NATO C2COE

RUSSIAN COMMAND AND CONTROL IN INFORMATION WARFARE AND REFLEXIVE INFLUENCE

Implications for NATO and Counter-Reflexive Control

Dr. Ivana Stradner, Rear Admiral (Ret.) Mark Montgomery

The authors would like to thank Stephen Zhukov for providing valuable research assistance for this article.

Abstract

This paper reviews Russia's approach to C2 in the information environment. This approach relies on the Soviet technique of "reflexive control," in which Russian operatives model an adversary's decision-making structure and plant subversive information that leads the adversary to make seemingly logical decisions that benefit Moscow. Using reflexive control, the Kremlin aims to subvert NATO's decision-making infrastructure by inciting disunity and disfunction in the alliance. Moscow uses nuclear signaling in the framework of reflexive control to try to fracture the alliance's resolve against Russia. The paper concludes with policy recommendations for NATO's consideration: the introduction of a Perception Management Warfare Assessment Unit and the implementation of a tactic of Counter-Reflexive Control.

Keywords:
Cognitive warfare, nuclear signaling, perception management, reflexive control, Russia

Introduction

In the modern-day digital environment, those who can effectively leverage the digital space wield the most power in the global system. Learning how to conduct not only cyber-attacks, but information operations (IO), psychological operations, and social media campaigns afford beneficiaries significant power over the cognitive functions of their adversaries. Russia has not only learned these tactics but has institutionalized them into its Command and Control (C2) infrastructure (NATO C2OE , 2026). Within this framework, C2 assumes a fundamentally different meaning from how it is understood in the West. While NATO typically views C2 as a purely technical means of executing strategic and operational goals, the Kremlin uses C2 to target not only NATO's technical architecture, but also its cognitive resiliency, seeking to degrade NATO's ability to plan and execute missions from its very foundations.

This situation calls for an immediate reevaluation of NATO IOs, and the creation of new measures that can mitigate the effects of a vulnerable information environment. This paper argues for two key recommendations: The creation of the "Perception Management Warfare Assessment Unit," (PMWAU) and the implementation of a tactic of "counter-reflexive control" (CRC). These initiatives will address the exploitation of NATO's operations while helping the alliance develop robust protocols to avoid exposing its decision-making systems to Russia and thus bypass the carefully laid traps the Kremlin has set for it. In reducing these vulnerabilities, NATO will build a more transparent and effective information system and level the playing field in the information confrontation with Russia.

I Russia's Information Warfare C2 Model

Russia's approach to cyber and information warfare (IW) differs fundamentally from the Western model. The United States, and much of NATO, conceptualizes cyber space as a military domain analogous to air, sea, land, or space, focused on network defense, operational disruption, and domain superiority (NATO, 2024). In Russia, by contrast, cyber is not primarily about defending networks or even technical exploitation alone. It is part of a broader political warfare infrastructure designed to shape perception, influence decision-making, and manage cognitive environments (Creery, 2018). Instead of the term "cyber security," (кибербезопасность) Russia's 2021 National Security Strategy uses the term "information security" (информационная безопасность) (President of the Russian Federation, 2021, p. 19). While this may appear as a semantic difference, it is actually intentional and consequential in the language of the Kremlin. Hence, in this paper we use Russia's term "information security." The Kremlin's prioritization of IW is exemplified in the 2021 National Security Strategy, which states "...information security is achieved through... the development of the forces and means of information warfare." (President of the Russian Federation, 2021, p. 21)

Russia has holistically integrated IW into its C2 system. Per the Ministry of Defense's 2011 Conceptual Views Regarding the Activities of

the Armed Forces of the Russian Federation in the Information Space, "The leadership and the command staff of all levels directly participate in the organization of the activity in the information space during the peacetime and the wartime, in the preparation and in the course of the operations (military engagement)." (Ministry of Defense of the Russian Federation, 2011, p. 8) Influencing the information space is not isolated to wartime activities for the Kremlin; its intelligence agencies work tirelessly to dominate the cyber sphere, using C2 as its framework.

