DEFENSE DOSSIER

ISSUE 44

DECEMBER 2025

AFPC

AMERICAN FOREIGN POLICY COUNCIL

AFPC

AMERICAN FOREIGN POLICY COUNCIL

Explaining the World. Empowering Policymakers.

DEFENSE DOSSIER

DECEMBER 2025 | ISSUE 44

LETTER FROM THE EDITORS

Welcome to the December 2025 issue of AFPC's *Defense Dossier*. Russia's war against Ukraine has revealed how modern state competition is increasingly being waged through information, industry, and political coercion—often below the threshold of open conflict. The challenge for the United States and its allies is no longer whether Ukraine matters, but whether we are learning the right lessons from a conflict that spans continents, activates new domains, and increasingly blurs the traditional boundaries between peace and war.

This issue examines those lessons from multiple perspectives. We begin with Russia's global ambitions, which persist despite material constraints, before exploring how Moscow weaponizes the information domain to erode Western cohesion. We then turn to the material foundations of modern warfare—how supply chains have become instruments of coercion and how Ukraine has transformed itself into a defense innovation laboratory under fire. The issue concludes with an analysis of NATO's evolving mission as it confronts a spectrum of provocations calibrated to fracture unity without triggering collective defense.

Taken together, these essays argue that Ukraine is not only a battlefield, but a warning and an opportunity. The war has exposed vulnerabilities in Western institutions while demonstrating how adaptation and innovation can offset material disadvantage. Whether the United States and its allies absorb these lessons—or continue to rely on outdated assumptions—will help determine the global balance of power in the years ahead.

All the best,

Ilan Berman
Chief Editor

Richard M. Harrison
Managing Editor

Understanding Russia's Global War

Stephen Blank

Russia's aggression against Ukraine has become a global war against the West. Yet, in their analysis of the conflict, virtually all the experts emphasize the constraints on Russian power projection. How, then, to reconcile the Kremlin's efforts global power projection with the very real limits that are now placed upon Russian capabilities?

AN INTERNATIONAL FOOTPRINT

In Asia, Russia has forged an alliance with China, without whose help it simply could not continue to prosecute this war.[1] In return, it is supporting China's military machine in a manner of ways (including by training Chinese airborne forces for future assaults on Taiwan.)[2] Along with Chinese air and naval forces, Russia now regularly conducts military probes (i.e., submarine reconnaissance and aerial overflights) of Japan, South Korea, and the Pacific Arctic, Alaska and the Aleutian Islands. The Kremlin has also signed a formal defense alliance with North Korea, without whose help its warmaking capabilities would be severely diminished. In return, it has rewarded Pyongyang with economic, diplomatic, and military support to the point of sending it nuclear submarine technologies.[3] Finally, in East and South Asia, Russia's aggression is being fueled by Indian and Chinese purchases of oil and gas.

In the Middle East, Moscow has parlayed its partnership with Tehran into meaningful Iranian assistance in the form of supplies of thousands of drones, as well as help in building an indigenous capability to build more of the same. In return, Russia is believed to have provided material support in the forms of weapons or technologies for Iran's military and its nuclear program.[4] This help, moreover, has trickled down to Iranian proxies, with terrorist groups like Yemen's Houthis receiving Russian weapons and intelligence support.[5]

In Europe, the situation is even worse. Moscow was waging a non-kinetic war throughout the continent for at least a generation before its current claims of European aggression. And that practice has continued.[6] Apart from continental-wide attacks on infrastructure, Moscow is carrying out assassinations, arsons, attempting to blow up civilian airline flights in mid-air, recruiting organized and individual criminals to execute these attacks, spending billions to subsidize pro-Russian media, politicians, and parties, using energy blackmail, and influence operations to bring pro-Russian parties to power and disrupt if not reverse the continuing trend towards European integration.

In Africa and South America, the so-called "Global South," Russia utilizes many of the same instruments to powerful effect. Indeed, some observers attribute Russia's spreading influence in Africa, particularly in the Sahel and Southern Africa, to its long-running informational campaigns there.[7] In the Sahel, Moscow has also gained leverage through its willingness to support local dictatorships against Islamic terrorist threats—first via the (ostensibly private) Wagner Group and now through its openly state-controlled Africa Corps. In return, Russia has gained valuable control over mining and raw materials in these countries—resources that enrich the Russian state and help bankroll its war machine. The ultimate prize here, though, are naval and/or air bases from which Russia can expand its influence over local politics, position itself as a global great power, and challenge NATO and U.S. power projection and fleets.[8] Those same campaigns are equally ubiquitous across Latin America, and aim to establish lasting influence over the politics and economics of Latin American states.

RUSSIA'S IDEOLOGY OF WARFARE

Yet despite these global ambitions and the scope of Russian power, most observers tend to denigrate or belittle Russia's capabilities. Admittedly, these are significantly

***Dr. Stephen Blank** is Senior Fellow at the Foreign Policy Research Institute in Philadelphia, PA.*

> **Russia's unceasing quest to regain (and force others to acknowledge) its imperial and global great power status presupposes constant war with all its interlocutors.**

constrained as a result of Western pressure. Yet Russia's record of power projection is still quite impressive. One way to understand the apparent disparity between resource constraints and global capacity is to grasp Russia's ideology of warfare.

First Russia has undergone a counter-revolution that has restored the patrimonial Muscovite autocracy with a service state headed by a Tsar, Vladimir Putin, who towers over his Boyar entourage. This service state—in which rank, status, and property are held on condition of loyalty and state service—has also become more repressive, and is entwined with a neo-Tsarist ideology of autocracy, orthodoxy, and Russian nationality. This system's motor is its economic-political internal colonialism and the ideology that has arisen around it.[9] At the same time, it has gravitated to the idea that it possesses a unique, and holy, civilizational identity. This ideology derives from Russian reactionary thinking of the XIX -XXI centuries, including Russian Eurasianism.[10] This ideology attributes to Russia a primordial and divinely ascribed status as a holy empire that must be reacquired in order for the state to survive.

Since empire is the fundamental corollary of autocracy and intrinsically denotes the diminished sovereignty of all neighboring territories and states, Russia's unceasing quest to regain (and force others to acknowledge) its imperial and global great power status presupposes constant war with all its interlocutors. Yet, as its rulers fully grasp, Russia remains comparatively backward in the sinews of war, e.g. economics and military capabilities except for manpower. Therefore, the current Russian government necessarily employs every conceivable instrument of war, as did its Soviet predecessor, to unhinge, derange, and destabilize governments in Europe, North and South America, and Asia. This should come as no surprise, since Russia's current leadership represents either KGB veterans or their biological and ideological heirs.

From its inception, Putin's Russia was forged in war—first against the Chechens and then increasingly against the West. Since his mission, as many have attested, is to "regather Russian lands," it is no surprise that Russia under Putin has swung decisively to the embrace of an imperial ideology. Tactically too, Russian policy has moved steadily and with increasingly open coerciveness to subordinate the Caucasus, Central Asia and Belarus to the greatest degree possible.[11]

Since the concept of empire inherently presupposes the ever-present use of force, it is to be expected that Russian security policy originates from the presupposition of conflict. Even when they are consciously lying, Russian spokesmen fully believe that Russia is constantly under siege, if not under actual threat of attack and even extinction.[12]

Furthermore, because they believe in this threat, preservation of the governing system becomes inextricably linked to the restoration of empire. Catherine the Great reportedly declared in her day that she had no way to preserve her frontiers other than to expand them. That opinion holds true today.

THE PARAMETERS OF WAR

On this basis, we can see how Russia—in spite of all of its present problems—can nonetheless represent a global challenge. Since Russia's strategic borders, as presented in official statements (rather than reality or international law), impinge on Europe, Central, and Northeast Asia, and the greater Middle East, it consistently demands a voice in those regions—whether or not such status is warranted.

Third, the nature of the state allows it to posit itself simultaneously as aggressor and victim, as colonizer and colonized. And it permits it to assert itself, via incessant propaganda, as the leader of a great cause, notwithstanding the venality of its motives.

> **Russia remains comparatively backward in the sinews of war, e.g. economics and military capabilities except for manpower. Therefore, the current Russian government necessarily employs every conceivable instrument of war, as did its Soviet predecessor, to unhinge, derange, and destabilize governments in Europe, North and South America, and Asia.**

Fourth, since its leaders can never be satisfied with their gains, Russia has long since globalized its interests and capabilities. Since 1917, its military thinking and state behavior, often manifested through proxies like the Comintern, Wagner, and its current network of Eurasian proxies, has developed previously unimagined instruments of power that extend the Kremlin's capabilities and promote its interests abroad. These manifestations can be seen today in the so-called hybrid attacks plaguing Europe, and in Russia's reinvigorated weaponization of disinformation and false narratives to change global perceptions about itself and its objectives.

The innovative nature of Russian thinking concerning war and peace enable it to punch above its weight globally. Russia is generating new sources and methods of power, and thereby greatly expanding the terms of reference for contemporary warfare. To the degree that we continue to, discount, overlook, and ignore Russia's capabilities and the ideology underpinning them, we will continue to be surprised when Moscow behaves in unpredictable ways. That, in turn, is precisely what Moscow wants.

ENDNOTES

[1] Elina Rybakova, Testimony before the U.S.-China Economic and Security Review Commission, February 20, 2025, https://www.uscc.gov/sites/default/files/2025-02/Elina_Ribakova_Testimony.pdf.

