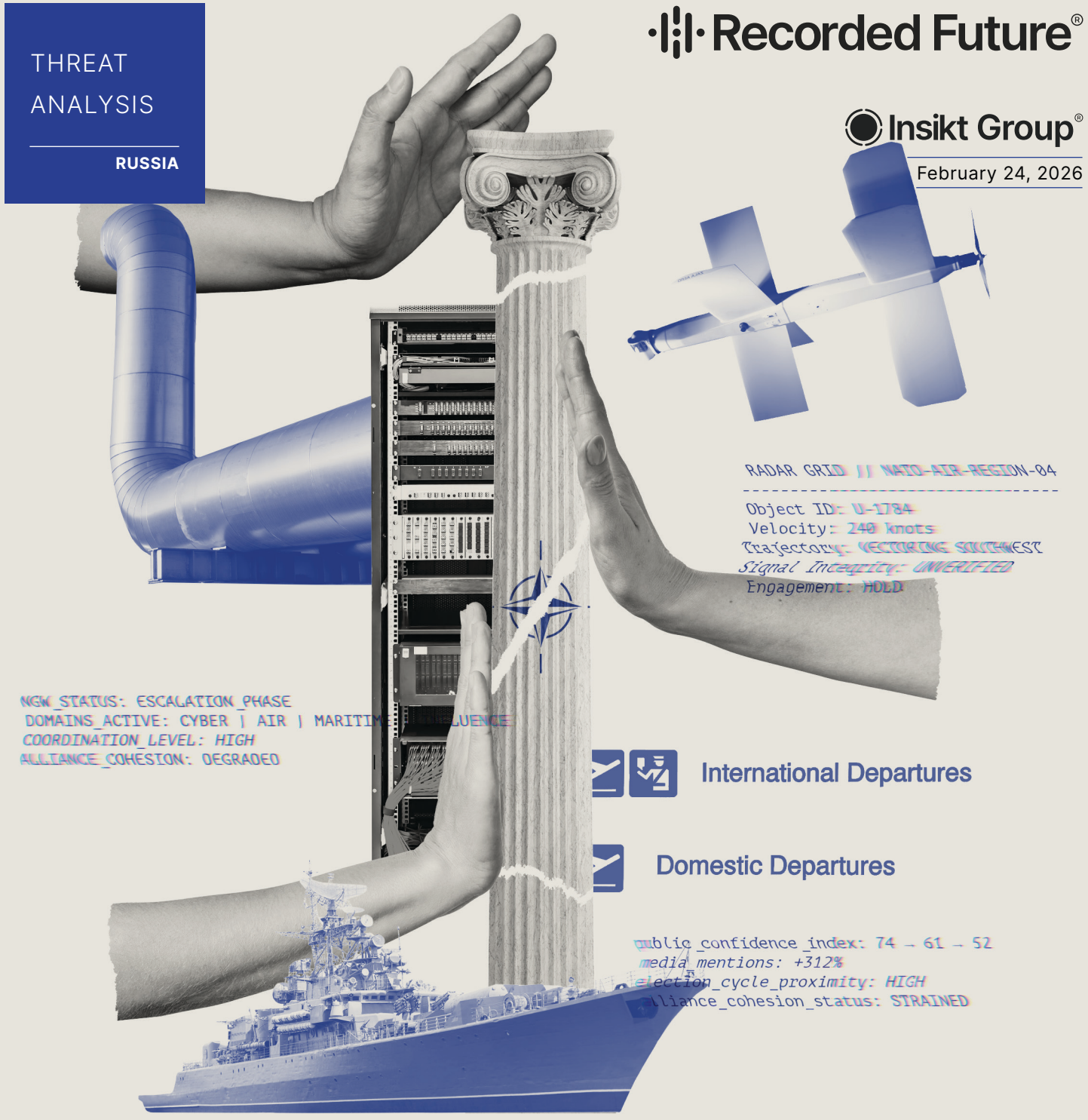
THREAT ANALYSIS

RUSSIA

Recorded Future®

Insikt Group®

February 24, 2026



Preparing for Russia's New Generation Warfare in Europe

Since 2022, Russia's hybrid warfare campaign against NATO has been aggressive, but it is opportunistic and not reflective of Russia's full capabilities.

Putin likely sees a near-term opportunity to test NATO's capabilities and exploit US-NATO tensions, likely via a coordinated hybrid campaign that aligns with Russia's New Generation Warfare doctrine.

A New Generation Warfare campaign would very likely disrupt critical infrastructure, increase reputational risk for impacted firms, and reduce public trust in the reliability of critical services.

Executive Summary

Since its full-scale invasion of Ukraine in February 2022, Russia has waged what we assess is largely opportunistic, though increasingly aggressive, hybrid warfare in NATO territory. Moscow has very likely not yet leveraged its full capability to integrate cyber, political, and sabotage tools into a full-scale campaign.

Over the next two years, Russian President Vladimir Putin will likely escalate Russia's hybrid warfare campaign against NATO members into a full-fledged campaign likely consistent with a Russian military doctrine called New Generation Warfare (NGW). Putin will likely use this campaign to degrade NATO political unity and defense capabilities, reinforce Russia's network of overt and covert assets across NATO, and optimize the physical and political environment, should Putin decide to launch a military incursion into NATO territory.

In a full-scale NGW campaign in NATO territory, Russia would likely move from its current pattern of influence operations efforts combined with largely opportunistic cyber and sabotage targeting to a Europe-wide campaign that is more intentionally planned and aims to project Russian power and weaken European defenses on a systemic level. An NGW campaign would very likely involve Russia using the same tactics it is currently using, including sabotage operations, influence operations, territorial waters and airspace violations, and exploitation of some NATO states' dependence on Russian oil and gas. The primary differences between Russia's current operations in Europe and an NGW campaign would include greater geographic breadth of those operations; greater frequency of operations; and Russia likely using tactics simultaneously and in coordinated ways. For example, likely Russia-directed threat actors might use a drone to violate the airspace over a NATO state's airport, forcing the temporary closure of that airport, coupled with a distributed denial-of-service attack on the airport's internal communications system. Russia might then post a video of the incidents through one of its overt or covert propaganda outlets, arguing that they show NATO cannot adequately protect its aviation network.

An NGW campaign in NATO territory would very likely have significant implications for private and public sector entities, including degradation of critical infrastructure, reputational risk for individuals and companies named in Russian influence operation campaigns, and reduced public confidence in the government's ability to ensure their safety.

Over the next three to five years, Putin will likely evaluate the feasibility of moving from an NGW-like campaign in Europe to a kinetic military incursion. Factors Putin would likely weigh when making such a decision include NATO military capabilities, the likelihood that the US would defend a NATO state if it were attacked, and Russian military capabilities. However, even if the necessary conditions for such an operation emerge, the probability of a proactive Russian military operation into NATO territory very likely remains low.

