Two U.S. Air Force F-35A Lightning IIs assigned to Hill Air Force Base, Utah, and two Dassault Rafales assigned to Saint-Dizier–Robinson Air Base, France, break formation during flight over France, May 18, 2021, as part of exercise Atlantic Trident 21 (U.S. Air Force/ Alexander Cook)

All Quiet on the Eastern Front
NATO Civil-Military Deterrence of Russian Hybrid Warfare

By Andrew Underwood, Andrew Emery, Paul Haynsworth, and Jennifer Barnes

Major Andrew Underwood, USA, is Executive Assistant to the Deputy Director for Strategy, Plans, and Policy (J5), Europe, NATO, Russia. Colonel Andrew Emery, USAF, is the Space and Missile Defense Planner in the U.S. Military Delegation to the NATO Military Committee (JCS) at NATO Headquarters, Brussels, Belgium. Lieutenant Colonel Paul Haynsworth, USA, is currently serving in the Commander's Action Group in the NATO Special Operations Headquarters at Supreme Headquarters Allied Powers Europe, Mons, Belgium. Commander Jennifer Barnes, USN, most recently served in the Commander's Action Group at U.S. Africa Command Headquarters in Stuttgart, Germany.

Russia's 2014 invasion of and continued threats (and now active war) against Ukraine have forced the North Atlantic Treaty Organization (NATO) to acknowledge that the era of European territorial conquest has

Special tactics operators assigned to 352nd Special Operations Wing radio to Swedish C-130H during controlled landings and takeoffs in Sweden, November 9, 2020, to support bilateral exercise in Baltic Sea region (U.S. Army/Patrik Orcutt)

not ended. Despite its success at deterring Soviet aggression during the Cold War, NATO must evolve to effectively counter Russia's 21st-century model of illicit actions and activity against NATO members—often referred to as hybrid warfare. To achieve credible deterrence, NATO's policy and strategy instruments must focus on imposing costs on Russian adventurism and limiting the effectiveness of Russian hybrid warfare campaigns. The preparation of civil institutions and structures as part of deterrence warrants study. The Alliance should consider how future conflicts would likely manifest between NATO and Russia and how Allies and partners could collectively deny or decrease the benefits available to Russia through its hybrid warfare approach.

The term *hybrid warfare* (or *hybrid threats*) lacks a universally accepted definition,[1] and Department of Defense terminology predates the 2014 invasion.[2] Hybrid warfare can include conventional and unconventional forces or be carried out by other state and nonstate actors. It occurs across the diplomatic, informational, military, and economic dimensions of power. It may be overt but is just as often covert or clandestine, complicating attribution. Rather than attempting a formal definition, for the purpose of this article hybrid warfare refers to all available means undertaken by a state—in this case, Russia—across all power dimensions, including through intermediaries, to achieve its objectives against an adversary in such a manner that does not give rise to traditional war.

Russia uses hybrid warfare (though it does not name it as such; the term originates in the West) to advance national objectives using means not typically considered clear acts of war to manipulate facts on the ground without provoking external intervention.[3] It is, in effect, delivering a fait accompli before its adversaries can respond. For its part, the joint European Union (EU)–NATO European Centre of Excellence for Countering Hybrid Threats defines *hybrid warfare* as "an action conducted by state or non-state actors, whose goal is to undermine or harm a target by combining overt and covert military and non-military means."[4]

Effective deterrence and defense require credibility, capability, and communication.[5] Major NATO policy statements over the past decade from Warsaw, Wales, Brussels, and London mention "an appropriate mix of nuclear, conventional, and missile defence capabilities" as the primary components of the Alliance's deterrence posture.[6] Deterrence in this context should be considered in terms of cost and benefit—one could deter an adversary by increasing the costs for taking action, reducing the benefit of taking action, or ideally both, to encourage adversary restraint. The 2019 London Declaration acknowledges the need to "prepare for, deter, and defend against hybrid tactics" but fails to articulate *how* the Alliance should proceed.[7] Since Russian hybrid warfare manifests in ways clearly distinct from direct armed conflict between states, the use of military means in response might be difficult to legitimize. Just as hybrid warfare has evolved, responses to hybrid warfare must evolve and expand into other domains.

Building on NATO's work, thinking, and publications on countering hybrid/gray zone warfare, the analysis presented here provides a framework on the Soviet and contemporary Russian methods within the current operational environment. It then proposes specific actions that NATO must adopt to impose costs on or deny benefits to Russia for employing these tactics, while also encouraging Russian restraint against future hybrid warfare.