[2] Oleksandr V. Danylyuk and Jack Watling, "How Russia Is Helping China Prepare to Seize Taiwan," RUSI, September 26, 2025, https://www.rusi.org/explore-our-research/publications/commentary/how-russia-helping-china-prepare-seize-taiwan.

[3] Ryan Chan, "Russia Gives North Korea Nuclear Submarine Technology: Report," *Newsweek*, September 18, 2025, https://www.newsweek.com/russia-gives-north-korea-nuclear-submarine-technology-2131662.

[4] See, for instance, Alexander Palmer and Sofiia Syzonenko, "The Limits of Russia's Friendship: How Moscow Sees the Iran Crisis," Center for Strategic & International Studies, July 8, 2025, https://www.csis.org/analysis/limits-russias-friendship-how-moscow-sees-iran-crisis.

[5] Stephen Blank, "Restoring Deterrence and Freedom of Navigation in the Red Sea: The Interaction of Regional and Foreign Actors," *Journal of Policy and Strategy* 5, iss. 2, 2025, 61-90, https://nipp.org/wp-content/uploads/2025/06/Analysis-Blank-5.2.pdf.

[6] "Briefing on Incursion of Russian Aircraft into Estonian Airspace," Security Council Report, September 21, 2025, https://www.securitycouncilreport.org/whatsinblue/2025/09/briefing-on-incursion-of-russian-aircraft-into-estonian-airspace.php.

[7] Jason Warner and Mark Duerksen, "Why do Skeptics Ignore the Evidence of Russian Influence Operations in Africa?" Modern War Institute, March

19, 2025, HTTPS://MWI.WESTPOINT.EDU/WHY-DO-SKEPTICS-IGNORE-THE-EVIDENCE-OF-RUSSIAN-INFLUENCE-OPERATIONS-IN-AFRICA/.

[8] Stephen Blank, "Gunboat Diplomacy a la Russe: Russia's Naval Base In Sudan and Its Implications," *Defense & Security Analysis* XXXVIII, no. 3, 1-21, 2022, https://www.tandfonline.com/doi/full/10.1080/14751798.2022.2122204.

[9] Alexander Etkind, *Internal Colonialism: Russia's Imperial Experience* (London: Polity Press, 2011).

[10] Mark Bassin, Sergei Glebov and Marlene Laruelle, eds., *Between Europe and Asia: The Origins, Theories, and Legacies of Russian Eurasianism* (Pittsburgh: University of Pittsburgh Press, 2015)

[11] Svante Cornell, "Is Central Asia Stable? Conflict Risks and Drivers of Instability," Central Asia-Caucasus Institute *Silk Road Paper*, May 2025, https://www.silkroadstudies.org/resources/2505-Instab-final_merged.pdf.

[12] Dmitry Minic, "La dissuasion nucléaire russe à l'épreuve de la guerre en Ukraine [Russian Nuclear Deterrence Put To the Test By the War in Ukraine]," Institut Francais des Relations Internationales, October 6, 2025, https://www.ifri.org/fr/etudes/la-dissuasion-nucleaire-russe-lepreuve-de-la-guerre-en-ukraine.

The Informational Front in Russia's War

Ivana Stradner

While policymakers in Washington and European capitals tend to debate troop movements and sanctions, focusing on conventional kinetic warfighting techniques, the Kremlin is busy waging a non-kinetic information war against the West. Russia's theoretical framework positions information warfare as one of the key domains of future conflict, with prominent military leaders and theorists projecting a "sixth generation" of "non-contact" warfare where conflicts "will be resolved… primarily by taking advantage of information superiority."[1] In this new domain of warfare, the strategic objective is not battlefield dominance, but rather degrading adversary decision-making, controlling perceptions, and eroding institutional and societal cohesion before kinetic engagement even begins.

The United States, in turn, needs to recognize information warfare as the threat it is. Countering it requires the same urgency as do responses to military threats, because in the Kremlin's conception of warfare, they are one and the same.

THE EVOLUTION OF RUSSIA'S INFLUENCE OPERATIONS

The Russian Ministry of Defense defines information warfare as a confrontation "between two or more States in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic, and social systems, a massive psychological manipulation of the population to destabilize the society, as well as coercing the state to take decisions for the benefit of the opposing force."[2] The Kremlin has developed several techniques for influencing adversaries, which it has updated from the Cold War to the contemporary information environment.

Reflexive control—Reflexive control is a Soviet concept from the 1950s. A key psychological component of information warfare, it exploits information to shape an adversary's decision-making process.[3] To make the information most effective, the Kremlin identifies and exploits existing vulnerabilities in the target society. Moscow then floods the information environment with related moral arguments and psychological pressures.

Active measures—Active measures (*aktivnye meropriyatiya*) are the offensive operations through which reflexive control is executed. The concept encompasses disinformation, deception, sabotage, and espionage, and is institutionalized through networks of agents of influence and centralized military command structures.[4]

The Kremlin has operationalized these tools to conduct an array of disruptive information operations across Europe.

REDEFINING UKRAINE

Most visibly, the Kremlin has intensified its information campaigns surrounding Ukraine to justify its invasion and continued aggression.[5] Analysis of more than 130,000 messages across major platforms in 2023 identified 86 incidents involving 462 Russia-affiliated sources and 223 detected bots, some of which impersonated Ukrainian outlets.[6] In occupied Ukrainian territories, severe water shortages are forcing residents to queue for hours while Kremlin disinformation places blame on the "evil and aggressive West."[7] The Kremlin has even weaponized climate policy to attempt to evade blame for the war, framing the EU's Green Deal as "green tyranny" to protect its fossil fuel-dependent war economy.[8]

European NGO EUvsDisinfo identifies "Nazi Ukraine" and "lost sovereignty" as the two most domi-

***Dr. Ivana Stradner** is a Research Fellow at the Foundation for Defense of Democracies, where her research focuses on influence operations. She is also a special correspondent for the Kyiv Post.*

nant Kremlin information campaign narratives.[9] This narrative exploits historic collective memory to achieve psychological control, portraying Kyiv as a proponent of Nazism and a puppet of the West to justify the Kremlin's illegal invasion. Another prominent narrative links Ukrainian President Volodymyr Zelenskyy to corruption and alleges Ukraine resells the weapons it has received from the West. In April 2025, the Kremlin flooded Ukraine's information environment with fake AI-generated TikTok videos portraying "ordinary Ukrainians" promoting opposition to mobilization and blaming Ukraine for the inability to reach a peace agreement.[10] The Russian Ministry of Foreign Affairs also claimed Ukraine was building "dirty bombs” and alleged the U.S. shipped toxic chemicals to Ukraine in an effort to hamper continued U.S. aid to Ukraine and cast doubts around Zelenskyy's administration.[11]

> **In this new domain of warfare, the strategic objective is not battlefield dominance, but rather degrading adversary decision-making, controlling perceptions, and eroding institutional and societal cohesion before kinetic engagement even begins.**

WEAPONIZING RELIGION

The Orthodox Church represents another important messaging device. Russian information operations routinely fuse religion with politics, and for good historical reason.[12] After 1943, the leadership of the Russian Orthodox Church consisted almost entirely of agents or collaborators of the state security services, thereby providing ideological cover and religious sanction to the USSR's policies. That bond still persists, with Russian President Vladimir Putin exploiting the credibility of the Church to justify his illegal actions, portraying Moscow as a pillar of traditional, moral and spiritual values.

Russia's National Security Strategy defines traditional values as "life, dignity, human rights and freedoms, patriotism, civic consciousness, service to the Fatherland and responsibility for its fate, high moral ideals, strong family, constructive work, prioritizing the spiritual over the materialistic, humanism, mercy, justice, collectivism, mutual aid and respect, historical memory and continuity across generations, [and] unity of the nations of Russia."[13] Mirroring this, Russia's 2023 Foreign Policy Concept prioritizes actions aimed at "countering the falsification of history” and "the incitement of hatred against Russia.”[14] Russia's Defense Ministry, for its part, links “upholding and preserving traditional values” as key to the “protection of our sovereignty.”[15]

Domestically, Putin has used the Church's values to maintain censorship and control over the media space. Back in 2012, his government faced the largest protests since the fall of the Soviet Union. A large part of the success of these protests was their organization via social media.[16] In response, Putin enacted myriad internet censorship laws under the guise of protecting citizens from outside influence harmful to Russia's traditional, spiritual, and moral values.[17] In discussing such laws, Russian Foreign Minister Sergei Lavrov emphasized the need to quell the West's “destructive neoliberal attitudes” that cause “serious damage to people's moral health.”[18]

Putin likewise exploits the Church's reach to maintain geopolitical influence, claiming efforts to violate the sovereignty of European states represent an attempt to reunify the former Orthodox Russian Empire. According to Alexey Drobinin, Director of the Foreign Policy Planning Department of the Russian Foreign Ministry, the West distorts human rights concepts to “interfere in the internal affairs of other countries,” culminating in a “long list of ‘colour revolutions.”[19] In 2014, Putin justified his annexation of Crimea in this fashion, claiming the region needed to be protected from attempts to “deprive Russians of their historical memory.”[20] And in Spring 2022, Putin launched his full-scale invasion of Ukraine under the religious guise of protecting traditional spiritual values; he framed the war as a defensive reaction to the West's efforts “to destroy our traditional values and force on us their false values that would erode us.”[21] Patriarch Kirill has repeatedly endorsed the war, blessing crosses for “war heroes” and casting the Ukraine invasion as "holy struggle" against the “satanic” West’s attempts to attack traditional values and Russian Orthodoxy.[22]

> **Although Russia has no rational incentive to conduct a nuclear strike, this cognitive manipulation does not rely on strategic reality; instead, it uses fear-inducing rhetoric to muddy the information waters. Through this environment of uncertainty, Putin can then bend key Western decision-makers to his will.**

NUCLEAR BLUSTER

Beyond A March 2025 report from the Office of the Director of National Intelligence (ODNI) warned of the "catastrophic damage" that Russian nuclear forces could inflict on the United States.[23] Putin, for his part, is all too aware of Washington’s intense fear of nuclear escalation. Since the start of Russia’s full-scale invasion of Ukraine in 2022, the Kremlin has relied on nuclear threats to instill fear and manipulate Ukraine's western allies to enact a policy of self-deterrence.[24] Although Russia has no rational incentive to conduct a nuclear strike, this cognitive manipulation does not rely on strategic reality; instead, it uses fear-inducing rhetoric to muddy the information waters. Through this environment of uncertainty, Putin can then bend key Western decision-makers to his will.

