SPOTLIGHT ON THE SHADOW WAR

INSIDE RUSSIA'S ATTACKS ON NATO TERRITORY

A REPORT BY THE U.S. HELSINKI COMMISSION STAFF

Special credit to report author Sophia McGrath, 2024 Max Kampelman Policy Fellow

SUSPECTED AND ATTRIBUTED RUSSIAN HYBRID OPERATIONS SINCE FEBRUARY 2022

Figure 1: A non-exhaustive illustration of suspected and attributed Russian hybrid operations in NATO territory from February 2022 - November 2024.

IDENTIFIED HYBRID OPERATIONS 2022-2024

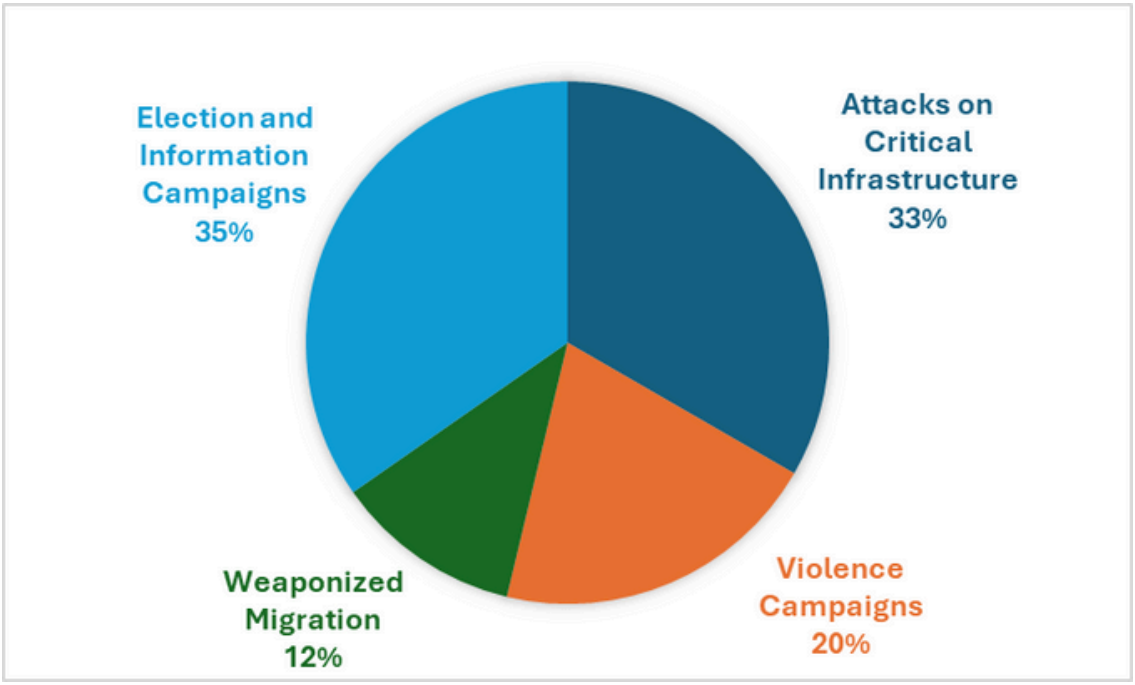

Figure 2: Percentage of suspected and attributed Russian hybrid operations in 4 key categories from February 2022 - November 2024

EXECUTIVE SUMMARY

Since the outset of Russia's full-scale invasion of Ukraine, Russian sabotage campaigns across North America and Europe have accelerated. Calculated campaigns of hybrid warfare show that Russia's antagonistic foreign policy knows no bounds. In conjunction with its war in Ukraine, Russia is simultaneously executing a shadow war on NATO to destabilize, distress, and deter the transatlantic alliance from its staunch support of Ukrainian sovereignty.

The efficacy of Russia's active measures inside of NATO stems from its nature as a "below the threshold of war" means of attack. However, the escalation of Russia's recent hybrid campaigns represent more than mere capers of destabilization. Rather, Russia is engaged in calculated posturing toward the transatlantic alliance to pair with its genocidal invasion of Ukraine. Hybrid campaigns can range from cyberattacks on train stations that cause scheduling delays to attempted assassination and terrorism plots; a deniable, one-off incident does not make a war in and of itself, but the scale and calculated nature of Russian hybrid threats within NATO borders since 2022 amount to a covert shadow war.

