NATO
C2COE

RUSSIA'S COMMAND AND CONTROL OF COGNITIVE WARFARE:

LESSONS FROM THE BALTICS

Rear Admiral (Ret.) Mark Montgomery , USA N
Senior director of the Foundation for Defense of Democracies' (FDD) Center on Cyber and Technology Innovation (CCTI).

Dr. Ivana Stradner
Research Fellow at FDD

Introduction

Russia's threats against the Baltic region demonstrate that its strategy extends beyond conventional military force to a coordinated command-and-control (C2) approach that integrates military, cyber, information, and intelligence capabilities. Through this multi-domain strategy, Moscow seeks to create strategic ambiguity, slow NATO's decision-making, and test Alliance cohesion without provoking a conventional military response. Understanding how Russia employs its C2 system to synchronize these capabilities is essential to assessing the threat it poses to NATO's eastern flank. Strengthening NATO's resilience will therefore require not only implementing the Alliance's Readiness Plan but also enhancing integrated C2 processes that enable faster decision-making, improved coordination, and more effective responses to Russia's evolving multi-domain operations.[1]

Russia's Multi-Domain Pressure on NATO

Russia's full-scale invasion of Ukraine marked a significant challenge to the post-Cold War European security architecture and underscored the Kremlin's willingness to employ military force in pursuit of its strategic objectives. While the war in Ukraine remains Russia's primary military effort, Moscow has continued to engage in activities intended to test NATO's cohesion, readiness, and capacity for collective decision-making. Within this broader strategic context, the Baltic region occupies a central position because of its geographic proximity to Russia, strategic importance to the alliance, and perceived vulnerability to coercive measures below the threshold of conventional war. Russian military posturing, cyberattacks, information operations, and other forms of hybrid activity collectively serve to probe NATO's C2 mechanisms and political resolve while increasing pressure on Estonia, Latvia, and Lithuania across multiple domains.

By operating in the "gray zone," Russia seeks to generate strategic ambiguity that complicates NATO's political and military decision-making while reducing the likelihood that its actions will trigger a unified allied response or escalate into open conflict with the alliance.

Russia's influence operations against NATO have been far reaching. America's civilian cyber defense agency reported that Russian hackers conduct serious cyberattacks on NATO Critical Infrastructure.[2] Russian GPS spoofing attacks have diverted Ukrainian drones to NATO territory, forcing Lithuania to shelter its capital after a runaway drone appeared in Vilnius'[3] airspace. Most recently, while NATO members met in Ankara, Russia held naval exercises in the Baltic Sea, aiming to increase tension levels.[4]

1 NATO, NATO Standardization Office, "NATO Standard AJP-10 Allied Joint Doctrine for Strategic Communications," March 2023. (https://mpsotc.army.gr/wp-content/uploads/2025/07/AJP-10-Strategic-Communications_March-23-1.pdf)

2 U.S. National Coordinator of Protection of Critical Infrastructure Security and Resilience, "Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure," December 18, 2025. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a)

3 Katie Livingstone, "How Russia is turning Ukraine's drones against NATO," DefenseNews, May 29, 2026. (https://www.defensenews.com/global/europe/2026/05/29/how-russia-is-turning-ukraines-drones-against-nato/)

4 "Russia holds naval drills in Baltic Sea during major NATO exercises," Reuters, June 9, 2026. (https://www.reuters.com/business/aerospace-defense/russia-holds-naval-drills-baltic-sea-during-major-nato-exercises-2026-06-09/)

Russian Shahed

In the Baltics, Moscow has an established history of aggravating NATO. In September 2025, Russia's drones breached the airspaces of Poland, Romania, and Estonia.[5] A month later, Vilnius repeatedly closed its' airspace after detecting Russian balloons.[6] Additionally, a suspicious Russian spy plane flying over the Baltic Sea was intercepted.[7] In the past weeks, however, Russian escalation in the Baltics has dramatically increased. On May 19, the Russian Foreign Intelligence Service (SVR) accused Latvia of allowing Ukrainian drone launches from Latvian territory.[8] The SVR's public accusation ended by threating that "NATO membership will not protect you."[9] Russian media quickly spread the SVR's message and reaffirmed that Riga, and by extension NATO, was initiating escalation.[10] Even more alarmingly, the Danish news agency, DR, published satellite images of Russia upgrading existing military bases, deploying troops, and increasing militarization alongside the Russian-Baltic border.[11] Scandinavian officials claim that Moscow is preparing infrastructure capable of housing over 100,000 troops, marking the current threat level as "higher than during the Cold War".[12]