In February 2022, Russia placed its nuclear forces on high alert. Putin's subsequent, September 2022 warnings prompted Washington to publicly suggest a future "Armageddon,” amplifying the fear that Russia sought to instill in U.S. leaders and citizens. This campaign resulted in the U.S. withholding long-range missiles from Ukraine, a move that aligned with the Kremlin’s agenda.[25] Russia reinforced its pressure by moving tactical warheads to Belarus in 2023 and revising its nuclear doctrine to lower the threshold for nuclear retaliation. Yet, despite three years of threats, no nuclear action has occurred, reflecting the hollowness that reflexive control depends on concealing.[26]

ENGAGING THE GLOBAL SOUTH

At the same time, Russia is influencing the “Global South” through the BRICS organization. TV BRICS, headquartered in Moscow and linked to sanctioned entities, broadcasts in six languages and claims to reach 1.5 billion people through 100+ media partners.[27] TV BRICS facilitates information laundering, where state media is disseminated through local outlets under the facade of cooperation.[28] Most recently, TV BRICS has partnered with Prasar Bharati, India's largest media broadcaster.[29] Mexico is a prominent case in point. Russia maintains 85 diplomats in Mexico, and SVR/GRU officers are known to use tourist resorts for covert exchanges.[30] At Mexico's National Autonomous University, Kremlin-affiliated media representatives have gained growing presence since 2022, with RT participating in panels on fake news and media manipulation.[31]

ELECTION INTERFERENCE

In September 2024, the U.S. Justice Department charged two employees of Russia’s state-backed RT in connection with the transfer of $10 million to a Tennessee-based media startup.[32] U.S. officials accused these individuals of money laundering and failing to register as foreign agents, but their case revealed a wider threat: the continued efforts of Russia and other U.S. adversaries to poison the U.S. information environment. Prior presidential election cycles, in 2016 and 2020, saw similar attempts by Russia and other actors to introduce disinformation into the media diets of Americans.[33]

Russia has also meddled in elections abroad, seeking to elect Kremlin-aligned officials. For instance, Romania annulled its November 2024 presidential election after determining Russian interference compromised the vote.[34] Moldova faced similar campaigns, and Georgia's ruling Georgian Dream party has been linked to Russian influence operations.[35]

TAKING THE OFFENSE

Since 2016, the United States has taken some steps to protect its domestic information space. U.S. Cyber Command has targeted Russian trolls and hackers to deter them from threatening U.S. elections.[36] U.S. intelligence officials have worked to publicly expose foreign influence operations and the U.S. government has sanctioned individuals and media outlets involved in these malign activities.[37] Unfortunately, such efforts are typically uncoordinated and organizationally stunted. Furthermore, the U.S. typically waits to be attacked, then approaches combatting information operations on the defensive. Instead, the U.S. needs to adopt a proactive approach.

Historically, the U.S. has gone on the offensive during periods of heightened concern regarding national security. During the Cold War, the U.S. successfully ran offensive information operations through the inter-agency Active Measures Working Group and the State Department's U.S. Information Agency.[38] Through these mechanisms, the U.S. influenced those living in the Soviet Union and across the globe with music, art, and literature lauding American culture and quality of life. The U.S. further amplified its campaigns through networks like the *Voice of America* and *Radio Free Europe/Radio Liberty*.[39] By allowing foreign publics to see the apparent lies in Soviet information, and to decide for themselves which narrative they preferred, the U.S. was able to successfully shift public support toward the West.

That experience is relevant today. Although recent months have seen governmental efforts to dismantle much of it, the U.S. still has an arsenal of tools that it can harness to fight back against Putin's information warfare and target Russia's command and control in the information space. It should do so without delay.

ENDNOTES

1. Mason Clark, "The Russian Military: Forecasting the Threat," Institute for the Study of War, October 27, 2025, https://understandingwar.org/wp-content/uploads/2025/10/The-Russian-Military-Forecasting-the-Threat.pdf; Roger N. McDermott, "Russian Military Thought on the Changing Character of War: Harnessing Technology in the Information Age," in Matthew Czekaj, ed., *Russia's Path to the High-Tech Battlespace* (Washington, DC: The Jamestown Foundation, 2022), 45, https://jamestown.org/russian-military-thought-on-the-changing-character-of-war-harnessing-technology-in-the-information-age/.
2. Bilyana Lilly and Joe Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces," in T. Jančárková et al., eds., *20/20 Vision: The Next Decade*, (Tallinn: NATO Cooperative Cyber Defence Centre Publications, 2020), 133, https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf.
3. Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies* 17, iss. 2, 2004, https://www.tandfonline.com/doi/abs/10.1080/13518040490450529.
4. Jolanta Darczewska and Piotr Żochowski, "Active Measures: Russia's Key Export," Centre for Eastern Studies, June 2017, https://www.osw.waw.pl/sites/default/files/pw_64_ang_active-measures_net_0.pdf.
5. "Rewriting borders of truth: How Russian FIMI falsifies historical memory," *EUvsDisinfo*, December 11, 2025, https://euvsdisinfo.eu/rewriting-borders-of-truth-how-russian-fimi-falsifies-historical-memory/.
6. "Identification and Analysis of Russian Information Threats on Corruption in the Ukrainian Media Space," Center for Strategic Communications and Information Security, April 2024, https://spravdi.org/wp-content/uploads/2024/05/analysis-of-russian-information-threat-on-the-subject-of-corruption-in-the-ukrainian-media-space.pdf.
7. "When propaganda replaces policy: Russia's water crisis in occupied Ukraine," *EUvsDisinfo*, November 21, 2025, https://euvsdisinfo.eu/when-propaganda-replaces-policy-russias-water-crisis-in-occupied-ukraine/.
8. "Weaponising climate change to undermine the West," *EUvsDisinfo*, October 30, 2025, https://euvsdisinfo.eu/weaponising-climate-change-to-undermine-the-west/.
9. "Key Narratives in Pro-Kremlin Disinformation," *EUvsDisinfo*, September 20, 2022, https://euvsdisinfo.eu/key-narratives-in-pro-kremlin-disinformation/.
10. "Russia spreading fake TikTok videos to promote narrative of 'peace at any cost' in Ukraine – CCD," *Ukrinform*, November 4, 2025, https://www.

ukrinform.net/rubric-society/4055171-russia-spreading-fake-tiktok-videos-to-promote-narrative-of-peace-at-any-cost-in-ukraine-ccd.html.

11. Natasha Lander Finch and Ryan Arick, "How the US and Europe can counter Russian information manipulation about nonproliferation," Atlantic Council, October 4, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-the-us-and-europe-can-counter-russian-information-manipulation-about-nonproliferation/.
12. Office of the President of Russia, "Meeting with Patriarch Kirill of Moscow and All Russia," November 20, 2025, http://en.kremlin.ru/events/president/news/78507.
13. "Указ Президента Российской Федерации от 02.07.2021 № 400 'О Стратегии национальной безопасности Российской Федерации' [Decree of the President of the Russian Federation No. 400 'On the National Security Strategy of the Russian Federation']," Official Publication of Legal Acts (Russia), July 3, 2021, http://publication.pravo.gov.ru/Document/View/0001202107030001.
14. "Указ Президента Российской Федерации от 31.03.2023 № 229 'О Концепции внешней политики Российской Федерации' [Decree of the President of the Russian Federation No. 229 'On the Concept of Foreign Policy of the Russian Federation']," Official Publication of Legal Acts (Russia), March 31, 2023, http://publication.pravo.gov.ru/Document/View/0001202304010007.
15. Andrey Ilnitsky, "The Antichrist as a technology," *International Affairs* (Russia), February 7, 2024, https://en.interaffairs.ru/article/the-antichrist-as-a-technology/.
16. Ruben Enikolopov, Alexey Makarin, and Maria Petrova, "Social Media and Protest Participation: Evidence from Russia," *VoxEU*, Centre for Economic Policy Research, December 17, 2019, https://cepr.org/voxeu/columns/social-media-and-protest-participation-evidence-russia.
17. Andrey Tselikov, "The Tightening Web of Russian Internet Regulation," Berkman Center *Research Publication* No. 2014-15, November 20, 2014, https://ssrn.com/abstract=2527603.
18. Russian Ministry of Foreign Affairs, "Foreign Minister Sergey Lavrov's Remarks at the 44th Meeting of the Foreign Ministry's Council of Heads of Constituent Entities of the Russian Federation," April 16, 2025, https://mid.ru/en/foreign_policy/news/1987058/.
19. Alexey Drobinin, "Why is the choice of traditional values so important?" *International Affairs* (Russia), November 30, 2023, https://en.interaffairs.ru/article/why-is-the-choice-of-traditional-values-so-important/.
20. Office of the President of Russia, "Address by President of the Russian Federation," March 18, 2014, http://en.kremlin.ru/events/president/news/20603.
21. "Our Experts Decode the Putin Speech That Launched Russia's Invasion of Ukraine," Atlantic Council, February 22, 2023, https://www.atlanticcouncil.org/blogs/new-atlanticist/markup/putin-speech-ukraine-war/.
22. "Наказ XXV Всемирного русского народного собора 'Настоящее и будущее Русского мира' (Edict of the XXV World Russian People's Council 'The Present and Future of the Russian World')," Orthodox Church of Russia, March 27, 2024, http://www.patriarchia.ru/db/text/6116189.html; Jerry Fisayo-Bambi, "Putin asks Russian Orthodox church patriarch to consecrate Christmas gifts for troops in Ukraine," *Euronews*, January 7, 2025, https://www.euronews.com/2025/01/07/putin-asks-russian-orthodox-church-patriarch-to-consecrate-christmas-gifts-for-troops-in-u.
23. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," March 2025,14-20, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.
24. Congressional Research Service, "Russia's Nuclear Weapons," December 11, 2025, https://crsreports.congress.gov/product/pdf/IF/IF12672.
25. David R. Shedd and Ivana Stradner, "With Nuclear Threats, Putin Plays the West Like a Fiddle," *Foreign Policy*, September 6, 2023, https://

