TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Committee on Foreign Affairs
Subcommittee on Europe

Weaponized Mass Migration: A Security Risk to Europe and the United States

RADM (RET.) MARK MONTGOMERY

Senior Director and Senior Fellow, FDD's Center on Cyber and Technology Innovation
Foundation for Defense of Democracies

Washington, DC
February 10, 2026

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

Chairman Self, Ranking Member Keating, and distinguished members of the committee, on behalf of the Foundation for Defense of Democracies, thank you for the opportunity to testify again before you today.

I am pleased that this committee's leadership continues to focus on Russia's efforts to destabilize Europe. I would be remiss if I did not say again that I remain convinced that the greatest threat to Euro-Atlantic stability and international peace is Russia's illegal war in Ukraine. If Russia prevails in Ukraine, we can expect to see a barrage of the same tactics, this time directed towards America's treaty allies.

But the focus of today's hearing is Russia's "New Generation Warfare" efforts, a hybrid warfare strategy that cuts across a range of activities including weaponizing migration across Europe. Russia is actively exploiting the refugee crisis incited by the war in Ukraine, sowing societal discord and destabilizing European Union (EU) nations. This effort is coupled with other New Generation Warfare tools — influence and information operations, cyberattacks against critical infrastructure, drone incursions, and the sabotage of utilities, transport lines, and undersea cables. The effects of weaponized migration are only compounding. Many of these efforts are done in collaboration with Russia's puppet state, Belarus. The Kremlin's exploitation of the migrant crisis helps Putin achieve his political objectives in countries like Poland and the Baltics, but no European state is immune from attack.

And the United States is next. Long before the start of the Ukraine war, Russia has viewed the North Atlantic Treaty Alliance (NATO) as a Western ploy to burrow deep into Eastern Orthodox civilization. Weaponized migration puts NATO allies under duress, throwing them into a state of chaos, undermining democratic institutions, and reducing their ability to devote resources to defense and security spending. When Russia successfully compromises even one of our European partners militarily or societally, America's ability to fight with and through its allies is put in grave jeopardy.

My testimony will discuss Russia's New Generation Warfare with a deep dive into weaponized migration, and the overall impact on NATO's military readiness. I will also provide a number of policy recommendations to combat this hybrid warfare and its associated malicious activities.

Russia's New Generation Warfare

At its core, Russia's conception of New Generation Warfare rests on the implicit assumption that a conventional conflict between Russian and Western civilization is not only imminent but already taking place. However, while the United States has historically treated hybrid measures like information operations as secondary to conventional combat, Russia has long integrated and prioritized hybrid techniques in its military strategy. For Russia, hybrid campaigns cover an array of non-kinetic activities, including covert and overt influence operations, cyberattacks, election meddling, and weaponized migration. As Western conventional military technology remains dominant, the Kremlin understands there is a strategic advantage to employing more non-kinetic means of attack. In line with this understanding, the chief of staff of the Russian military, General Valery Gerasimov, valued nonmilitary to military measures as four to one.[1]

The strategies and goals of weaponized migration fit into Russia's broader doctrine of New Generation Warfare. While the term varies across countries, with the U.S. calling it "hybrid warfare," the definition remains largely the same: to conduct an operation against an adversary at a level just below the threshold of true war, to achieve a favorable political outcome. As its name alludes to, this approach involves a combination of traditional kinetic military measures, alongside non-kinetic methods. Russian military doctrine outlines how the desired outcome of these measures is to cause "controlled chaos" and

"destruction and attrition."[2] In a state of domestic unrest and chaos, the Kremlin can then more easily employ influence operations and other means of shaping political decision-making.

One can observe how the tool of weaponized migration fits into Russia's broader New Generation Warfare strategy by analyzing its application in the current war in Ukraine.

Russia's invasion of Ukraine has caused the greatest refugee crisis in Europe since World War II. Throughout the war, Russia has targeted civilian and energy infrastructure, likely to further exacerbate the crisis. Just in the first few months of the invasion, Russian forces displaced over 6.5 million people, overwhelming EU energy and food resources and placing countries in a state of chaos. The overall effect is staggering.

This effect has been compounded by Russia altering the flow of non-European migrants as well. Since the Ukrainian war began, the EU border agency FRONTEX found a 200 percent increase in non-European migrant arrivals along the EU's eastern borders, and a corresponding decrease in passage along more traditional routes like the Mediterranean, signaling Russia's active efforts to manufacture a migration crisis in the EU. Migration surges along the EU's eastern border have often correlated with rises and falls in Russia's progress on the battlefield in Ukraine and the timing of Western sanctions on Russian oil, demonstrating the Kremlin's efforts to exploit migration to distract and deter the West from aiding Ukraine.

The Kremlin's use of weaponized migration both as a weapon of chaos and influence reflects the larger strategy outcome in New Generation Warfare of enacting "controlled chaos" through non-kinetic means. Later, I will address case studies of Russia's weaponization of migration in Syria, Eastern Europe, and the Baltic States. As in Ukraine, the Kremlin weaponizes migration to polarize Western society and foment chaos.