On May 25, Putin ratified a law allowing Moscow to deploy the military to foreign states that arrested Russian citizens.[13] Although framed as a measure to protect Russian nationals abroad, the law provides the Kremlin with a legal pretext for military intervention beyond Russia's borders and could be used to justify coercive actions under the guise of protecting its citizens. In June, the Latvian Constitution Protection Bureau shared a report stating that Russia is abusing the international legal system, essentially conducting lawfare against the Baltic states.[14] The report asserted that Putin is preparing to sue the Baltic states in the International Court of Justice for mistreating Russian citizens in their territories, as a pretext for invasion.

Germany has stated that Russia may be ready to invade NATO territory as early as 2029.[15] In response, the alliance has committed to strengthening its Eastern border.[16] However, traditional military might is not enough to combat the Russian threat, as the Kremlin's greatest strength lies in its ability to conduct information operations. To effectively counter Moscow's actions, NATO should understand Russia's unique approach to C2 and establish robust offensive and defensive mechanisms to protect and enhance its own C2 capabilities.

---

5 North Atlantic Treaty Organization, "Statement by the North Atlantic Council on recent airspace violations by Russia," September 23, 2023. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/09/23/statement-by-the-north-atlantic-council-on-recent-airspace-violations-by-russia)

6 Ferdinand Knapp, "Lithuania suspends air traffic over capital due to balloons," Politico, October 30, 2025. (https://www.politico.eu/article/lithuania-air-traffic-vilnius-balloons/)

7 The Foundation for Defense of Democracies, "Polish Fighter Jets Intercept Russian Spy Plane Over Baltic Sea," October 29, 2025. (https://www.fdd.org/analysis/2025/10/29/polish-fighter-jets-intercept-russian-spy-plane-over-baltic-sea/)

8 The Foreign Intelligence Service of the Russian Federation "УКРАИНА ГОТОВИТ УДАРЫ ПО РОССИИ С ТЕРРИТОРИИ ЛАТВИИ," May 19, 2026. (http://svr.gov.ru/smi/2026/05/ukraina-gotovit-udary-po-rossii-s-territorii-latvii.htm)

9 The Foreign Intelligence Service of the Russian Federation "УКРАИНА ГОТОВИТ УДАРЫ ПО РОССИИ С ТЕРРИТОРИИ ЛАТВИИ," May 19, 2026. (http://svr.gov.ru/smi/2026/05/ukraina-gotovit-udary-po-rossii-s-territorii-latvii.htm)

10 "Latvia sets precedent by enabling strikes on Russia — expert," TASS, May 19, 2026. (https://tass.com/world/2133007)

11 Niels Fastrup and Lisbeth Quass, "Rusland opruster langs Europas grænser og gør klar til en mulig krig (Russia is arming along Europe's border, preparing for a possible war," Danish Broadcasting Corporation, June 10, 2026. (https://www.dr.dk/nyheder/indland/moerklagt/nye-satellitbilleder-afsloerer-russisk-oprustning-langs-graensen-til-norden)

12 Ewan Jones, "'Preparing for conflict': Russia builds bases for over 100,000 troops near NATO borders," TVP World, November 6, 2026. (https://tvpworld.com/93751971/russia-develops-bases-for-115000-soldiers-by-baltic-nato-borders)

13 "Putin Signs Law on Use of Army to Aid Russians Detained Abroad," Bloomberg, May 25, 2026. (https://www.bloomberg.com/news/articles/2026-05-25/putin-signs-law-on-use-of-army-to-aid-russians-detained-abroad)

14 Constitution Protection Bureau of the Republic of Latvia, "RUSSIA INTENSIFIES LAWFARE AGAINST THE WEST TO JUSTIFY MORE AGGRESSIVE ACTIVITIES," June 2026. (https://www.sab.gov.lv/files/uploads/2026/06/SAB_public_report_2_Lawfare.pdf)