Moscow's IW C2 effort centers around targeting three areas of cognitive influence. First, Moscow has built an offensive response to adversarial information and psychological operations. Its intelligence agencies operate as if an attack is imminent, developing, planning, and implementing preventative offensive operations and striking preemptively (Lozovsky et al., 2019). Second, Moscow's C2 works to constantly weaken its adversaries' information capabilities. This includes anything from outright sabotage, targeting power plants and electrical infrastructure abroad to sowing doubts in existing information capabilities. Finally, Moscow conducts offensive IOs against adversary troops and populations to create an information environment that is beneficial to Kremlin policies.

Unlike NATO where a centralized cyber or IW command may oversee operations, Russian C2 is distributed and reflexive (Vasara, 2020, p. 71). The system is organized as a hierarchy: priorities, goals, and targets are defined at the highest level of state authority, and execution is segregated by responsibility and dispatched to the corresponding agency. By consolidating priorities at the top, the regime can ensure that all actions are aligned with the leadership's strategic objectives, regardless of which department executes them (Vasara, 2020, p. 71). Sitting directly underneath the executive leadership, Russia's Security Council combines intelligence assessments across agencies, integrating leadership from the Federal Security Service (FSB), the Main Directorate of the General Staff (GU) and the Foreign Intelligence Service (SVR), alongside the Kremlin-sponsored media ecosystem (President of the Russian Federation, n.d.).

Federal Security Service (FSB)

The FSB primarily focuses on shaping and protecting the domestic information environment while also contributing to offensive IOs. To shield Russian decision-making from external manipulation, the FSB secures the domestic cognitive environment combining internal control with counter-reflexive shielding. Currently, the FSB is responsible for the implementation of large-scale internet suppression and censorship in Russia (Kolmychenko, 2026)[1]. By monitoring public sentiment, and limiting foreign informational influence, the FSB preserves Russia's cognitive resilience (Government of the Russian Federation, 1995).

The Main Directorate of the General Staff (GU)

The GU operationalizes Russia's C2 doctrine most directly, bearing the primary responsibility for modelling adversary reactions, testing escalation thresholds, and adapting tactics based on the observed responses from the target. Operationally, the GU operates the most direct equivalent of an embedded cognitive assessment capability within military planning, with specialized Units such as 29155, 26165 or 74455 working to integrate cyber-attacks and psychological operations into cohesive campaigns (UK Foreign, Commonwealth, and Development Office, 2025).

Foreign Intelligence Service (SVR)

The SVR primarily conducts cyber espionage operations to collect intelligence in support of Russian strategic objectives.[2] However, the infrastructure it develops and the data it steals

1 http://www.kremlin.ru/acts/assignments/orders/79927 and https://home.treasury.gov/news/press-releases/jy1572

2 More about Russia's SVR operations https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3931959/nsa-issues-updated-guidance-on-russian-svr-cyber-operations/ . Also, see Russia's APT 29 https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/russia-cyber-threat-operations/russia-apt29

are also used to enable cyber-enabled influence and IOs (Bowen, 2022). The U.S. government identified the SVR as one of the two Russian cyber units responsible for cyber campaign-related activities during the 2016 U.S. presidential election. Also, the SVR targets adversary political elites, think tanks, academic institutions, and business networks (Panyi, 2026). Rather than immediate destabilization, the SVR seeks gradual penetration of decision-making ecosystems, seeking to alter critical decision-making infrastructure. This approach reflects Russian doctrine's view of IW as a sustained competition over influence rather than a series of isolated events.

Kremlin-Sponsored Media Ecosystem

Russia's media ecosystem plays a vital role in its IW environment, functioning as both an amplifier and a sensor. State-owned media outlets such as Sputnik and RT (formerly Russia Today) broadcast Russian narratives across the world in a variety of languages and media formats (U.S. Department of State, 2022). They aim not only to propagate the Russian government's version of reality, but more fundamentally to foment social division and "to undermine the official version of events, even the very idea that there is a true version of events and foster a kind of policy paralysis." (MacFarquhar, 2016). Kremlin-sponsored bloggers on social media sites like Telegram allow further dissemination of narratives, often disguising their true origins (Global Disinformation Unit, BBC World Service, 2025). This architecture constitutes a distributed but coherent command-and-control system for IW. It is centralized in intent, decentralized in execution, and continuous in operations, whether peacetime or conflict (Bondar, 2026). This structure creates the ideal circumstance for IOs, in which leadership can quickly distribute instructions to initiate new campaigns or adjust those in progress. At the same time, decentralized execution makes it difficult to attribute operations back to the Kremlin, while acting as a force multiplier as IOs are carried out from multiple outlets and directions.