Weaponized Migration

As described above, weaponized migration (and New Generation Warfare, more broadly) fits into Russia's larger long-game strategy to disrupt and influence the longevity and stability of Western political society, with a particular focus on NATO.

Weaponized migration is a tool in Putin's hybrid warfare strategy. Weaponized migration is defined by Kelly Greenhill (a leading expert on migration) as "the manipulation of population movements as operational and strategic means to political and military ends."[3] In Russia's case, the primary political and military end of the Kremlin's campaign of weaponized migration is to polarize the West and fragment and destroy NATO unity.

U.S. leaders and political scientists have noticed the growing role of weaponized migration in Russia's hybrid strategy, observing how the Kremlin exploits migration crises to exacerbate social divisions, economic strains, and political polarization in the West. Russia employs migration not as a foreign policy instrument, but as a weapon of war. Rather than a traditional battlefield victory, though, the Kremlin's aim is to influence Western politics in a direction favorable to Russia's interests. In addition to weakening the EU and NATO, achieving this political goal also means fostering social divisions, encouraging far-right regimes, and creating the type of instability that is lethal to a democracy. Illustrating the appeal of weaponized migration to a leader like Putin, Greenhill found that in half of the 81 historical cases of weaponized migration she studied, the political objectives of the weaponizing country were either partially or fully met.[4]

Russia values the role of weaponized migration in exposing NATO's soft underbelly and fomenting domestic chaos in the West. Russian doctrine largely rests on the idea of unique civilizational histories. In Russia's view, while Russia has developed its own unique civilization around Orthodoxy, the West, for instance, has developed according to Protestant and Catholic civilizational patterns. The Kremlin views NATO's involvement, especially as it "encroached" east towards states formerly under Soviet control, as a Western incursion on Russian civilization.

Russian military theorists have long suggested migration as a potential weapon of war below the threshold for full-out conflict. Such works discuss how the traditionally Christian Western civilization is experiencing growing migration crises. Within these crises, theorists note that mass (in this case, Islamic) immigration is creating destabilizing effects and demographic changes. Consequently, these theories purport that the societal impacts of this migration crisis will hurt Western prestige and lead NATO to fail in its stated mission of protecting its member nations.

Syria (2015-2016)

Throughout the uprisings in Syria against the authoritarian Assad regime, Putin attempted to prop up his ally, Bashar al-Assad. In October 2015, Russia conducted a month-long bombing campaign against the opposition. The strikes appeared to have been indiscriminate and destructive of civilian infrastructure — creating an extensive population of displaced persons. To try and limit European responses, Putin and Assad conspired to drive these refugees and displaced people into a migration pattern towards Europe.

In February 2016, the European Union hit a crisis point with the refugee crisis from the civil war in Syria. U.S. General Philip Breedlove, the NATO supreme commander, claimed, "Together, Russia and the Assad regime are deliberately weaponizing migration from Syria. In an attempt to overwhelm European structures and break European resolve." In a Senate hearing, Breedlove referenced Russia and the Assad regime's indiscriminate bombing of vast civilian areas and claimed this was an intentional act to encourage migration and overwhelm the EU.

In addition to his goals to create domestic unrest, Putin may have also employed migration as a hybrid tool to influence political decisions in his favor. When the Brexit referendum took place just six months later, in June 2016, most analyses found immigration to be the strongest issue causing voters to want to leave the EU. Brexit was a victory for the Kremlin's longstanding effort to weaken the European Union.

Joint Russian-Belarusian Operations Against European States (2021-today)

Russia and its close ally, Belarus, share borders with several EU states. The Kremlin has exploited these borders, encouraging and resourcing influxes of migrants from the Middle East and Africa to transit through Russia and Belarus and then enter and overwhelm EU states. The primary goals are weakening EU security, overwhelming leaders, and instilling chaos and unrest. Since 2021, Belarus has offered unrestricted access to migrants from the Middle East into the European Union.[5] In the immediate ramp up to Russia's illegal invasion of Ukraine in February 2022, the Lukashenko administration flew migrants to the capital city Minsk and then transported them via state buses to the borders of EU countries, including Latvia, Lithuania, and Poland. As these countries had been leaders in sanctioning Russia and aiding Ukraine, this operation was likely intended to destabilize the area, and perhaps distract, as Russia prepared to launch its attack on Ukraine.

Poland and Germany

The route from Belarus to Poland is a promising one for many migrants, with Poland historically offering a one-month visa-free stay, and a direct path to desirable nations like Germany.[6] The Belarusian and

Russian-associated crime rings employ several methods to secure visas and transport, in one case registering new companies online in Poland and requesting permits to employ the migrants and coordinating with Belarusian border officials to cut fences to allow entry into the European Union.[7] The situation at the border has devolved into violence and chaos, which the Kremlin as well as European right-wing extremists use to push their agendas.