Framework to Consider Russian Hybrid Warfare

Hybrid warfare is not a new concept for Russia. The Soviet use of special forces, secret police, KGB (*Komitet Gosudarstvennoy Bezopasnosti*, Committee for State Security) agents, and other means to create political influence, manipulate perceptions, and undermine the spread of democracy is well documented. President John F. Kennedy described the Soviet Union as a "tightly knit, highly efficient machine that combines military, diplomatic, intelligence, economic, scientific, and political operations."[8] Similarly, in 2017, RAND identified six primary types of Russian hybrid activity: information operations, cyber, proxies, economic influence, clandestine measures, and political influence.[9] What the Cold War–era tactics highlighted by Kennedy captured is a blurred nondelineation of norms and practices applied both internally and externally to achieve objectives. Moreover, these tactics continue to this day. This distinction among activities and domains remains novel to many (though certainly not all) of NATO's members.

Russia leveraged ethnic Russians as deniable proxies to stoke instability in Estonia in 2007 while simultaneously conducting cyber attacks.[10] The next year, Russia encouraged separatism within South Ossetia and Abkhazia and surged mercenaries and volunteers into the region, before transitioning to open conflict as its "peacekeeping" force took direct action and conquered Georgian territory in August 2008.[11] Russia's success in employing hybrid warfare tools perhaps emboldened the state to undertake a grand-scale, near-seamless synchronization of hybrid activity that ultimately achieved the objectives of seizing and integrating Crimea and introducing a contested battleground within eastern Ukraine in 2014. Russia's comprehensive hybrid campaign was as successful on the battlegrounds of Crimea and southeastern Ukraine as it was in winning within the international rules-based order. Despite the objections of the plurality of nations, Crimea remains under Russian political control today, the contested area in eastern Ukraine remains a warm frozen conflict (which Ukraine refers to as the Anti-Terrorist Zone), and the threat of broader armed Russian incursion remains.[12]

During the Cold War, the Soviet Union employed hybrid warfare as a tool of global power competition to further the ideological struggle between communism and capitalism. Russia's contemporary use of these operations is not as easily linked with an ideological narrative. Some argue that Russian actions are driven by President Vladimir Putin's desire for other nations—and especially the United States—to acknowledge and respect Russia.[13] Others contend that NATO member expansions, activities, and partnerships threaten Russia.[14] Russian activity and objectives likely cover the gamut of Putin's international and domestic priorities, from Moscow to the former Soviet states, to all of Europe and around the globe.

As the greatest power among the former Soviet states and the Soviet Union's geopolitical successor, Russia wants to retain regional influence and be the region's preeminent partner over others, such as the EU or the United States. When many of these states aligned with NATO or the EU in the post–Cold War era, it was as much a rejection of Russia's influence as it was a threat to Russia's geopolitical future. Estonia, Georgia, and Ukraine have suffered Russia's hybrid retaliation in response.

Russia's desire for legitimacy as a Great Power extends beyond its "near abroad" into the rest of Europe and around the world. Despite shared heritage with many European nations, Russia's frequent rejection of Western norms has kept Europe from fully embracing post–Cold War Russia into its clique. Exacerbating this gulf, Russia uses its hybrid muscle to undermine the European rules-based institutional framework.[15] It focuses its hybrid energies to ensure Russian operations can continue unconstrained by the European Union while attempting to fracture the NATO alliance. The invasion of Ukraine was a masterstroke at asserting its Great Power status, challenging the European security architecture, and demonstrating the impotence of the rules-based international order in constraining its actions.

Russia's objectives appear to be to cement its own internal political legitimacy through restoring its international prestige as a Great Power, asserting regional influence across Europe, and undermining liberal Western democratic institutions. Russian threats of broader conflict or actions might indicate broader desires. Regardless, Russia uses a variety of methods of hybrid warfare to advance these goals, which can be categorized into three areas: activity that might be considered immoral or unethical by the United States and other nations but is not illegal (such as economic or political coercion), activity that occurs within the gaps and seams of international law and norms (such as cyber activity), or activity that is clearly in violation of international law or agreed norms but is not easily or clearly attributable to Russia as a state actor (such as intra- and extraterritorial assassinations). Given this intentional ambiguity surrounding Russia's malign activity, deterring hybrid warfare is distinct from the context and logic of NATO's conventional and strategic deterrence efforts during the Cold War.

