting Article 5 for Graduated Responses to Hybrid Warfare

## Description

*Editorâ??s Note: this article is being republished with the permission of Small Wars Journal as part of a republishing arrangement between IWI and SWJ. The original article was published on 07.15.2025 and is available here.*

SWJ Logo Tall

The Soviet-era bronze statue in Tallinn was relocated long ago, but the cyberattack it precipitated in 2007 has overhauled NATOâ??s approach to collective security. When Russian-linked hackers debilitated Estoniaâ??s digital infrastructure following riots sparked by the controversial relocation, NATO members were forced to reconcile with the fact that Article 5, the cornerstone of collective defense, was crafted to respond to conventional threats â?? like tanks rolling over the borders of member states â?? rather than ambiguous hybrid attacks. But what use was it now against enemies who could use keyboards, ethnic tensions, and commercial vessels as weapons to elicit strategic effect, even without firing a shot?

Today, as Russian hybrid attacks against NATO members have nearly tripled, the Alliance faces an urgent question: How should collective defense evolve when adversaries deliberately operate in the gray zone between war and peace? The answer requires rethinking Article 5, not by abandoning its principles but by adapting its application to confront threats that are increasingly hybrid, persistent, and ambiguous.

### The Wider Black Sea Region as a Laboratory of Hybrid Warfare

Russian military doctrine views hybrid warfare (Ð³Ð¸Ð±Ñ?Ð¸Ð´Ð½Ð°Ñ• Ð²Ð¾Ð¹Ð½Ð°, *gibridnaya voina*) as a systematic strategy integrating conventional and special-operations forces, cyber- and electronic-warfare strikes, information-psychological operations, economic coercion, political subversion, energy manipulation, and proxy forces to achieve strategic objectives while maintaining plausible deniability. While Estoniaâ??s 2007 cyber siege captured global attention, Russia has since turned the Wider Black Sea Region into its main laboratory for refining hybrid warfare tactics. The 2008 synchronized cyber and kinetic operations against Georgia demonstrated Moscowâ??s evolving

playbook, notably by combining traditional military force with digital attacks to multiply strategic effects. Ukraine became the next testing ground. With the 2014 stealth invasion of Crimea, the Kremlin unveiled a hybrid approach honed to aesthetic perfection: â??little green menâ?• who popped up without insignia marks, information warfare aimed at Russian-speaking ethnic minorities, and cyber operations in Zelenopillya that disrupted Ukrainian military radio signals, leaving two battalions as targets for massed artillery strikes within minutes. These activities were just the beginning of Russiaâ??s hybrid warfare evolution.

Perhaps the most chilling development took place in Romania â?? a NATO member state â?? during the 2024 presidential election. Through coordinated TikTok manipulation involving 25,000 reactivated accounts and support from Russian and Iranian networks, Pro-Russian ultranationalist CÄ?lin Georgescuâ??s shocking first-round victory forced Romaniaâ??s Constitutional Court to take the unprecedented step of annulling the election results. The sophistication of this â??algorithmic invasion â?• revealed how hybrid warfare could install Moscow-friendly leaders in NATO capitals without firing a shot.

**The Escalating Hybrid War**

Russiaâ??s campaign against NATO has evolved from isolated incidents to what intelligence officials now describe as a â??staggeringly reckless campaignâ?• of sabotage and subversion. Recent data reveal the scope: 34 recorded attacks in 2024 alone, targeting everything from undersea cables to weapons factories. The Wider Black Sea Region bears particular scars. In Bulgaria, explosions rocked EMCO company ammunition warehouses just days after Sofia announced they would be joining the coalition to supply shells to Ukraine. The message was unmistakable: supporting Ukraine carries costs. Russian hybrid operations are not limited to the Wider Black Sea Region, however. The NotPetya cyberattack of 2017, though only targeting Ukraine, spread globally to cause over $10 billion in damage. As one NATO official noted at the time, â??You canâ??t really find a space in Ukraine where there hasnâ??t been an attackâ?•.

**NATOâ??s Response to Hybrid Threats**

The Alliance has not stood still. Since the 2014 Wales Summit first acknowledged that cyber attacks could trigger Article 5, NATO has progressively expanded its understanding of collective defense. The 2016 Warsaw Summit recognized cyberspace as an operational domain, while the 2023 Vilnius Summit launched new cyber defense capabilities and acknowledged that cumulative hybrid activities could constitute an armed attack. Events in the Wider Black Sea Region have played a large part in this development. Capabilities developed as a result of Ukraineâ??s relationship with NATOâ??s Cooperative Cyber Defense Center of Excellence mitigated a number of strategic cyber effects in

Russiaâ??s 2022 invasion. The Tallinn Mechanism, launched in 2023, facilitates civilian cyber assistance to Ukraine â?? a recognition that when it comes to hybrid defense, we need hybrid partners.

Implementation, however, lags behind rhetoric. Despite operations like Baltic Sentry and an increase in Black Sea maritime patrols, NATOâ??s defensive posture hasnâ??t deterred escalation. The weaponization of migration, political subversion, and systematic sabotage continue unabated.

Article 5â??s power lies in its clarity: an armed attack against one is an attack against all. But hybrid warfare deliberately exploits the ambiguities of the gray zone. When Russian psychological operations and algorithmic manipulation nearly install a pro-Moscow president in Bucharest, is that an attack? When sabotage targets Bulgarian arms shipments bound for Ukraine, does that cross the threshold?