Key Findings

- Russia's hybrid warfare campaign in NATO territory between February 2022 and January 2026 has been increasingly aggressive, but likely opportunistic and not reflective of Russia's full cyber, influence operations, and sabotage capabilities.
- Putin likely views the next two years as an opportunity to test NATO's defensive capabilities and prepare the physical and psychological environment, should he decide to launch a military incursion. Putin likely assesses that the 2028 US presidential election could lead to a US president more willing to commit US resources to NATO. As such, Putin likely views the next two years as an opportunity to exploit existing US-NATO tensions to weaken NATO's unity and ability to defend itself.
- Russia's escalated aggression against NATO over the next two years is likely to have the hallmarks of a Russian military doctrine called New Generation Warfare (NGW), which combines sabotage operations, cyberattacks, influence operations, and other non-military actions to undermine the enemy's confidence and prepare the physical and psychological environment, should Russia elect to escalate into a kinetic military campaign.
- A full-scale NGW campaign would likely involve an intensified campaign of tactics Russia has used against NATO in the last few years, including sabotage operations, influence operations, violations of NATO airspace with drones and jets, violations of NATO states' territorial waters, targeting of undersea cables, and exploitation of some NATO states' dependence on Russian gas and oil. Russia would likely deploy these tactics more frequently, across more states simultaneously, and would likely use tactics simultaneously in an attempt to strain NATO resources.
- A full-scale NGW campaign would have significant implications for private and public sector entities operating in NATO territory, including disruption to critical services, reputational risk for individuals and firms named in influence campaigns, supply chain disruptions, and reduced public trust in the government's ability to safeguard critical infrastructure. The fact that most of the critical infrastructure in NATO territory is privately owned means public-private partnerships will be essential in mitigating the impact of escalated Russian aggression.

Table of Contents

Russia Likely to Escalate into New Generation Warfare Campaign in Europe Over Next Two Years

Since Russia's full-scale invasion of Ukraine in February 2022, it has waged what Insikt Group assesses is largely opportunistic, though increasingly aggressive, hybrid warfare in Europe. These actions, though destructive, have very likely not leveraged Russia's full capability to integrate cyber, political, and sabotage tools into a full-scale campaign.

Nonetheless, Russian president Vladimir Putin very likely still prioritizes weakening European unity and defensive capabilities in service to his overarching foreign policy goal of replacing the US-led international system with a multipolar world in which Russia, the US, and China are relatively equal in terms of geopolitical influence. Putin very likely judges that uneven US assistance to European defensive efforts creates a window of opportunity for Russia to weaken Europe's ability to resist Russian aggression. Putin likely views recent US-NATO tensions, such as the US's articulated intention to control Greenland, as an opportunity to exacerbate the strategic distance between the US and NATO, thereby weakening the transatlantic partnership that has formed the core of the US-led, post-World War II security architecture. Putin also likely views the next two years as an opportunity to optimize the physical and informational environment in Europe, should he decide to launch a kinetic military attack against Europe.

Putin very likely views this window of opportunity as finite. He likely recognizes that the 2028 US presidential election could result in a US president more willing to commit US military and political resources to amplifying Europe's defensive capabilities. As such, over the next two years, Putin will likely escalate Russia's hybrid warfare against Europe into an expanded campaign that is likely consistent with the principles of Russian New Generation Warfare (NGW) — a warfare doctrine espoused by senior Russian military officials emphasizing control of the information and psychological spaces, as well as the use of undeclared special forces, to weaken an enemy prior to using traditional military forces.

Europe's efforts to bolster its defenses against current levels of Russian hybrid warfare likely reinforce Putin's perception that Europe is motivated to weaken Russia, thereby likely making him more motivated to target Europe. Putin's perception that Europe's defensive efforts are actually a threat to Russia is likely rooted in his calculus that NATO is fundamentally an anti-Russia bloc. Putin has substantiated this assessment by pointing to actions such as NATO's expansion to include former Warsaw Pact countries and its decision to install missile defense systems in Poland.[1]

New Generation Warfare Origins and Principles

Insikt Group assesses that much of Russia's aggressive foreign policy actions since the annexation of Crimea in March 2014 — which marked the beginning of Putin's more assertive efforts to push back

[1] *hxxps://en[.]kremlin[.]ru/events/president/transcripts/24034*

against perceived Western efforts to weaken Russia — have been consistent with NGW, a Russian doctrine in which the state aims to bring about political change in another country primarily by using overt and covert influence tools, as opposed to conventional military force. These tools can include influence operations, sabotage operations, and exploiting economic leverage.

New Generation Warfare is typically associated with Chief of the General Staff Valery Gerasimov's 2013 article in the Russian journal *Military-Industrial Kurier*, though NGW is essentially a modern version of Soviet active measures. "Active measures" (*aktivnye meropriyatiya*) was a term used by the Soviet Union from the 1950s onwards to describe covert influence and subversion operations, including establishing front organizations, backing pro-Soviet political movements abroad, and attempting to orchestrate regime change in foreign countries. Active measures declined during the 1980s and 1990s, but Putin revived its use in the early 2000s. Indeed, in 2007, retired major-general Alexander Vladimirov alluded to that revival when he stated that "modern wars are waged on the level of consciousness and ideas" and that "modern humanity exists in a state of permanent war" in which it is "eternally oscillating between phases of actual armed struggle and constant preparation for it."[2]

Despite the long history of Russia using active measures, Gerasimov's 2013 article provides the most comprehensive account of how current Russian military leaders likely view this doctrine. Gerasimov's article suggests that he views NGW both as the reality of modern warfare and as a preferred way of weakening enemies. Gerasimov argued that the Arab Spring demonstrated that modern wars are not declared conflicts between traditional militaries, but instead depend more on a combination of declared military force and tactics such as domination of the information space, targeting of critical enemy facilities, "asymmetric and indirect operations," and the use of unofficial special forces. He argued that "the very 'rules of war' have changed. The role of nonmilitary means of achieving political and strategic goals has grown and, in many cases, they have exceeded the power of force of weapons in their effectiveness."

The following table, taken from a translation of the article, shows Gerasimov's view of traditional warfare as opposed to New Generation Warfare:

[2] Alexander Vladimirov, "Kontseptualnye osnovy natsionalnoi strategii Rossii: Voyennopoliticheskii aspekt" (Nauka, 2007): 105, 130