II Reflexive Control as the Core Logic

Russian information-warfare command and control can best be understood as the institutionalization of reflexive control (Snegovaya, 2015). Reflexive control (рефлексивное управление) has been central to Russian strategy since the Soviet era. Developed by Vladimir Lefebvre in the 1960s, reflexive control seeks to transmit carefully prepared information to an adversary so that the adversary voluntarily makes decisions favorable to the initiator wrongly believing those decisions are autonomous. It aims to structure the opponent's perception so that certain choices appear logical and necessary, while actually being predetermined and subversive (Lefebvre & Smolyan, 1968).

Lefebvre's framework seeks to mathematically model decision-making by mapping a target's layered perceptions: not only how the target perceives himself and relevant others, but how he believes others perceive him and each other in turn (Lefebvre & Smolyan, 1968, p. 20). Understanding the system, cultural nuances, and global environment that decisions are embedded in is key to shaping an adversary's decision-making process. It models how injecting specific information into the system at select times would shape decision making not just at the crux, but at every layer of the decision-making process (Snegovaya, 2015, p. 10). Beyond influencing a single decision, the reflexive game theory model alters how the adversary analyzes every input from the system through the desired lens, unknowingly forfeiting control to Russia.

Russian IW therefore does not primarily aim to "win arguments." It seeks to overload cognition, exploit bias and trigger desired adversary's responses. The adversary is treated as a system with different inputs so Russia can design stimuli that generate desired outputs (Merriam, 2023).

In practice, this operational loop of reflexive control begins with modeling the adversary. With this model, Russia can construct detailed assessments of political culture, ideological fault lines, media behavior or legal constraints (Thomas, 2004). The adversary modeling phase is continuous and feeds strategic planning (Merriam, 2023). Despite their varied responsibilities, each agency's approach

remains aligned with the goals of the Presidential administration, a key feature of the system's organization (Galeotti, 2020).

A core goal of Russia's IW C2 model is to disrupt or disorganize the functionality of its adversary's command-and-control structure. Timothy Thomas wrote in detail how Russia has been using reflexive control to disrupt adversary's C2 (Thomas, 2019). Major General Yuriy Lastochkin, head of the Defense Ministry's electronic warfare force (REB), established "disorganizing adversary C2" as the guiding principle of the REB's combat employment strategy.

III NATO as a Target of Reflexive Influence

Russia's strategic approach to NATO is grounded in the logic of reflexive control. Rather than prioritizing direct kinetic confrontation with NATO, Moscow seeks to influence how the Alliance interprets signals and how it deliberates under pressure. The central target is not territory or force posture alone, but the Alliance's decision-making process itself (Thomas, 2016).

Russia models NATO as a multi-member, consensus-driven alliance characterized by diverse political cultures and varying threat perceptions (NATO, n.d.). For example, Slovakia and Hungary have very different interests from France or the United Kingdom. Countries on the alliance's Eastern flank are frequently more "hawkish" on Russia than other member states (Kamiński & Śliwa, 2023). Decision-making requires consultation and unanimity, and Moscow has sought to exploit these differences. Russia's objective is not necessarily to fracture NATO outright, but to maximize indecision or produce asymmetric responses (Galeotti, 2025). One state may call for escalation, another for caution that would slow action and project fragmentation. Even temporary misalignment can produce strategic leverage. Russia also conducts such attacks to test NATO's reaction and build a strategy for future endeavors based on any discovered weaknesses.

For instance, Russia might conduct a drone incursion in Poland to cause chaos in NATO decision-making and strain the viability of their key Article 5 mutual defense clause (NATO, n.d.). A drone incursion would likely warrant an immediate air defense alert and military aircraft response, and likely an emergency session to consult NATO and determine an appropriate response in the following days. If this process leads to indecision and Article 5 is not invoked, Russia could point to this as another example of NATO's weakness and inability to protect its own, sowing potential mistrust amongst its more vulnerable members.

This exact scenario played out in September 2025, when a Russian drone invaded Polish airspace. Polish Foreign Minister Radoslaw Sikorski noted that the Kremlin "wanted to test the readiness of NATO allies" (O'Connor, 2025). Russia likely modeled the severity of the immediate military response, determining how quickly members could convene and if the incursion could be considered a violation of Article 5. In the ensuing months, Russia's operational loop of reflexive control has likely taken in the inputs of how the incursion impacted NATO's decision-making and fed these into models to understand and evaluate which desired outcomes were achieved and what operational changes might need to be made for future attacks.