Army Soldiers assigned to 1st Battalion, 319th Airborne Field Artillery Regiment, 3rd Brigade Combat Team, 82nd Airborne Division, operate M-777 Howitzer during live-fire exercise as part of Swift Response 21 at Tapa Central Training Area, Estonia, May 10, 2021 (U.S. Army/Michael Gresso)

A POS
AIRBORNE
AA

Deterrence in a Hybrid Warfare Context

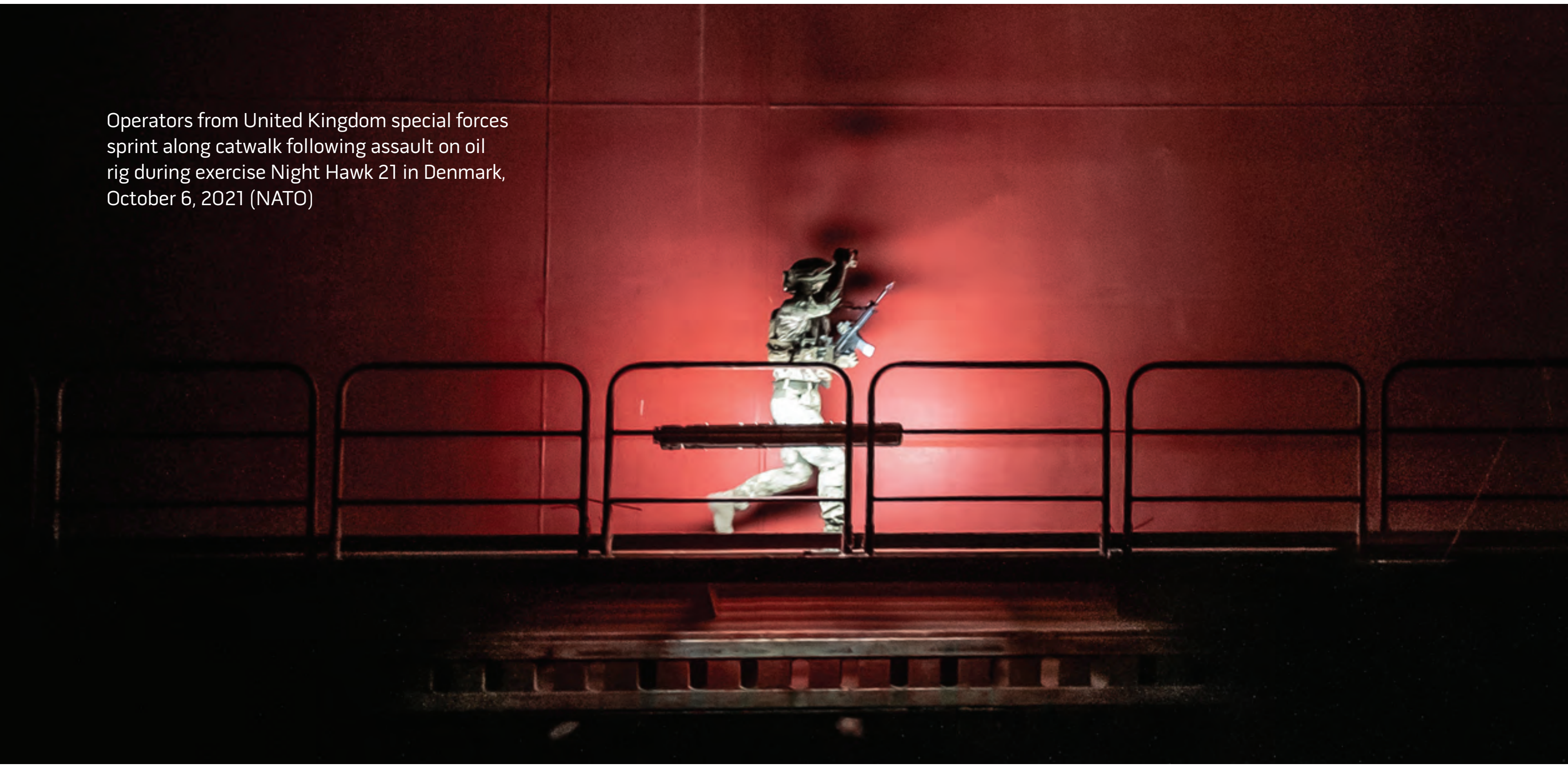
Traditional Cold War deterrence used the capability/credibility/communication model within the context of mutually assured nuclear annihilation, and—despite academic debates about causality—it appears to have worked. Perhaps the most useful reframing of the problem is to consider hybrid warfare not as a single *thing* to be deterred. Rather, it is a *continuum* of activity synchronized to achieve a strategic objective, and it requires a collection of deterrence activity to reduce its likelihood and impact.

To deter Russia's use of hybrid warfare, the nation's operational approach must first be analyzed via component activities. Then, deterrence strategies that seek to impose costs and deny benefit should be created for each activity to limit Russian strategic flexibility and choice. While NATO can work within the Alliance to deny benefits for hybrid tactics, it lacks the ability to respond efficiently—or at all—as a unified front to impose costs by way of punishment. It is unlikely that a hybrid attack below the level of armed conflict against a NATO member would be met with a unified NATO response. This is not necessarily a weakness, since NATO is not designed to engage in retributive attacks that do not meet the criteria for an Article V response.[16] However, as deterrence *credibility* hinges on a strong multilateral response, even if the response originated as a non-Alliance effort, it must appear to be a collective response within NATO's consensus-based decisionmaking process.