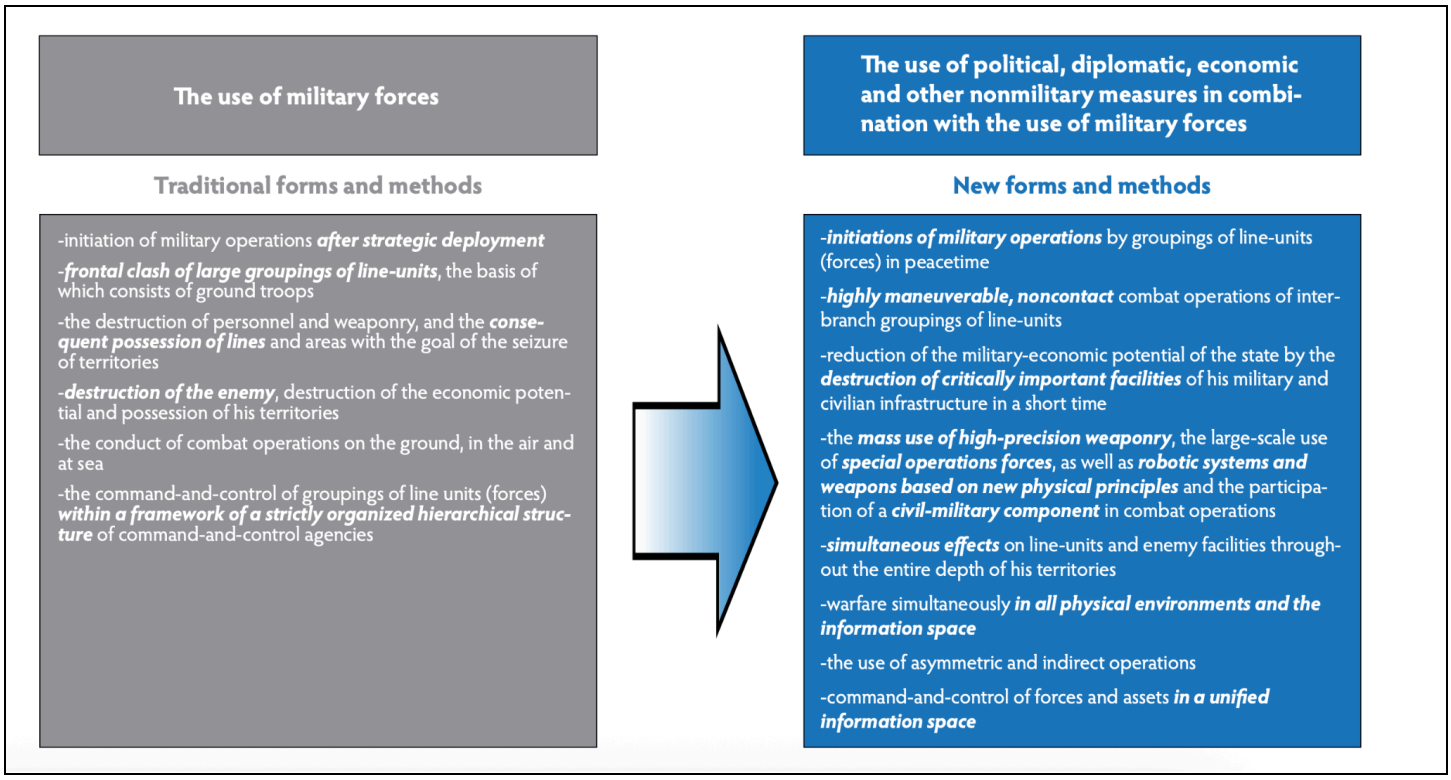


Figure 1: *New Generation Warfare and traditional warfare forms and methods (Source: Military Review)*

We assess that Russia's campaign in Ukraine, starting with the annexation of Crimea in March 2014 and extending to its ongoing full-scale military operation, bears many of the hallmarks of NGW. Russia's military operations more closely aligned with NGW principles from 2014 through 2021; after Russia's full-scale invasion of Ukraine in February 2022, the Russian military transitioned to more traditional operations. Russia's exploitation of influence operations and asymmetric warfare has been a feature of its operations since 2014, and since 2022, Russia has expanded asymmetric and sabotage operations in Europe likely as part of a multi-faceted strategy to use power exertion in Ukraine and Europe to weaken the Western geopolitical system.

This does not mean that Russian military leadership have consciously used NGW as their guiding principle in Ukraine at all times; indeed, we lack the insight into Russian military leadership thinking to assess with high confidence the principles they are employing. Rather, the combination of Gerasimov's writings and observation of Russian operations in Ukraine means we can assess with medium confidence that Russia's Ukraine operations prior to 2022 often reflected NGW principles. As such, we assess that NGW is a useful framework for understanding Russian military operations.

NGW Principle	Example of How the Ukraine Operation Exemplifies Principle
Initiation of military operations by groupings of line units in peacetime	**March 2014–February 2022:** Russian regular line units (Russian Airborne Forces [VDV], Naval Infantry, and Main Intelligence Directorate [GRU]-controlled unit formations) entered Ukrainian territory, annexed Crimea, and operated in eastern Ukraine without a declared state of war. In eastern Ukraine, troops operated under attempted deniability, with Moscow claiming the operations were being conducted by sympathetic Ukrainian separatist forces. **February 2022–January 2026:** Though Russia acknowledged its presence throughout Ukraine, it still operates[3] without a full declaration of war, instead casting its campaign as a "special military operation."
Highly maneuverable, noncontact combat operations of interbranch groupings of line units	**March 2014–February 2022:** Russian battalion tactical groups (BTGs) generally demonstrated high operational mobility, integrating ground forces, artillery, electronic warfare, and intelligence, surveillance, and reconnaissance (ISR) assets. **February 2022–January 2026:** As Russia has attempted to take more territory, it has transitioned to a greater emphasis on attritional, contact-heavy warfare.
Reduction of the military-economic potential of the enemy state via the destruction of critically important military and civilian infrastructure	**March 2014–January 2026:** Russia has consistently attempted to degrade Ukraine's critical infrastructure, including through long-range strikes and cyberattacks targeting power plants, transportation and logistics hubs, and defense-industrial facilities.
Mass use of precision weaponry, special operations forces, and robotics systems	**March 2014–January 2026:** Russia has increasingly used precision weapons (for example, Iskander-M ballistic missiles, Kalibr cruise missiles, Kh-101/555 air-launched cruise missiles), GRU special operations units (including the 3rd Separate Spetsnaz Brigade and the 346th Independent Spetsnaz Brigade); and unmanned systems (such as Orlan-10, Lancet, Shahid-136 drones, and ground robots for logistics and mine-clearing operations).
Simultaneous effects on line-units and enemy facilities throughout the enemy state's territory	**March 2014–January 2026:** Russia has conducted strikes across Ukraine, using frontline units, operational rear units, missile and ground attacks, and cyber operations.

[3] *hxxps://en[.]kremlin[.]ru/events/president/transcripts/by-date/24.02.2022*

NGW Principle	Example of How the Ukraine Operation Exemplifies Principle
Warfare simultaneously in physical and information space	**March 2014–January 2026:** Russia has consistently used covert and overt means to propagate narratives meant to justify intervention and regime change in Ukraine. These include allegations of Nazism in the Ukrainian military and government writ large; discrimination against Russians in Ukraine; and Western government efforts to foment revolution in Ukraine.
Use of asymmetric and indirect operations	**March 2014–February 2022:** Russia's operations were indirect because they included non-acknowledged units, private military companies, and proxy forces such as Donetsk People's Republic (DPR) and Luhansk People's Republic (LPR) militias. **February 2022–January 2026:** Russia escalated its use of asymmetric and indirect operations against Europe, including targeting undersea cables and critical infrastructure, likely to pressure Europe and Kyiv to abandon efforts to resist Russia's Ukraine campaign.
Command and control of forces and assets in a unified information space	**March 2014–January 2026:** Russia has attempted to integrate its C2 structures, including shared ISR, targeting data, and operational planning, across services, and has centralized strike coordination for long-range fires. However, limitations have been apparent in Russia's ability to accomplish this, especially since February 2022, likely stemming from deficiencies such as poor inter-service coordination, rigid command structures, and underestimation of Ukrainian capabilities and willingness to fight.