In June 2024, as nearly 400 migrants were crossing the Poland-Belarus border every day, a Polish soldier was stabbed to death through the fence by a migrant on the Belarusian side.[8] In response to the Polish appeal for Belarusian support in de-escalating, Belarusian Foreign Ministry Spokesman Anatoly Glaz shifted the blame to Poland for cutting cooperation initially between Poland and Belarusian border control agencies and stated that Belarus was willing to cooperate.[9] In 2025, four tunnels likely used to smuggle migrants were discovered leading from Belarus into EU territory. In August 2025, Polish authorities reported that in one day "over 120 attempts to illegally cross the border" took place.

Russia's weaponization of migration has led to political strife in Poland. As Poland's presidential elections neared in May 2025, Poland's social media was flooded with false information, fueling more attention towards the migration crisis. One fake video showed illegal migrants entering Krakov at night, along with the caption, "Fake asylum seekers are dumped ... when Poles are sleeping." Another popularized, false narrative claimed Germany was sending Muslim, Ukrainian, and Black migrants into Poland for state benefits. Far-right candidates used this to fuel their campaigns, as they ridiculed the ruling pro-European party's migration policy. The election of President Karol Nawrocki, a conservative nationalist, who opposes Ukraine's ascension to NATO and the EU, was certainly a favorable result for the Kremlin.

Indeed, it seems Moscow has Germany in its sights in the information war against the West, initially aiming to leverage the migrant crisis to weaken voter trust in Chancellor Angela Merkel.[10] In 2016, Russian media reported a story about a 13-year-old Russian German girl who was allegedly raped by migrants. The story was quickly revealed to be fake, but not before it was extensively covered by Russian foreign and domestic media.

The effects of the migrant crisis go beyond information warfare. From March 2022 to February 2025, refugees cost the European Union an estimated 36.4 billion euros. Poland, meanwhile, paid an estimated 29.3 billion euros. In addition to the resulting political polarization and chaos, the consequent social and economic strain has certainly made it more difficult for these countries to provide aid and defense coordination to Ukraine.

In November 2021, Poland deployed 15,000 troops to its Belarus border, pulling forces from other defense missions. The border crisis forced Lithuania, Latvia, and Poland to increase border protection efforts. The border crisis began a month before the active phase of the Zapad drills, Russia's largest maneuver in its western strategic direction in 2021. This coordination reveals how weaponized migration serves as battlefield preparation, testing allied response times, decision-making processes, and willingness to maintain defensive postures under political pressure. These operations systematically drain military capacity from deterrence missions. Poland constructed a 400-kilometer border wall costing approximately 350 million euros, representing substantial capital diverted from conventional defense spending.

Baltic States

In addition to the Belarus-Poland migration route, Russia and its close ally Belarus have also leveraged their border with the Baltic states as an EU entry point. Since August 2021, Russia has coordinated with Belarus to launch a sustained campaign of weaponized migration. Since then, authorities have stopped 24,508 illegal migrants from entering Lithuania, and 39,724 entering Latvia. Migrants often try to cross

the border multiple times. Their transit is facilitated not only by Belarusian and in-country travel agencies, but also by Latvian and Lithuanian nationals using minivans or cars.[11] In September 2021, Lithuania called in NATO's Hybrid Threat Support Team after receiving over 4,000 migrants illegally entering through the Belarusian border.[12]

On January 15, 2026, the Latvian Ministry of Defense released a statement on current weaponized migration, that "confirms the involvement of law enforcement and military structures of the Republic of Belarus in directing illegal migrants toward the Latvian state border."[13] Attempts to increase and arm border patrols have been met with international pushback and humanitarian concerns, while little is being done to ease the root of the problem.

Other border countries, too, are facing the consequences of the Russian-induced migration crisis: In the first quarter of 2016, Finland received over 1,000 asylum seekers through its arctic border crossings, leading decision makers to tightening restrictions to try and limit the flow. On coming to power in 2023, the right-wing National Coalition Party, which stands on a firmly anti-immigrant platform and deported over 2,070 foreign nationals between January and September 2025, again closed Finnish borders to migrants, fueling a Russian disinformation campaign claiming that Finland itself orchestrated the migration crisis to isolate Russia after Finland's accession into NATO.[14]

Russian Attacks on Critical Infrastructure

In addition to weaponizing migration, Russia's New Generation Warfare has concentrated on critical infrastructure attacks. Russia understands that modern societies are networked, and networked societies have chokepoints. Moscow's approach to war is not confined to the front line. It is designed to break a nation's ability to function — first by degrading essential services, then by eroding confidence in government, and finally by shaping political decision making. When critical infrastructure fails, everything else gets harder: military mobility, economic stability, public morale, and strategic communication. That is why Russia targets energy systems, communications networks, transportation systems, and logistics hubs — and why it blends kinetic strikes, cyber operations, and sabotage to keep defenders off-balance.

A brief look at Ukraine makes the logic clear. Russia has repeatedly treated Ukrainian energy infrastructure as a strategic target. It relies on missile and drone attacks to impose blackouts and force Kyiv into a constant cycle of emergency repairs. The International Energy Agency noted that on August 26, 2024, Russia launched more than 200 missiles and drones primarily targeting Ukraine's energy infrastructure. The strikes led to widespread outages affecting around 8 million households.[15] This was one of the largest aerial attacks at that time. The Russian attacks over the past three weeks have been even larger and more damaging, making a wicked winter even colder.

