

Light Upon Obfuscation: Russia's Kinetic Grey War Against NATO and Its Implications for Global Hostilities

Christian Desira

Politics, Philosophy, and Economics

June, 2026

Faculty Adviser: Scott Radnitz, Ph.D.

Essay completed in partial fulfillment of the requirements for graduation with Global Honors,
University of Washington, Tacoma

Light Upon Obfuscation: Russia’s Kinetic Grey War Against NATO and Its Implications for Global Hostilities

Christian Desira
Politics, Philosophy, and Economics
June, 2026

Faculty Adviser: Scott Radnitz, Ph.D.

Essay completed in partial fulfillment of the requirements for graduation with Global Honors,
University of Washington, Tacoma

Approved:

DocuSigned by:

Scott Radnitz

AA1DCA2AB4CB459...

Faculty Adviser

6/16/2026

Date

DocuSigned by:

Dinya McMillin

261564B519C646F...

Associate Vice Chancellor, IIGE

6/23/2026

Date

Light Upon Obfuscation

Buildings burning, drones overhead, foreign military forces invading the territory of a sovereign nation. These are the textbook hallmarks of war. These actions are not merely isolated incidents but part of a coordinated campaign by a known actor. This instigator indeed is a nation-state already actively entrenched, not far away, in an offensive conventional war of imperialism, and regularly threatens to expand that war to their own soil. The targets of this campaign, the members of the North Atlantic Treaty Organization, have faced such aggression for years and yet, enigmatically, remain in official peace. The Russian Federation is helmed by a government that has openly challenged the sovereignty of European states within NATO. While words may only frighten, Russia has used forceful measures to demonstrate substance to these threats.

Indications are clear in the political and military realms that Russia is an obvious instigator of aggression in the grey zone, working to challenge the sovereignty of NATO members through modern methods. This campaign has serious indications and potential to serve as the prologue to an open conflict between NATO and Russia. Previously, such an intent was widely understood as preposterous, given NATO's deterrence policy of collective defense, further assured through nuclear weapons. However, overt and covert pressures originating from Russia have sought to test the alliance, with members along NATO's eastern flank placed under particular strain. There is little doubt that the current campaign is a trial to determine the veracity of NATO's collective defense policy and, accordingly, the structural integrity of the alliance.

Russia has employed a combination of information warfare and kinetic grey-zone activities in a campaign of physical coercion. These activities flirt with the threshold of war, at times even crossing lines clearly defined in international law. Countries that have fallen victim to this aggression are left with a grim dilemma of either initiating grand hostilities over infractions

that others may perceive as insufficient or continuing to endure Russian harassment. Russia has backed NATO into a corner, presenting the alliance with two choices: fatal concessions that would destroy the alliance and leave its members vulnerable to conquest, or the initiation of a potentially apocalyptic third world war.

This analysis will explore how the Russian Federation has successfully maneuvered around and exploited the modern, rules-based international order to wage an offensive kinetic war in the grey zone against NATO members in Europe. Preceding this evaluation will be an initial clarification of what defines kinetic grey-zone warfare and an explanation of why some powers choose this approach to advance their interests. Following that will be a review of Russia's incentives and goals for its grey zone campaign. Building on these concepts, an analysis of the current crisis will follow, trailed by an evaluation of potential countermeasures and responses against kinetic grey zone activities. Finally, the ways in which Russia's aggression against Europe has contributed to global hostilities will be assessed, as well as methods to confront it.

Background

The study of grey zone warfare has been a convoluted and imprecise exercise for roughly as long as it has been researched and analyzed. It is a noteworthy imperative that the establishment of a terminological consensus would be constructive for future discussion of this topic, enabling a more coherent, widely accessible, and constructive discussion. Incongruent language is a hindrance to the evaluation and explanation of these real world threats, as well as the circulation of those findings in both applied settings and among general audiences. Furthermore, the inconsistency and disjointedness with which this topic has been discussed have been a critical impediment to understanding and subsequently responding to grey zone threats.

Accordingly, in the interest of both rhetorical brevity and analytical efficiency, this document will follow a streamlined and utilitarian definition inspired by general themes across prominent analyses of the subject.

Definitions

Grey zone warfare refers to the use of measures, tools, or activities that would ordinarily be associated with conventional warfare, even when the conflict between the involved powers is not officially classified as such a war. Grey zone measures, as they will be referred to henceforth, are characterized by their covert, deniable, ambiguous, or otherwise indirect motive and/or attribution (Hughes 133-136). Due to their nature of application, victims are limited in how they can respond. The official and implicit attribution are usually different, but due to the assailant power not officially engaging in any sort of aggressive activity, it leaves the victim officially appearing as an aggressor if they respond directly. The aggressor may engage in additional measures, such as information warfare, to either further obfuscate or infer their involvement while remaining out of reach. This may make the victim government appear alarmist, paranoid, and untrustworthy, or ineffectual and weak, leaving them few or zero operations to effectively respond. This combination of grey zone measures can be understood as an operation. Grey zone operations provide more forceful means of advancing the interests of a power and/or its allies without officially engaging in hostilities, all while minimizing or negating consequences due to the obscure application.

Grey zone warfare finds utility in the space between political definitions of war and peace. In the general discourse of international relations, be it within societies amongst citizens or in large-scale political discourse, there is a shared understanding that nations exist within a binary paradigm of peace and war. There are numerous valid criticisms of understanding warfare

in such a binary manner, as many, if not most, nations do not exist entirely within one category or another (Ehrhart 269-270). This binary understanding, however, retains strong utility as a general means of indicating to countries on the international stage, as well as to citizens within those countries, the state of a conflict and the consequences of participation. It is generally understood by nations around the world that war is objectionable and that those who instigate such conflicts should be punished; this consensus is constructive for world peace. Almost every world government would agree that war is bad, and that is good.

Peace is generally understood as a state in which a power is not actively engaged in armed conflict. Powers, for the sake of this analysis, primarily refer to nation-states, but can also include ascendance oriented organized militant groups. This analysis will work with the understanding that war, henceforth regarded as “conventional war” in this analysis, are defined by the primary use of military forces in an operation or campaign to achieve partial or total victory against an adversarial power. The definition of what constitutes a conventional war is largely subjective and based on individual considerations of powers, but generally is officially acknowledged as such by at least one involved side. The First and Second World Wars are the most definitive modern examples of conventional wars. However, additional broader examples also include the Korean, Vietnam, Soviet-Afghan, the US-led War in Afghanistan, and Iraq wars, despite some being largely defined by counterinsurgency. As a result of various historical developments, the foremost of which being international law, it has been increasingly beneficial for powers to avoid openly declaring war when pursuing their interests. This is where the modern phenomenon of grey zone warfare emerged.

In grey zone warfare, powers may declare that they are only using measures associated with or appearing as war as just another means of achieving a goal, but they notably avoid or

downright reject the suggestion that they are engaging in one. Other characteristics of grey zone conflict are the overt denial of activities altogether, and instead attributing such activities to other powers or actors, typically regional. Conventional wars, particularly insurgencies can be fought by proxy through the assistance of select powers or other actors. Sometimes, a suspected involved power may gradually legitimize their involvement in the conflict over time under guises that categorize their involvement as something else other than active engagement in conflict. A power could claim evidence against them is fabricated, and a part of a slanderous campaign by the accuser or other party that may benefit. There are a wide variety of configurations for wars fought in the grey zone, but they can generally be identified as hazy, unofficial conflicts fought between two powers without the declaration of war. As an example, the Cold War can be understood as a protracted war in the grey zone between the United States and the Soviet Union.