Ways and Means to Deter Hybrid Warfare

Comprehensive Defense. If Russia employs all available means of national power in a hybrid warfare campaign, how could NATO equally mobilize resources to counter the threat? The first pillar to this answer is the concept of comprehensive defense. In comprehensive defense, policymakers designate their uniformed military forces as the focal point around which to organize a whole-of-society approach to national defense. This approach seeks to leverage the unique skills and capabilities of the military within joint military–civil society initiatives that respond to complex security threats that no single institution acting alone could fully confront or effectively defeat. In this model, military forces drive unity of effort by organizing, training, motivating, and as appropriate, equipping the remaining population to achieve strategic objectives. By engaging the whole of their populations prior to a hybrid warfare campaign, NATO's Allies and partners could provide a multilayer defense to counter and preempt the full-court press of Russia's hybrid warfare strategy. Although defense and cost imposition occur on a continuum, the strategy can best be conceptualized using three distinct stages: baseline activities, competition below armed conflict, and armed conflict.

During baseline activities, comprehensive defense could be used to signal intent, build credible defense capability, and counter potentially hostile messaging campaigns against the population. Once organized into territorial defense units, auxiliary corps, neighborhood watches, concerned citizens groups, or any other number of structured organizations,



Operators from United Kingdom special forces sprint along catwalk following assault on oil rig during exercise Night Hawk 21 in Denmark, October 6, 2021 (NATO) a nation's populace transforms from a potential target to a protective force. Instead of being ripe for exploitation by hybrid warfare tactics, a nation's population becomes a deterrence against them. Additionally, the act of organizing one's populace signals a nation's intent *not* to be a soft target for belligerent nations to manipulate. Once effectively transmitted, this signal alters the risk analysis of any country considering the use of hybrid warfare tactics. This is especially important in regions with ethnically Russian populations, such as Crimea or the Latgale region of Latvia, which are often the target of Russian hybrid activities. Organizing and uniting these populations with their states in advance places the initiative squarely on the friendly nation and denies many of the tactical advantages that Russian hybrid warfare relies on. Utilizing a whole-of-society approach amplifies the credibility of a nation's military defenses. A side benefit of organizing a country's population for comprehensive defense is that civilian organizations could also perform critical functions outside of countering hybrid warfare tactics. For example, maritime auxiliary units could perform migration control–related tasks, and neighborhood watches could provide tips to fight organized crime or prevent acts of terrorism. Importantly, funding territorial defense units would allow a country to meet NATO defense spending targets while stimulating its own economy.

During competition below armed conflict, a nation's population could expose Russian actions, gather and pass intelligence, and counter Russian information operations (IO). A well-organized, informed, and motivated civilian population could be used to counter this aspect of hybrid warfare by denying an aggressor the ability to exert dominance in the information domain. Open-source and social media investigative organizations have already proved potent at countering Russian IO. Bellingcat, an independent collective of researchers and journalists, utilized simple, concrete investigative techniques to disprove numerous Russian disinformation campaigns, from their responsibility in the downing of Malaysian Airliner MH17 over Ukraine to poisonings by Russia throughout Europe.[17]

Bellingcat shows the power of the public to counter IO. Trained by their military counterparts with similar capabilities (such as civil and public affairs or military intelligence and security forces), civilian organizations that understand the indicators of Russian hybrid warfare could identify and report malign activity—either to official government channels (becoming intelligence) or through the public domain (exposing the malign activity), informing populations in NATO and around the globe. This is especially important in areas with a large Russian diaspora or ethnic Russian population. The Alliance already recognizes that it faces Russian IO and combats the messaging in the Russian language.[18] Yet NATO need not assume sole responsibility to counter these threats. By organizing, educating, and training the population, a state could preempt and negate future Russian attempts to influence or take advantage of these vulnerable sectors. Additionally, both intelligence and information generated from organizing one's population are effective methods of imposing costs and limiting strategic options. Accurate and timely intelligence could support friendly nation counteractions while

broad exposure of malign activity helps build coalitions and sway public opinion. Timing is critical in this aspect of comprehensive defense—the earlier a population could accurately identify and report malign activity, the easier it would be for NATO's members and partners to develop and implement a rapid response.