Russia's cyber operations complement these kinetic attacks. Ukraine has been a proving ground for Russian cyber tactics aimed at its critical infrastructure, designed to interfere with operational technology and the networks that manage it. The 2015 Russian attack on the Ukrainian power grid attack was an early demonstration where power companies experienced unscheduled outages after a cyberattack, creating real-world disruption at scale.[16] U.S. federal agencies and international allies and partners published a joint advisory attributing widely publicized energy attacks in 2015 and 2016 to Russia's military intelligence agency, the GRU.[17]

Russia has continued using this playbook. An hour before launching its full-scale invasion against Ukraine in early 2022, Moscow moved to blind and isolate the country by targeting Ukraine's communications infrastructure. Cyberattacks against Viasat's KA-SAT satellite network disrupted

satellite broadband communications in Ukraine and users beyond Ukraine.[18] This is a clear demonstration of Russia's strategy to degrade a nation's ability to coordinate and defend itself before its forces cross the border. The United States later attributed cyberattacks to Russian state-sponsored actors,[19] and the European Union also issued a declaration condemning malicious cyber activity targeting the KA-SAT network.[20]

Importantly, spillover risk is not confined to Ukraine. Russian cyber activities routinely push across borders — sometimes by design, sometimes as a second-order effect of targeting shared providers, software, energy, and transportation markets. As European allies and partners deepen support to Ukraine, Moscow's incentives expanded to include retaliation, intimidation, distraction, and imposition of costs on the coalition sustaining Kyiv. In January 2026, researchers assessed that Sandworm — a Russian state-sponsored hacking group — targeted Polish energy utilities using malware designed to wipe systems and degrade operations.[21] The operation did not achieve its intended impact, but that is not the right metric. Even a failed attack forces defenders to divert scarce resources to defend, investigate, and recover — consuming resources and creating political pressure. This is how Russia competes at scale: it forces democracies to spend time, money, and attention just to stay in place.

That brings us to the maritime domain. Undersea infrastructure is the physical backbone of Europe's connectivity and energy system. It includes fiber-optic cables that carry cross-border data traffic, electricity interconnectors that help stabilize national grids, and gas pipelines that deliver fuel across the region. These links run through contested waters, are difficult to monitor in real time, and can be disrupted in ways that enable plausible deniability, making them attractive targets for Russian sabotage. Since Russia's invasion of Ukraine, the Baltic Sea region has seen a steady drumbeat of disruptions to these subsea systems.

The reason the threat is so effective is because of attribution. Some incidents may be accidental, some (most) may be sabotage, while others fall in the gray zone where intent is difficult to prove publicly, especially in real time. After damage to undersea cables connecting Estonia and Finland on December 25, 2024, NATO held consultations and announced it would enhance its military presence in the Baltic Sea to maintain vigilance and deter future incidents.[22] Since then, NATO has launched Baltic Sentry, an initiative to strengthen cooperation with industry on protecting undersea infrastructure.[23] Finland, the European Commission, and Baltic Sea states have taken additional steps, including efforts to enhance monitoring and surveillance capacity in the Gulf of Finland.[24] The Finnish Defence Command's 2026 military intelligence review concluded that Russia will "likely persist" in efforts to try and damage undersea infrastructure in the Baltic Sea, even as Finland notes that no definitive evidence has tied Russia — or other states — to recent incidents.[25]

The United States, NATO, and Europe as a whole have much to learn from Ukraine's response to Russia's persistent, malicious cyberattacks against critical infrastructure. Ukraine's national-level cyber defense has proven to be highly adaptable and effective, even within a limited technology and personnel development pipeline. But existing cyber resources are primarily concentrated in Kyiv, and while this has assisted in the defense of the capital and its key infrastructures, the centralized response model slows regional-level cyber detection, containment, and coordination.

Decentralized cyber capabilities are increasingly needed to keep Russia's persistent and developing cyber threat at bay. To confront Russian aggression, European nations, most importantly Ukraine, should establish regional Security Operations Centers (SOC) and Computer Security Incident Response Teams (CSIRT). Regional SOC and CSIRT teams can provide improved immediate response capabilities and facilitate more agile national and regional collaboration, enabling faster mitigation of potentially devastating cyberattacks. These regional centers can also facilitate stronger information sharing, bolstering the alliance and strengthening European cyber defense as a whole.

Impacts on NATO Readiness

Russia's New Generation Warfare — whether it is weaponized migration or critical infrastructure attacks — is testing NATO's readiness every day through hybrid operations intended to fracture allied resolve. Readiness is the alliance's ability to execute at speed and scale. NATO's readiness, therefore, is not a narrow question of "how many troops can be mobilized?" Instead, the alliance's readiness is its ability to move, communicate, fight, and sustain combat power at speed under hybrid pressure. The alliance must be able to do all of this while Russia targets civilian infrastructure, commercial networks, and democratic institutions at the same time — because that is exactly how Moscow fights.