15 Lucas Rogers and Felix Gasper, "Germany's New Military Concept: Responsibility for Europe," International Centre for Defense and Security, June 3, 2026. (https://icds.ee/en/germanys-new-military-concept-responsibility-for-europe/)

16 Lucas Rogers and Felix Gasper, "Germany's New Military Concept: Responsibility for Europe," International Centre for Defense and Security, June 3, 2026. (https://icds.ee/en/germanys-new-military-concept-responsibility-for-europe/)

Russian Command and Control for Cognitive Warfare

Russia's approach to information operations (IO) greatly differs from NATO's comprehension of traditional C2 structures. Understanding Moscow's tactics, techniques, and procedures is critical to preventing aggressive action and defending the NATO's Baltic border.

Consistent with Russia's concept of new generation warfare, military and non-military tools are integrated to achieve strategic objectives below the threshold of conventional war. Unlike in most Western countries IOs are not confined to periods of armed conflict. Rather, Moscow continuously shapes the information environment to influence public opinion, undermine adversaries, and create conditions favorable to Moscow's strategic objectives.

Furthermore, the Kremlin's priority for cyber is not focused on defending domestic networks; rather, it is a component of a warfare campaign aimed at undermining NATO's decision-making, and influencing perception.[17] When paired with Russia's C2 model, this campaign in the information space is designed to disorganize its adversaries' C2 structure, leaving the adversary confused and unable to react.[18] Russian C2 is organized as a hierarchy, with priorities being established at the highest rank of state rule, while execution is divided by responsibility and assigned to corresponding agencies.[19] Specifically, Russian media organizations disseminate Kremlin-aligned narratives that can be adapted and amplified across the information environment. This approach enables Russian information operations to spread rapidly and effectively while maintaining consistency with Moscow's strategic objectives.

The SVR works to influence and manipulate information outside of Russia, prioritizing combating NATO's digital presence. Instead of focusing on short-term destabilization, the group aims to fundamentally undermine the C2 structure and decision-making abilities of adversaries.[20] By targeting the cognitive and informational foundations of adversary C2, these efforts aim to create uncertainty, delay decision-making processes, and reduce the effectiveness of command structures.

The Federal Security Service (FSB) is responsible for supporting Russia's offensive and defensive capabilities in information warfare.[21] It enforces the Russian domestic narrative through media influence and surveillance. By reducing the influence of foreign information, while enforcing the Kremlin-sponsored account, the FSB ensures that only approved information circulates the Russian media ecosystem.[22]

The Main Directorate of the General Staff (GU) contributes to Russia's broader concept of information confrontation by integrating intelligence, cyber operations, and information activities to achieve strategic effects. Through these capabilities, the GU can identify vulnerabilities within an adversary's C2 architecture and disrupt decision-making processes while creating uncertainty. These activities reflect

17 Madison Creery, "Russia Strategic Understanding of Cyber: Not an Information War -- War on Information," Georgetown Security Studies Review, December 5, 2018. (https://georgetownsecuritystudiesreview.org/2018/12/05/russia-strategic-understanding-of-cyber-not-an-information-war-a-war-on-information/)

18 Timothy Thomas, "Russia's Conduct of War: How and with What Assets," The MITRE Corporation, January 2021, pg 19; Y. I. Lastochkin, Y. L. Koziratsky, Y. Y. Donskov, and A. L. Moororescu, "Боевое применение войскрадиоэлектронной борьбы как важнейшая составляющая оперативного искусства Сухопутных войск," VoyennayaMysl, 2017, p. 25.

19 Antti Vasara, Theory of Reflexive Control: Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy, National Defence University, 2020, page 71. (https://www.doria.fi/bitstream/handle/10024/176978/Vasara_FDS22_Theory%20of%20Reflexive%20Control%20%28web1%29-1.pdf)

20 Andrew Bowen, "Russia's Foreign Intelligence Services," Library of Congress, 3 December 2025, Web. https://www.congress.gov/crsproduct/IF12865#:~:text=As%20Russia's%20primary%20civilian%20foreign,Russia%20or%20the%20Russian%20government.