Grey zone warfare is an umbrella term for other terms that refer to specific types, methods, or combinations of grey zone measures. The most relevant term in circulation on this topic has been hybrid warfare, which encompasses the broadest scope of gray zone warfare as it is used in this analysis. Emerging in the 2000s as a term to describe threats the United States posed to opponents in the Middle East, the term has since been adapted, twisted, warped, and politicized to loosely fit a variety of understandings and narratives (Sokov 6-9). Unfortunately, as a result of the term's overly ubiquitous use, it has largely been deprived of its analytical utility. As a theme, however, it is generally understood as a combination of civilian and military measures used against an opposing state, often targeting the civilian population specifically to undermine popular support, or the military in order to covertly weaken or provoke it. Both areas pressure powers through coercion. Grey zone warfare is characterized by the use of non-military means to advance policy objectives, particularly to undermine popular cohesion or political will,

thereby degrading the target's capacity to resist or respond. Grey zone warfare can be used as means to pressure another power to permit concessions or even seizures, with expanding operations capable of facilitating further losses on the victim. Depending on the situation, anything can be targeted for alteration, removal, or seizure by the aggressor power, including the victim's sovereign interests, assets, territory, or security forces. Theoretically, grey zone operations can be escalated to a point where the victim is left with no capability or other choice beyond partial or total capitulation to aggressor's pressures.

Military force is used on a small, precise scale, either to support activities or deliver a decisive blow. Common goals of grey zone operations are regime or policy change in the target government or country. An example of hybrid warfare is the use of civilian agents or assets against a target country, be that acting as agents of propaganda, disinformation, sabotage, disorder, or cyberwarfare. For a broader exploration of what constitutes grey zone warfare, refer to Geralt Hughes's article, "War in the Grey Zone," which is a work cited for this analysis.

Finally, the kinetic element. Kinetic grey zone warfare is simply a category of grey zone warfare that includes physically destructive or coercive measures. Kinetic grey zone warfare demands particular attention, as it represents a more treacherous category of escalation that poses concerning prospects for further, catastrophic escalation into conventional war. As a reminder, the verified culpability of a kinetic attack by one power against another is universally understood as a justified catalyst for conventional war. Despite this, kinetic actions are seen as useful by some powers as a means of advancing their own interests through the grey zone.

Kinetic actions such as sabotage are usually coordinated by the intelligence organs of an aggressor power, often manifesting as clandestine operations within or against the victim power, their sovereign domain. Intelligence agencies may also solicit the services of "third-country

nationals.” These are individuals who sympathize or are compelled to engage in activities against a target country without holding any formal allegiance to that country or the aggressor country. An example of this has been Russia’s employment of a “gig economy,” using social media to solicit individuals residing in NATO countries to engage in various hostile activities within that country (Edwards). This will be expanded on later on in this analysis.

This paper proceeds on the understanding that kinetic grey zone warfare comprises covert, ambiguous, or deniable activities used coercively or destructively by one power against another, usually between nation-states. Operations include a variety of civil and military means, allowing the aggressor to pursue policy goals more directly, mitigate their own punishment, control escalation, and keep the conflict below the threshold of conventional war. Finally, operations often mitigate or negate the target’s capacity to respond to and/or defend against aggression (Sokov 33).

Why Russia Chooses Grey Zone Warfare

The Russian perception of the international system is that it is balanced against itself and its interests. This conception has been influenced by a variety of events and circumstances. The most influential of these are specific historical events, a fundamental misunderstanding of why the Soviet Union lost the Cold War, and the belief that the US has been engaged in a hybrid war against Russia. Additionally Russia’s perceived intertwining interests and national security often conflicts with international legal principles of national sovereignty, which originated in the west.

Vladimir Putin has served as the President of the Russian Federation since 2000 (with a brief period as prime minister between 2008 and 2012). His regime can be characterized as a populist autocracy, capitalizing on grievances perceived by the Russian public and the desires of influential elites (Fish 61-63). One of the more fundamental sources of resentment in Russia has

been the belief that the United States and the West have created the international system to humiliate and weaken Russia. The government of Russia does not fully understand that Russia's position, as the successor state of the Soviet Union, is the result of that country's quantifiable losses in the Cold War across the board (Kotkin 6). Policy choices by the Soviet government further worsened Russia's inherited geopolitical and economic circumstances, such as its rejection of the post-World War II global financial system. The downfall of the Soviet Union was followed by a post-collapse period of economic and political chaos as the country tried to navigate unfamiliar economic and governance systems. This crisis was lengthened by problematic and broadly unsuccessful government reforms. (McFaul and Stoner-Weiss 69-70).

The perception that the international system is corrupt and driven by Western interests is a valid concern grounded in actual events. Namely, the U.S. invasions of Afghanistan and, particularly, Iraq without UN approval made the U.S. appear hypocritical (Toal 228). Furthermore, in 2008, the U.S. and Europe broke with a longstanding precedent regarding state recognition requirements by recognizing Kosovo, a breakaway region of Serbia and a Russian ally. The Russians subsequently recognized the breakaway regions of Abkhazia and South Ossetia in Georgia. While most of the world would ultimately recognize Kosovo's independence, most would not recognize that of the Georgian breakaway republics, including the United States. This apparent act of hypocrisy by the U.S. government was justified on the grounds that Kosovo was an exceptional case, while the Russian government argued that a new precedent had been established (Toal 155). This contributed to the growing consensus within the Russian government and public that the West's claimed sanctity of international law was also seen as hypocritical and as selectively applied in pursuit of its own policies. The Kosovo precedent would again be claimed with Russia's recognition of Donetsk and Luhansk in the Ukrainian

Donbas in 2014, which leads to the third reason for Russia's grey war: NATO expansion, particularly into Russia's "near abroad."

The Russian government has contested NATO's continued existence, viewing the alliance as a threat to Russian security and interests (Toal 30). While NATO is an officially defense-based alliance, a Russian history fraught with invasion from the West has informed an effective paranoia of amassments of Western military strength approximate to Russia. Indeed, Russia's geographical vulnerabilities, such as the absence of naturally defensible borders, leave Russia with a vast, open country exposed to invasion. The long, traditional response across the historical iterations of the Russian state has been a sort of aggressive, offensive defense, a legacy extending back to the Imperial Tsars (Kotkin 4). This state of geopolitical thinking is incompatible with the rules-based international order, contributing to Russian distrust of these institutions. As such, while Russia will still contribute to these organizations and abide by many of their rules to maintain its position and broader global stability, it feels justified in deviating to advance its own interests (McFaul and Stoner-Weiss; Kotkin; Toal). The most relevant of these interests is the maintenance of its historical sphere of influence, which it sees as necessary for national security, despite this coming at the evident expense of those countries' sovereignty.

Historically, including under the Putin administration, the countries most sacred to Russia's sphere are in the "near abroad," or today's former territories of the late Soviet Union (Toal). While this includes Ukraine, it also includes the three Baltic states of Latvia, Lithuania, and Estonia, which are members of NATO. Some assessments have excluded the Baltic states from the near abroad, but Russia has demonstrated a pattern of pressuring, coercing, and questioning these countries' sovereignty during its current grey zone campaign (Edwards, Seidenstein; Rekawek, Lanchès). As for Ukraine, Western support for its accession to NATO

and the EU crossed a Russian red line, despite Ukraine's voluntary choice of a more Western path (Putin). This ultimately led to Russia's increasingly direct involvement in Ukraine, first with the annexation of Crimea, then its intervention in the Donbas insurgency, and finally with the full-scale invasion in 2022.

NATO's support of Ukraine has been described by official sources within the Russian government as participation of NATO on Ukraine's behalf in a war against Russia, framing the war as a battle against the West for Russia's existence (Stanford, Faulconbridge). Russian government sources had, however, claimed for years before that the West was engaged in a hybrid war against Russia. The Russian government, along with government-owned media organizations, has long fought to control the narrative that similar Russian activities are merely those of defense, fall short of war, and are a direct result of Western operations threatening Russian security (Sokov; Dickson, Harding). They also shape the narrative around these operations, often denying involvement in deniable operations and/or claiming these activities would be justified if Russia were involved or if they are found to be involved. They will often claim that Western evidence proving Russian involvement is forged, and part of a wider campaign of "Russophobia" meant to further weaken Russia's reputation in the international system, particularly in their critical time of war.