Table 1: *New Generation Warfare principles (Source: Recorded Future)*

New Generation Warfare Toolkit

In a full-scale New Generation Warfare campaign in Europe, Russia would likely move from its current pattern of influence operations efforts combined with largely opportunistic cyber and sabotage targeting to a Europe-wide campaign that is both proactive and reactive. It would likely involve the same tactics Russia has used against NATO states for the past few years. The difference would likely be that Russia would deploy these tactics more frequently and across a greater number of states at once. A full NGW campaign would likely also involve using some operational methods simultaneously and in ways that amplify one another.

Even in a full-scale NGW campaign, Russia would very likely aim to keep destruction below the threshold that risks NATO invoking Article 5. NATO officials have not specified precisely what the Article 5 threshold is; indeed, former NATO Secretary General Jens Stoltenberg stated that the grounds for

invoking Article 5 "must remain purposefully vague." However, it is likely that it would include a mass casualty event or the use of a chemical or biological weapon. The text of Article 5 specifies that the threshold involves "an armed attack." NATO officials said in 2022 that a cyberattack could constitute grounds for invoking Article 5, though they did not specify what kind of cyberattack would qualify.

Russia is likely to face few downsides during an NGW campaign, due to minimal risk of Russian casualties and the campaign's tactical flexibility. Unlike a conventional military campaign, which risks a high level of casualties that can cause domestic public dissatisfaction, an NGW campaign very likely would involve minimal risk to Russian citizens. In addition, an NGW campaign inherently offers significant tactical flexibility, as it is not a declared campaign in which Russia needs to articulate goals to justify the campaign to the Russian public and elites. As such, Putin would likely have the option to draw down tactics that are proving less effective and increase the use of more effective tactics, without needing to justify tactical failures. This flexibility would likely allow Putin to continue at least aspects of an NGW campaign in the likely event that Europe responds to an NGW campaign with escalated efforts to counter Moscow.

Influence Operations and Propaganda

Russian "active measures" serve as a force multiplier for Moscow's broader political warfare, integrating influence operations, propaganda, and sabotage. In Europe, these efforts aim to weaken transatlantic cohesion, erode public and political support for Ukrainian sovereignty and assistance to Kyiv, and exacerbate internal societal divisions, economic uncertainty, and other challenges. By cultivating sanctions fatigue and encouraging selective bilateral re-engagement with Russia through active measures, Moscow seeks to mitigate its international isolation and undermine the rules-based international order, thereby advancing a Russia-favored multipolar system characterized by exclusive spheres of influence. Notably, these activities also include angles of domestic preservation by portraying the West as chaotic, corrupt, and immoral, and thereby discouraging the expansion of liberal democracies elsewhere, particularly from within.

Since Russia's full-scale invasion of Ukraine in 2022, Insikt Group has observed concentrated Russian influence operations targeting the domestic audiences of what Moscow likely views as Kyiv's core European supporters: the UK, France, Germany, and Poland. Insikt Group investigations, in addition to public reporting, have previously identified multiple influence operations targeting the above-mentioned major European allies, including Doppelgänger, Operation Overload, Operation Undercut, and CopyCop. These influence operations have commonly impersonated national and pan-European media outlets to disseminate messages aligned with Kremlin propaganda, including anti-Ukraine themes and content that denigrates pro-European political figures. Elsewhere, Russian influence operations have sought to use fear and physical demonstrations to manipulate public opinion. In France, for example, Russia-linked physical intimidation very likely intended to provoke public anxiety and societal unrest included the Star of David and red hand graffiti, as well as the placement of caskets near the Eiffel Tower ahead of the 2024 Paris Olympic Games. Similar efforts have also appeared elsewhere in Europe, including the emergence of pro-Russian billboards in Italy and the "Children of War, Alley of Angels" exhibit in Germany.

Russian influence efforts have also leveraged illicit financing and alleged bribery to attempt to favorably reshape European politics. For example, in spring 2024, Czech authorities attributed the Voice of Europe, an organization linked to Viktor Medvedchuk, to paying politicians in several EU countries to spread anti-Ukraine messages. In September and October 2024, Moldovan police reported that a Russia-linked network, allegedly run by fugitive oligarch Ilan Shor, channeled tens of millions of dollars to buy votes ahead of Moldova's October 20, 2024, presidential election and EU referendum. In December 2024, Romanian prosecutors conducted raids and opened probes into alleged illegal campaign financing and payments to TikTok users and influencers associated with the then-annulled presidential vote. More recently, former UK Member of the European Parliament (MEP) Nathan Gill was sentenced on November 21, 2025, after pleading guilty for accepting bribes to make pro-Russian statements.

Insikt Group assesses Russia's NGW against Europe will likely consist of aggressive influence operations targeting Europe that aim to erode European unity and advance Russia's quest for a multipolar world order. NGW will very likely continue supporting Moscow's core objectives of eroding political and public support for Ukrainian sovereignty and assistance to Kyiv, accelerate sanctions fatigue, and exploit domestic political crises and election cycles to fracture European cohesiveness and transatlantic cooperation. Moscow will likely expand its reliance on access to third parties and intermediaries, including sympathetic socio-political organizations and fringe movements, to launder Kremlin-aligned messages into the European information environment.

Across Europe, Russia will almost certainly continue to attempt to delegitimize existing democratic institutions and Europe's information ecosystem by continuing to foster distrust in elections, mainstream media, the EU, and pro-European government figures. In a post-war environment, assuming European sanctions on Russian media enterprises are lifted, Russia will very likely attempt to reestablish its state media presence while also hardening itself to withstand future disruptions, legal restrictions, and platform or government takedowns in the event of a kinetic conflict with Europe.

New Generation Warfare operations against Europe will very likely incorporate much of Russia's current-era influence tradecraft, including social media influence via human and automated networks, media impersonation and covert media outlet brands, illicit financing and bribery, and cyber-enabled influence such as hack-and-leak narratives. Further, Insikt Group assesses Moscow will very likely continue attempting to cultivate sympathetic allies through covertly funded fringe socio-political organizations, using these entities to astroturf "grassroots" support, amplify Kremlin-aligned narratives, and catalyze or intensify domestic unrest across Europe. We assess that Russia will also adapt emerging technologies, particularly AI, to scale the production, localization, and quality of influence content, increase dissemination efficiency, and optimize targeting. Continued advances in generative AI will almost certainly improve the realism of propaganda images and fabricated reporting, forged documents and correspondence, and synthetic impersonations of public figures, including audio and video deepfakes.