21 US Department of the Treasury, "Treasury Sanctions Russian Intelligence Officers Supervising Election Influence Operations in the United States and Around the World," June 23, 2023. (https://home.treasury.gov/news/press-releases/jy1572)

22 "ФЕДЕРАЛЬНЫЙ ЗАКОН, О ФЕДЕРАЛЬНОЙ СЛУЖБЕ БЕЗОПАСНОСТИ," Article 8, Government of the Russian Federation, 1995, https://www.consultant.ru/document/cons_doc_LAW_6300/

Russia's approach to new generation warfare, in which information-related capabilities are employed continuously to shape the operational environment and undermine an adversary's ability to respond effectively.[23]

State-controlled media organizations such as RT, Sputnik, and TASS serve as instruments of Russia's broader information confrontation strategy by disseminating Kremlin-aligned narratives to domestic and international audiences. Beyond promoting specific messages, these outlets seek to shape perceptions, exploit societal divisions, and weaken trust in democratic institutions and information ecosystems.[24]

Moscow has crafted the environment for information operations, as leadership can rapidly disseminate goals and instructions, while being shielded from direct responsibility for operations.[25] The Kremlin's C2 system for IO fundamentally relies on the mechanization of reflexive control.[26] This Soviet technique aims to implant prepared subversive information to an adversary who will make logical decisions from that information. However, their decisions will be predetermined and favorable for Russia. Russian operatives' model possible adversary reactions to find the weakest point of decision making and input misleading critical information there.[27] By understanding an opponent's culture and geopolitical position, the Russian military shapes their decision-making process, fundamentally altering their ability to perform accurate analysis. [28]

Today, Russia combines the theoretical framework of Soviet-era reflexive control with contemporary technological developments to conduct highly effective information operations. Critically, reflexive control seeks to shape how an adversary thinks and perceives events, rather than simply what they think. For example, cyber-enabled information operations, such as hack-and-leak campaigns, can be understood as a form of reflexive control. These operations target not only the technical dimensions of cybersecurity but also its cognitive dimensions. Rather than generating only short-term military advantages, these operations fundamentally reshape the information environment, creating long-term strategic benefits for Russia. Furthermore, instead of relying exclusively on centralized state messaging, contemporary reflexive control leverages digital information ecosystems in which domestic actors such as political groups, media organizations, and social media influencers, may amplify or reinforce Russian narratives. This enhances the effectiveness of these campaigns by increasing the credibility and reach of the intended messages as they look like grassroot movements.

Russia's concept of reflexive control provides a useful framework for understanding how information activities may seek to influence NATO's C2. Rather than attempting to physically disrupt NATO's command structures, reflexive control focuses on shaping the perceptions and decision-making environment of an adversary so that leaders make choices favorable to Russia's strategic objectives. In the Baltics, where NATO decisions depend on political consultation and coordinated action among multiple allies, efforts to create uncertainty or competing interpretations of events could damage the alliance's C2 system.

---

23 Alexis A. Blanc, et al., "The Russian General Staff: Understanding the Military's Decision-Making Role in a "Besieged Fortress,"" RAND, 2023, Web. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1200/RRA1233-7/RAND_RRA1233-7.pdf

24 Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," The New York Times, 28 August 2016, Web. https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html

25 Kateryna Bondar, "How Russia Is Reshaping Command and Control for AI-Enabled Warfare," Center for Strategic and International Studies, February 10, 2026. (https://www.csis.org/analysis/how-russia-reshaping-command-and-control-ai-enabled-warfare)

26 Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," Institute for the Study of War, September 2015. (https://understandingwar.org/wp-content/uploads/2024/05/Russian20Report20120Putin27s20Information20Warfare20in20Ukraine-20Soviet20Origins20of20Russias20Hybrid20Warfare.pdf)

27 Timothy Thomas, "Russia's Reflexive Control Theory and the Military," Journal of Slavic Military Studies, 2004. (https://impiousdigest.com/wp-content/uploads/2017/08/Thomas_2004.pdf)

28 Vladimir Lefebvre and Georgi Smolyan, Conflict Algebra (Moscow: Znanie Press, 1968).

The Kremlin can exploit NATO's reliance on consensus-based political decision-making by launching information activities that create divergent threat perceptions to weaken member states' unity. Through information operations Russia seeks to contest the information environment in which NATO leaders assess risks and make decisions. The key to Russian strategy lies not in the material impact of escalatory actions, but in how escalatory actions are perceived by member states. Russia uses escalation to subvert NATO's perception of Moscow's true intentions and threat level, effectively paralyzing the alliance's ability to combat Russian encroachment. Therefore, the central challenge for NATO is not only protecting the technical systems that enable C2, but also preserving cognitive resilience by ensuring that commanders and political leaders can maintain a shared understanding of the information environment, assess adversary actions accurately, and make timely decisions despite hostile influence activities.