Finally, an organized and focused population could be used to supplement police forces, provide critical logistics and intelligence, and even augment friendly military forces during the transition from competition into armed conflict. The Russian hybrid warfare model has included a degree of armed (violent) conflict, although to a lesser intensity than the traditional fighting that would be a part of state-on-state armed conflict. For example, in eastern Ukraine, Russia's hybrid warfare model quickly advanced from organizing demonstrations to the armed seizure of government buildings and military facilities.

During armed conflict, comprehensive defense could provide NATO members and partners with a large pool of resources. The concept of comprehensive defense also allows a nation to maintain this basic military capability at a much lower cost compared with maintaining a large active-duty force. History is replete with examples of nations rapidly expanding their military forces at the beginning of armed conflict—comprehensive defense provides the framework to do so and the deterrence against aggressors who seek to avoid this escalation.

Several aspects of comprehensive defense are already being implemented in the Baltic states. According to a 2019 RAND report, "total defense and unconventional warfare techniques and forces can support deterrence, early warning, de-escalation, [and] defense against invading forces."[19] Estonia, Latvia, and Lithuania, as well as Poland, are increasing the capability of their territorial forces, national guards, and reserve forces and generating whole-of-society resilience and resistance efforts. These efforts to organize and engage the population are proving critical to counter Russian hybrid warfare efforts in the Baltics and should be used by all threatened NATO members and partners as a template to combat Russian hybrid warfare. Individual members should seek to bolster comprehensive defense among Allies with every training event, exercise, or deployment available to NATO. Coordination with EU initiatives is a further mechanism to enable NATO members to pursue comprehensive defense. Initiatives such as the enhanced forward presence and tailored forward presence provide platforms for members to work together on comprehensive defense in addition to multinational conventional interoperability. U.S. joint force rotations are particularly capable of bolstering comprehensive defense through deterrence activities (such as the bomber task forces), intelligence support to the Alliance, deescalation, or if needed, defense with rotational presence.

Information Operations. Another critical aspect of imposing costs and limiting options available through Russia's hybrid warfare approach is effective IO attribution and response. IO is substantive enough a factor in Russian hybrid warfare to be considered beyond comprehensive defense. Staying abreast of Russian hybrid objectives, methods, and tools prevents Allies and partners from being caught flat-footed. It also enables a better understanding of Russian intent and options for hybrid activity, both in traditional spheres and within the gaps and seams of 21st-century technology as an information platform. This analysis focuses on the intelligence- and information-gathering and strategic communication aspects of IO. Intelligence- and information-gathering are critical to identify Russia's hybrid options and intent and to mobilize NATO member states toward the activity. Conversely, strategic communication is a proactive, comprehensive defense measure to specifically limit Russian hybrid options and to broadcast the costs Russia would incur if it moved forward with them.

For intelligence-gathering to be effective in today's operating environment, countries must be willing to break down stovepipes and widely share information within their own government structures as well as with Allies and partners. The coordinated actions of hybrid warfare allow Russia to exploit regional, national, and international seams. Building intelligence-sharing apparatuses both within and without ministries among and across countries helps to close those seams. Effective intelligence-sharing could occur at levels ranging from joint/multinational collection teams to finished intelligence analysis at ministerial or national levels. In other words, information-sharing does not always have to be top-down driven; sometimes bottom-up is effective.

One goal of shared intelligence is to reduce the time required for NATO to consult and respond in part or as a whole. This effort could be facilitated by a common intelligence picture shared by all parties. Partial, inconsistent, or stovepiped intelligence might slow NATO's response process by creating doubt or failing to correctly attribute malign activity to the Russian government. In addition, whether internal to a state or between allied states, stovepiping challenges coordinated action against hybrid warfare. Better intelligence-sharing would allow states to deny Russia the benefit of using IO techniques in hybrid warfare to isolate specific states or populations. A common intelligence picture also makes it more likely, for example, that a Russian intelligence operative or team preparing to assassinate a dissident would be identified and detained, and have the network and messaging compromised. An example of intelligence-sharing success within NATO nations against hybrid activity is the Baltic Special Operations Forces Intelligence Fusion Cell, a budding Estonian, Latvian, Lithuanian, and Polish initiative that operates with assistance from the United States.[20] If implemented properly, such intelligence fusion cells might provide key indications and warnings of Russian hybrid warfare operations across the spectrum of IO, denying Russia the benefit of being able to claim noninvolvement/noninterference and could serve as a template for future initiatives among other Allies and partners. Furthermore, such fusion cells provide a path for connecting information across the Alliance's multiple stovepipes, that is, the intra- and inter-bureaucratic inertia and the multilingual nature of the information environment. This enables

Army jumpmaster assigned to 1st Squadron, 91st Cavalry Regiment, 173rd Airborne Brigade, inspects paratroop door on C-130 Hercules before exiting paratroopers from III Infantry Brigade, Georgian Defence Force, during exercise Agile Spirit 21, Vaziani Training Area, Tbilisi, Georgia, August 1, 2021 (U.S. Army/John Yountz)

a common intelligence picture and, consequently, the ability of the Allies to collectively deny Russian IO to access seams unfettered and without attribution.