IV Nuclear Information Operations as Russia's Cognitive Weapon

Nuclear weapons are a mainstay of Russian foreign policy, and the Kremlin frequently defers to nuclear signaling when it faces international opposition. Putin has repeatedly threatened to use "all available means" to defend Russia and has leveraged its arsenal of nuclear capable missiles to discourage NATO support for Ukraine (The Associated Press, 2022). Indeed, when losing on the battlefield in Ukraine in September 2024, Putin resorted to saber rattling, conducting an exercise with possible nuclear weapons on the border of Ukraine (Schnieder, 2024). Just as recently as May 2026, Russia organized a three-day nuclear exercise in Belarus, where they first began repositioned tactical nuclear forces in 2022 (Arms Control Association, 2024: The Associated Press, 2026). Nuclear reflexive control is not primarily about actual nuclear weapons use. It is about shaping NATO behavior through manipulated perception.

Nuclear signaling serves a broader strategic purpose than purely deterring NATO: following Russia's principle of "escalate to de-escalate," (Haney, 2016) the Kremlin leverages nuclear signaling to both shape and fracture NATO responses, forcing NATO members to rapidly evaluate the credibility of the threat and unanimously decide how to "escalate or de-escalate". Unanimity is considerably more difficult when faced with a direct threat, often causing fragmentation among the more risk-averse members and the more "volatile" members over an appropriate response. To avoid direct confrontation or unnecessary loss of life, Russia projects that NATO will choose de-escalation or diplomacy, making nuclear signaling a very effective weapon (Horovitz & Arndt, 2022).

In the context of nuclear IOs, Russia's IW begins with perception targeting. Russia may announce nuclear exercises, highlight nuclear force deployments, adjust readiness postures (even just rhetorically), or allow selective leaks suggesting escalatory intent (Matle & Rácz, 2026). These actions do not necessarily indicate imminent weapons use. Instead, they are designed to elevate perceived risk inside NATO capitals. By increasing uncertainty around intent, Moscow seeks to widen the gap between objective capability and subjective threat perception.

Reflexive nuclear IOs unfold in stages. First, Russia targets NATO's perception of threat by elevating uncertainty around intent. Second, it exploits alliance decision patterns, such as consensus requirements, risk aversion, and domestic constraints. Third, it operates at the level of "perception of perceptions": shaping what NATO believes other NATO members believe (Selhorst, 2016). Finally, it leverages multi-member variability. A frontline state may perceive imminent danger; another may interpret posturing.

One consistent success the Kremlin has achieved through its reflexive information campaigning is its ability to muddy the decision-making process surrounding NATO's relationship to Ukraine. NATO members have long disagreed on the feasibility and benefits of admitting Ukraine into NATO. Because a consensus is difficult to reach, the Kremlin has found multiple avenues of systematic exploitation of NATO's indecision. By framing NATO as an internally fractured and indecisive body unwilling to take risks to fully support Ukraine, and amplifying narratives of the futility of NATO accession to Ukrainian audiences, the Kremlin is encouraging further decision-making paralysis and infighting (Lange-Ionatamišvili, 2016, p. 17-19). A prime example of NATO's fractured response to the conflict in Ukraine was in 2022 and 2023, when Ukraine requested long-range missiles from the United States (Trevelyan & Osborn, 2022). These missiles would afford Ukraine the ability to reach targets deeper inside Russian occupied territory, including supply lines, airbases and rail networks. Despite their clear tactical advantage and Washington's vocal support for the Ukrainian war effort, Kremlin saber rattling proved effective in the short-term; the US repeatedly denied Ukrainian requests in the first years of the war as Putin threatened that NATO involvement would be met with swift escalation. This position was notably backed by Germany and other NATO members, who worried that Russia's "red lines" were a credible threat. Through nuclear signaling, Russia leveraged NATO's varied risk-appetites to achieve its desired end goal of limiting military support for Ukraine.

Reflexive nuclear IOs also operates at a meta-perception level, what might be called "perception of perceptions". Russian planners consider not only what NATO believes Russia is doing, but what NATO believes other NATO members believe. By shaping the information environment through media amplification, Russia can cloud diplomatic engagements with outside noise (false narratives), hampering efforts to clarify state intentions and perceptions (Stradinger, 2024).