This report builds on the Helsinki Commission's September 2024 hearing, *Russia's Shadow War on NATO*, in which experts testified to the widespread and calculated efforts Moscow deploys to destabilize its democratic adversaries across the Atlantic. To visualize the breadth of the Kremlin's efforts, Helsinki Commission staff have mapped nearly 150 hybrid operations executed in NATO territory occurring since the outset of Russia's invasion of Ukraine that have been attributed to or suspected of Russia (see Figure 1). The identified hybrid operations fall into four categories: critical infrastructure attacks, violence campaigns, weaponized migration, and election interference and information campaigns.

It is critical that NATO leaders are united in their recognition of the intent and extent of Russia's hybrid operations. Hybrid warfare efforts present real threats to society and democratic governance. NATO was founded to counter Russian aggression, and Russia's ongoing attempts to undermine the security and stability of members of the alliance must be recognized as an affront to the foundations and core mission of the alliance.

INTRODUCTION

Eighty days into Russia's full-scale invasion of Ukraine, Russian foreign minister Sergei Lavrov claimed NATO was launching a "total hybrid war" on Russia. Lavrov's claim that the West's swift response of united condemnation and sanctions implementation amounted to a hybrid war was not only intentionally false, but an exercise in projection. Since 2022, the Kremlin has executed calculated hybrid warfare operations against the democratic societies that stand in the way of its imperialistic goals in Ukraine.

While Moscow has long weaponized hybrid operations against its adversaries, Russia has escalated its hybrid campaigns within NATO borders in response to unified support for Ukrainian sovereignty and victory. Utilizing open-source intelligence, the Helsinki Commission has created a non-exhaustive map of Russian hybrid operations in NATO countries since the outset of Russia's invasion of Ukraine to shed light on Moscow's covert war on NATO.

Why Target NATO?

Russia's active measures against NATO countries are calculated efforts to undermine democratic values, sow distrust within free societies, and destabilize the Alliance's resolved unity. NATO, as the cornerstone of Western security and a bulwark against Russian aggression, represents a direct obstacle to Moscow's imperial ambitions.

Hybrid warfare—a blend of cyberattacks, disinformation, sabotage, covert operations, and other active measures—offers Moscow a low-cost, deniable, and highly disruptive method to challenge the West's stability and solidarity. These tactics allow Russia to exploit vulnerabilities within open democratic systems while avoiding direct military confrontation with NATO. Often disguised as one-off acts of hooliganism, hazardous coincidences, or robust information campaigns, these hybrid operations are intentional, extensive and amount to a shadow war being waged within NATO's borders.

CRITICAL INFRASTRUCTURE ATTACKS

Attacks on critical infrastructure such as hospitals, trains, and water facilities are a means to threaten public safety and undermine trust in essential resources. Successful cyberattacks on passenger and cargo railways across Europe have generally resulted in inconveniences such as ticketing issues and schedule delays, however more sinister campaigns such as railroad arson and a foiled plot to derail weapons freight to Ukraine have been identified as well.

Cyber campaigns against hospitals have accounted for a significant number of Russian attacks on NATO over the past two years. Patient data is often held hostage for ransom, and critical hospital services are sometimes shut down, depriving the public of critical care. Hospital networks are particularly appealing targets due to their reach; a February 2024 ransomware attack on the largest insurer in the United States disrupted thousands of pharmacies across the country and is thought to have impacted the personal information of "a substantial proportion of people in America." That same month, more than 100 health care institutions in Romania were taken offline following a ransomware attack. Cyberattacks on medical facilities over the past two years account for more than one fifth of the critical infrastructure attacks pinpointed on the map below.

Figure 3: Map highlighting identified hybrid warfare attacks on critical infrastructure attributed and suspected of Russia. Includes GPS signal jams, cyberattacks on hospitals, railway disruptions and other sabotage on infrastructure systems.

Cyberattacks can also have physical ramifications. An alarming trend of GPS signal disruptions originating from Russia's Kaliningrad exclave has increasingly impacted European aviation. In December 2023 widespread GPS jamming affected flights across Sweden, Finland, Denmark, Germany, Poland and the Baltics. In March 2024, Russia was suspected to have jammed the GPS signal of a plane carrying the British defense minister, reaching a new point of escalation.

Russia-affiliated cybercriminals have also infiltrated water facilities in Texas, France and Poland breaching security systems and potentially putting public access to clean drinking water at risk. US officials have previously warned of vulnerabilities in water facilities, noting that "they are a lifeline critical infrastructure sector but often lack the resources and technical capacity to adopt rigorous cybersecurity practices."