Airspace Incursions by Drones and Jets

Beginning in September 2025, suspected violations of NATO airspace by Russia-directed drone operators or Russian jets increased to unprecedented levels, as Russia likely sought to project power across NATO territory and test NATO resolve while maintaining plausible deniability. Insikt Group tracked 30 suspected or confirmed violations between September 2025 and January 2026, compared to 23 suspected or confirmed violations between March 2022 and August 2025. The most commonly targeted countries since March 2022 have been Poland and Romania; however, suspected Russian violations of NATO airspace have occurred outside of Russia's historic sphere of influence, including in Germany, UK, Denmark and Norway. Violations have most frequently targeted critical infrastructure, such as military bases and airports.

In a full-scale New Generation Warfare-like campaign in Europe, Russia likely would escalate the frequency and level of aggressiveness of these violations. Russia's targeting would likely continue to focus on critical infrastructure, but violations would very likely significantly increase in frequency. Russia would also likely use drones to fly closer to targets and perhaps hover over them for extended periods of time, in a likely effort to test NATO's willingness to shoot down drones and perhaps collect intelligence on critical infrastructure facilities. Indeed, in September 2025, Polish authorities said they shot down Russian drones that violated Poland's airspace.

Other ways Russia would likely escalate the aggressiveness of its airspace violations include timing those violations with major NATO events, such as military exercises and summits. Russia could escalate its use of drones as electronic warfare mechanisms, perhaps to disrupt NATO military exercises or the functioning of critical infrastructure facilities.

Russia would likely also use its drones to amplify its psychological warfare as a way of projecting power and demonstrating to the public that Moscow can disrupt everyday life in NATO countries. Russia could do this via tactics such as hovering drones over civilian transportation infrastructure, like railways or airports, which have already been forced to temporarily close. Russia could also launch drones over facilities hosting political summits, such as the annual NATO Summit, or over polling places during elections to stoke public fear. In a full-scale NGW campaign that involves coordination of multiple tactics, Russian propaganda outlets might release footage of these incidents to propagate a narrative that NATO states cannot protect their infrastructure. Russia could also combine drone or jet violations with sabotage operations to further sow public panic and force NATO governments into a defensive posture.

Russia would very likely seek to maintain some level of deniability and would avoid airstrikes and mass casualty events, which would almost certainly guarantee an Article 5 declaration.

Territorial Waters Violations and Targeting of Undersea Cables

Insikt Group assesses that, since February 2022, Russia has increasingly used violations of NATO states' territorial waters[4] and targeting of undersea cables to test the alliance's resilience, collect intelligence, keep NATO in a reactive, defensive posture, and attempt to deter NATO from undermining Russian strategic interests. In June 2023, Deputy Chairman of the Security Council Dmitriy Medvedev stated that, "if we proceed from the proven complicity of Western countries in blowing up the Nord Streams, then we have no constraints — even moral — left to prevent us from destroying the ocean-floor cable communications of our enemies." Medvedev's comments were likely purposefully hyperbolic; however, they likely reflect a Kremlin perception that NATO is targeting Russian strategic interests, thereby justifying retaliatory action.

Examples of Russia likely targeting undersea cables and maritime assets include an April 2025 incident in which the UK identified Russian sensors attempting to collect intelligence on UK nuclear submarines and other underwater critical infrastructure; the Russian Yantar surveillance ship sailing near cables carrying data for Google and Microsoft under the Irish Sea in November 2024; and reports suggesting that the Russian Eagle S ship accused of damaging multiple undersea cables in December 2024 carried spy equipment to monitor naval activity.

Russian ships have also violated NATO states' territorial waters, likely to test NATO resilience, force NATO into a defensive posture, and project power. Examples include a July 2025 incident in which a Russian border guard vessel entered Estonian territorial waters without permission; a July 2024 incident in which a Russian naval vessel entered Finnish territorial waters without authorization; and frequent encounters between NATO states and Russia-linked "shadow fleet" vessels. These vessels are tankers sailing under other flags, which often refuse inspection or orders from local navies.

During a full-scale New Generation Warfare campaign against NATO, Russia likely would escalate its targeting of undersea cables and violations of territorial waters. This could include more frequent cable targeting, likely to cause minor but persistent damage to undersea critical infrastructure that tests NATO resilience and Russian destructive capabilities without provoking an Article 5 declaration. Russia could also conduct electronic jamming operations during cable repairs to inhibit communications and use Russian ships to harass those conducting repairs.

Russia would also likely attempt longer and more provocative territorial waters violations, including placing Russian ships near NATO vessels and expanding these activities into areas such as the Mediterranean; conducting concurrent hybrid activity such as GPS jamming and automatic identification system (AIS) spoofing; refusing escort out of territorial waters; and combining territorial waters violations with airspace violations by Russian aircraft or targeting of undersea infrastructure.

[4] "Territorial waters" is defined as the area twelve nautical miles from a state's coastline, which is the area over which a state has jurisdiction, per the United Nations Convention on the Law of the Sea (https://www.un.org/depts/los/convention_agreements/texts/unclos/part2.htm).

Russia would likely aim to overwhelm NATO's existing efforts to prevent sabotage of undersea infrastructure. In January 2025, Estonia, Latvia, and Lithuania launched Baltic Sentry — a campaign that uses tools such as frigates, maritime patrol assets, and naval drones to deter sabotage of undersea infrastructure. Since the launch of Baltic Sentry, the Baltic Sea has experienced very few undersea sabotage efforts; however, it is not clear whether this is the result of Baltic Sentry or a lack of planned operations.

Sabotage Operations

We assess Russia has escalated its use of sabotage operations in NATO territory since its full-scale invasion of Ukraine in 2022, likely to test the resilience particularly of NATO states' critical infrastructure; propagate a narrative that Western states cannot protect their populations from threats; harm NATO's ability to collectively respond to Russian aggression by forcing NATO into a reactive, defensive posture; and degrade NATO states' ability to provide material support to Ukraine. Sabotage operations are loosely defined, but typically consist of targeting civilian or dual-use infrastructure with physical security attacks by deniable entities.

Particularly since 2022, Russia-linked entities have focused sabotage operations on critical infrastructure in NATO states, exploiting vulnerabilities wrought from deferred maintenance and lack of sufficient public or private investment in upkeep. Within critical infrastructure, the most frequently targeted sectors include undersea telecommunication and power cables; water supply and distribution; transportation; military; healthcare; and telecommunications. The number of Russian sabotage operations has quadrupled from 2023 to 2024, and in 2025, it was likely at levels consistent with 2024. Operations have occurred across NATO, as opposed to being focused in Russia's historic sphere of influence. That said, the most commonly targeted states between January 2018 and June 2025 were Germany, Estonia, Latvia, Lithuania, and Poland.

In a New Generation Warfare-like campaign targeting NATO territory, Moscow would likely move from what we assess has thus far been largely opportunistic sabotage to operations with more consistency and geographic breadth, and that complement other tactics.