At the 2023 Vilnius Summit, NATO leaders adopted a new generation of regional defense plans and emphasized the importance of rapid reinforcement, large-scale exercises, and capability growth — especially in munitions and air and missile defense.[26] The momentum from the Vilnius Summit has been reinforced by visible demonstrations of force generation and reinforcement, especially since Russia's full-scale invasion of Ukraine. During the 2024 Washington Summit, former NATO Secretary General Jens Stoltenberg reported that roughly 500,000 troops are available at high readiness — exceeding the 300,000-troop goal set at the 2022 Madrid Summit.[27] Those numbers are important, but they are not decisive unless NATO can move those forces to the right place fast enough.

Recently, Congress also reinforced European deterrence by sustaining focused cooperation through the FY26 National Defense Authorization Act, which provided limited funding for Ukraine, reauthorization and funding for the Baltic Security Initiative and various other European and NATO-focused measures. That kind of congressional attention is a strong signal to Moscow that the United States is not drifting, and that allied cohesion is not a temporary condition. The United States benefits from strong allies; sustained support enables our allies to stand with us against authoritarian aggression. The Baltic Security Initiative requires the secretary of defense and the head of U.S. European Command (EUCOM) to put forth a strategy for increasing regional cooperation. Another provision requires the interagency to report on the progress of U.S. cybersecurity and cyber resilience support to the Western Balkans.

Weaponized migration can impact alliance readiness by forcing allies to divert military resources, stretch border infrastructure, and create sustained operational pressures along critical frontiers. The previously mentioned November 2021 example caused Poland to deploy 15,000 troops to its Belarus border, pulling these forces from other defense missions. The 2021 border crisis also forced Lithuania, Latvia, and Poland to all increase state service efforts, divert forces to protecting borders, while introducing uncertainty in the general populations about the security situations, a vulnerability that could be exploited to influence public mood and societal resilience.

NATO readiness is also inseparable from critical infrastructure resilience. A warfighting alliance depends on enablers: ports, rail, airfields, fuel, power, and communications. If those enablers are disrupted, readiness collapses no matter how good the plans look on paper. NATO's seven Baseline Requirements of National Resilience framework describes civil preparedness as having three core functions: continuity of government, essential services to the population, and civil support to military operations.[28] Essentially, if a nation cannot keep its government functioning, essential services running, and support military operations under stress, it is not resilient.

Meanwhile, European leaders have acknowledged significant bottlenecks that hinder effective military mobility across Europe. The European Commission's Military Mobility Action Plan 2.0 describes capacity constraints and infrastructure competition with civilian transport operations, while also naming "complex, paper-based" border clearance procedures with inconsistent timelines across EU member

states.[29] The commission also notes that cross-border permission timelines can vary dramatically, with some member states requiring 45 days' advance notice, exceeding the timeline to grant permissions within three working days committed by members in the 2024 Military Mobility Pledge.[30] This is more than an administrative inconvenience. In a crisis, it will lead to an operational failure.

Independent oversight has reinforced these findings. In 2025, the European Court of Auditors assessed the EU's efforts on military mobility and concluded that its member states' armed forces were not able to move quickly across the union, citing infrastructure design weaknesses. The auditors also found that, despite good intentions, the European Commission did not thoroughly assess infrastructure needs before launching Action Plan 2.0, limiting its ability to target funding effectively across its member states.[31] NATO does not control EU policies, but its readiness outcomes are affected by these realities. NATO's reinforcement routes and sustainment networks rely on the same infrastructure, commercial logistics providers, and cross-border procedures. So, when Europe's systems slow down, NATO's war plans slow down with them and Moscow benefits without firing a shot.

Europe's digital networks are another challenge in the readiness equation. NATO relies on ports, rail, airfields, and cross-border processes that run on networked systems that are vulnerable to cyber disruption. Russia does not need to confront NATO forces on the battlefield to create strategic paralysis. It can conduct cyberattacks on scheduling systems, disrupt logistics visibility, degrade communications, and force commanders into conservative operating modes that trade speed for safety. For instance, the 2017 NotPetya malware deployed by Russia is widely treated as a destructive campaign because it disrupted major global firms, including shipping and terminal operations, causing over $10 billion in damages globally.[32]

Alongside mobility and resilience, NATO readiness is increasingly defined by capability gaps that Russia has made brutally visible: air and missile defense and stockpiles of critical munitions. NATO's Washington Summit Declaration in July 2024 emphasizes that allies are resolved to deter and defend against air and missile threats by enhancing NATO's integrated air and missile defense, and it underscores that investment beyond 2 percent of GDP is needed to remedy shortfalls.[33] In Washington, NATO leaders also declared the Enhanced Operational Capability of NATO's ballistic missile defense to further advance its posture.[34] These commitments matter because if NATO cannot defend critical infrastructure and population centers from missile and drone threats, it will struggle to receive reinforcements, sustain tempo, and protect the political will that keeps the alliance united.