Once Russian hybrid warfare IO activity is recognized and NATO agrees a response is appropriate, strategic communication would likely be employed as the principal countermeasure and vanguard to prevent Russian activity. The situational awareness derived from the shared information and intelligence discussed in the previous section would be critical to crafting targeted messages. Strategic communication would likely be split between two audiences: external actors and an audience internal to the conflict (that is, the targeted population). Internal strategic communication efforts should focus on countering the information aspect of hybrid warfare. Prior to a campaign, successful strategic communication might limit the vulnerability to target audiences, such as the Russian-speaking minorities of the Baltic states, or a Russian hybrid campaign. This is achieved by negating Russia's plausible deniability concerning the sponsorship of the conflict's version of "little green men" (or whatever the aggressor looks like in that campaign). Internal strategic messaging campaigns must be swiftly organized and executed because they are most effective if they prevent Russia from gaining a tactical advantage during the initial "fog of war" period. Once a hybrid warfare campaign has begun, the focus of external strategic communication should be to expose Russian activities to NATO (and the rest of the world). This might undermine Russian public support for such activities, would inform decisionmakers during NATO deliberations, and should unite the international community against the malign actor.

Ally and Partner Contribution and Collaboration. Comprehensive defense enables unity of effort across militaries, governmental institutions, and societies within the Alliance. This unity of effort requires a strategic evolution within NATO, particularly in understanding and combating nonstandard aggression outside the traditional attacks or threats captured within Article IV and Article V of the Washington Treaty.[21] NATO member states and partners have tremendous capacity beyond their armed forces to deter Russian hybrid warfare activity and impose costs. Experience and specialization among NATO's members allow for nuanced strategic planning to anticipate and respond to the use of hybrid warfare and enable distinct capacities to be employed to impose costs. NATO leadership could harmonize efforts and ensure that resistance measures synthesize among member states.

Simplifying hybrid warfare deterrence means analyzing synchronized Russian activities and countering them separately. To this end, individual member states might utilize and reinforce their civil and military strengths to combat discrete hybrid activities. NATO should complement these efforts and enable specialization and interconnectedness among Allies. In the traditional military model, NATO desires uniformity and interoperability. Against hybrid activities, individual member states' niche capabilities and strengths are assets. For example, after the unprecedented 2007 Russian cyber attack on Estonia targeting nonmilitary infrastructure via nonstandard means, Estonia revolutionized its cyber capability and capacity in both military and civilian infrastructure and expertise.[22] Estonia's encryption and defense of its electronic systems led in generating civil-government cooperation, and Estonia understands how Russian cyber activity regularly targets its information technology networks. This development helps to deter Russian attacks. Furthermore, the ability to attribute such activity by an Ally helps the collective Alliance impose costs, which, as former Estonian President Toomas Hendrik Ilves demonstrated, need not be responded to in-kind in the cyber environment.[23] Alliance members could respond with other instruments of power (for example, diplomatic or economic) as the result of individual member strengths. This proficiency demonstrates how one Ally could contribute to the security of all. As a regional leader in cyber security, Estonia now serves as a capacity and capability vanguard for the other Allies, from whom Allies should learn and grow. For example, U.S. Cyber Command recently collaborated with its Estonian counterparts to strengthen both nations' cyber defenses.[24]

Indeed, while NATO is perceived to be at a disadvantage because it comprises 30 states with 30 different national priorities, strategies, interests, and militaries, NATO's diversity could also be a source of strength. Allies could spearhead initiatives based on their strengths and share the boon of their efforts. There is significant capacity among Allies to build resistance networks that would impose costs. Poland and the three Baltic states are among those NATO members that have militias or civil institutions organized to combat occupation. These forces could also partner with other elements, such as border guards and police forces, to ensure that a nonstandard attack or provocation is prevented or subverted to deny hybrid warfare options to Russia and encourage restraint.

Other partners have experience with Russian hybrid warfare threats, often at a level much higher than other NATO nations. NATO could learn tremendously through the expansion of cooperation with Georgia and Ukraine, both of which have suffered for years from Russia's hybrid activity. Both nations have adapted to multiple issues—occupied terrain, denied access to populations, and competition over media narratives and legitimacy, as well as a constant pressure on their political, civil, and social institutions.