Russia would likely still focus its sabotage operations on critical infrastructure, but would likely place a premium on damaging the critical infrastructure of NATO states that either would be probable targets of a Russian military incursion — such as Poland or the Baltic states — or would lend significant assistance to those states, such as the UK, Germany, or France. This is because in an NGW campaign, Russia would likely view sabotage operations as, in part, a way to test the resilience of potential victim states and their allies. Russia's sabotage operations against those targets would likely be more frequent and could coincide with significant events such as elections or military exercises. Russia would likely pair sabotage operations with other tactics, such as offensive cyber operations or airspace violations, to augment the destructive impact of the operations and try to strain NATO states' capacity by forcing them to respond to multiple disruptions at once, while still staying below the threshold that would risk an Article 5 declaration.

Offensive Cyber Operations for Disruption and Counterintelligence

Russian cyber activity directed at European targets has consistently emphasized access-oriented operations, including attacks on internet-facing firewalls, virtual private networks (VPNs), email services, and web portals. This activity aligns with documented Russian cyber practices focused on enabling intelligence collection, operational reach, and long-term flexibility rather than immediate disruptive effects. Recent Insikt Group reporting highlights BlueEcho activity targeting perimeter infrastructure to establish footholds and enable follow-on credential capture and lateral movement, while BlueDelta campaigns demonstrate sustained credential harvesting at scale using impersonated Microsoft Outlook Web App (OWA), Sophos VPN, and Google login workflows. This tradecraft is low-cost, repeatable, and consistent with long-term counterintelligence targeting of government, defense, and research entities.

Russian cyber activity affecting Europe has been broad in scope, with targeting observed across multiple regions and sectors. If cyber operations were used for more overtly disruptive purposes, effects would likely be more pronounced in states with weaker cybersecurity maturity or slower coordinated response mechanisms, such as fragmented local-government IT environments or limited national incident response surge capacity. This does not preclude activity against major NATO states, where Russian cyber operations have historically focused more heavily on intelligence collection and access. BlueDelta's targeting of NATO-aligned and defense-related organizations reflects continued Russian interest in strategically valuable European targets aligned with GRU intelligence requirements.

Observed Russian cyber activity also provides insight into how operations could escalate if strategic conditions were to change and Russia were to launch a full-scale NGW campaign. Russian threat actors have demonstrated the ability to establish and maintain access over time, including through persistent connections and tunneling, which could be repurposed to degrade remote access services, manipulate edge-device configurations, or cause temporary service disruption. In Ukraine, cyber activity has been observed alongside influence operations and physical sabotage, including Recorded Future–tracked influence campaigns such as CopyCop, which leveraged automated content replication and spoofed media infrastructure to amplify pro-Russian narratives in parallel with other forms of hybrid activity. If applied elsewhere, similar coordination could increase pressure on incident response capabilities and undermine public confidence in the reliability of essential services. Credential-harvesting operations further provide pathways beyond inbox access, including potential compromise of identity providers, VPN portals, and privileged administrative portals.

Russian cyber operations have historically involved establishing and maintaining access to targeted networks over extended periods, a pattern also documented in prior campaigns in Ukraine. However, there is no public evidence demonstrating that the access currently observed in European networks is intended for future disruptive operations. If a kinetic conflict were to escalate in Europe, Russia would likely seek to expand or prioritize access within relevant networks to support intelligence collection, operational coordination, or potential disruption. Russia also has a documented history of tolerating or leveraging cybercriminal activity alongside state-directed operations, including overlap with criminal

infrastructure and access brokers, which may allow operators to expand scale, complicate attribution, and generate disruptive effects without overtly exposing state-linked capabilities. Collectively, activity associated with BlueAlpha, BlueDelta, BlueEcho, Sandworm, and Dragonfly illustrates Russia's ability to scale cyber operations from access and intelligence collection toward disruption if strategic conditions were to change, consistent with broader hybrid and New Generation Warfare practices.

Exploitation of European Dependence on Russian Oil and Natural Gas

Russia has long exploited other states' dependence on its natural gas and oil to exercise leverage over them, typically by strategically decreasing supply flows, particularly during high-demand periods, such as winter. For example, in 2006, Georgia accused Russia of intentionally cutting gas supplies during an unusually cold period to increase political pressure on Tbilisi. In the run-up to Russia's full-scale invasion of Ukraine in February 2022, Russian state gas company Gazprom reduced natural gas deliveries to Europe, likely in an effort to pressure Europe into abandoning a unified stance on supporting Ukraine.

Since 2022, many NATO states have sought to reduce their dependence on Russian natural gas and oil; however, several states remain dependent, including Slovakia, Hungary, and Türkiye. In a full-scale New Generation Warfare campaign in Europe, Russia would very likely escalate its exploitation of those states' dependence on Russian energy imports to demonstrate Moscow's ability to degrade European critical infrastructure, undermine NATO unity, gauge the resilience of these states' critical infrastructure, and test Russia's ability to handicap critical infrastructure, should Putin decide to launch a military incursion into NATO territory.

Moscow's willingness to exploit these states' dependence on Russian energy likely varies by state. Moscow is less likely to exploit Hungary's dependence on Russian oil and gas, given Budapest's strong relations with Russia. Slovakia is a more likely target, as it seeks a positive relationship with Moscow, but is likely of less strategic importance to Russia than Hungary. Moscow's relations with Türkiye have fluctuated between positive and adversarial; the likelihood of exploiting Türkiye's dependence on Russian energy imports would likely depend, in part, on how positive the overall Russia-Türkiye relationship is at that time.

Escalation of economic critical infrastructure targeting would likely take the form of both more frequent and more geographically broad operations, particularly during high-demand periods such as the winter and perhaps during NATO military exercises or elections. Russia could also escalate its use of pricing manipulation to punish states that work against Russia's strategic priorities in Ukraine, and reward pro-Russia states such as Hungary.

Russia would also likely combine supply cuts with sabotage operations. For example, in 2006, Moscow cut gas supplies in Georgia at the same time it sabotaged an electricity line. Following a successful operation, pro-Russia propaganda outlets would likely amplify narratives that claim European critical infrastructure is weak and vulnerable, and that this demonstrates the inadequacy of democracy and the Western political system writ large at fulfilling basic public needs.

In a New Generation Warfare campaign against Europe, Russia would be unlikely to seek permanent damage to European critical infrastructure or mass civilian harm from disruption of energy flows. Russia would also likely avoid long-term disruption of oil and gas deliveries to limit the financial impact, since oil and gas revenues comprise roughly 25% of Russia's annual federal revenue.