foreignpolicy.com/2023/09/06/putin-nuclear-war-ukraine-russia-biden-west-armageddon-psychology-influence-operations-disinformation-manipulation/.

26. Mark Montgomery and Ivana Stradner, "Trump Shouldn't Fall for Russia's Nuclear Bluster," *National Review*, July 26, 2025, https://www.nationalreview.com/2025/07/trump-shouldnt-fall-for-russias-nuclear-bluster/.

27. "About *TV BRICS*," TV BRICS (Russia), n.d., https://tvbrics.com/en/about/.

28. Peter Benzoni, Larissa Doroshenko, and James Conway, "What Is TV BRICS? The Sanctions-Linked, Russia-Backed Influence Broker," German Marshall Fund of the United States, February 11, 2025, https://www.gmfus.org/news/what-tv-brics-sanctions-linked-russia-backed-influence-broker.

29. "India strengthens its information presence in BRICS through *TV BRICS*," TV BRICS (Russia), December 5, 2025, https://tvbrics.com/en/news/india-strengthens-its-information-presence-in-brics-through-tv-brics/.

30. Armand Chouet, "Russia's Intelligence Infrastructure in Mexico: A Strategic Challenge to U.S. National Security and Hemispheric Stability," Robert Lansing Institute, December 9, 2025, https://lansinginstitute.org/2025/12/09/russias-intelligence-infrastructure-in-mexico/.

31. Armando Chaguaceda and Vladimir Rouvinski, "Russia's Capture of Intellectual Elites in Latin America," Wilson Center, September 10, 2024, https://www.wilsoncenter.org/blog-post/russias-capture-intellectual-elites-latin-america.

32. U.S. Department of Justice, Office of Public Affairs, "Two RT Employees Indicted for Covertly Funding and Directing U.S. Company that Published Thousands of Videos in Furtherance of Russian Interests," September 4, 2024, https://www.justice.gov/archives/opa/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published-thousands.

33. U.S. Office of the Director of National Intelligence, "Foreign Threats to the 2020 US Federal Elections," March 10, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

34. "Romania Annulled Its Presidential Election Results Amid Alleged Russian Interference. What Happens Next?" Atlantic Council, December 6, 2024, https://www.atlanticcouncil.org/blogs/new-atlanticist/romania-annulled-its-presidential-election-results-amid-alleged-russian-interference-what-happens-next/.

35. Ancuța Hansen, "How Russia Tried to Manipulate Moldova's Election – and What It Reveals," Lowy Institute (Australia), November 27, 2025, https://www.lowyinstitute.org/the-interpreter/how-russia-tried-manipulate-moldova-s-election-what-it-reveals; Mary Ilyushina, "Georgia Moves Closer to Russia, Banning Parties and Jailing Opposition," *Washington Post*, November 11, 2025., https://www.washingtonpost.com/world/2025/11/11/georgia-elections-eu-russia-opposition/.

36. David E. Sanger and Nicole Perlroth, "Cyber Command Expands Operations to Hunt Hackers From Russia, China, Iran," *New York Times*, November 2, 2020, https://www.nytimes.com/2020/11/02/us/politics/cyber-command-hackers-russia.html.

37. U.S. Department of Justice, Office of Public Affairs, "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere," September 4, 2024, https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence.

38. Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," National Defense University, Institute for National Strategic Studies, June 2012, https://inss.ndu.edu/Media/News/Article/693590/deception-disinformation-and-strategic-communications-how-one-interagency-group/.

39. Fred Weir, "'Connected to Another World': What Voice of America Meant to Russians in Cold War," *Christian Science Monitor*, March 21, 2025, https://www.csmonitor.com/World/.Europe/2025/0321/putin-russia-voa-cold-war.

Supply Chains and Security: Lessons from the Ukrainian Front

Catarina Buchatskiy

In December 2024, Oleksandr Yakovenko, founder of TAF Drones, was finalizing negotiations to purchase 100,000 FPV (first person view) drone motors from a Chinese factory. But before Yakovenko could close the deal, Russian buyers acquired the factory outright. In a similar story, Oleksii Babenko of Vyriy Drone watched his Chinese motor supplier suddenly regain the capacity to sell to them once again—but only after rival Russian buyers went elsewhere.[1]

These episodes tell a larger story. To casual observers, China may appear to have remained relatively "neutral" in the Russia-Ukraine war. Indeed, Beijing speaks of territorial integrity and the UN Charter, while emphasizing Russia's "legitimate security concerns."[2] And while the PRC provides immense industrial capacity to Russia's war machine, Ukrainian drone companies buy their motors and magnets from China, too.

But this apparent evenhandedness obscures a deliberate strategy. China's control of nearly the entire drone component supply chain gives it immense leverage—leverage that Beijing deploys without hesitation. Denying Ukraine access to critical components, imposing export restrictions that triple prices, allowing Russia to localize supply lines while constricting Ukraine's: these are policy choices that directly impact the battlefield, and show China's hand in tipping the geopolitical scales.

World War II was won by Allied industrial might—what FDR called the Arsenal of Democracy. The war in Ukraine is likewise a war of industrial scale. But this time, the Allies are on the back foot. We've abandoned military industrial doctrine, while our adversaries have perfected it. America's greatest victories have come when the U.S. treated industrial capacity as the weapon system it is. It's time to reindustrialize once again.

INDUSTRIAL POLICY AS WARFARE

Watching Russia operate is a lesson in how industrial military doctrine works in practice: the systematic use of state power to shape supply chains and production as instruments of war. Acquiring factories, relocating production lines, and establishing exclusive supply relationships. When Russian buyers purchased the Chinese motor factory that TAF Drones was negotiating with, they executed a state-backed strategy with clear military objectives: deny adversaries access while building domestic capacity.

The United States cannot replicate this approach directly. China won't sell strategic capacity to Washington the way it does to Moscow. But the doctrinal lesson remains: adversaries treat supply chains as a battlespace requiring state resources and strategic planning. Western responses, meanwhile, remain reactive and commercial.

Consider the contrast: Russia spends an estimated $145 billion annually on defense, with significant portions directed toward industrial base expansion.[3] Europe's Defence Fund, meanwhile, allocates €7.3 billion for the entire continent over the span of six years.[4] When China imposed export controls in September 2024, Ukrainian firms were forced to adapt by diversifying suppliers, accelerating domestic production, and substituting vulnerable components. Similarly, when it was discovered in 2022 that there was a Chinese component in the F-35, the Pentagon was forced to issue a waiver allowing continued Chinese magnet use while scrambling to fund domestic alternatives—a process that has taken years. For the most advanced fighter program in history, costing $1.7 trillion, the United States didn't have full supply chain visibility.

Catarina Buchatskiy *is the Director of Analytics at the Snake Island Institute, where she leads a team of analysts producing research on modern warfare, spanning topics from emerging defense technologies and battlefield tactics to military industrial policy.*

The path forward doesn't necessarily require matching Russian tactics. But it does require adopting the same seriousness as Russia regarding industrial capacity. Rather than waiting for market forces to diversify supply chains, NATO should be deploying state resources to cultivate allied production: subsidizing component factories in partner nations, licensing technology to accelerate localization, and establishing long-term contracts that justify private investment in strategic capacity. Ukraine's existing production base, meanwhile, offers a fast track to this sort of diversification.