For the Russian government, grey zone warfare is an option for using tools more easily accessible to Russia in order to affect countries' actions when Russia situationally lacks sufficient influence to effect such policy changes. Additionally, some have perceived such activities as desperate due to their apparent recklessness and implementation in contexts relevant to Russian national security or associated interests. Russian grey zone activities themselves provide Russia with the opportunity to still advance its interests without engaging in open conventional warfare

(Sokov). The most relevant historical campaigns that serve as examples of this Russian strategy are its grey zone campaigns in Georgia and Ukraine before 2022.

Russian strategy begins with high-level political overtures that, if they fail to generate the desired response or concessions, lead to the introduction of coercive measures in the grey zone within those countries to augment political pressure (Sokov). Activities can be carried out by a variety of actors. The general pattern is that Russian security services will involve what or whoever they can, as long as the Russian government can maintain deniability and control over escalation. Often, Russian security services will involve themselves directly, particularly in realms that don't require physical human presence, such as cyber warfare. These activities in the grey zone are meant to coerce the government, largely through fear, which can be stoked through the population of the target country as well as information warfare (Sokov; Ehrhart; Hughes). As time goes on, activities grow increasingly bold, dramatic, and destructive, while following a careful progression up the escalation ladder. Generally, small escalations will not warrant large-scale responses by the target government, as they are likely to be perceived as disproportionate and may lack sufficient support. However, the largest hurdle of all for a defending government's response is that Russian activities are inherently deniable and leave little or no room for clear attribution. This leaves strong potential for the victim to appear as an official aggressor depending on their response. This is a crucial inherent operational strength.

The introduction of kinetic activities is a particular threshold on the escalation ladder that usually signals a belief, likely within the Kremlin, that policy ends can no longer be achieved through political means. These operations become increasingly drastic, bold, and destructive, beginning with attacks on civilian infrastructure and escalating into targets of military value. Attacks on civilian infrastructure, for example, are meant to sow discord through fear and

disruption. The hope is that the country's population will inevitably compel the government to abandon a course of action Moscow finds undesirable (Sokov). As has been observed, escalation has included the successful initiation of insurgent rebellions in breakaway regions, evolving into civil wars, which eventually see involvement by Russian armed forces, though initially through non-declared means. While analysts were previously uncertain about Russia's willingness to escalate into a full-scale conventional war, the 2022 invasion of Ukraine demonstrates the current Russian government is willing and capable of making such a gamble.

Russia's Kinetic Grey Zone Warfare Against NATO

Russian activities in the grey zone against European countries have long been a feature of modern Russo-European relations, beginning in the 2000s and continuing throughout the 2010s. Tensions between NATO and Russia took a turn for the worse with the 2014 Russian annexation of Crimea. With the 2022 Russian invasion of Ukraine, European members of NATO saw a major rise in Russian grey zone activities, with frequency, intensity, and boldness of incidents increasing year-on-year.

These operations are conducted in a manner that limits victims' capacity to respond, either due to national legal shortcomings or to grey areas in international law. Existing international law precludes responses to grey zone activities, and national policies often further hinder responses from victim nations. It has been observed that Russian operations exploit these legal loopholes in ways tailored to the target countries. These Western countries, perhaps more than any others in the world, are constrained by domestic legal shortcomings that can impede effective responses to defend their national security. This leaves target countries with a choice “between their immediate border security and the values and rules that are the basis of liberal Western democracy.” (Ålander)

Russian kinetic operations represent a clear, bold provocation against NATO, which runs a considerable and serious risk of catalyzing a conventional war. While not all of the following measures are outright destructive in their own right, they are disruptive and facilitate other, more destructive operations by providing adequate operational conditions and intensifying the fallout.

The Digital Realm

Russia's cyber operations are doctrinally offensive and can be divided into two categories: information-technical and information-psychological (Dickson, Harding 4). The former includes cyberwarfare as traditionally understood in Western research: cyberattacks between states, often carried out by ambiguous third-party actors. Information-psychological is defined by the Military Encyclopedia of the Russian Defense Ministry as influencing "the enemy's information resources, the consciousness and feelings of their military personnel and population, as well as a set of measures to protect one's own information and psychological resources." (Dickson, Harding 5) This is what Western research would categorize as information warfare.

Before any exploration of Russian kinetic grey zone warfare, it is imperative to understand the importance of information warfare. This can come in multiple forms. In target countries, this can take the form of the propagation of rhetorical narratives through domestic media sources or the injection of these narratives into international media. Another method employed on a wide scale by Russia, particularly during active kinetic operations, is the oversaturation of information streams with false, misleading, or inconsistent information (Morley-Davies 2; Sokov 11). This can be used to cloud online discourse, precluding individuals from forming a clear picture of the crisis or dissuading them from trying to clarify. The use of AI and bots has increasingly automated this method, enabling the flooding of social media with

disinformation to confuse populations and governments, and slow responses (Roussi; Vicens). Information warfare is an enormous tool that enables operational environments and guides target populations through operations as activities unfold. Combinations of different sources of information can begin to build narratives and an illusion of popular support to justify attacking certain targets. A very recent example is the increasing claims that Ukraine is using a NATO base in Latvia to launch attack drones against Russia (Sytas, Laizans). Accordingly, this would make this base, owned by and located in the territory of NATO members, a valid military target for Russia. It would, additionally, support claims that NATO is playing an active military role in fighting Russia.

Such claims and their responses allow Russian decision-makers to do two main things. Firstly, test with various key populations and governments (in this case, those of local and prominent NATO allies, as well as those allied with Russia) to see whether they believe such claims and, if so, provide Russia with the operational environment to conduct such a strike. Secondly, they add to the mountain of claims Russia can use to justify future actions, including, but not limited to, attacking the site in question if a better operational environment presents itself.

“Information-technical” cyber warfare operations by Russia were also widespread prior to 2022 and have increased significantly since the invasion (McManus 26-41). As pioneers of cyberwarfare, Russian hacking operations involve a variety of actors: agents of the state security services, civilian actors, including “hacktivists,” and criminals. While hacking institutions within government have greater resources, organization, technological sophistication, and advanced knowledge, civilian hacking offers several valuable advantages in the grey zone. Civilian hacking resources can augment those within government, either by providing greater manpower

and technical resources or by offering enhanced flexibility due to their unique characteristics. Their foremost utility is, of course, plausible deniability (Dickson, Harding; McManus).

Russian hacking operations have been used across the board to target physical and digital resources, services, and infrastructure of military, civil, government, and business targets. They have been used to weaken or disable government services, medical services, transportation systems, military equipment, business infrastructure, and even media outlets (Ribeiro; Holm). Cyberattacks can take down defensive systems that enable or worsen kinetic attacks, disabling response systems that could mitigate or stop the attack, which further opens the door to disaster. These operations can prevent the government from responding to and stabilizing a crisis and obstruct political and media figures from doing so as well. Cyberattacks are a critical force multiplier, capable of turning ordinarily small incidents into massive catastrophes. Nations with highly digitized government infrastructure are vulnerable to having a nationwide shutdown of government services and media, leaving the country crippled with no understanding of what is happening. This exact kind of crisis took place in Estonia in 2007 (Kauschanski).

Sabotage & Crime

Russian security services have been able to capitalize on the massive and discrete networking of the internet to impose a campaign of covert sabotage against NATO. With successful political measures by these countries having largely mitigated physical activities by Russian intelligence personnel, the Russians have creatively hired hands through the internet via a “gig-economy.” Using web platforms such as TikTok and Telegram, Russia has recruited people with no formal ties to Russia to conduct reconnaissance and sabotage missions on its behalf (Ciesnik; Chersicla). Hired operatives often have little idea who their handlers are or why they are conducting these operations, but do so for payment (Rekawek, Lanchès). Equipment is

often simple, including rudimentary explosives and incendiary devices. Experience is also usually minimal, although it appears that Russia is trying to solicit more police officers, mercenaries, and paramilitary types as operatives to mitigate this shortcoming. These operatives were once thought to be single-use, but more recent analysis suggests that Russian security services are instead seeking to establish networks of operatives (Ciesnik). Tasks are often posited as challenges, offering enticing sums for simple tasks, and offering more money for bolder ones, often in local currency. Recruiting operations naturally target economically disadvantaged groups, which are therefore more vulnerable to falling into these schemes. Some operatives have a rudimentary understanding of the purpose of these operations and participate for ideological reasons. These, however, are most probably a minority of operatives. (Rekawek, Lanchès).