NATO must be able to produce more, faster, in an environment where deterrence depends not only on superior systems designed for lethality, survivability, and strategic capability, but also on sustained readiness across land, sea, and air domains. In Vilnius, NATO leaders committed to increasing stockpiles of battle-decisive munitions.[35] Since then, NATO has translated its commitment into action. In February 2025, NATO published an updated Defence Production Action Plan that focused on increasing defense industrial capacity and production through aggregating demand and addressing industrial capacity challenges.[36] If NATO cannot replenish, it cannot deter — and if it cannot deter, it will eventually have to fight from a deficit.

Finally, NATO readiness also has a financial dimension. The Washington Summit Declaration welcomed the fact that more than two-thirds of its members had met the 2 percent GDP commitment. However, NATO leaders also underscored that expenditures above 2 percent will be necessary to meet requirements across all domains.[37] The Hague Summit in June 2025 set a sharper target, with a consensus across member states that a 5 percent of GDP commitment by 2035 would comprise 3.5 percent for core defense requirements and capability targets and up to 1.5 percent for critical infrastructure protection and industrial base protection.[38] The key is that defense spending must be aligned with the fight NATO needs to win.

Recommendations

1. **Raise Awareness of Russian "New Generation Warfare" and Weaponized Migration Tactics.** Russia's information operations are intended to polarize Europe on migration issues. Countering these campaigns requires both reactive and preemptive action. The United States and NATO should expose Russian operations — publicly identifying the units and individuals responsible and explaining their methods. Proactively, the United States and its NATO allies should use their own information campaigns to both reveal the truth and shape the narrative that interference and cognitive warfare is part of Russia's aggression against Europe.

2. **Assist Allies in Combatting Russian Hybrid Warfare.** The United States and its NATO allies should provide technical assistance to other members of the alliance and to other beleaguered democracies facing Russia and its Axis of Aggressor partners. The United States needs resilient allies whose societies can withstand and repel Russian hybrid warfare. Washington should bolster intelligence and cyber threat information sharing with its allies to help them identify Russian aggression. U.S. partners and allies may also need surveillance and border security technology to combat Russia's weaponized migration and technologies, strategies, and software to thwart Russia's cyber campaigns.

3. **Organize and Equip NATO for Hybrid Warfare.** Currently, the United States and Europe treat hybrid warfare actions as separate, often stand-alone incidents. This misunderstands the threat. Hybrid warfare is a low intensity warfare campaign conducted by a hostile state to gain legal and political freedom to act — and NATO member states must understand it as such. To remediate this, NATO should establish hybrid warfare units that specifically monitor Russia's command and control and work to disrupt campaigns. NATO should also develop hybrid warfare training platforms that support border protection, cyber protection, and countering influence operations.

4. **Pressure Belarus.** Russia is using Belarus to conduct weaponized migration and other tactics to provide for plausible deniability. The United States should work with allies to expose Moscow for the puppet master that it is. This effort should include imposing more sanctions on President Aleksandr Lukashenko's regime, not relaxing sanctions, and also secondary sanctions on companies (including airlines) that facilitate migrants' movements.

5. **Make the 1.5 Percent in Defense Related Spending Count.** This spending should go to security and resilience efforts to include bolstering cyber defense, military mobility, critical infrastructure protection, supply chain resilience, energy security, innovation, and civil preparedness. If NATO does not build good business rules early, not all 1.5 percent efforts will be created equally or wisely. This spending requirement can too easily be written off by pointing to ongoing economic infrastructure projects. These projects may be national priorities, but economic infrastructure does not equal societal resilience and military continuity. To avoid this problem, it is imperative that NATO's planners at SHAPE drive some of this spending. The SHAPE planners could go into the logistics and transport annexes of their newly developed plans and identify infrastructure initiatives that support military mobility. They would likely highlight, for example, the systems that get U.S. and UK forces onto the continent and U.S., UK, and French armies into the fight. The bottom line is we need to ensure that the 1.5 percent is informed by the NATO planners' work. If necessary critical infrastructure investments become too burdensome on a country, then NATO and the European Union should take steps to incentivize this work with grants, loans, or other support.

6. **Treat Military Mobility as a Readiness Program, Not Europe's Transportation Project.** Europe is moving toward dual-use transport corridors and military mobility initiatives, but progress is uneven and bottlenecks persist. Congress should task the Secretary of Defense, through EUCOM in coordination with NATO, to define "time to reinforce" targets by corridor and capability — then align exercises, prepositioning, and infrastructure investments to meet mission critical needs. Successful large-scale exercises are not enough. What the alliance needs is to know whether heavy units, fuel, munitions, and troops can traverse specific routes within specified timelines — and whether those routes would remain usable under cyber and physical attacks.

7. **Measure Readiness Through Munitions, Maintenance, and Surge Capacity.** NATO leaders have explicitly called for urgent action on battle-decisive munitions, air and missile defense, and exercises that test the new defense plans.[39] Europe is starting to put real money behind the industrial base, but it is still early and not yet scaled to meet wartime demand. The next step is to link dollars to deliverables. The Secretary of Defense should deliver to Congress clearer reporting on what NATO capability targets actually translate to in terms of production rates, stockpile depth, and sustainment capacity. A useful framework is to require trendlines on 1) current production rate vs. required surge rate, 2) stockpile depth expressed in days/weeks of high-intensity operations, and 3) repair or overhaul throughput for the infrastructure NATO actually needs in the first 30-60 days of a conflict.