> **China's control of nearly the entire drone component supply chain gives it immense leverage—leverage that Beijing deploys without hesitation. Denying Ukraine access to critical components, imposing export restrictions that triple prices, allowing Russia to localize supply lines while constricting Ukraine's: these are policy choices that directly impact the battlefield, and show China's hand in tipping the geopolitical scales.**

RUSSIAN INDUSTRIAL WARFARE IN ACTION

Moscow's military industrial doctrine is clear: deploy state resources to capture supply chains, while denying adversaries access to critical materials and assembly lines. One of Russia's largest manufacturers reportedly imported $577 million in parts from China between 2023 and 2025.[5] In August of 2025, China's exports of lithium-ion batteries to Russia stood at $47 million. Their exports of lithium-ion batteries to Ukraine, meanwhile, were a mere $11 million.[6]

But Russia's real strategy rests on acquisition and denial. Russia operates with state backing and can absorb higher costs, longer timelines, and supplier consolidation. Ukrainian manufacturers report Russian buyers routinely outbidding them for entire production runs, or even purchasing complete assembly lines for relocation to Russia.[7] Russia, in other words, is running an industrial-scale denial operation to weaken and disrupt the Ukrainian defense industrial base.

As a result, Ukrainian firms are forced to compete in fragmented commercial markets, where every export restriction translates into weeks of delay and a doubling of prices. Meanwhile, in exchange for components, Moscow transfers advanced military technology to China, including submarine operations, stealth aeronautical design, and missile capabilities—technology that Moscow had previously been reluctant to share.[8] The partnership deepens China's defense capabilities while weakening Ukraine's industrial base through systematic supply chain denial.

TOWARD A UKRAINIAN ARSENAL OF DEMOCRACY

Ukraine's wartime drone industry is unprecedented. It surged from just a handful of producers at the outset of the war in 2022 to more than 500 in 2024, and now produces millions of systems annually.[9] It is also increasingly self-sufficient; from 99% import dependence in 2022—when perhaps only a few thousand drones were produced domestically—Ukraine now boasts roughly 95% of systems assembled inside the country.[10] This represents an industrial renaissance that rivals the freedom's forge of old.

As a result, Ukraine is well positioned to serve as the arsenal of Europe. It has the best experience in scaling a defense industrial base, it produces equipment at unrivaled levels and is the absolute best bet for Western nations that want to outcompete China, Russia, and Iran and stock their arsenals fast enough to potentially defend themselves from a larger Russian onslaught or to defend Taiwan from Chinese aggression. Ukrainian IP, know-how, and particularly its feedback and R&D loop make the country a very attractive armory.

Ukraine is also actively working on localization. Over 70% of Ukrainian manufacturers say that they want to move away from Chinese components, and the number of Ukrainian-based components manufacturers is steadily

When Russian buyers purchased the Chinese motor factory that TAF Drones was negotiating with, they executed a state-backed strategy with clear military objectives: deny adversaries access while building domestic capacity.

increasing.[11] But what's important to understand now is that if the United States wants a self-sufficient European defense industry, a diversified supply chain, and less of dependence (by itself or its allies) on China, it should be making real, up-front investments in securing the drone supply chain all the way down to the components level.

Rebuilding the West's industrial military doctrine requires several shifts:

Secure component chokepoints through direct investment now, and fund immediate capacity expansion. This involves licensing magnet production technology, subsidizing battery cell factories in allied nations, and establishing redundant supply chains. The CHIPS Act model should extend beyond semiconductors to other component categories where adversaries hold monopolistic positions.

Consider a joint program with Ukraine by supporting them in acquiring components as a complement to complete drones. Ukrainian manufacturers can integrate such components (including video transmitters, antennas, motors, navigation modules) into battle-tested designs faster than Western contractors can deliver finished systems. This approach stimulates Ukraine's defense industry, sustains the military R&D workshops that drive rapid iteration, and ensures steady component flows for the exchange networks that accelerate battlefield adaptation. Ukrainian military R&D workshops consume hundreds of thousands of these components daily, providing the steady demand and persistent usage patterns that justify scaled-up production.

Integrate Ukraine's existing production base into NATO procurement systematically. Ukrainian firms already operate at wartime scale with battle-tested designs and rapid iteration capacity. Each Ukrainian-made motor, sensor, or avionics package adopted by Alliance members reduces collective dependence on Chinese suppliers. Ukrainian component manufacturers consistently cite lack of guaranteed contracts as the primary barrier to scaling production, even when manufacturing capacity exists. Changing this state of affairs requires structured support, including the fast-tracking of certifications, guaranteed procurement volumes that justify factory expansion, and technology transfers that accelerate component localization.

Treat supply chain warfare as actual warfare. When Russian buyers acquire Chinese factories to deny Ukrainian access, that constitutes military operations conducted through commercial channels. When China imposes export controls that triple component prices overnight, that represents economic coercion with battlefield intent. Western responses should deploy state resources accordingly: counter-acquisitions, export financing for allied suppliers, and secondary sanctions on entities enabling adversary supply chain capture.

Western policymakers face a choice with narrowing time horizons. Europe's rare earth alternatives won't mature until 2030. Ukraine's component dependencies persist despite rapid localization. Russia continues executing industrial denial operations backed by state resources. Every month of inaction allows adversary supply chain advantages to harden into permanent strategic exposure. But the solutions are specific and achievable, provided we decide to take the supply chain security threat seriously.

ENDNOTES

1. Rustem Khalilov, "'When the Russians massively sit on FPV drones with machine vision, there will be trouble.' How the new generation of drones can change the course of war," *Ukrainska Pravda*, January 25, 2024, https://www.pravda.com.ua/articles/2024/01/25/7438746/.
2. "China says it respects Ukraine's sovereignty and Russia's security concerns," Reuters, February 25, 2022, https://www.reuters.com/world/europe/china-says-it-respects-ukraines-sovereignty-russias-security-concerns-2022-02-25/.
3. Darya Korsunskaya and Gleb Bryanski, "Russia hikes 2025 defence spending by 25% to new post-Soviet high," Reuters, September 30, 2024, https://www.reuters.com/world/europe/russia-hikes-national-defence-spending-by-23-2025-2024-09-30/#:~:text=Summary,5.5%20trillion%20roubles%20on%20defence.
4. European Commission, "The European Defence Fund in detail," n.d., https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en.
5. Christian Shepherd and Rudy Lu, "Behind Russia's battlefield drone surge in Ukraine? Chinese factories," *Washington Post*, October 13, 2025, https://www.washingtonpost.com/world/2025/10/13/china-russia-drone-parts-ukraine/?fbclid=IwY2xjawN12T5leHRuA2FlbQIxMAABHqKtVkRK5bPOUszbgH8OcU8oHjixiVJsgwWTGBEP5Bj1I_yL8XxxocaspJsK_aem_MuJLmZoP6VpB1ZUrk7vbXw.
6. Ibid.
7. Khalilov, "'When the Russians massively sit on FPV drones with machine vision, there will be trouble.' How the new generation of drones can change the course of war."
8. Jack Burnham and John Hardie, "China-Russia Defense Cooperation Showcases Rising Axis of Aggressors," FDD *Policy Brief*, June 10, 2025, https://www.fdd.org/analysis/policy_briefs/2025/06/10/china-russia-defense-cooperation-showcases-rising-axis-of-aggressors/.
9. Jake Rudnitsky and Gerry Doyle, "Ukrainian Drone Industry's Next Target Is NATO Markets," Bloomberg, November 11, 2025, https://www.bloomberg.com/news/features/2025-11-11/ukraine-drone-industry-targets-nato-markets.
10. Snake Island Institute, "Building the Arsenal," September 2025, https://snakeisland-bucket.s3.eu-north-1.amazonaws.com/reports/Building+the+Arsenal.pdf.
11. Ibid.

Ukraine and the Making of a Defense Innovation Industry

Anna Harvey

When Russian President Vladimir Putin launched his full-scale invasion on February 24, 2022, he expected to topple the Ukrainian government swiftly and with little opposition from its people. Instead, the Russian military met fierce resistance, both from the professional Ukrainian military and from the country's civilians, who formed territorial defense units, provided intelligence to authorities, and resisted the invading force in individual acts of bravery.[1]

Since the initial days of the invasion, Ukraine's armed forces have continued to battle back against larger Russian military through asymmetric solutions and technological ingenuity. Ukrainian military units independently innovated existing drone technologies and tactics in new combat conditions, and Ukrainian engineers and military enterprises stepped up to design, field, and scale new unmanned systems. The Ukrainian government, meanwhile, has sought to cut bureaucratic red tape in the research and development process, accelerate procurement timelines, increase communication between engineers and frontline warfighters, and increase joint agreements with foreign producers to facilitate defense cooperation with and testing within Ukraine. The country's Brave1 initiative has further allowed foreign defense companies to collaborate with Ukrainian defense firms to test weapons systems in battle conditions and to receive immediate feedback on their effectiveness.

In the process, Ukraine has become a vital testing ground for both domestically produced and foreign weapons systems, especially unmanned systems (UAS) and counter-UAS technologies. The United States, in turn, needs to leverage the opportunity to learn from the Ukrainian military and integrate improvements into its own military.

THE EVOLUTION OF THE UKRAINIAN DEFENSE INDUSTRY

Following the collapse of the USSR in 1991, Ukraine inherited approximately thirty percent of the Soviet arms industry, including production capacity and research and development facilities.[2] However, in the immediate post-Soviet era, Ukraine's defense industry was still deeply integrated with Russia's, relying on Russian supply chains for production and research partnerships for innovation.[3] Additionally, Ukraine exported the majority of its inventory without investing in modernization, limiting production capacity and stymying innovation.[4] This left the Ukrainian defense industry, despite its substantial size, weak and reliant on foreign partnerships and purchasers.