Operations have been conducted against a wide spectrum of targets. Primarily, European Central Infrastructure (ECI) has been the main target of these operations due to its high vulnerability, high importance, and the high cost and difficulty of defending from such attacks (Edwards, Seidenstein). Examples of this kind of infrastructure include energy, resource, communications, road, and rail infrastructure. These are targets of both civil and military value whose destruction would cause obvious destruction and disruption. ECI is typically around 40 years old, privately owned, and poorly defended, making them easy and vulnerable targets. Networks in which they are part also often lack redundant systems, enabling relatively large-scale disruption from relatively simple operations. Operations have also involved the use of ambiguously owned assets, such as the Russian shadow fleet, to conduct disruption operations. These have mainly been used for the destruction of undersea pipes and cables, as well as launch points for drones to invade NATO airspace (Chersicla). The latter method has been used to shut down airports by cluttering the airspace with small, difficult-to-intercept targets of ambiguous

origin. Additionally, these drones have been flown in a disruptive manner against military targets (Mykhailenko).

Other major civilian targets have been large, privately owned targets of significant economic or military value. These have included everything from shopping malls to weapons factories. The general objective of these operations is to achieve a substantial shock, such as the complete destruction of Poland's largest shopping mall, Marywilska 44, in May 2024 (Gera). Attacks against the defense industry have been widespread, primarily targeting crucial war-making material and factories that produce equipment sent to Ukraine during the war. In July, 2024, there was even a failed plot to assassinate the CEO of Rheinmetall, one of the largest and most important defense contractors (Edwards, Seidenstein 6).

Additionally, official military and government-owned facilities have been hit, including warehouses, bases, vehicles, and even personnel. These attacks have also primarily targeted equipment bound for Ukraine or facilities instrumental in transporting that aid. Many of these attacks have been purely provocative, however. There have been various incidents of military bases in NATO countries being targeted, and a recent incident involved the assault of German soldiers outside of a Dutch military base ("NATO-Soldaten attackiert").

Russian Military Involvement

The Russian military plays a careful, delicate, yet bold and reckless role in Russian grey zone warfare. The general theme of these intrusions are brazen activities used as a precise means of provocation. These activities are often used to test military response and governmental resolve, with these measures, above all else, putting the spotlight on the victim country and NATO on the international stage.

Under the guise of air defense operations, the Russian military has drastically increased jamming and spoofing activities of GPS and satellite communications. Additionally, military hacking operations have augmented communications sabotage, particularly through the hacking of satellites (Tkachuk 19-20). Communications jamming and spoofing not only target civilian and military operations alike but also disrupt navigation services, leaving aircraft and maritime vessels vulnerable to accidents. Incidents of jamming in the Baltic Sea, hundreds of miles away from Ukraine, have increased drastically over the last four years. Between 2023 and 2025, incidents increased from just 55 a year to over 733 (Walsh, Burrows).

Military exercises and flights in close proximity to the territory test responses and capabilities as tensions rise. NATO military forces are put on high alert as large concentrations of military forces operate in close proximity to alliance members' borders. This fear is compounded by concerns that such exercises naturally enhance the operational readiness of military forces and could be used as cover for an invasion. There have been various incidents of Russian military aircraft flying near NATO airspace without transponders or a flight plan, which, apart from being a violation of the International Civil Aviation Organization (of which Russia is a member), is also a provocative activity (Morse; "Russia Blocked from ICAO Council"). There have been notorious incidents of Russian aircraft getting dangerously close to oil wells, military vessels, and military aircraft belonging to NATO countries. One of the most dramatic of these incidents was when a US MQ-9 Reaper Drone was rammed by Russian Su-27 Fighters on March 14th, 2023 (Sabbagh).

Russia has violated international law and committed acts of war using its military through violations of airspace and sovereign borders. This has been a fairly recent development, but a dramatic one that has caused much controversy. On September 19, 2025, Russia flew three MiG-

31 Foxhound Interceptors through Estonian Airspace for 12 minutes (North Atlantic Council). They were intercepted by NATO fighters and repeatedly ignored demands to depart the airspace. The Kremlin responded to this incident by denying the accusation and claiming the aircraft were operating in international airspace. This act was a blatant violation of international law. Another incident, on December 17th of 2025, involved Russian border guards walking over the Estonian border and loitering for a period of 20 minutes before departing (Müller, Blackburn). These incidents are brazen violations of international law and Estonian sovereignty. NATO members have responded to these intrusions by threatening to use lethal force against future violations. Moscow has regarded these statements as “reckless” (“NATO Ready to Down Warplanes”).

Patterns of Escalation

Since the beginning of the war, incidents of grey zone activity have increased dramatically. From the 3 confirmed incidents in 2022, the number increased to 12 in 2023 and 34 in 2024. While there appeared to be a lull in the first half of 2025, the summer saw a major wave of activity, leading to a significant escalation in the crisis (Rekawek, Lanchès). As of February 2026, the number of confirmed incidents of Russian sabotage stands at 151. Information on incidents in 2026 is more limited due to delays in incident identification. As addressed by GLOBSEC, “many incidents only become public once investigations are concluded or when new evidence emerges that allows for confidently attributing responsibility to the Kremlin” (Rekawek, Lanchès). The current pace of activities based on year-to-year precedent and current activities as of this year suggests that 2026 will be one of, if not the biggest, year of Russian provocation since 2022.

Specific operations are often conducted at specific times and within bounds best understood as a ladder of escalation. As previously explained, operations gradually grow bolder

as the line is pushed forward, yet some clear lines remain uncrossed. Despite the discovery of some plots to do so, no Russian activities have directly resulted in any deaths, as of June 1st, 2026. This is likely because the perception of real, mortal losses resulting from these activities could drive a civil response toward a more drastic, undesired escalation against Russia (Ålander). This issue remains a volatile, unprovoked, unknown quantity.

The greatest challenge to this rule occurred just this week, when a Russian Geran-2 attack drone flew off course and crashed onto the roof of a Romanian apartment near the Ukrainian border, wounding two civilians. Attribution remains officially undetermined and will likely remain so. It is the author's opinion that this incident could very well have been intentional on Russia's part, as these drones are launched in waves, and Ukrainian GPS spoofing would most likely have caused more drones to divert similarly. Additionally, based on the currently available public information, the drone's approach course appears suspiciously intentional.

Operational Objectives

These operations have multiple goals. The most immediate aim is that they impose civil and physical costs on the provision of aid to Ukraine. Indeed, attack “distribution strongly suggests that support for Ukraine is the single most important factor shaping target selection.” (Rekawek, Lanchès) Russia seeks to share the burden of the war more broadly by punishing NATO countries for contributing to it, recognizing that their involvement is pivotal to Ukraine's continued resistance. In effect, this can be seen as Russia fighting the war in Ukraine beyond its borders. Limited, small-scale, destructive attacks in the grey zone are strategically inefficient in terms of the proportion destroyed relative to overall equipment sent, but they impose unexpected and undesired costs, testing resolve. NATO countries now have to consider their own personal

security more seriously before sending aid. The civil element is particularly fragile, and public opinions are arguably more malleable to acts that are categorically most similar to terrorism.

Furthermore, these activities test alliance cohesion by forcing alliance members to consider whether they will accept escalated tensions in exchange for properly responding to superficially minor infractions. Before 2022, there was a lack of political will to even acknowledge Russia as a security threat (Ålander). This campaign is not really treated as an overall campaign for various reasons, mainly regarding stability, and so individual incidents are treated incidentally. Therefore, victim countries must face the question of whether their allies will support them if they decide to respond to infractions in a manner perceived as escalatory, potentially putting the security or interests of other alliance members in jeopardy.