Conclusion

Russia's aggression is not just about regional and territorial ambitions. Putin seeks to undermine NATO's credibility and upend the storied and essential transatlantic relationships that underpin Western success. When New Generation Warfare undermines societal resilience through weaponized migration, or critical infrastructure is attacked or perceived as vulnerable, allies begin to question reliability, global markets price in risk, and populations lose confidence in their governing institutions. Without robust security, the personnel, technologies, and systems needed to fight and win can be compromised, jeopardizing NATO's ability to prevail. Resilient critical infrastructures can partially mitigate the risk, but even more important is the cohesion and resilience of societies themselves. Russia's tactics across Europe are designed to break down the ability of nations to withstand cyber and physical attacks. If even one NATO ally begins to wobble in standing up to Russia, the rest of the alliance is at risk.

---

1. Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks*, March 11, 2016. (https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts)
2. Janis Berzins, "Not 'Hybrid' but New Generation Warfare," *The Jamestown Foundation*, February 2019. (https://www.researchgate.net/publication/331521752_Not_'Hybrid'_but_New_Generation_Warfare)
3. Kelly M. Greenhill, "When Migrants Become Weapons," *Foreign Affairs*, February 22, 2022. (https://www.foreignaffairs.com/articles/europe/2022-02-22/when-migrants-become-weapons)
4. Ibid.
5. Jyri Lavikainen, "Russia's hybrid operation at the Finnish border: Using migrants as a tool of influence," *FIIA Comment*, November 2023. (https://fiia.fi/en/publication/russias-hybrid-operation-at-the-finnish-border; Sonya Ciesnik, "Latvia presents evidence of organized migrant transfers through Belarus," *InfoMigrants* (EU), January 16, 2026. https://www.infomigrants.net/en/post/69256/latvia-presents-evidence-of-organized-migrant-transfers-through-belarus)
6. European Parliament, "Migration And Asylum In Central And Eastern Europe," accessed February 5, 2025. (https://www.europarl.europa.eu/workingpapers/libe/104/poland_en.htm)
7. "Thousands of migrants entered Poland on illegal visas, officials say," *tvp.info* (Poland), December 23, 2025. (https://www.polskieradio.pl/395/7784/Artykul/3625373,thousands-of-migrants-entered-poland-on-illegal-

visas%C2%A0officials-say); "Die Here or Go to Poland," *Human Rights Watch*, November 24, 2021. (https://www.hrw.org/report/2021/11/24/die-here-or-go-poland/belarus-and-polands-shared-responsibility-border-abuses)
8. "On Poland's Border, A Continued Pushback Against Migrants 'Weaponized' By Belarus," *Radio Free Europe*, June 4, 2024. (https://www.rferl.org/a/poland-russia-belarus-borders/32978538.html)
9. "МИД Беларуси: Минск рассмотрит ноту Варшавы по гибели польского военного [The Belarusian Foreign Ministry: Minsk will consider Warsaw's note regarding the death of a Polish soldier.]" *Sputnik* (Russia), June, 7, 2024. (https://sputnik.by/20240607/mid-belarusi-minsk-rassmotrit-notu-varshavy-po-gibeli-polskogo-voennogo--1086933698.html)
10. Dr. Lev Topor and Dr. Alexander Tabachnik, "Russian Cyber Information Warfare," *Marine Corp University Press*, accessed February 5, 2025. (https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-vol-12-no-1/Russian-Cyber-Information-Warfare)
11. Republic of Latvia, Ministry of Foreign Affairs, Press Release, "The Ministry of Foreign Affairs warns of the rapidly increasing number of Latvian nationals detained abroad for transporting illegal migrants," July 24, 2025. (https://www.mfa.gov.lv/en/article/ministry-foreign-affairs-warns-rapidly-increasing-number-latvian-nationals-detained-abroad-transporting-illegal-migrants)
12. Republic of Lithuania, Ministry of National Defense, Press Release, "NATO's team of experts on countering hybrid threats concludes its work in Lithuania," September 13, 2021. (https://kam.lt/en/natos-team-of-experts-on-countering-hybrid-threats-concludes-its-work-in-lithuania)
13. Sonya Ciesnik, "Latvia presents evidence of organized migrant transfers through Belarus," *InfoMigrants* (EU), January 16, 2026. (https://www.infomigrants.net/en/post/69256/latvia-presents-evidence-of-organized-migrant-transfers-through-belarus)
14. "Finland's crackdown on undocumented migrants sparks fear," *France 24* (France), November 1, 2025. (https://www.france24.com/en/live-news/20251101-finland-s-crackdown-on-undocumented-migrants-sparks-fear); "DISINFO: Finland organised the migration crisis as a pretext for closing borders after joining NATO," November 21, 2023. (https://euvsdisinfo.eu/report/finland-organised-the-migration-crisis-as-a-pretext-for-closing-borders-after-joining-nato)
15. The International Energy Agency, "Ukraine's Energy System Under Attack," September 19, 2024. (https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter/ukraines-energy-system-under-attack)
16. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Cyber-Attack Against Ukrainian Critical Infrastructure," July 20, 2021. (https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01)
17. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," May 9, 2022. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a)
18. Viasat, "KA-SAT Network Cyber Attack Overview," March 30, 2022. (https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview)
19. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "U.S. Government Attributes cyberattacks on SATCOM Networks to Russian State-Sponsored Malicious Cyber Actors," May 10, 2022. (https://www.cisa.gov/news-events/alerts/2022/05/10/us-government-attributes-cyberattacks-satcom-networks-russian-state-sponsored-malicious-cyber-actors)
20. European Council, Press Release, "Russian Cyber Operations Against Ukraine: Declaration by the High Representative on Behalf of the European Union," May 10, 2022. (https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union)
21. A.J. Vicens, "Russian military intelligence hackers likely behind December cyberattacks on Polish energy targets, researchers say," *Reuters*, January 23, 2026. (https://www.reuters.com/technology/russian-military-intelligence-hackers-likely-behind-december-cyberattacks-polish-2026-01-23); Maggie Miller, "Russian government hackers blamed for major recent cyberattack on Polish energy grid," *Politico*, January 26, 2026. (https://www.eenews.net/articles/russian-government-hackers-blamed-for-major-recent-cyberattack-on-polish-energy-grid)
22. North Atlantic Treaty Organization, "NATO to enhance military presence in the Baltic Sea," December 30, 2024. (https://www.nato.int/en/news-and-events/articles/news/2024/12/30/nato-to-enhance-military-presence-in-the-baltic-sea)