"Perception of perceptions" is an important example of Russia's emphasis on C2 disorganization. By targeting NATO's ability to organize and understand its own members positions, while facing the threat of nuclear escalation, Russia stuns the alliance's ability to act quickly and in a unitary fashion. Disorganization is especially pronounced and effective in a multi-member alliance. Different states may interpret identical signals differently.

V "Perception Management Warfare Assessment Unit," (PMWAU)

Neutralizing reflexive control in the nuclear domain requires protecting decision-making from manipulated perception. To this end, NATO should develop a Perception Management Warfare Assessment Unit (PMWAU). The establishment of a PMWAU within NATO would offer a structured countermeasure to mitigate this vulnerability. The purpose of a PMWAU would not be to dominate narratives or outcompete disinformation in the public sphere. Rather, it would protect Alliance decision-making from adversary-induced distortion.

A PMWAU would perform three core functions. First, it would provide real-time threat assessment, distinguishing actual military or operational risk from perception-driven escalation. Second, it would identify cognitive biases or distortions introduced by Russia's signaling and manipulating emotional response. Third, it would deliver corrective feedback to decision-makers, ensuring that policy choices are grounded in calibrated assessments rather than manipulated decisions.

Operationally, the integration of a PMWAU into NATO would reduce both overreaction and undue hesitation. By providing perception-corrected analysis, it would narrow inter-member divergence and strengthen synchronized responses. In effect, it would transform NATO from a reflexive target reacting predictably to information shocks into a more resilient decision network capable of absorbing and contextualizing Russia's cognitive stimuli.

VI Modeling a Perception Management Warfare Assessment Unit response to Kremlin Reflexive Nuclear Information Operations

The first function of a PMWAU in a nuclear signaling scenario would be signal verification. The PMWAU would evaluate reported adversarial deployments, exercises, or readiness changes to determine whether they reflect substantive shifts in capability or posture, or whether they constitute demonstrative signaling. This assessment would integrate satellite imagery, cyber intelligence, national contributions, and doctrinal analysis. By grounding deliberation in verified indicators, the PMWAU would reduce the likelihood of perception-driven escalation, protecting NATO decision-making from attempted reflexive influence.

The PMWAU's second function would be bias correction. Nuclear signals are designed to amplify fear. A PMWAU would provide perception-adjusted assessments that distinguish between credible threat indicators and political messaging. By explicitly separating emotional salience from operational likelihood, it would build NATO's resiliency against cognitive manipulation.

Third, a PMWAU would facilitate coordinated decision-making. Asymmetries in information distribution and skepticism regarding foreign intelligence assessments frequently impede the NATO decision-making process and open gaps our adversaries can exploit.

Finally, a PMWAU would provide feedback and adaptation. For instance, in late 2025, Russia announced it was moving nuclear weapons close to the EU border (Khomenko, 2025). NATO could use the PMWAU to analyze Russian signaling patterns such as recurring drills near NATO borders or synchronized media amplification over time to identify reflexive tactics. Continuous monitoring would enable the Alliance to anticipate and contextualize future signals, reducing their disruptive potential. The aim is to prevent each episode from being treated as unprecedented when it follows an identifiable pattern.

VII Counter-Reflexive Control (CRC): How to put Russia on the defensive

As Russia increasingly employs reflexive control tactics against NATO, alliance disputes and hesitation will become more commonplace. To rectify the situation before a more serious disagreement arises, it is imperative for NATO to develop measures to maintain a united front. To do this, NATO should begin implementing the tactic of Counter-Reflexive Control, aimed at facilitating inter-alliance communication and mitigating the effects of Russian IW tactics. CRC should deny Russia the ability to predict or manipulate Alliance decision-making through cognitive exploitation and

reaction-forcing tactics. Beyond the PMWAU, the use of CRC provides a comprehensive framework for protecting Alliance decision autonomy, one which recognizes that adversaries exploit NATO's transparency, consensus procedures, legal thresholds, and pressure for speed (Merriam, 2023).

CRC tactics also include measures to cut the enemy off from information about one's own decision-making, which would vastly degrade adversarial reflexive cognitive capabilities. For Western countries which place value on transparency, this can be a challenge. However, measures can be taken which limit Russian access to feedback information, within the limits set by the legal requirements for transparency (Vasara, 2023).