Fast forward to 2014, and Kyiv faced the task of rapidly disentangling its defense industry from that of Russia after the latter's annexation of Crimea and support for separatists in eastern Ukraine.[5] To do so, Ukraine had to rapidly diversify its international procurement and ramp up domestic manufacturing.[6] The country further banned defense cooperation with Russia and focused on indigenizing production through its state-owned defense conglomerate, *Ukroboronprom*. But on the whole, between 2014 and 2022, the state-backed revival of this industry was inefficient and impaired by both corruption and bureaucracy.[7]

During this time, Ukraine and Russia both used drones, albeit predominantly for reconnaissance and surveillance.[8] The most common drone used in Ukraine between 2014 and 2022 was the Chinese DJI Mavic.[9] However, its high cost prohibited widespread usage, and prompted Ukrainian manufacturers to begin developing Ukrainian-designed and -manufactured unmanned systems. The Ukrainian government began contracting

Anna Harvey is Research Fellow and Program Officer at the American Foreign Policy Council in Washington, DC.

Ukrainian drone companies to develop systems for use on the frontline, and drone engineers introduced domestically tested and developed drones to the Ukrainian Armed Forces in 2015.[10] Between 2014 and 2022, private Ukrainian defense companies developed close relationships with the military.[11] These private companies were often founded by veterans and engineers, were smaller and more agile than *Ukroboronprom*, and focused on emerging technologies, including unmanned systems.[12] Ukrainian manufacturers initially prioritized low-cost first-person-view (FPV) quadcopter drones as sustainable systems to counter Russian-backed separatists in eastern Ukraine. By 2024, Ukraine had developed a domestic analogue to the DJI Mavic, known as the "Shmavik," which better resisted combat damage and electronic warfare.[13]

The country has created a defense industry that is able to respond within weeks to emerging Russian technologies. It does so by conducting research and development rapidly and in communication with frontline warfighters, who test innovations and provide feedback to rear engineers. In other words, Ukraine has created an environment in which frontline warfighters play the role of forward-deployed engineers.

UKRAINE'S DRONE INDUSTRY FACES THE FULL-SCALE INVASION

When the full-scale invasion began in February of 2022, the Ukrainian defense industry was initially unprepared to meet the needs of the Ukrainian military. But it grew rapidly thereafter.[14] Officials in Kyiv immediately grasped the need to bolster Ukraine's drone capabilities in order to counter Russia's superiority in manpower and traditional systems, including mechanized vehicles and aircraft, as well as to provide frontline reconnaissance support.[15]

The result was notable. In February 2022, there were only a handful of unmanned systems companies in Ukraine, but by April 2025 there were over 500 with more than 1,100 individual products. And such firms continue to emerge; over 200 new munitions companies have been established since the start of the full-scale invasion.[16] In the process, drones became the primary strike asset of the Ukrainian military, helping to compensate for artillery shell shortages and limited air defense systems.[17]

By 2023, Ukrainian President Volodymyr Zelenskyy introduced a wartime economic model to direct government resources toward defense, including through a "military-tech cluster" initiative that incentivizes joint ventures, technology transfer between the military and IT companies, and public-private collaboration.[18] Ukraine also introduced significant tax incentives to encourage growth among defense start-ups.[19] In May 2023, Ukraine's legislature, the Verkhovna Rada, voted to exempt domestic drone producers from customs duties and valued-added tax (VAT) in order to lower the production costs shouldered by defense companies.[20] (Two years later, the Rada endorsed bills to provide tax and customs breaks for fiber-optic drone manufacturers, as well—an indicator that the Ukrainian government remains committed to lowering costs for drone producers as new technologies emerge.[21])

However, economic incentives and low barriers to entry are not the only factors driving the rapid growth and remarkable success of the Ukrainian drone sector. The country has created a defense industry that is able to respond within weeks to emerging Russian technologies. It does so by conducting research and development rapidly and in communication with frontline warfighters, who test innovations and provide feedback to rear engineers.[22] In other words, Ukraine has created an environment in which frontline warfighters play the role of forward-deployed engineers.[23]

This has been made possible by developing a bottom-up defense innovation cycle and fostering immediate

> **Ukraine has become a vital testing ground for both domestically produced and foreign weapons systems, especially unmanned systems (UAS) and counter-UAS technologies. The United States, in turn, needs to leverage the opportunity to learn from the Ukrainian military and integrate improvements into its own military.**

communication between frontline warfighters and suppliers. To that end, Ukraine introduced an official military-wide app, dubbed Army+, that is integrated with the DOT-Chain online weapons marketplace and which allows Ukrainian units to purchase needed materiel directly from suppliers, thereby cutting out lengthy procurement timelines and bureaucratic bottlenecks.[24] The DOT-Chain initiative reportedly delivered 17,000 drones to frontline units in its first two months of operation. The average delivery time for ordered equipment is approximately ten days, with some deliveries made in as few as three.[25] The incorporation of frontline feedback into the research and development process and the removal of red tape in procurement have produced a drone industry that is agile and highly responsive.

Ukraine's innovations are now going global. In July 2025, Brave1, the procurement and investment hub originally established to allow Ukrainian military units to order arms directly from Ukrainian defense companies, announced that it would begin collaborating with foreign arms companies to allow them to test their weapons on the front lines and Ukrainian testing grounds.[26] The testing system is similar to that of the U.S. Defense Advanced Research Projects Agency (DARPA), but significantly cuts down on development timelines, allowing for the implementation of innovations over the course of weeks rather than years.[27] The majority of foreign applications to participate in the testing program are from drone manufacturers, as well as producers of communications, navigation and electronic warfare systems, and Ukraine is prioritizing the testing of unmanned systems, counter-drone technologies, and air defense systems.[28]

UKRAINE AS LABORATORY

Drones have come to dominate and define warfighting in Ukraine, where the smaller Ukrainian military has sought to inflict asymmetric damage on Russia's more numerous forces. Ukraine and Russia have normalized drone warfare as a means of frontline combat and are locked in an arms race to control the skies. As a result, drones currently account for approximately 80% of casualties on both sides of the conflict.[29] This situation is unlikely to change, especially as Russia continues to employ meatgrinder tactics on the battlefield, sending wave after wave of disposable and poorly-trained Russian (or foreign) soldiers toward Ukrainian positions in hopes of making marginal tactical gains.

This dynamic should be instructive for Washington as well. Supporting the Ukrainian military and defense industry should rank as a strategic priority for the United States, insofar as Ukraine's transition into an efficient and agile defense innovation hub represents a massive transformation in modern warfare. Despite the overwhelming pressure of Russia's full-scale invasion, Ukraine constructed an environment that fosters innovation through warfighter feedback, rapid iteration, decentralized production, and public-private collaboration. The drone industry in particular has proven itself to be agile and creative, responding in days to the changing needs on the frontline.

America can learn from these wartime successes. The war in Ukraine has proven that inexpensive, rapidly adaptable weapons systems can inflict asymmetric damage on a larger, better-resourced adversary. As the United States faces pacing threats not only from Russia but also from China, seizing the opportunity to gain real-time insights into how drones, counter-drone systems, electronic warfare, and other weapons perform in combat conditions will help strengthen U.S. security and preparedness. By treating Ukraine not just as a recipient of aid but as a partner in military innovation in its own right, Washington can strengthen both Ukrainian sovereignty and its own defense industrial base and long-term military edge.

ENDNOTES

1. Liam Collins and John Spencer, "Urban Warfare Project Case Study Series: Cast Study #12 – Kyiv," Modern War Institute, February 21, 2025, https://mwi.westpoint.edu/urban-warfare-project-case-study-12-battle-of-kyiv/.
2. Kateryna Kuzmuk and Lorenzo Scarazzato, "The transformation of Ukraine's arms industry amid war with Russia," Stockholm International Peace Research Institute, February 21, 2025, https://www.sipri.org/commentary/topical-backgrounder/2025/transformation-ukraines-arms-industry-amid-war-russia.
3. "Renaissance: From Soviet Legacy to NATO Standards," *Lviv Herald*, May 23, 2025, https://www.lvivherald.com/post/ukraine-s-defence-industry-renaissance-from-soviet-legacy-to-nato-standards.
4. Ibid.
5. JIT MH17 Joint Investigation Team, "Report: Findings of the JIT MH17 investigation into the crew members of the Buk TELAR and those responsible in the chain of command," Openbaar Ministerie, February 2023, https://web.archive.org/web/20230327231233/https://www.prosecutionservice.nl/binaries/prosecutionservice/documenten/publications/mh17/map/2023/report-mh17/Rapportage+MH17+ENG.pdf; Nigel Walker, "Conflict in Ukraine: A timeline (2014-eve of 2022 invasion)." House of Commons Library. August 22, 2023, https://researchbriefings.files.parliament.uk/documents/CBP-9476/CBP-9476.pdf.
6. Thomas Laffitte, "Ukraine's Defense Industry and the Prospect of a Long War," Foreign Policy Research Institute, September 21, 2022, https://www.fpri.org/article/2022/09/ukraines-defense-industry-and-the-prospect-of-a-long-war/; Kateryna Kuzmuk and Lorenzo Scarazzato, "The transformation of Ukraine's arms industry amid war with Russia," Stockholm International Peace Research Institute, February 21, 2025, https://www.sipri.org/commentary/topical-backgrounder/2025/transformation-ukraines-arms-industry-amid-war-russia.
7. "Renaissance: From Soviet Legacy to NATO Standards." *Lviv Herald*.
8. Government of France, Ministere de L'Europe et des Affaires Etrangeres, "Understanding the situation in Ukraine from 2014 to 24 February 2022," June 2022, https://www.diplomatie.gouv.fr/en/country-files/ukraine/situation-in-ukraine-what-is/understanding-the-situation-in-ukraine-from-2014-to-24-february-2022/.
9. Kateryna Bondar and Gregory C. Allen, "The Russia-Ukraine Drone War: Innovation on the Frontlines and Beyond," Center for Strategic and International Studies, May 28, 2025, https://www.csis.org/analysis/russia-ukraine-drone-war-innovation-frontlines-and-beyond.
10. Pavel Krasnomovets, "Born to fly. Since 2014, a whole drone industry has grown in Ukraine. Will war help it become a global player?" *Forbes*, September 8, 2022, https://forbes.ua/ru/innovations/narodzheni-litati-z-2014-roku-v-kraini-virosla-tsila-galuz-virobnitstva-bpla-chi-dopomozhe-viyna-ukrainskomu-military-tech-stati-globalnim-gravtsem-06092022-8150.
11. Ibid.
12. "Renaissance: From Soviet Legacy to NATO Standards." *Lviv Herald*.
13. Krasnomovets, "Born to fly."
14. Jake Epstein, "Inside Ukraine's drone boom," *Business Insider*, April 24, 2025, https://www.businessinsider.com/ukraine-drone-defense-tech-industry-warfare-russia-attacks-2025-4; Thomas Laffitte, "Ukraine's Defense Industry and the Prospect of a Long War," Foreign Policy Research Institute, September 21, 2022, https://www.fpri.org/article/2022/09/ukraines-defense-industry-and-the-prospect-of-a-long-war/
15. Krasnomovets, "Born to fly."
16. Epstein, "Inside Ukraine's drone boom"; Joyce Hakmeh, "What Ukraine can teach Europe and