The Romanian case is particularly troubling. As Germanyâ??s Ministry of Foreign Affairs warned, â??Putin aims to divide us and undermine unity within the EU and NATO.â?• Had Georgescu won, Romaniaâ??guardian of NATOâ??s southeastern flank and home to crucial missile defense systemsâ??might have pivoted away from supporting Ukraine. The strategic impact could have exceeded many conventional military operations.

The Wider Black Sea Region offers crucial lessons for adapting Article 5. First, hybrid operations often precede conventional escalation. For instance, Russia employed hybrid tactics such as cyberattacks on Georgian government and media networks, extensive passportization campaigns providing Russian citizenship to residents in separatist regions, and support for separatist proxy groups, prior to the 2008 invasion of Georgia. Russiaâ??s 2014 hybrid campaign in Ukraine preceded the 2022 full-scale invasion. Treating hybrid attacks as mere nuisances rather than potential precursors to war invites strategic surprise.

Second, cumulative effects matter more than individual incidents. Romania didnâ??t face a single decisive cyber-attack but rather a â??persistent operational frictionâ??â??years of narrative seeding that Russian actors activated at a critical moment. Bulgaria experienced not one explosion but a pattern of sabotage targeting Ukraineâ??s supply chains. NATO must assess campaigns, not just incidents.

Third, geographic patterns reveal strategic intent. The concentration of hybrid attacks in the Wider Black Sea Region isnâ??t random, reflecting Russiaâ??s goal to destabilize Romania, isolate Moldova, and undermine support for Ukraine. Understanding regional dynamics helps distinguish harassment from strategic campaigns that warrant a collective response.

## A Nuanced Framework for Hybrid Scenarios

Resolving this dilemma doesnâ??t require rewriting Article 5. It does require developing a more nuanced framework for its application in hybrid scenarios. Three principles should guide this evolution:

First, **effects-based assessment** should supplement traditional means-based analysis. Whether Romania faces tanks or TikTok manipulation matters less than the strategic effects. The potential installation of a pro-Russian government in Bucharest could have neutralized NATOâ??s largest planned defense facility in Europe more effectively than any military strike.

Second, **regional context** must inform thresholds. Hybrid attacks against allies in the Wider Black Sea Region directly undermine NATOâ??s ability to support Ukraine and other NATO Partnership for Peace countries, such as Moldova and Georgia, and maintain regional stability. The Alliance should recognize that attacks on states that serve as primary conduits for military assistance will have broader strategic implications and warrant a lower threshold for collective response.

The Wider Black Sea Region requires particular attention in NATOâ??s hybrid defense strategy. Romaniaâ??s vulnerability to information operations, Bulgariaâ??s exposed defense supply chains, and the ongoing hybrid pressure on Georgia and Moldova demand enhanced regional coordination.

NATO should establish a Hybrid Defense Hub for the Wider Black Sea Region, building on the Tallinn Centerâ??s cyber expertise but addressing the full spectrum of hybrid threats. This hub could monitor regional patterns, develop attribution capabilities for coordinated Russo-Chinese operations, and coordinate responses to campaigns that target multiple allies simultaneously.

Third, **graduated response options** should match hybrid escalation. Rather than binary Article 5 activation, NATO needs intermediate collective response mechanisms that can address hybrid campaigns without triggering full collective defense. Professor Corneliu Bjolaâ??s Dynamic Information Resilience (DIR) framework for countering information threats provides a model for how such graduated mechanisms could operate across other hybrid domains.

Investment in offensive capabilities also deserves consideration. NATOâ??s primarily defensive posture hasnâ??t deterred escalationâ??Russian attacks have increased despite expulsions, sanctions, and arrests. The Alliance should develop proportional offensive options, clearly communicating that hybrid attacks on Black Sea allies will incur costs beyond purely defensive responses.

## Conclusion

From Tallinnâ??s Bronze Soldier to Bucharestâ??s annulled election, the evolution of hybrid warfare demands parallel evolution in collective defense. The Wider Black Sea Regionâ??s experienceâ??from Georgiaâ??s synchronized cyber-kinetic attacks to Romaniaâ??s algorithmic invasionâ??demonstrates that twenty-first-century threats require twenty-first-century interpretations of Article 5, not perspectives rooted in 1949.

This adaptation requires neither abandoning collective defenseâ??s core principles nor revealing every red line. Instead, NATO must develop frameworks that preserve strategic ambiguity while enhancing deterrence, recognizing effects over means, regional patterns over isolated incidents, and graduated responses over binary choices.

The stakes extend beyond Alliance credibility. As the Wider Black Sea Region becomes a proving ground for Russo-Chinese hybrid warfare cooperation, NATOâ??s response will shape global norms for decades. By evolving Article 5 for the hybrid age, the Alliance can demonstrate that collective defense remains relevant whether threats arrive through missiles or malware, tanks or TikTok, armies or algorithms. The alternativeâ??clinging to outdated interpretations while NATOâ??s adversaries perfect new forms of warfare in its own backyardâ??risks rendering the Allianceâ??s cornerstone guarantee hollow precisely when solidarity matters most.

### About the Author

LCDR Ciprian Clipa is a Romanian Special Operations Forces officer with over a decade of distinguished SOF service and is currently pursuing a Master of Science in Defense Analysis, majoring in Irregular Warfare, at the U.S. Naval Postgraduate School in Monterey, California. His research focuses on the role of SOF in countering Russian hybrid threats in the Black Sea region, with particular emphasis on Romania.

This article was originally published by Small Wars Journal

**Date Created**
2025/08/27