Finally, CRC techniques offer a means to better understand and categorize threats, which can reduce the time pressure that frequently pushes actors towards making decisions that are either more predictable or not fully vetted for potential adversarial reflexive influence. As discussed above, nuclear threats particularly take advantage of time stress to put pressure on decision-making.

NATO should measure the success of CRC tactics not by narrative dominance but by preserved cohesion, avoided premature escalation, maintained autonomy, and increased adversary uncertainty. Experts point to the publication of Russian troop movements and attack plans in early 2022 as a particularly effective example of countering reflexive control techniques, one which disrupted Kremlin propaganda and paved the way to strengthening and expanding the NATO alliance (Vasara, 2023).

VIII Strategic Implications

The central insight from analyzing Russia's C2 modeling and reflexive influence campaigning against NATO is that decision-making itself is a contested capability. Russia's command and control system institutionalizes reflexive control, integrating intelligence, media, cyber operations, and political direction to shape adversary cognition. Russia's conception of C2, as well as its understanding of hybrid war, persistently place it on the offensive against NATO's cognitive space. NATO's structural strengths of transparency, consultation, and democratic legitimacy can become vulnerabilities if rendered predictable. Putin's saber rattling has already made it more difficult for NATO countries to maintain a unified response, leveraging Russia's nuclear arsenal as both a kinetic and psychological weapon. Using response reflexive control modelling, the Kremlin clouds threat credibility, exploits vulnerabilities in NATO's consensus-driven system, and alters perceptions.

Ultimately, Russia's IW model seeks to govern adversary reactions rather than defeat adversary forces directly. The information space has risen to prominence as the primary battleground, and hybrid warfare is the new norm for NATO adversaries. Putin's regime is actively using Ukraine as a test ground for its reflexive control tactics, learning how to leverage perceptions and strategic information input to shape real outcomes. In this space, where ideas are weapons, NATO should build cognitive resiliency.

To this end, establishing a PMWAU will be paramount in regulating NATO's information space, assessing threat credibility, evaluating Russian nuclear signaling based on historical precedents, and coordinating alliance decisions to render Russian psychological tactics ineffective. Although this article focuses on reflexive control in the context of nuclear weapons, the concept can be broadly applied to other scenarios in which Russia seeks to influence, disrupt, or manipulate NATO's C2 decision-making processes.

NATO should also invest in Counter-Reflexive Control tactics and techniques to ensure that it retains freedom of action by defending its cognitive domain. The PMWAU and CRC will work together to empower NATO to make decisions without any Kremlin poison seeping in. In a monitored and coordinated information space, Russian strategies that rely on altered perceptions will no longer have the same effect on NATO decision-making, affording the alliance to make unified, informed decisions to achieve strategic goals. If NATO does not invest in these critical resources, it risks losing before the fight even begins.

References

Associated Press. (2021). *Cornered by war, Putin makes another nuclear threat.* The Hill. https://thehill.com/homenews/ap/ap-international/ap-cornered-by-war-putin-makes-another-nuclear-threat/

Copp, T., & Weisgerber, M. (2022). Poland offers fighter jets for Ukraine, but US rejects swap-and-send idea. *Defense One*. https://www.defenseone.com/threats/2022/03/poland-offers-fighter-jets-ukraine-will-us-agree-twist/362928/

Creery, M. (2018). *Russia strategic understanding of cyber: Not an information war — a war on information.* Georgetown Security Studies Review. https://georgetownsecuritystudiesreview.org/2018/12/05/russia-strategic-understanding-of-cyber-not-an-information-war-a-war-on-information/

Bondar, K. (2026). *How Russia is reshaping command and control for AI-enabled warfare.* Center for Strategic and International Studies. https://www.csis.org/analysis/how-russia-reshaping-command-and-control-ai-enabled-warfare

Bowen, A. (2022). *Russian cyber units.* Congressional Research Service. https://www.congress.gov/crs-product/IF11718

Bowen, A. (2025). *Russia's Foreign Intelligence Services.* Library of Congress. https://www.congress.gov/crsproduct/IF12865#:~:text=As%20Russia's%20primary%20civilian%20foreign,Russia%20or%20the%20Russian%20government