A further incentive of this grey zone campaign is to establish networks and discover vulnerabilities that could be exploited in a limited or conventional open war. While this can be perceived as counterintuitive, as striking vulnerable areas can prompt strengthening in those areas, the fact is that NATO countries are not responding in this way on a large enough scale. Vulnerabilities discovered in one country do not guarantee innovation in similar industries, even across a country, much less across regions or, indeed, the European continent. The continuation of similar attacks in the same NATO countries and regions over the years demonstrates a relatively lackadaisical pattern of effective responses to vulnerabilities. Furthermore, these operations allow Russia to develop methods and strategies that could be employed in an open conflict. They do indeed serve, particularly in the short term, to degrade the capabilities of the European defense industry, which is naturally a major vulnerability for both target countries and those reliant on defense exports from them.

Responses and Countermeasures

The point has likely passed at which the current regime in Russia can be negotiated with to fundamentally change its own perspective within the international system to a position that is mutually acceptable. It is unlikely that Russia and NATO, as they currently exist, would be able to successfully negotiate a full de-escalation of this conflict back to a peaceful standing. The ideological and worldview differences appear as simply too critical to overcome. At this point, Russia appears to be interested only in concessions on NATO's behalf as it pursues grand strategic positioning and its realization as a geopolitical superpower. Consequently, it is imperative that NATO prepare for further Russian hostilities, as until Russia has exhausted their offensive energy or reached a satisfactory point for their interests, Russia will not stop pushing.

Societies are being penetrated and stoked into states of fear and confusion that are being used to the detriment of national security. What is necessary is a whole-of-society approach to national defense that begins with developing a common understanding. A common language that provides consolidated, tangible concepts and terminology in widespread information campaigns. Authoritative sources that repeat the same, clear facts in times of crisis can be relied on by populations. As a sidebar, in the interest of developing and preserving civil trust in government, such sources should be used carefully and in an unpoliticized manner only for national security issues. In the wake of the 2018 Salisbury Poisoning in the UK by Russian agents, the United Kingdom successfully controlled the narrative war against Russia. Key lessons included the initial, clear attribution against Russia and a sustained, consistent, authoritative information campaign against Russia (Stewart). Partnerships among the military, government, and civil society that work together to educate populations and institutions about the nature of threats and how to spot them are imperative. Many Nordic and Baltic countries have made extensive use of such societal partnerships, and they have proven to be robust defenses, leading to a lower-than-

average rate of covert activities by Russia (Ålander; Rekawek, Lanchès; “Lessons from Estonia’s Approach”). Any resilient defense against Russian covert activities should begin with a common language, from government down to the people, and across national borders.

Furthermore, passive and reactive defensive posture against these threats leaves defending parties forever submissive in the escalation space. As long as Russia continues to dominate the offensive threat environment, it will escalate the situation further and further until defending actors are inevitably unable to mount effective, adequate resistance and are forced to concede. It is apparent and necessary that NATO adapt its approach beyond a benign defensive posture to this aggression, as continuation of current practices will inevitably result in a slow, disintegrating, and devastating defeat. It is imperative that European members of NATO change their footing to one that is adequately and appropriately postured against the threats that they face. If there was ever a time to engage in a faithful rearmament, it would be now.

While the current threat environment may leave some industrial and infrastructure developers questioning whether they could be victims and whether investment in defenses is necessary, the crisis is only escalating. Developments must expand and be built robustly to face threats that have been evidenced elsewhere. Investments in decentralized, effective, redundant defenses should be prioritized across the physical and cyber realms. Estonia, a country with a highly digitized society, faced a catastrophic cyberattack in 2007 that disabled government and internet services for up to three weeks (Rain; Kauschanski). This event was pivotal to Estonia’s subsequent development and expansion of its cyber-based infrastructure, after which it remained on the same course of digitization while building resilient cyber infrastructure. Key developments that have proven their utility against continued Russian cyber attacks include independent cyber forces, resilient cyber infrastructure development, and education and

collaboration efforts across the whole of society (Kauschanski; “Lessons from Estonia’s Approach”). With the rise of AI in augmenting offensive cyber capabilities, cyber security professionals have a new tool for augmenting cyber defenses (Microsoft). Another significant factor in success has been the establishment of the aforementioned dedicated cyber forces. These see tremendous investment and enjoy close cooperation with the relevant civilian industry to enhance resources and flexibility. As European societies and governments grow increasingly digitized, lessons of Estonian development should be heeded.

Ukraine, too, has developed durable cyber defenses that have proven quite effective, even during full-scale war. From 2014, they faced a large and increasing cyber campaign by Russia, to which they responded by reaching conclusions similar to Estonia's. Ukraine also offers Europe other lessons for efficient and robust defense against Russia. While a whole-of-society approach that sees civil, government, and military collaboration in defending against covert activities such as sabotage would be beneficial, the kinetic defense space would also benefit from Ukrainian lessons.

With the increasing employment of drones as low-cost tools of attack and provocation, a key problem to countering such intrusions has been the cost exchange problem. In short, the cost-exchange problem is that it costs a defender more to intercept the threat than it costs the belligerent to attack. Just one example has been NATO’s frequent use of the AIM-120 AMRAAM air-to-air missile, which costs roughly \$1 million per unit, to intercept Russian drones invading NATO airspace. These drones cost, on average, between \$10,000 and \$50,000 (“Missile Interceptors by Cost”; “Catch Me If You Can”; Arranz et al.). The suboptimal employment of these weapons has been a result of insufficient inventories of cost-effective drone interception tools. Unfortunately, their continued employment depletes valuable weapons needed

for other purposes, namely for potential use against more expensive and capable aircraft, like manned military aircraft. Additionally, the stockpiles and manufacturing times and scales of these weapons do not compare with even remote favorability to their drone counterparts. Thus, it is inherently unsustainable to use them to defend oneself. In Ukraine, since the start of the war, they have faced the cruel dilemma of whether it is more effective at scale to try and intercept drones versus just letting them impact, obviously threatening a destructive and human cost. Ukraine has faced this quandary by developing very low-cost interceptor drones, which cost even less than the targets they are launched at (one Ukrainian Sting Interceptor drone costs roughly \$1,000) (Zhyhinas, et al.). It would be in NATO's interest to invest heavily in purchasing these or similar weapons and in developing associated production. This would both directly bolster NATO's defenses, as well as Ukraine's, whose continued involvement in the war against Russia further degrades Russia's capabilities to engage in aggression in Europe. This initiative could indeed be used to alleviate Ukraine's war debt to potential NATO clients. Such a partnership would also help enhance Ukraine's waning public image among European publics, who face an emerging sentiment that the cost of sending aid to Ukraine is not sufficiently justified.

Beyond Ukraine are other emerging or existing technologies that can be used as low-cost interceptor munitions. Ukraine has made fervent use of laser-guided rockets, which can be purchased from the United States (the Advanced Precision Kill Weapon System II), or from Belgium, a European NATO member (the FZ 275). Such weapons cost roughly \$10,000 to \$35,000 (Finnerty; Jeffs). As a final note, directed-energy weapons (lasers) are an emerging technology that could prove a very cost-effective solution for intercepting drones, though bring their own with their own logistical shortcomings. They are, nonetheless, tremendously cost

effective, with the British DragonFire system having had its development fast-tracked and claims to be able to down drones for £10 (\$13) per shot (Ministry of Defence).

When it comes to developing efficient solutions to address threats posed by Russia, the emphasis should be placed not only on more cost-effective weapons, but also on sustainable development. The fact is that the likelihood of a direct conflict between NATO and Russia is not out of the question, and there is a very real chance that Russian grey zone operations could be paving the way for such a conflict. Rearmament is a necessary priority. The United States has proven, particularly during the time it took to research this analysis, to, at best, be a potentially unreliable defense partner. As a result, it would be in the interest of European NATO members to look to their domestic defense industries to address current and potential Russian threats. This aligns with the broader theme that industries must see a flexible, resilient, sustainable, and reliable development to maximize their effectiveness, rigidity, and utility.