the world about innovation in modern warfare," Chatham House, March 2025, https://www.chathamhouse.org/2025/03/what-ukraine-can-teach-europe-and-world-about-innovation-modern-warfare.

17. Krzysztof Nieczypor and Slawomir Matuszak, "Game of drones: the production and use of Ukrainian battlefield unmanned aerial vehicles," Centre for Eastern Studies, October 14, 2025, https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-10-14/game-drones-production-and-use-ukrainian-battlefield-unmanned
18. Krasnomovets, "Born to fly."
19. Hakmeh, "What Ukraine can teach Europe and the world about innovation in modern warfare."
20. "Ukrainian lawmakers back tax breaks for domestic drone producers," Reuters, May 29, 2023, https://www.reuters.com/technology/ukrainian-lawmakers-back-tax-breaks-domestic-drone-producers-2023-05-29/.
21. Olha Pokotylo, "Ukrainian parliament to consider tax benefits for fibre-optic drone manufacturers," *Defender Media*, May 28, 2025, https://thedefender.media/en/2025/05/rada-to-lift-taxes-on-fiber-optic/.
22. Kateryna Bondar, "How and Why Ukraine's Military Is Going Digital," Center for Strategic & International Studies, October 6, 2025, https://www.csis.org/analysis/how-and-why-ukraines-military-going-digital.
23. Phillip Karber, "Defense Industrial Base Lessons from Russia-Ukraine | Conflict in Focus," Center for Strategic & International Studies, March 13, 2025, https://www.csis.org/analysis/defense-industrial-base-lessons-russia-ukraine-conflict-focus.
24. Richard Thomas, "Ukraine's DOT-Chain delivers as Russia claims Pokrovsk capture," *Army Technology*, December 2, 2025, https://www.army-technology.com/news/ukraines-dot-chain-delivers-as-russia-claims-pokrovsk-capture/.
25. Ibid.
26. Sabine Siebold, "Ukraine offers its front line as test bed for foreign weapons," Reuters, July 18, 2025, https://www.reuters.com/business/aerospace-defense/ukraine-offers-its-front-line-test-bed-foreign-weapons-2025-07-17/.
27. Ryan Robertson, "Ukraine offers front lines as testing grounds to foreign firms," SAN, August 13, 2025, https://san.com/cc/ukraine-offers-frontlines-as-testing-grounds-to-foreign-firms/.
28. Ibid.
29. Richard Thomas, "Drones Now Account for 80% of Casualties in Ukraine-Russia War," *Army Technology*, April 8, 2025, https://www.army-technology.com/news/drones-now-account-for-80-of-casualties-in-ukraine-russia-war/.

Understanding NATO's New Mission

James S. Robbins

When NATO was formed in 1949, its mission was clear: deterring Soviet expansionism through armed collective security, anchored by an enduring American military commitment to Western Europe. After the Cold War, some questioned whether this mission, and more broadly the NATO alliance itself, was still necessary. However, Russia's aggressive strategic posture has reaffirmed NATO's purpose, showing Moscow's willingness to engage in sustained confrontation with the Atlantic order that the Alliance was created to defend.

But while NATO's original mission is still relevant, military deterrence is no longer sufficient. As recent events have shown, the Alliance now faces a continuum of provocation from Russia that includes probing operations, coercion, sabotage, and various forms of political warfare. These actions are carefully calibrated by Moscow to fracture Alliance cohesion without triggering an Article 5 cause for collective military action.

Thus, NATO's new mission is to deter, confront and deny Russian strategic gains even below the threshold of war. Deterrence in this framework is not only preventing armed invasion but being able to rapidly respond to Russian gray-area operations aimed at subverting alliance member states. The continued credibility of NATO's deterrence increasingly depends on how the Alliance deals with actions that fall short of tanks crossing borders.

RUSSIA'S GRAY-ZONE PLAYBOOK

NATO's deterrence strategy has been effective at preventing large scale conflict involving member states. However, while the Kremlin has thus far avoided directly confronting NATO on the battlefield, Moscow has sought other ways to pursue the strategic objectives of expanding Russian influence and territorial control.

The 2022 NATO Strategic Concept notes that authoritarian actors "interfere in our democratic processes and institutions and target the security of our citizens through hybrid tactics, both directly and through proxies. They conduct malicious activities in cyberspace and space, promote disinformation campaigns, instrumentalize migration, manipulate energy supplies and employ economic coercion." Their purpose is to "undermine multilateral norms and institutions and promote authoritarian models of governance."[1]

When targeting NATO members, Russia stays below the Article 5 threshold but still tests the political resolve of the alliance using hybrid methods intending to create instability. It does so in a number of key ways.

Cyber operations

Cyberattacks play an increasing role in Russia's gray area activities. The most notable Russian cyber attack took place in Estonia in 2007, in which large-scale distributed denial-of-service (DDoS) attacks crippled government websites, banks, media outlets, and telecommunications. The conflict was triggered by a political dispute over Estonia relocating a Soviet-era war memorial. This was the first overt, major cyberattack against a NATO member state, and in response NATO set up the Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn the following year.

Other malign cyber activities include the GRU-linked APT28/Fancy Bear hacking group penetrating the German Bundestag's IT systems in 2015 and stealing stole large volumes of data, including MPs' emails and sensitive documents. In the United States, there have been persistent cyber intrusions into political institutions, think tanks, defense contractors, and election infrastructure. Across NATO countries, we have seen ransomware attacks targeting global corporations, as well as assaults

***Dr. James S. Robbins** is Senior Fellow for National Security Affairs at the American Foreign Policy Council, and Dean of Academics at the Institute of World Politics.*

on critical infrastructure. These pressures prompted NATO to declare cyberspace a domain of operations in 2014, and to subsequently state that a cyberattack could in fact trigger an Article 5 response.

Drone incursions

Russia has also made use of drones for probing missions. In September 2025, a wave of drones appeared over Poland, some of which were shot down. Days later, drones penetrated Romanian airspace, and other incidents took place in Denmark, Belgium, the Netherlands, and Germany, targeting both military and civilian infrastructure. Russia has either denied culpability in these incidents or claimed that the incursions were due to technical malfunctions.

In the case of Poland, NATO initially responded with a massive, coordinated air operation involving Polish, Dutch and Italian aircraft, though in general it is impractical and expensive to launch such operations in response to every drone incursion. In September 2025, the Alliance launched Operation Eastern Sentry, a flexible and continuing mission to strengthen allied air and multi-domain defenses, enhance integrated surveillance and readiness, and reinforce NATO's political and military resolve to deter further such provocations below the threshold of open conflict. NATO is also consulting with Ukrainian experts on counter-drone technology.[2]

GPS jamming and electronic warfare

Countries bordering Russia – especially Estonia, Lithuania, Latvia, and Finland – have reported a significant surge in GPS interference and signal disruption incidents. Lithuania in particular has reported hundreds of GPS jamming incidents, likely originating from the Russian Baltic enclave of Kaliningrad. Estonia and Finland reported interference with air and maritime navigation which was traced to Russian sources in the Kola peninsula.[3]

On June 23, 2025, Finland, Latvia, Lithuania and Estonia protested the "substantial growth" in such disruptions to the International Telecommunication Union. Estonia noted that 85 percent of flights in the country experience problems with navigation signals and coordinate spoofing. This activity presents an obvious danger to travel and commerce and can even be targeted. In March of 2024, an aircraft carrying UK Defence Minister Grant Shapps experienced 30 minutes of GPS signal jamming while flying near Kaliningrad from Poland to Britain. And in September 2025, a plane on which European Commission President Ursula von der Leyen was flying was hit by GPS jamming while over Bulgaria.