Galeotti, M. (2020). *The Presidential Administration: The Command and Control Nexus of Putin's Russia.* George C. Marshall European Center for Security Studies. https://www.marshallcenter.org/en/publications/security-insights/presidential-administration-command-and-control-nexus-putins-russia-0

Galeotti, M. (2025). *When disinformation meets disruption: Russia's strategy of paralysis.* Фондация за хуманитарни и социални изследвания -– София. https://www.ceeol.com/search/article-detail?id=1373757

Global Disinformation Unit, BBC World Service. (2025). *The Telegram channels spreading pro-Russian propaganda in Poland.* BBC News. https://www.bbc.com/news/articles/c0eqdd53dd7o

Government of the Russian Federation. (1995). *Федеральный закон "О федеральной службе безопасности".* https://www.consultant.ru/document/cons_doc_LAW_6300/

Haney, C. (2016). *Project on nuclear issues capstone conference.* U.S. Strategic Command. https://www.stratcom.mil/Media/Speeches/Article/986478/project-on-nuclear-issues-capstone-conference/

Horovitz, L. & Arndt, A. (2022). *Russia's catch-all nuclear rhetoric in its war against Ukraine.* Stiftung Wissenschaft und Politik. https://www.swp-berlin.org/en/publication/russias-catch-all-nuclear-rhetoric-in-its-war-against-ukraine

Kamiński, M., & Śliwa, Z. (2023). *Poland's threat assessment: Deepened, not changed.* PRISM. https://www.researchgate.net/publication/371874715_Poland's_Threat_Assessment_Deepened_Not_Changed

Khomenko, I. (2025). *Russia parks Oreshnik nuclear missiles in Belarus—but aims at the West.* United24 Media. https://united24media.com/latest-news/russia-parks-oreshnik-nuclear-missiles-in-belarus-but-aims-at-the-west-14603

Kolomychenko, M. (2026). *Who is responsible for the demise of the Russian internet?* Carnegie Endowment for International Peace. https://carnegieendowment.org/russia-eurasia/politika/2026/04/russia-internet-crackdown

Lange-Ionatamišvili, E. (2016). *Handbook of Russian information warfare.* NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf

Lefebvre V., & Smolyan G. (1968). *Conflict Algebra.* Moscow: Znanie Press.

Lozovsky, V., Kuzmenko, A., & Kuznetsov, A. (2019). *Информационная безопасность: защита от внутренних и внешних воздействий в киберпространстве*. Voyennaya Mysl. https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-zaschita-ot-vnutrennih-i-vneshnih-vozdeystviy-v-kiberprostranstve/viewer

NATO Command and Control Centre of Excellence. (2026). *Information operations in Russian command and control.* https://c2coe.org/wp-content/uploads/Library%20Documents/Articles/20260520%20Information%20Operations%20in%20Russian%20Command%20and%20Control%20Shortread.pdf

North Atlantic Treaty Organization. (n.d.). *Collective defence and Article 5.* https://www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5

North Atlantic Treaty Organization. (2024). *Cyber defence.* https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

North Atlantic Treaty Organization. (n.d.). *What is NATO?* https://www.nato.int/en/what-is-nato

MacFarquhar, N. (2016). *A powerful Russian weapon: The spread of false stories.* The New York Times. https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html

Matle, A. &, Rácz, A. (2026). *Russia's nuclear signaling in 2026 and the implications for European security.* German Council on Foreign Relations. https://dgap.org/en/research/publications/russias-nuclear-signaling-2026-and-implications-european-security

Merriam, J. (2023). *One move ahead — diagnosing and countering Russian reflexive control.* The Journal of Slavic Military Studies. https://www.tandfonline.com/doi/full/10.1080/13518046.2023.2201113

Ministry of Defense of the Russian Federation (2011). *Концептуальные взгляды на деятельность вооруженных сил Российской Федерации в информационном пространстве.* https://info.publicintelligence.net/RU-CyberStrategy.pdf

O'Connor, T. (2025). *Poland deputy PM seeks 'toughest' pressure on Russia after drone incursion. Newsweek.* https://www.newsweek.com/poland-will-take-toughest-measures-over-russia-drone-incursion-deputy-pm-2131497