Another axis of utility could be a deeper partnership between NATO and the European Union. The European Union wielded significant influential political and economic power and has already proven versatile in countering hybrid warfare. Finland, when facing hybrid threats, has often turned to EU mechanisms to counter them effectively rather than to NATO. Additionally, “as a political union, the EU can in some cases be more suitable for escalation management purposes than NATO can as a military alliance” (Ålander)

Finally, NATO should revise its policies to more effectively counter and deter Russia's grey zone threats. A balance needs to be struck between policies that are effective and that can't be exploited to form an escalation trap, where such a policy's actions would prompt Russia to meaningfully escalate as well. While potentially posing risks, the firm line of international and

domestic laws regarding sovereignty and acts of war must be inflexibly adhered to above all.

NATO must stand by the system for which it stands, represents, and defends.

NATO has recently fallen short of this by allowing Russian MiG-31s to invade Estonian airspace for a dozen, unmolested minutes. Discussions in the wake of the incident led to Russia claiming that shooting down any of their aircraft would be an act of war. However, NATO has successfully downed a Russian aircraft without causing a major escalation. On November 24th, 2015, after a series of provocations of Turkish Airspace, the Turkish Air Force downed a Russian Su-24 Bomber after it had invaded Turkish airspace for a span of merely 17 seconds. This incident was immediately mitigated by successful diplomatic efforts (Rainsford; Bradsher). Russian airspace provocations of Turkey reduced considerably after this fact. While circumstances and tensions are different, it is reasonable to believe that NATO could successfully conduct a lethal interception of an invading aircraft, especially if it could control the narrative afterward. Accordingly, it would be advisable to have actionable plans in place that could be employed at a moment's notice to widely publicize a consistent story, domestically and internationally, to immediately gain control of the narrative if such an incident occurred. Such contingencies must not be limited to airspace violations. Any other violations of national sovereignty should be readily handled openly, appropriately, and swiftly, and this includes kinetic responses. The world must understand the gravity of Russia's infringement in clear terms so as not to let it get away with it. Successful deterrence of this kind shows democracy is not an exploitable, weak, paper tiger, as has been a growing sentiment world wide. Indeed, successful defensive actions can serve to encourage democratic states worldwide to stand against grey zone aggression.

Global Implications of the Current Crisis

It is blatantly clear to NATO adversaries and the world at large that NATO has thus far employed no means to effectively deter Russian grey zone operations; the conflict's escalation into the kinetic realm reflects this fact. This sets a dangerous precedent for current and potential international conflicts of interest. Poor responses and failed deterrence are practical enablers for the widespread application of the grey zone toolbox worldwide, with kinetic tools being the most dangerous and volatile of tools.

Violence contributes to the continuation and escalation of violence. Regional, national, civil, and ethnic tensions have been heightened as a result of this conflict, which has been inflamed by and arguably a large result of the Russian information warfare operations (Morley-Davies). This intensifies the broader issue, as hostile rhetoric can drive other parties to adopt a responsive tone, ultimately creating a self-generating cycle of escalation. Responses in the spaces of rhetorical discourse can be perceived as threatening by any of the parties involved, often resulting in political, economic, or military escalation. This has been an evident pattern throughout the escalation cycle between NATO and Russia. Military shows of force can prompt parties to escalate with their own responsive provocations as a means of deterrence. Without successful intervention, tensions can deteriorate into an escalatory spiral and eventually armed hostilities.

Internationally, Russia's allies could expect support for their own escalation of tensions, as their opponents are usually those aligned with the West and/or NATO and therefore their defeat is often in line with Russian interests. Russian government rhetoric has made clear that it seeks an alternative to Western-led international political, economic, and financial systems. In particular, the apparent Western dominance of financial systems has been used as a powerful hedge against Russia and other countries worldwide that have faced similar sanctions. Such

institutions include the United Nations, the International Criminal Court, the International Monetary Fund, the World Bank, the World Trade Organization, and the G7, among others.

Russian narratives have asserted that the West has used these institutions to coerce nations into adopting policies aligned with Western interests, often at the expense of those countries, thereby enabling the West's exploitation (Ingber).

Through the international economic organization BRICS, a union of diplomatically neutral or non-Western-aligned countries, the Russian state has sought its desired alternative. It is a concern in the West that, through BRICS, Russia may garner support for alternatives to Western-led economic and financial systems. A key obstacle preventing states around the world from engaging in any type of hostilities, whether grey zone or conventional, is the potential backlash and suffering they may face from the international system. Removing this obstacle would be a major blow to world peace and to the capacity of these status quo global institutions, which have arguably contributed positively to world peace and stability. Countries that defy international law could find their economic and financial lifelines outside the current international system, thereby threatening the globally stabilizing forces these institutions facilitate through sensitive global ties. Potential agitators could avoid much, if not most, of the effective pressure imposed by global economic, diplomatic, and financial institutions that make up the current global order and ensure global stability. Finally, if an alternative global economic system arose to compete with that of our current status quo, competing interests between the two systems could very well bring opportunities for further conflicts.

Beyond concerns of providing a safer space to conduct physically coercive activities, Russian operations against NATO have further innovated and developed the craft of grey zone warfare, in tandem with large scale, capable warmaking on the cheap. As a result of Western

isolation of Russia from conventional diplomatic, economic, and financial spaces, as previously evaluated, Russia has increasingly developed its measures in areas independent of Western pressures. This is a concern for global stability, as it makes grey zone warfare more readily available to potential agitator states worldwide. For example, the aforementioned gig-economy approach, advanced by Russian covert operations, has been a remarkably successful means of developing intelligence and sabotage networks cheaply and discreetly. Drones are another method of cheap and deniable provocations and attacks. Russian developments in grey zone warfare, particularly knowledge, can be easily spread either digitally or through advisors.

With a key incentive for grey zone operations being their low cost, Russian efforts have no doubt closed that cost gap even further. Developments have almost certainly streamlined operations, enhancing discretion and effectiveness, and presumably enhancing scaling. Exports would boost the Russian economy during wartime, right when it's needed most. Countries that may value access to tools to advance their own interests may too have resources that Russia finds valuable, namely natural resources. This too would serve as quite useful for Russia's war effort.

Overall, years of Russian kinetic grey zone operations against NATO have most likely generated more effective and accessible capabilities and knowledge for other potential agitators around the world to conduct their own. The potential proliferation of these capabilities and knowledge is inherently destabilizing. In tandem with provisions for an alternative global system that potential agitators may be able to look to for support, Russian experience in grey zone activities against NATO is one clear potential threat to world stability.

Options for Responses

The broadest way to address grey zone warfare is through policy decisions. This could take the form of both multilateral partnerships and changes in international law. With most major

powers, including the five permanent members of the UN Security Council, all participating in their own campaigns of grey zone warfare, changes to international law would not come easily. Additionally, smaller, weaker countries benefit the most from international law, something Russia has taken full advantage of (Ålander). Measures that would add to or modify existing laws to close legal loopholes are likely to face strong resistance. Changes will require sustained effort, likely within the respective countries that hold VETO power. Accordingly, it may be most fruitful, at least in the short term, for individual nations to pursue more personalized initiatives to ensure their security against war in the grey zone.

Regional partnerships or alliances with major powers will likely remain the most effective means of ensuring national security for individual countries. These relationships might consist of regional partnerships between countries with common interests, and/or ties with more powerful or influential governments. These partnerships could broaden the burden a potential attacker faces, serving as a natural deterrent, so long as the alliance is perceived externally as sufficiently resolute. Furthermore, these partnerships could serve to further collective policy interests, both actively and passively. Collaborations with intelligence sharing are one example. Another example would be technology sharing, particularly with powers with major industrial capabilities, which could yield defensive measures tailored to respective threats.

Broadly, there are trends that most countries should recognize as increasingly relevant to maintaining a resilient defense. Independent cyber forces have emerged among defenders of real, modern threats as a vital asset for facing threats in a modern world. Cyber forces defend against threats that can enable or enhance the effectiveness of kinetic attacks, which are also expected to reemerge. The most prolific rising kinetic threat as observed both in Europe and other conflicts worldwide is the onset of drones, observed at a wide scale in the Iran war and the 2025 India-

Pakistan Conflict (Nadimi; Azad). Cost-effective weapons to counter drones are key, so long as they are developed in flexible, upgradable ways to adapt to current threats. Broadly speaking, as the global fire rises, investments in national defense are advisable.