Indicators of NGW Campaign in Europe, Implications for Public and Private Sectors, and Recommended Mitigations

Tactic: Influence Operations		
Indicators of NGW Campaign	**Implications for Public and Private Sectors**	**Recommended Mitigations**
Increased convergence of narratives across propaganda outlets, including state media, inauthentic social media accounts, and so on Parallel narratives tailored to each country or region	Public Sector: more pronounced political polarization; reduced public trust in government competence Private Sector: brand damage if firms are targeted in influence operation (IO) campaigns; employee or executive harassment or doxxing	Ensure communication response protocols are in place, such as rapid rebuttal measures Ensure information environment monitoring is attuned to Russia-nexus narratives so inauthentic behavior can be detected quickly

Tactic: Airspace Incursions by Drones and Jets		
Indicators of an NGW Campaign	**Implications for Public and Private Sectors**	**Recommended Mitigations**
More frequent incursions that last longer and target strategic sites such as military training grounds, critical infrastructure nodes, and so on Incursions are conducted at lower altitudes, with transponders turned off Violations are clustered around NATO decisions or major military exercises	Public: forced closures of critical infrastructure sites during airspace violations, thereby disrupting operations, as well as likely escalation of public alarm and potential decrease in public confidence in the government's ability to keep critical infrastructure safe Private: business operation disruptions due to critical infrastructure closures	Strengthen counter-measures against unmanned aircraft systems (UASs) around critical sites Ensure joint civil-military air incident protocols are in place, including aviation alerts and Notice to Airmen (NOTAM) coordination Improve GPS resilience

Tactic: Territorial Waters Violations and Targeting of Undersea Cables		
Indicators of an NGW Campaign	**Implications for Public and Private Sectors**	**Recommended Mitigations**
More frequent territorial waters violations Violations by state-linked vessels Non-compliance with escort or hails; risky maneuvering around NATO state vessels, perhaps to provoke potential collisions Increased loitering of suspicious vessels near cable routes and landing areas Repeated "anchor drag" incidents Interference with repair ships Simultaneous cyber activity against telecommunications and energy operators	Public: intermittent communications degradation; potential harm to energy infrastructure Private: major potential operational losses for telecommunications, finance, and other key sectors; potential increases in insurance costs for shipping companies, should territorial waters violations at ports become common	Consider mapping alternative sea routes in case primary routes are disrupted; consider rapid reroute contracts Ensure sufficient port and state coordination Ensure physical hardening at cable landing sites Expand Baltic Sentry efforts to other locations

Tactic: Sabotage Operations		
Indicators of an NGW Campaign	**Implications for Public and Private Sectors**	**Recommended Mitigations**
More frequent operations, including arson, vandalism, explosions, and rail disruptions Targeting of high-priority	Public: potential reduction in public confidence in government's ability to protect critical infrastructure and residential areas; in the event of significant escalation in sabotage operations, emergency services	Expand insider threat and contractor vetting at critical infrastructure sites Ensure physical security measures are in place, including

Tactic: Sabotage Operations		
Indicators of an NGW Campaign	**Implications for Public and Private Sectors**	**Recommended Mitigations**
sites, such as military logistics hubs, defense suppliers, and so on Targeting of civilian sites, such as shopping malls or residential neighborhoods Concurrent operations in multiple geographic regions, suggesting intentional planning Combined sabotage operations and airspace or territorial waters violations	could be strained Private: facility damage or loss; threat to worker safety; supply chain interruption; business interruption; reputational liability	perimeter detection, anti-drone measures, camera coverage, and access control Enhance public-private partnerships, as most of the critical infrastructure NATO relies upon is commercially owned Ensure rapid liaison channels with law enforcement and intelligence services

Tactic: Offensive Cyber Operations		
Indicators of an NGW Campaign	**Implications for Public and Private Sectors**	**Recommended Mitigations**
Campaigns that target strategic pressure points, such as logistics and transportation hubs, defense supply chains, and local government entities Intrusion and distributed denial-of-service (DDoS) activity spikes at politically significant moments, including elections, military exercises, or geopolitical summits Campaigns that blend state and proxy activity, such as hacktivist DDoS	Public: DDoS and ransomware campaigns can undermine public confidence in the reliability of institutions; compromise of government narratives can result in less public confidence in the truth of government messaging; even attempted election manipulation can reduce confidence in voting systems Private: elevated risk of disruption of key logistics, transport, rail, and aviation systems; hack and leak operations pose risk to reputation, personally identifiable information, and intellectual property rights; targeting of critical infrastructure can result in operational disruption	Enforce phishing-resistant multi-factor authentication Implement conditional network access based on geopolitical and risk factors Patch for commonly exploited software Reduce exposure (lock down admin portals; restrict by IP address; remove unused services) Use DDoS protection, autoscaling Coordinate with the national computer emergency response team (CERT) and National

Tactic: Offensive Cyber Operations		
Indicators of an NGW Campaign	**Implications for Public and Private Sectors**	**Recommended Mitigations**
campaigns that amplify Kremlin-aligned narratives Coupling of multiple tactics, such as cyber and influence operation hybrid campaigns		Counterintelligence and Security Center (NCSC), as well as upstream providers; rehearse continuity plans Require multi-factor authentication (MFA) and logging parity from third-party providers; segment privileged access; monitor for abnormal remote management activity

Tactic: Leveraging Economic Dependence		
Indicators of an NGW Campaign	**Implications for Public and Private Sectors**	**Recommended Mitigations**
Supply manipulation, including threats or actions to raise price volatility Exploitation of legal measures, including sudden contract disputes or claims of force majeure More frequent cessation of oil and gas supplies, especially during high-demand periods such as winter	Public: higher energy bills and supply disruption, potentially leading to public dissatisfaction Private: price shocks, supply uncertainty, costs related to resolving alleged contract disputes	Diversify suppliers and routes Ensure on-site backup generation where feasible

Outlook: Putin Likely Evaluating Feasibility of Russian Military Incursion in NATO Territory Over Next Three to Five Years

We assess that Putin is likely evaluating the feasibility of a Russian military incursion into NATO territory, particularly in former Soviet states, including Poland, Romania, and the Baltic states. The strategic and tactical conditions necessary for such an operation could materialize over the next three to five years. However, even if the necessary conditions for such an operation emerge, the probability of a proactive Russian military operation into NATO territory very likely remains low.

Over at least the last year, Russian officials have adopted policies and made statements that suggest Putin has not ruled out a Russian military operation in NATO territory. In November 2025, Putin signed[5] a law moving Russia to a year-round military draft — a move likely meant to ensure manpower for operations in Ukraine in the short-term, but which would also be consistent with efforts to replenish Russia's military strength for a NATO-based operation. In November 2025, in response to German Defense Minister Boris Pistorius's warnings that Russia could start a war with NATO as early as 2029, Russian Foreign Ministry spokesperson Maria Zakharova said there is "no doubt about who the aggressor is." Kremlin Press Secretary Dmitriy Peskov said that Russia "may be forced to take measures to ensure its security." In March 2025, Russian Foreign Minister Sergey Lavrov accused Moldova and the Baltic states of adopting racist policies against Russians living there. Allegations by Russian government officials of anti-Russian discriminatory policies preceded several of Russia's incursions into its near abroad, including Transnistria in 1992, Georgia in 2008, and Ukraine in 2014.