At the same time, Russia planes often fly with their transponders off, and Russian military ships and aircraft conduct close approaches, aggressive maneuvers and other harassing moves. These incidents, like other gray-area activities, are difficult to attribute and create persistent safety risks without an obvious attack taking place. They are a signal from the Kremlin that Russia has the capacity to degrade civilian and military systems without kinetic action.

Sabotage, covert action and targeted violence

Russia is also suspected to be conducting a covert sabotage campaign on NATO territory, particularly (though not exclusively) linked to interdicting arms and other aid bound for Ukraine. Back in 2014, agents of Russia's GRU were identified as responsible for blowing up two ammunition depots in the Czech Republic that were storing weapons heading for Ukraine. Multiple explosions and sabotage incidents have also occurred at arms factories and warehouses in Bulgaria and are allegedly linked to Russian intelligence.

Some attacks are meant more to destabilize and intimidate, such as the May 2024 fire at the Marywilska 44 shopping center in Warsaw, which the Polish government blamed on Russian intelligence. Around the same time, German police broke up a group planning bombings and arson inside Germany targeting military facilities, transport infrastructure, and other targets. Other similar plots have been suspected in Lithuania, Latvia, the UK and Sweden.

There have also been several cases of sabotage involving undersea telecommunications and power cables in the Baltic Sea that likewise fall under the hybrid warfare model. In January 2025, Sweden seized the cargo vessel *Vezhen* for damaging an undersea communications cable in what Stockholm called "a serious act of sabotage." Subsequently, in late December 2025, Finnish authorities seized the commercial ship *Fitburg*, sailing from St. Petersburg, which also had severed an undersea telecommunications cable.

> **NATO's new mission is to deter, confront, and deny Russian gains below the threshold of war.**

Weaponized migration and border pressure

Another Russian gray zone tactic is weaponizing migration flows to destabilize European countries. Russia not only facilitates migrant movement across borders but engages in disinformation campaigns to encourage migrants to travel to targeted countries. This has a direct impact in terms of putting pressure on the social support systems of NATO countries, and exacerbates political pressures within them.

Russia is known to exploit networks in North Africa and the Middle East to facilitate migrant flows. This is coordinated by mercenary factions active in the area, such as the RSB group led by fugitive former tech boss Jan Marsalek.[4] In 2024, Finland was forced to close its border with Russia after a surge in the number of undocumented migrants, mostly from the Middle East and Africa.

Disinformation and influence operations

Moscow has a long tradition of using disinformation and influence operations to exploit the openness of democratic systems and erode political cohesion within NATO. Russia's primary objective is delegitimization, undermining trust in elections, media, and governing institutions. Russian-linked actors amplify polarizing narratives on immigration, national identity, energy policy, and NATO itself through coordinated social media campaigns, proxy outlets, and fringe media ecosystems. Hack-and-leak operations, such as those targeting elections in the United States, France, and Germany, are timed to maximize disruption rather than persuasion, reinforcing public cynicism and uncertainty at critical political moments. These efforts are deliberately calibrated to remain below legal and political thresholds that would prompt decisive collective responses.

Crucially, Russian influence operations are cumulative and asymmetric: small, persistent interventions can generate outsized political effects in pluralistic societies constrained by free speech norms and decentralized media landscapes. Moscow leverages local grievances and domestic actors to launder narratives that weaken support for sanctions, military assistance, and alliance solidarity. For NATO, the challenge is not simply countering falsehoods but recognizing that information manipulation has become a core instrument of state power, aimed at hollowing out the political foundations on which collective security ultimately depends.

THE LARGER PATTERN

Russian gray-zone actions are not episodic, disconnected or simply opportunistic. Rather, they are mutually reinforcing elements of a deliberate strategy to erode NATO cohesion, slow decision-making, weaken Western morale and political resilience, and normalize a state of permanent confrontation below the threshold of war. Their strategic effect lies in the normalization of fatigue.

Moscow's theory of victory emphasizes fragmentation, intimidation, and erosion of trust. Russia's goal is to produce concern in frontline allies they are perpetually vulnerable, to convince Western publics that resistance is costly and escalation inevitable, and to influence NATO leaders so they believe that restraint is the safest course.

Using these and other hybrid warfare methods to diminish the resilience and cohesion of NATO may also be a strategic precursor to more aggressive action. In some cases, such as the Baltic states (which have significant ethnic Russia populations), demoralization could be the prelude to the type of "plausibly denied" armed action seen in the emergence of the "little green men" in eastern Ukraine in 2014. Russia looks to create and nurture a political environment in which NATO members question whether it is worth supporting such small and difficult to defend member states and make insufficient preparations to do so. Ideally, from the Kremlin's point of view, this effort will contribute to Moscow's longstanding dream of driving a wedge between the U.S. and Europe and separating America from the Alliance.

However, seen in this light, Russia's invasion of Ukraine in 2022 was a strategic blunder that strengthened NATO. It renewed the sense of threat from Moscow that had spurred the Alliance's formation and focused NATO members on increasing their military expenditures. It drove two historically neutral countries, Sweden and Finland, into NATO ranks. And it showed that Russia was willing to use conventional force against a sovereign state to pursue its revisionist aims – something not seen in Europe on this scale since World War II.

EXPANDING NATO'S TOOLKIT

To bolster deterrence in the face of Russian gray-area aggression, NATO must internalize several premises, among them:

- Political warfare is now as central a battlefield as conventional military warfare.
- Alliance cohesion and resilience are strategic assets, not supporting functions.
- Deterrence must operate below the level of armed attack.

To be successful in this effort, NATO must complement military deterrence with societal and political resilience and deny Russia the ability to achieve political effects through non-military means.

One aspect of this evolution is not to allow Article 5 issues to dominate NATO thinking and planning. While Moscow calibrates its activities to stay below the Article 5 threshold, the rise of hybrid methods has brought increased attention to Article 4. Under this provision, any member country can bring an issue to the attention of the North Atlantic Council "whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened." As soon as Article 4 is invoked, the issue is discussed and can potentially lead to a joint decision or action on behalf of the Alliance.

Article 4 has been invoked 9 times in its history, and more clearly applies to the type of political warfare strategy Russia is pursuing. For example, on September 10, 2025, Poland requested to hold consultations in the North Atlantic Council under Article 4 following the violation of Polish airspace by Russian drones. This led to the robust NATO response, which may have had a deterrent effect on the Kremlin.

While Article 4 does not expressly commit member states to act beyond consultation, it does broaden the framework for decision making and collective action and could evolve into a quick-reaction mechanism for responding to non-military, gray-area or hybrid provocations.

REDEFINING THE MISSION, PRESERVING PURPOSE

NATO's mission must evolve to face the new and evolving strategic environment. NATO's concept of what aggression means in the hybrid war environment must adapt to how warfare is actually being waged. Alliance cohesion depends on aligning these threat perceptions, not just military capabilities.

Deterrence remains the foundation of NATO's mission, but it is no longer simply military deterrence. Maintaining political cohesion and being able rapidly to respond to gray-area provocations are now part of the credible deterrence framework. The greatest risk the Alliance faces is not military escalation, but political erosion: of credibility, cohesion, and will. NATO's success in the coming decade will be measured less by whether it fights a war—and more by whether it prevents Russia from winning without one.

> **The greatest risk the Alliance faces is not military escalation, but political erosion: of credibility, cohesion, and will. NATO's success in the coming decade will be measured less by whether it fights a war—and more by whether it prevents Russia from winning without one.**

ENDNOTES

1. North Atlantic Treaty Organization, *NATO 2022 Strategic Concept*, 2022, 3, https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf.
2. David Kirichenko, "Drone superpower Ukraine is teaching NATO how to defend against Russia," Atlantic Council *UkraineAlert*, October 2, 2025, https://www.atlanticcouncil.org/blogs/ukrainealert/drone-superpower-ukraine-is-teaching-nato-how-to-defend-against-russia/.
3. Atle Staalesen, "Spoofing and jamming from Kola Peninsula jeopardise safety in Norway," *Arctic Today*, February 18, 2025, https://www.arctictoday.com/spoofing-and-jamming-from-kola-peninsula-jeopardise-safety-in-norway/.
4. Hayley Dixon, "Russian spymaster's plot to use private army to control migration into Europe," *The Telegraph*, March 8, 2025, https://www.telegraph.co.uk/news/2025/03/08/russian-spymaster-plot-private-army-migration-europe/.

AFPC

AMERICAN FOREIGN POLICY COUNCIL

Explaining the World. Empowering Policymakers.

Ilan Berman	Chief Editor
Richard Harrison	Managing Editor
	Graphic Design and Layout

MANUSCRIPTS SHOULD BE SENT TO the attention of the Editor at 509 C Street, NE, Washington, DC 20002, or submitted via email to defensedossier@afpc.org. The Editors will consider all manuscripts received, but assume no responsibility regarding them and will return only materials accompanied by appropriate postage. Facsimile submissions will not be accepted.

EDITOR'S NOTE: The opinions expressed in the *Defense Dossier* (ISSN 2165-1841) are those of the author(s) alone and do not necessarily represent the opinions of the American Foreign Policy Council.

ABOUT THE AMERICAN FOREIGN POLICY COUNCIL

For more than four decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.