On the home front, governments should facilitate increasing cooperation between civil society, populations, and the military to build broader, whole-of-society barriers to grey zone threats. These may be among the few effective defenses against such an elusive, maneuverable, and discreet threat. As for infrastructure, both the cyber and physical worlds must see intelligent, robust development. In a chaotic, dynamic global threat environment, one should not wait for a sufficient threat to emerge before investing in such developments, since they take years to cultivate. The world must be ready to face a bold new threat environment characterized by aggressive measures tailored to the existing facets and structures of the world as we know it today.

As for NATO, its developments in these fields could very well generate lessons and products that can be proliferated to the broader world. Europe has the opportunity to lead the way in countering future threats, whose monetization could further bolster NATO's defenses against Russia.

Conclusion

The regime of Vladimir Putin's Russia seeks to subvert the international system and rebuild a Russian Empire in the 21st century. The Russian state has invested in a decades-long effort to carve a new foothold into the world for the glory of Russia, at the expense of the old world it felt damned it to squalor. Russia's offensive hostilities in Europe demonstrate a violent resolve to advance these national interests, setting an example for countries worldwide who may desire an end to their perceived destitution. The North Atlantic Treaty Organization must face

the wrath and strain of a vengeful imperial power seeking to carve a new world order out of the status quo.

The European members of NATO have an opportunity to demonstrate to the world a course of action tailored to address these threats. By cooperating with knowledgeable and capable partners and members, NATO can leverage its relevant resources to develop a new doctrine to address aggression made in the grey zone between peace and war. This begins with a common language to address these threats, and the discourse of war in the gray zone should no longer be burdened by overly complex, competing definitions that preclude understanding. Governments must play a pivotal part in unifying whole countries through partnerships with, itself, the public, civil society, business, industry, and the military. Rearmament is paramount. Sustainable development in the real and digital worlds can serve as robust, tangible defenses against instigating threats. Militaries must be equipped to fight wars of modern coercion and be prepared to meet national defense needs if a conventional war arises. Plans must be developed to handle unexpected crises at a moment's notice. Most sacred to the stability of the NATO alliance is upholding alliance boundaries and preparing to stand strong when those limits are tested. All peoples of all nations of the whole alliance must understand and be ready to face the evasive and aggressive threat environment of the modern world. NATO members have the opportunity to develop new formulas to share with the world in the interest of maintaining the security of nations worldwide. Steadfast, effective efforts may well deter countless conflicts, and NATO has a responsibility to lead the way in shaping the future of global security.

Works Cited

- Ålander, Minna. "Death by a Thousand Paper Cuts: Lessons from the Nordic-Baltic Region on Countering Russian Gray Zone Aggression." Carnegie Endowment for International Peace, 14 Nov. 2024, carnegieendowment.org/research/2024/11/russia-gray-zone-aggression-baltic-nordic.
- Arranz, Adolfo, et al. "Cheap Drones Are Reshaping the War in the Sky." Reuters Graphics, 17 Mar. 2026, www.reuters.com/graphics/IRAN-CRISIS/DRONES/dwpkyamxqpm/.
- Azad, Tahir Mahmood. "The Strategic Use of Drones in Pakistan–India Irregular Warfare." Irregular Warfare Initiative, 17 Mar. 2026, irregularwarfare.org/articles/india-pakistan-drone-warfare/.
- Bradsher, Keith. "Turkey and Russia Clash After Jet Is Shot Down." The New York Times, 26 Nov. 2015, www.nytimes.com/2015/11/26/world/europe/turkey-russia-fighter-jet.html.
- Burrows, Emma. "What to Know About Russia's GPS Jamming of a European Official's Plane." PBS NewsHour, 2 Sept. 2025, www.pbs.org/newshour/world/what-to-know-about-russias-gps-jamming-of-a-european-officials-plane.
- Chersicla, Rick. "Sabotage as a 'New Normal.'" Irregular Warfare Initiative, 19 Nov. 2025, irregularwarfare.org/articles/sabotage-as-a-new-normal/.
- Ciesnik, Sonya. "Disposable Spies: Poland Records Unprecedented Number of Russian Espionage Cases." France 24, 9 May 2026, www.france24.com/en/europe/20260509-disposable-spies-poland-records-unprecedented-number-of-russian-espionage-cases.

“Deutsche NATO-Soldaten in den Niederlanden attackiert.” Der Spiegel, 13 May 2026, www.spiegel.de/politik/deutschland/deutsche-nato-soldaten-in-den-niederlanden-attackiert-a-b81fe411-1dcb-4d5a-90dc-5b037ad1926e.

Dickson, Julia, and Emily Harding. Evaluating Russia's Cyber Strategy: A Playbook for Winning the Cyber War. Center for Strategic and International Studies, Sept. 2025, csis-website-prod.s3.amazonaws.com/s3fs-public/2025-09/250903_Dickson_Playbook_Russia.pdf.

Edwards, Charlie, and Nate Seidenstein. The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure. International Institute for Strategic Studies, 19 Aug. 2025, www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations-against-europes-critical-infrastructure.pdf.

Ehrhart, Hans-Georg. “Postmodern Warfare and the Blurred Boundaries Between War and Peace.” Defence & Security Analysis, vol. 33, no. 3, 2017, pp. 263–75. Taylor & Francis, doi:10.1080/14751798.2017.1351156.

Faulconbridge, Guy. “Russian Official Warns Europe to Brace for More Drone Incidents After Romania Episode.” Reuters, 29 May 2026, www.reuters.com/world/europe/russian-official-warns-europe-brace-more-drone-incidents-after-romania-episode-2026-05-29/.

Finnerty, Ryan. “US Military Commits \$1.7bn for BAE's APKWS II Rockets to Counter Drone Threats.” FlightGlobal, 29 Aug. 2025, www.flightglobal.com/military-uavs/2025/08/us-military-commits-1-7bn-for-baes-apkws-ii-rockets-to-counter-drone-threats/.

Fish, M. Steven. "The Kremlin Emboldened: What Is Putinism?" *Journal of Democracy*, vol. 28, no. 4, Oct. 2017, pp. 61–63. Johns Hopkins UP, doi:10.1353/jod.2017.0066.

FP Analytics. "Lessons from Estonia's Whole-of-Society Approach to Cyber Defense." *Digital Front Lines*, 31 Aug. 2023, digitalfrontlines.io/2023/08/31/lessons-from-estonias-whole-of-society-approach-to-cyber-defense/.

Gera, Vanessa. "Poland Blames Russian Intelligence for Warsaw Shopping Center Arson Attack." *Associated Press*, 11 May 2025, apnews.com/article/poland-russia-420187f5755036f6f61c65122c11348f.

Holm, Petra. "Estonia's Cyber Security Model for Europe." *e-Estonia, Enterprise Estonia*, e-estonia.com/estonias-cyber-security-model-for-europe/.

Hughes, Geraint. "War in the Grey Zone: Historical Reflections and Contemporary Implications." *Survival*, vol. 62, no. 3, 2020, pp. 131–58. Taylor & Francis, doi:10.1080/00396338.2020.1763618.

Ingber, Sasha. "Report: Russia Exploits Western Legal Systems, Institutions to Its Advantage." *KUOW*, 12 June 2019, www.kuow.org/stories/report-russia-exploits-western-legal-systems-institutions-to-its-advantage.

Jeffs, Adam. "Thales Develops \$10K Laser-Guided C-UAS Rocket for Ukraine." *C-UAS Hub*, 7 Oct. 2025, cuashub.com/en/content/thales-develops-10k-laser-guided-c-uas-rocket-for-ukraine/.

Kauschanski, Alexander. "How Estonia Became the Front Line for Global Cyber War Defense." *Worldcrunch*, 26 Oct. 2025, worldcrunch.com/world-affairs/how-estonia-became-the-front-line-for-global-cyber-war-defense/.