Hybrid attacks on critical infrastructure extend beyond cyberspace to physical sabotage. In August 2024, the security threat level at Geilenkirchen NATO Air Base was raised due to an increased threat of Russian sabotage, following security incidents at Geilenkirchen and Germany's Cologne-Wahn military base. In September, the US warned of a buildup of Russian military activity near critical undersea cables in the Baltic Sea—raising concerns about potential sabotage to these critical channels for global internet and telecommunications access.

VIOLENCE CAMPAIGNS

Violence campaigns can range from petty vandalism to attempted acts of terrorism. Russia has been accused of recruiting and paying sympathizers from a variety of backgrounds to outsource their destabilization schemes. Menial acts of vandalism—such as antisemitic graffiti in France, property damage to a government official in Estonia, arson at a metal factory in Germany—gain significance when executed in a decentralized and calculated manner, creating a climate of insecurity across Europe.

More dangerous campaigns also occur. In early 2024, Polish authorities arrested a man recruited and paid thousands of dollars by either Russian or Belarussian operatives to bomb a paint factory in southwestern Poland. Similarly, in June, French authorities arrested a man near Charles de Gaulle international airport on bomb-making charges, disrupting a Russian-orchestrated sabotage plot north of Paris. Further stoking fear, a litany of mass bomb threats traced to Russian servers have been emailed to schools and other institutions in the United States, Greece, North Macedonia, Slovakia, and the Baltics.

Businesses and other institutions supporting Ukraine across Europe have also been targeted. In February 2024, a British man was charged under the UK's National Security Act for plotting an arson attack on a Ukraine-linked business, in association with Russia's Wagner Group. In April, German authorities arrested two men surveilling a number of targets for potential bomb plots, including Grafenwöhr Air Base in Germany, a US military base where Ukrainian troops are trained on M1 Abrams tanks.

Assassination attempts of the Kremlin's enemies have also been carried out on NATO soil. In 2023, Italian intelligence services intercepted Kremlin communications offering $15 million to the Wagner Group to assassinate Italian defense minister Guido Crosetto. In July 2024, US and German authorities foiled a plot to assassinate Armin Papperger, a German defense manufacturing executive whose company has led in producing artillery shells for the Ukrainian military.

WEAPONIZED MIGRATION

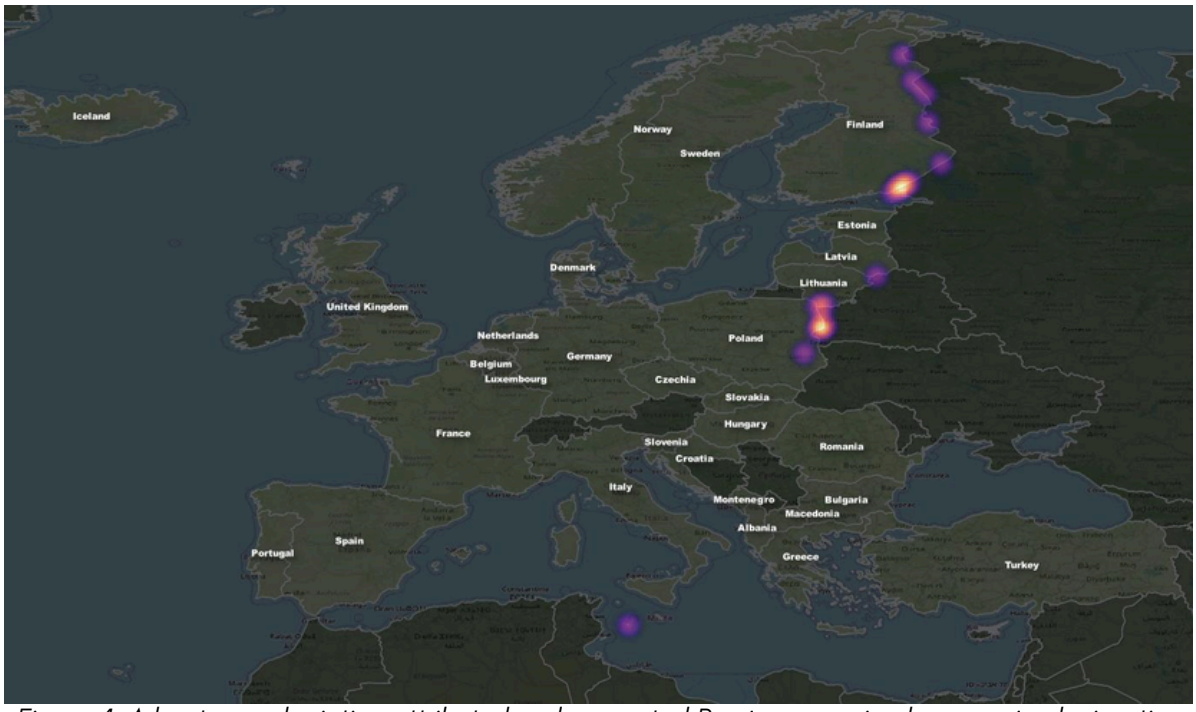

Figure 4: A heat map depicting attributed and suspected Russian-organized weaponized migration campaigns including border closures, allegations of migration surges, and news reports at border stations