23. North Atlantic Treaty Organization, "NATO strengthens cooperation with industry to protect critical undersea infrastructure," May 27, 2025. (https://www.nato.int/en/news-and-events/articles/news/2025/05/26/nato-strengthens-cooperation-with-industry-to-protect-critical-undersea-infrastructure)
24. Anne Kauranen, "Finland hopes to prevent cable damage with new surveillance centre," *Reuters*, January 26, 2026. (https://www.reuters.com/world/finland-teams-up-with-eu-baltic-sea-states-enhance-undersea-infrastructure-2026-01-26)
25. Anne Kauranen, "Russia likely to keep trying to damage Baltic Sea infrastructure Finland says," *Reuters*, January 22, 2026. (https://www.reuters.com/business/aerospace-defense/russia-likely-keep-trying-damage-baltic-sea-infrastructure-finland-says-2026-01-22)
26. North Atlantic Treaty Organization, "Vilnius Summit Communiqué," July 11, 2023. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2023/07/11/vilnius-summit-communique)
27. North Atlantic Treaty Organization, "NATO Defence Ministers agree plan to lead coordination of security assistance and training for Ukraine, address deterrence and defence," June 14, 2024. (https://www.nato.int/en/news-and-events/articles/news/2024/06/14/nato-defence-ministers-agree-plan-to-lead-coordination-of-security-assistance-and-training-for-ukraine-address-deterrence-and-defence)
28. North Atlantic Treaty Organization, "Resilience in NATO," December 15, 2023. (https://www.act.nato.int/article/resilience-in-nato)
29. European Commission, "Joint Communication To The European Parliament And The Council On Military Mobility," November 19, 2025, pages 3-4. (https://defence-industry-space.ec.europa.eu/system/files/2022-11/Action%20plan%20on%20military%20mobility%202.0.pdf)
30. Ibid., page 3. (https://defence-industry-space.ec.europa.eu/system/files/2022-11/Action%20plan%20on%20military%20mobility%202.0.pdf); European Commission, "Commission Staff Working Document on Military Mobility," November 19, 2025, page 53. (https://transport.ec.europa.eu/document/download/c925bad5-7d13-4551-bfaa-03152dd468dd_en?filename=SWD_2025_847.pdf)
31. European Court of Auditors, "EU military mobility not yet in the fast lane," May 2, 2025. (https://www.eca.europa.eu/en/news/news-sr-2025-04)
32. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *WIRED*, August 22, 2018. (https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world)
33. North Atlantic Treaty Organization, "Washington Summit Declaration," July 10, 2024. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration)
34. North Atlantic Treaty Organization, "Ballistic Missile Defense," August 1, 2024. (https://www.nato.int/en/what-we-do/deterrence-and-defence/ballistic-missile-defence)
35. North Atlantic Treaty Organization, "Vilnius Summit Communiqué," July 11, 2023. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2023/07/11/vilnius-summit-communique)
36. North Atlantic Treaty Organization, "Updated Defence Production Action Plan," February 13, 2025. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/updated-defence-production-action-plan)
37. North Atlantic Treaty Organization, "Washington Summit Declaration," July 10, 2024. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration)
38. North Atlantic Treaty Organization, "The Hague Summit Declaration," June 25, 2025. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration)
39. North Atlantic Treaty Organization, "Multinational capability cooperation," July 30, 2025. (https://www.nato.int/en/what-we-do/deterrence-and-defence/multinational-capability-cooperation)