Over the past year, declassified European intelligence estimates and statements by NATO officials also suggest an emerging consensus among senior European officials that Russia could be prepared to launch a military operation in NATO territory in 2026–2030. In December 2025, NATO Secretary General Mark Rutte said that, "Russia could be ready to use military force against NATO within five years." A Danish intelligence analysis declassified in February 2025 stated that "Russia sees itself in conflict with the West and is preparing for a war against NATO." In June 2025, Germany's top general stated that a Russian attack could occur within the next four years.

Within the last year, many NATO member states have also increased their defense spending, suggesting a concrete fear among European officials that the likelihood of a NATO-Russia conflict is increasing. Increased NATO defense spending is likely also a result of urging from the US and a judgment among NATO members that President Trump might be less willing to financially supplement European defense efforts than previous US presidents. At the 2025 NATO Summit at The Hague, NATO member states committed to investing 5% of their domestic GDP to defense by 2035 — an increase from the 2% the Alliance committed to in 2014. In 2025, all NATO states spent at least 2% of their GDP on defense. The highest spenders are those in close proximity to Russia, very likely because they judge they are at higher risk of Russia targeting them with hybrid warfare attacks. Poland spent the most, at 4.5% of GDP, with Lithuania and Latvia coming in next, at 4% and 3.75% of their GDP, respectively.

[5] *hxxps://www[.]kommersant[.]ru/doc/8179774?from=top_main_1*

As Putin evaluates the feasibility of a military operation in NATO territory, he is very likely to weigh domestic and external factors. The most important factor dictating Putin's decision likely is NATO's military strength and, specifically, Putin's assessment of the extent to which the US would uphold its Article 5 mutual defense commitment. Russia's military strength is likely an important, but secondary, concern for Putin. His persistence in keeping Russian forces engaged in ground combat in Ukraine in 2025, despite high casualties and nearly zero territorial gains, suggests Putin prioritizes strategic geopolitical gains over battlefield gains. That said, Putin is likely looking to avoid a repeat of the Russian military's failure to achieve its initial goals in Ukraine in 2022, in large part to prevent elite frustration, and therefore is very unlikely to launch a proactive military operation in NATO territory without some confidence of success in at least short-term tactical goals.

Putin's persistence in expansive territorial aggression since 2014, despite increased sanctions and economic isolation, suggests he will not place significant importance on the economic ramifications of a NATO-Russia conflict. Russia's authoritarian political system and what we assess has been the Kremlin's decimation of the Russian political opposition — which has accelerated over the last three years — suggest Putin is very unlikely to prioritize Russian public appetite for another war when considering whether to launch a military incursion into NATO territory.

Active fighting in the Russia-Ukraine war would likely have to substantially diminish before Putin initiates a military operation in NATO territory. Despite Putin's high casualty tolerance, he very likely would want to achieve at least an initial tactical victory in an incursion into NATO territory, and the Russian military almost certainly cannot sustain a two-front war. In addition, Putin likely assesses that there are domestic political benefits to keeping Russia engaged in an external conflict, making it slightly more likely that Putin initiates at least a small-scale incursion into NATO territory if the Russia-Ukraine war ends. Putin has largely transitioned Russia to a wartime economy, which likely creates institutional momentum to keep a war going. Transitioning Russia back to a more diversified, peacetime economy very likely would be difficult, given the fact that Russia is currently the most sanctioned country in the world and therefore lacks significant Foreign Direct Investment (FDI). In addition, Russian elites' patronage and graft flows have very likely increasingly flowed from the defense industry; transitioning Russia back to a peacetime economy would therefore require Putin to redirect those graft flows to avoid elite discontent. Finally, a large-scale economic transition likely risks a contraction during the transition period, which in turn would risk elite and public unrest.

Appendix A: Entities Connected to NGW Tactics

The following are select entities, groups, and other organizations connected to New Generation Warfare tactics Russia might employ in Europe. This is meant to help customers monitor Russia's deployment of NGW tactics. Recorded Future Platform queries are provided for each one.

Note: There is no separate list for sabotage operations because it is our assessment that Russia uses combinations of the entities in the other presented categories in sabotage operations. As such, customers interested in monitoring Russia-nexus sabotage operations should use the queries and lists built for the other NGW tactics.

NGW Tactic	Selected Entities/Groups/Organizations
Influence Operations	**Russian Government Departments** • Main Directorate of the General Staff (GRU) **Influence Operations Companies and Campaign Operators** • Social Design Agency (SDA) • ANO Dialog • Structura National Technology • Pravfund **State Media/State-Controlled Outlets** • RT • Sputnik • RIA Novosti • Izvestiya • Rossiskaya Gazeta • Rybar **Influence Operations Networks** • Doppelgänger

NGW Tactic	Selected Entities/Groups/Organizations
Airspace Incursions by Drones or Jets	**Long-Range ISR drones** • Orlan-10/Orlan-30 • Forpost/Forpost-R • Altius-RU **Combat/Strike-capable drones** • S-70 Okhotnik-B **Fighter/Interceptor Aircraft** • Su-27/Su-30SM • Su-35S • MiG-31 **Strike Aircraft** • Su-24M • Su-34 **Intelligence/Surveillance Aircraft** • Il-20/Il-22 • Tu-214R **Maritime Patrol/ASW** • Il-38 **Strategic Aviation** • Tu-95MS • Tu-160 **Helicopters** • Mi-8/Mi-17

NGW Tactic	Selected Entities/Groups/Organizations
Territorial Waters Violations and Targeting of Submarine Cables	**Intelligence, Seabed Reconnaissance, and Research Vessels** • Project 22010-class ships • Akademik Aleksandrov-class vessels • Project 22010 and Project 20180 • Russian Academy of Sciences-flagged vessels **Russian Ministry of Defense Vessels** • Belgorod (Project 09852) • Podmoskovye (Project 09787) • Losharik-linked vessels (AS-31) **Surface Combatants** • Admiral Grigorovich-class frigates • Steregushchiy-class corvettes • Buyan-M and Karakurt-class corvettes • Udaloy-class destroyers • Slava-class cruisers **Submarines** • Yasen-class (Project 885/885M) • Akula-class (Project 971) • Kilo (Project 636.3) **Auxiliary Vessels** • Tugboats (for example: Project 22890)
Offensive Cyber Operations	**GRU Units** • Unit 29155 (also involved in sabotage operations) • Unit 26165 (APT 28/Fancy Bear) • Unit 74455 (Sandworm) **SVR Units** • APT29/Cozy Bear

NGW Tactic	Selected Entities/Groups/Organizations
	FSB Units • Center 16 (Turla) • 18th Center of Information Security (Gamaredon Group)
Leveraging Economic Dependence	**Russian State Energy Companies** • Gazprom Export • Gazprom Neft • Rosneft • Transneft **Pipeline Infrastructure** • Nord Stream AG • Nord Stream 2 AG • Blue Stream • Yamal-Europe pipeline interests **Trading, Marketing, and Pricing Entities** • Gazprom Marketing & Trading • Rosneft Trading **Kremlin Oversight and Finance Bodies** • Russian Presidential Administration • Ministry of Energy • Gazprombank • VTB

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com