Ukrainian and Georgian partnership with NATO members is strong. Multiple initiatives exist to help modernize and professionalize the Ukrainian military. One notable example is the Comprehensive Assistance Package, which NATO members pledged to in the Warsaw 2016 Summit, and which explicitly identified hybrid warfare among its topic areas.[25] These initiatives guide NATO support to Ukraine and enable dialogue, including a joint platform on hybrid warfare last held in November 2018.[26] This platform should continue, as such collaborations could harden both Ukraine and the Alliance to hybrid warfare. Likewise, similar platforms should be built on and expanded to target Russia's calculus and prevent hybrid warfare against critical partners.

While Russian hybrid efforts stalled Georgia's 2008 Membership Action Plan into NATO, it has not halted continued partnership and collaboration.[27] The 2016 Substantive NATO-Georgia Package, a broad set of initiatives designed to modernize Georgia's military and achieve NATO interoperability because of the Wales Summit, oddly omits discussion of hybrid warfare.[28] This presents an opportunity for NATO to develop hybrid warfare platforms (like those with Ukraine) to collaborate with Georgia on. Through partnerships and collaborations such as these, NATO could learn from previous experiences and be better prepared to prevent future hybrid threats.

Conclusion

As Russia has evolved to increasingly rely on hybrid warfare as a major component of its strategy, NATO must adapt accordingly. NATO's model must shift from a reliance on traditional military deterrence and expand to incorporate political, economic, and social spheres to counter aggression below the level of armed conflict. Since NATO's structure does not readily support innovation or active (versus passive) deterrence measures, new ideas and emphases are needed to address these challenges.

Pursuing activities to deter hybrid warfare certainly poses risks and challenges to NATO and its member states and partners. Activities in these spheres might risk further blurring lines between military and nonmilitary responsibilities. Individual member laws and EU regulations might complicate these efforts. Civil institutions could be at risk of being identified as military targets in the event of a linear war.

Consequently, Allies and partners must update their methods to better deter Russian aggression by reducing Russia's strategic options and increasing their own ability to impose costs. Imposition of costs via Allies' domains of diplomatic, information, military, and economic levers are central to changing Russia's cost-benefit assessment regarding hybrid warfare and enabling deterrence. Doing this could be achieved through such concepts as comprehensive defense, improved IO, and expanded allied member and partner collaboration. While the overall goal of maintaining Alliance unity and solidarity remains the same, the means and ways through which Allies and partners achieve that goal should change. This includes embracing the diversity of members' strengths and capabilities and exploring increased partnerships with non-NATO members to leverage and learn from their experience with Russian hybrid warfare aggression.

The primary limitation of this analysis is the inability to prove the effectiveness of this proposal in deterring future Russian hybrid warfare. As deterrence prevents action, how does one measure inaction? How could one attribute causation? To this end, the lessons of nuclear deterrence during the Cold War might hold some answers. Further examination of academic literature and public policy best practices could help to identify and develop measures of deterrence effectiveness. Once this framework or methodology is established, the hypotheses and proposals laid out in this article could be tested like those at the height of the Cold War. **JFQ**

Notes

[1] James K. Wither, “Making Sense of Hybrid Warfare,” *Connections* 15, no. 2 (2016), 73–87.

[2] *Hybrid Warfare*, GAO-10-1036R (Washington, DC: U.S. Government Accountability Office [GAO], September 10, 2010), 1–19, available at <https://www.gao.gov/products/gao-10-1036r>.

[3] Wither, “Making Sense of Hybrid Warfare,” 79–81. Note that Russian terminology includes the terms *new generation warfare* as well as *nonlinear war*.

[4] The European Centre of Excellence for Countering Hybrid Threats, “Hybrid Threats,” available at <https://www.hybridcoe.fi/hybrid-threats/>.

[5] Kestutis Paulauskas, “On Deterrence,” *NATO Review*, August 5, 2016, available at <https://www.nato.int/docu/review/articles/2016/08/05/on-deterrence/index.html>.

[6] North Atlantic Treaty Organization (NATO), “London Declaration,” press release, December 4, 2019, available at <https://www.nato.int/cps/en/natohq/official_texts_171584.htm>.

[7] Ibid.

[8] John F. Kennedy, “The President and the Press: Address Before the American Newspaper Publishers Association, April 27, 1961,” Waldorf Astoria Hotel, New York City, John F. Kennedy Presidential Library and Museum, available at <https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/american-newspaper-publishers-association-19610427>.

[9] Christopher S. Chivvis, *Understanding Russian “Hybrid Warfare” and What Can Be Done About It*, Testimony Before the House Armed Services Committee, 115th Cong., 1st sess., March 22, 2017, available at <https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf>.

[10] “Estonia Fines Man for ‘Cyber War,’” BBC News, January 25, 2008, available at <http://news.bbc.co.uk/2/hi/technology/7208511.stm>.