Kotkin, Stephen. "Russia's Perpetual Geopolitics: Putin Returns to the Historical Pattern." *Foreign Affairs*, vol. 95, no. 3, May–June 2016, pp. 1–9,

www.foreignaffairs.com/articles/ukraine/2016-04-18/russias-perpetual-geopolitics.

McFaul, Michael, and Kathryn Stoner-Weiss. "The Myth of the Authoritarian Model: How Putin's Crackdown Holds Russia Back." *Foreign Affairs*, vol. 87, no. 1, Jan.–Feb. 2008, pp. 68–80, 82–84. Council on Foreign Relations, www.jstor.org/stable/20020268.

McManus, Michael. *Catching Sandworm: How Russia Wages Cyberwarfare Against Ukraine and NATO*. Henry Jackson Society, Jan. 2026, henryjacksonsociety.org/wp-content/uploads/2026/01/HJS-Catching-Sandworm-%E2%80%93Russia-Report.pdf.

Microsoft. *Microsoft Digital Defense Report 2025*. Microsoft, 2025, www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025.

Ministry of Defence. "Boost for Armed Forces as New Laser Weapon Takes Down High-Speed Drones." GOV.UK, 20 Nov. 2025, www.gov.uk/government/news/boost-for-armed-forces-as-new-laser-weapon-takes-down-high-speed-drones.

"Missile Interceptors by Cost." Missile Defense Advocacy Alliance, www.missiledefenseadvocacy.org/missile-defense-systems/missile-interceptors-by-cost/.

Morley-Davies, Joe. "Deterring Kremlin Grey Zone Aggression Against NATO." Royal United Services Institute (RUSI), 29 Aug. 2025, www.rusi.org/explore-our-research/publications/commentary/deterring-kremlin-grey-zone-aggression-against-nato.

Morse, Jasper Hufschmidt. "Russia's 'Catch Me If You Can' over the Baltic Sea."

Australian Institute of International Affairs, 26 Apr. 2024,

www.internationalaffairs.org.au/australianoutlook/russias-catch-me-if-you-can-over-the-baltic-sea/.

Müller, Franziska, and Gavin Blackburn. “Russian Border Guards Briefly Cross into Estonian Territory, Foreign Ministry Says.” Euronews, 18 Dec. 2025, www.euronews.com/2025/12/18/russian-border-guards-briefly-cross-into-estonian-territory-foreign-ministry-says.

Mykhailenko, Dariia. “Sweden Faces Heightened Risks as Russian Threat Intensifies, Security Service Says.” UNITED24 Media, 18 Mar. 2026, united24media.com/latest-news/sweden-faces-heightened-risks-as-russian-threat-intensifies-security-service-says-16996.

Nadimi, Farzin. “Iran’s Drone Strategy (Part 1): Wartime Performance and Adaptations.” The Washington Institute for Near East Policy, 22 May 2026, www.washingtoninstitute.org/policy-analysis/irans-drone-strategy-part-1-wartime-performance-and-adaptations.

North Atlantic Council. “Statement by the North Atlantic Council on Recent Airspace Violations by Russia.” North Atlantic Treaty Organization, 23 Sept. 2025, www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/09/23/statement-by-the-north-atlantic-council-on-recent-airspace-violations-by-russia.

Ottis, Rain. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. NATO Cooperative Cyber Defence Centre of Excellence, 2008, ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

Pifer, Steven. "Russia, Ukraine and Existential War." Center for International Security and Cooperation, Stanford University, 2023, cisac.fsi.stanford.edu/news/russia-ukraine-and-existential-war.

Putin, Vladimir. "Address by the President of the Russian Federation on Conducting a Special Military Operation." President of Russia, 24 Feb. 2022, en.kremlin.ru/events/president/news/67843.

Rainsford, Sarah. "Russia Sends Clear Message to Turkey: Don't Try It Again." BBC News, 25 Nov. 2015, www.bbc.com/news/world-europe-34925823.

Rekawek, Kacper, and Julian Lanchès. "Update: Russia's Crime-Terror Nexus: Hybrid Warfare in Europe." GLOBSEC, 2025, www.globsec.org/publication/update-russia-crime-terror-nexus-hybrid-warfare-europe.

Ribeiro, Anna. "Poland Faces Record Wave of Russian Cyber Sabotage, Sets €1 Billion Defense Budget." Industrial Cyber, 17 Sept. 2025, industrialcyber.co/critical-infrastructure/poland-faces-record-wave-of-russian-cyber-sabotage-sets-e1-billion-defense-budget/.

"Russia Blocked from ICAO Council." Ministry of Transport and Communications (Lithuania), 30 Sept. 2025, sumin.lrv.lt/en/news/russia-blocked-from-icao-council-RBDg/.

"Russia's 'Catch Me If You Can' Over the Baltic Sea." Kyiv Post, Post No. 46692, www.kyivpost.com/post/46692.

Roussi, Antoaneta. "Russia Uses AI to Hack Europe, Dutch Intelligence Warns." POLITICO Europe, 21 Apr. 2026, www.politico.eu/article/russia-uses-ai-hack-eu-europe-dutch-intelligence-warns/.

Sabbagh, Dan, Martin Belam, and Julian Borger. “US Releases Footage of Russian Jet Crashing into American Drone over Black Sea.” *The Guardian*, 16 Mar. 2023, www.theguardian.com/us-news/2023/mar/16/us-releases-footage-russian-jet-crashing-into-american-drone-over-black-sea.

Sokov, Nikolai. Russian Hybrid (New Generation) Warfare in the Time of a Systemic Political-Military Transition. Occasional Paper no. 65, James Martin Center for Nonproliferation Studies, Sept. 2025, nonproliferation.org/wp-content/uploads/2025/09/OP65-Russian-hybrid-warfare-occasional-paper-2025.pdf.

Stewart, Joshua. “The Grey Orchestra: Elastic Communication and the UK’s Response to Salisbury.” *The RUSI Journal*, vol. 167, no. 2, 2022, pp. 38–49, doi:10.1080/03071847.2022.2075117.

Sytas, Andrius, and Janis Laizans. “NATO Jet Shoots Down Drone in Estonia After Airspace Incursion, Delfi Reports.” *Reuters*, 19 May 2026, www.reuters.com/business/aerospace-defense/nato-jet-shoots-down-drone-estonia-news-website-delfi-reports-2026-05-19/.

Tkachuk, Nataliya. “Ukraine as the Frontline of European Cyber Defence: Building Resilience in the Face of Russian Cyber Aggression.” NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 5 Aug. 2025, ccdcoe.org/news/2025/new-tallinn-paper-analysis-russian-cyber-aggression-and-proposes-ways-to-strengthen-europes-cyber-defence/.

Toal, Gerard. *Near Abroad: Putin, the West and the Contest over Ukraine and the Caucasus*. Oxford UP, 2017.

Vicens, AJ. “Russian Defense Firms Targeted by Hackers Using AI, Other Tactics.”

Reuters, 19 Dec. 2025, www.reuters.com/world/europe/russian-defense-firms-targeted-by-hackers-using-ai-other-tactics-2025-12-19/.

Walsh, Aiofe. “Sweden Accuses Russia of GPS Jamming over Baltic Sea.” BBC News, 4 Sept. 2025, www.bbc.com/news/articles/clyx3ly54veo.

“Western Diplomats Warned Russia That NATO Ready to Down Warplanes Breaching Airspace.” The Moscow Times, 26 Sept. 2025, www.themoscowtimes.com/2025/09/26/western-diplomats-warned-russia-that-nato-ready-to-down-warplanes-breaching-airspace-bloomberg-a90632.

Zhyhinas, Dmytro, Derek Gatopoulos, and Vasilisa Stepanenko. “Ukraine Is Leveraging Its Powerful—and Cheap—New Drone Killers for Air Defense.” Associated Press, 22 Dec. 2025, apnews.com/article/c7b57962e573b344490b07b2cfead856.