A particularly heinous tactic deployed by Russia and Belarus is the weaponization of migrants. In November 2023, Finland closed its border with Russia following a surge of border crossings believed to be instigated by Russia; 900 third-country nationals arrived in Finland without valid documentation that month alone. In the summer of 2024, Poland saw a surge to nearly 400 illegal border crossings a day. The Polish efforts to combat Belarus' manufactured migration crisis are costing nearly $615,000 annually—but the costs are more than financial. Tragically, a Polish soldier stationed at a border site was fatally stabbed in May 2024.

Weaponized migration campaigns are not limited to Russia and Belarus's immediate neighbors. In March 2023, the Italian government attributed a surge in migrant boat crossings across the Mediterranean to Russia's Wagner Group, a mercenary group highly active in Africa.

These border crises are orchestrated to pressure state institutions, drain resources, and fuel anti-migrant rhetoric exploited by far-right parties across Europe. Russian and Belarusian authorities prey on vulnerable populations and recruit them with the false promise of a better life in Europe—only to be used as pawns in campaigns designed to incite hate and destabilize democratic societies.

ELECTION INTERFERENCE AND INFORMATION CAMPAIGNS

Election interference is a hallmark of Russia's hybrid warfare. Spreading false narratives and funding candidates sympathetic to Moscow are ubiquitous tactics. In March 2024, Czech and Belgian officials uncovered a massive Russian propaganda network spread across Europe attempting to influence European Parliament elections, including efforts to bribe EU lawmakers to promote Kremlin rhetoric.

In the United States, Georgia Secretary of State Brad Raffensperger debunked bomb threats made across several precincts on Election Day, attributing them to Russian origin. At least five other states received similar hoax threats as Americans went to the polls.

Beyond elections, Moscow's disinformation campaigns aim to fracture NATO unity. In 2023, the Swedish government accused Russian "state and state-like actors" of fueling disinformation campaigns related to the Quran burnings occurring earlier that year. The demonstrations came during Sweden's stalled bid to join NATO and inflamed Turkiye's relations with Sweden, causing further delay on Turkiye's approval for Swedish accession. Moscow's information campaigns against NATO countries also seek to undermine broader support for Ukraine. Earlier this year, French authorities took down a fake army recruitment page inviting 200,000 French people to enlist to fight in Ukraine; the site bore resemblance to previous Russian disinformation campaigns falsely claiming the French military will send a ground force to Ukraine. Similarly, in May, a fabricated article about a Polish draft repeatedly appeared on the Polish Press Agency's website, a cyberattack likely orchestrated by Russia.

CONCLUSION

The map assembled by the Helsinki Commission staff pinpoints nearly 150 suspected and attributed instances of Russian hybrid operations in NATO territory since February 2022. This stark visualization underscores the breadth and insidiousness of Russia's shadow war, yet it likely underestimates the true scale of the threat. Russia's hybrid warfare thrives on plausible deniability, leveraging decentralized tactics—outsourcing operations to low-level cybercriminals and employing diverse methods to relentlessly destabilize NATO countries, regardless of the success rate of individual attacks.

As Russia continues to escalate its war on Ukraine with ballistic missile strikes and North Korean troops, it simultaneously escalates in its shadow war against NATO. These two theaters—the kinetic war in Ukraine and the shadow war against NATO—are deeply interconnected. Failing to fully support Ukraine's defense only emboldens Russia to continue its hybrid attacks, knowing the West's response is inconsistent and restrained.

Deterring Russia requires a two-pronged approach. First, NATO must take the shadow war seriously, treating these operations as real and present threats to the Alliance's stability and security. Second, and equally critical, NATO and its member states must take decisive actions to support Ukraine in its fight against Russian aggression. Restricting aid or failing to meet the urgency of Ukraine's needs only signals weakness and invites further Russian escalation, both in Ukraine and within NATO's borders.

NATO's founding purpose was to serve as a bulwark against Russian aggression. That purpose is as vital today as it was at the Alliance's inception. Only by confronting Russia's hybrid warfare head-on and ensuring Ukraine's victory can NATO effectively deter further Russian provocations and uphold the democratic values it was established to defend.