NATO Policy Recommendations:

In the event of a Russian military operation against the Baltic states, Moscow would likely seek to disrupt NATO's C2 systems and complicate allied decision-making through a combination of military, cyber, and information activities. Therefore, strengthening resilience against manipulation of the information environment and interference in decision-making processes should be a priority. An effective approach should focus on three objectives: identifying and countering Russian interference, protecting critical decision-making channels, and limiting Moscow's ability to collect, analyze, and exploit information about allied responses.

First, NATO should develop a "Perception Management Warfare Assessment Unit" (PMWAU) to identify, highlight, and counter Russian influence within the NATO information environment.

Russia will likely employ information operations targeting NATO C2 structures and the domestic policy environments of member states during a crisis. To counter these efforts, NATO should establish a coordinated capability to monitor, assess, and respond to Russian influence operations. PMWAU would analyze Russian activities designed to shape decision-making, exploit political divisions, and weaken allied cohesion. By identifying emerging narratives and assessing their impact, PMWAU would help preserve NATO unity and improve resilience against information confrontation.

Second, NATO should adopt counter-reflexive shielding measures to prevent Russia from using the information environment to manipulate NATO's decision-making process. These measures include limiting access to decision-making details and creating ambiguity in the information environment.

NATO should limit Russia's understanding of the alliances' decision-making processes, especially while decisions are actively being discussed. This protective mechanism should focus on monitoring publicly available insights on decision makers, and the dates and locations of deliberations before a decision is made. Russian reflexive control requires information curators to understand the leaders who are responsible for making decisions. Restricting the publication of information about these leaders will disadvantage Russian information operations.

Another element of counter-reflexive shielding is polluting the information environment to put Russia on the defensive. NATO should conduct offensive information operations, such as swarming, to create ambiguity in Russia's perception of Western intentions. This does not require deception; rather, NATO can amplify multiple truthful and consistent, yet competing, narratives that complicate Russian decision-making without compromising its own credibility.

These operations will allow NATO to degrade Russia's ability to execute successful information campaigns against NATO by feeding misleading information about NATO decision-making deliberations. PMWAU would determine the sources of Russian information on NATO C2 and provide those Russian practices to an offensive team. Then offensive operations would be conducted against those nodes with narratives that confuse Russian analysts. These operations would effectively "disinform" Russian studies used to exploit NATO decision-making.

Finally, NATO should establish a readiness plan to demonstrate their will to respond to Russian aggression in the Baltics. The plan should be clear, establish a coalition of the willing, and be accompanied with continued military exercises near the Baltics.

The creation of a NATO Readiness Plan will demonstrate that NATO is ready to act and has the procedures in place to do so immediately. The plan should include a defined scale of escalation levels that give Russia less ambiguity to exploit.

Furthermore, military exercises in and near the Baltics should be implemented to increase preparedness. These exercises must include cyber forces, as Russia will use cyber to advance information operations. Strong cyber security will secure control networks so Russia cannot disable them and hurt NATO's front line strategic communication.

Conclusions

Russia's ability to challenge NATO's cohesion and decision-making processes represents a persistent threat to the security of the Baltic region. Through new generation warfare Moscow has demonstrated the ability to combine military pressure, cyber activities, and influence operations to exploit vulnerabilities within allied decision-making structures. NATO should therefore prioritize strengthening resilience against Russian information operations, while ensuring the security, resilience, and adaptability of its C2 systems and decision-making processes. Establishing dedicated capabilities to assess and mitigate information threats, while enhancing coordination among member states, will be critical to maintaining allied unity and ensuring a timely and effective response during a crisis. By addressing these vulnerabilities now, NATO can strengthen deterrence and reduce Russia's ability to exploit ambiguity and division within the alliance.


COMMAND AND CONTROL
CENTRE OF EXCELLENCE