[11] European Union, *Independent International Fact-Finding Mission on the Conflict in Georgia*, vol. 1 (September 2009), 18–22, available at <https://www.echr.coe.int/Documents/HUDOC_38263_08_Annexes_ENG.pdf>.

[12] For recent reference, see United Nations, “Resolutions Calling on Withdrawal of Forces from Crimea, Establishing Epidemic Preparedness International Day Among Texts Adopted by General Assembly,” press release, December 7, 2020, available at <https://www.un.org/press/en/2020/ga12295.doc.htm>.

[13] Fiona Hill, “This Is What Putin Really Wants,” Brookings, February 24, 2015, available at <https://www.brookings.edu/opinions/this-is-what-putin-really-wants/>; Julia Ioffe, “What Putin Really Wants,” *The Atlantic*, January/February 2018, available at <https://www.theatlantic.com/magazine/archive/2018/01/putins-game/546548/>.

[14] Uğur Celil Özgöker and Serdar Yilmaz, “NATO and Russia’s Security Dilemma Within the European Union’s Far Neighbors,” *International Relations and Diplomacy* 4, no. 10 (October 2016), 650–665.

[15] Bettina Renz and Hanna Smith, *Russia and Hybrid Warfare—Going Beyond the Label*, Aleksanteri Papers (Helsinki, Finland: Kikimora Publications at the Aleksanteri Institute, University of Helsinki, January 2016), available at <https://helda.helsinki.fi/bitstream/handle/10138/175291/renz_smith_russia_and_hybrid_warfare.pdf>.

[16] Article V of the Washington Treaty clarifies and affirms NATO members to collective defense in the event of an attack. See NATO, “The North Atlantic Treaty,” updated April 10, 2019, available at <https://www.nato.int/cps/en/natolive/official_texts_17120.htm>.

[17] Bellingcat, “About,” available at <https://www.bellingcat.com/about>.

[18] NATO, “NATO’s Approach to Countering Disinformation: A Focus on COVID-19,” updated July 17, 2020, available at <https://www.nato.int/cps/en/natohq/177273.htm>.

[19] The concepts of *total defense* and *unconventional warfare* are like the concept of *comprehensive defense*. The authors define *total defense* as “a whole-of-society approach to national defense and resilience . . . and broad-based, state-supported resistance against invaders . . . designed to enhance deterrence by denial and by increasing the cost of aggression.” This mutually supporting idea provides an example of how comprehensive defense is naturally evolving in the Baltics in response to potential Russian aggression. See Stephen J. Flanagan et al., *Deterring Russian Aggression in the Baltic States Through Resilience and Resistance* (Santa Monica, CA: RAND, 2019), 1, available at <https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2779/RAND_RR2779.pdf>.

[20] “How the Baltic States Spot the Kremlin’s Agents,” *The Economist*, August 1, 2019, available at <https://www.economist.com/europe/2019/08/01/how-the-baltic-states-spot-the-kremlins-agents>.

[21] Article IV of the Washington Treaty enables consultations among the Allies whenever the “territorial integrity, political independence or security” of any member is threatened. Article V clarifies and affirms the members to collective defense in the event of an attack. See NATO, “The North Atlantic Treaty.”

[22] Alison Lawlor Russell, *Cyber Blockades* (Washington, DC: Georgetown University Press, 2014), 69–72.

[23] Toomas Hendrik Ilves, “The Consequences of Cyber Attacks,” *Journal of International Affairs* 70, no. 1 (2016), 175–181.

[24] U.S. Cyber Command, “Hunt Forward Estonia: Estonia, U.S. Strengthen Partnership in Cyber Domain with Joint Operation,” December 3, 2020, available at <https://www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/>.

[25] NATO, “Relations with Ukraine,” updated January 11, 2020, available at <https://www.nato.int/cps/en/natolive/topics_37750.htm>.

[26] *NATO’s Support to Ukraine*, NATO factsheet (Brussels: NATO, November 2018), available at <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_11/20181106_1811-factsheet-nato-ukraine-sup.pdf>.

[27] Daniel Dombey, “U.S. Gives Way on NATO for Georgia and Ukraine,” *Financial Times*, November 26, 2008, available at <https://www.ft.com/content/b48201e0-bc00-11dd-80e9-0000779fd18c>; NATO, “Relations with Georgia,” updated August 25, 2021, available at <https://www.nato.int/cps/en/natohq/topics_38988.htm>.

[28] *Substantial NATO-Georgia Package (SNGP)*, NATO factsheet (Brussels: NATO, 2017), available at <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170221_1702-georgia-sngp-factsheet-en.pdf>.