Panyi, S. (2026) *The think-tank spy: Russian diplomat infiltrating Orbán's right-wing elite quietly expelled.* VSquare. https://vsquare.org/the-think-tank-spy-russian-diplomat-infiltrating-orbans-right-wing-elite-quietly-expelled/

President of the Russian Federation. (2021). *Стратегия национальной безопасности Российской Федерации. http://www.scrf.gov.ru/media/files/file/9htlEYM6sh7mr0riotJdAd7atKKM7w9J.pdf* .pdf

President of the Russian Federation. (n.d.). *Members – Security Council structure.* http://en.kremlin.ru/structure/security-council/members

Reynolds, J. (2026). *"Russia blames UK for deadly Storm Shadow missile strike on munitions factory,"* The Independent. https://www.independent.co.uk/news/world/europe/russia-britain-storm-shadow-missile-factory-ukraine-b2937047.html

Schnieder, M. (2024). *The Russian non-strategic (tactical) nuclear exercise.* RealClear Defense. https://www.realcleardefense.com/articles/2024/09/17/the_russian_non-strategic_tactical_nuclear_exercise_1058803.html

Selhorst, A. (2016). *Russia's perception warfare: The development of Gerasimov's doctrine in Estonia and Georgia and it's application in Ukraine.* Militaire Spectator. https://www.militairespectator.nl/sites/default/files/uitgaven/inhoudsopgave/Militaire%20Spectator%204-2016%20Selhorst.pdf

Snegovaya, M. (2015). *Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid warfare.* Institute for the Study of War. https://understandingwar.org/wp-content/uploads/2024/05/Russian20Report20120Putin27s20Information20Warfare20in20Ukraine-20Soviet20Origins20of20Russias20Hybrid20Warfare.pdf

Stradinger, J. (2024). *Narrative intelligence: Detecting Chinese and Russian information operations to disrupt NATO unity.* Foreign Policy Research Institute. https://www.fpri.org/article/2024/11/intelligence-china-russia-information-operations-against-nato/

Thomas, T. (2019). *Russian military thought: Concepts and elements*. The MITRE Corporation. https://oe.t2com.army.mil/site-content/OEE/FMSO%20Books/2019_08_01-Russian-Military-Thought_Concepts-and-Elements-_Timothy-Thomas_.pdf

Thomas, T. (2016). *Russia's 21st century information war: Working to undermine and destabilize populations.* NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/timothy_thomas.pdf

Thomas, T. (2004). *Russia's reflexive control theory and the military.* The Journal of Slavic Military Studies. https://www.tandfonline.com/doi/abs/10.1080/13518040490450529

Trevelyan, M., & Osborn, A. (2024). *Putin draws a nuclear red line for the West.* Reuters. https://www.reuters.com/world/europe/putin-draws-nuclear-red-line-west-2024-09-27/

Vasara, A. (2023). *How to respond to the challenge of reflexive control?* Russian Military and Security Research Group. https://rusmilsec.blog/2023/12/12/how-to-respond-to-the-challenge-of-reflexive-control/

Vasara, A. (2020). *Theory of reflexive control: Origins, evolution and application in the framework of contemporary Russian military strategy.* National Defence University. https://www.doria.fi/bitstream/handle/10024/176978/Vasara_FDS22_Theory%20of%20Reflexive%20Control%20%28web1%29-1.pdf

UK Foreign, Commonwealth, and Development Office. (2025). *Profile: GRU cyber and hybrid threat operations.* https://www.gov.uk/government/publications/profile-gru-cyber-and-hybrid-threat-operations/profile-gru-cyber-and-hybrid-threat-operations

U.S. Department of State, Global Engagement Center. (2022). *Kremlin-funded media: RT and Sputnik's role in Russia's disinformation and propaganda ecosystem.* https://2021-2025.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf

Author biography

Dr. Ivana Stradner
Rear Admiral (Ret.) Mark Montgomery

Dr. Ivana Stradner serves as a research fellow with FDD's Barish Center for Media Integrity. She studies Russia's security strategies and military doctrines to understand how Russia uses information operations for strategic communication. Her work examines both the psychological and technical aspects of Russian information security.

Rear Admiral (Ret.) Mark Montgomery serves as senior director of the Foundation for Defense of Democracies' (FDD) Center on Cyber and Technology Innovation (CCTI). Mark served for more than three decades in the U.S. Navy, held senior leadership roles in Congress, and is a recognized expert on cyber and technology policy.