Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Jim Derleth & Jeff Pickler
Connections QJ 21, no. 2 (2022): 11-23
https://doi.org/10.11610/Connections.21.2.01

Research Article

Twenty-first Century Threats Require Twenty-first Century Deterrence

Jim Derleth and Jeff Pickler

George C. Marshall European Center for Security Studies,
https://www.marshallcenter.org/en

Abstract: During the competition between the United States and the Soviet Union (USSR) after World War II, deterrence emerged as the primary U.S. security strategy. Historically, the USA focused on deterring conventional and nuclear threats. While this helped prevent a direct military conflict between the two superpowers, it did not end their political rivalry, simply pushing it into areas that decreased the risk of open military conflict. During the Cold War, both the USA and USSR used irregular tactics to try and achieve their strategic objectives in the grey zone, the area below the threshold for "use of force" or "armed attack" as described in the United Nations Charter. Technology limited the effectiveness of irregular tactics, not considered significant national security threats. Today, a globalized, interconnected, and ubiquitous information environment provides numerous opportunities for adversaries to achieve strategic objectives without crossing the strategic threshold that would have historically provoked a military response.

An increase in irregular attacks shows that while deterrence has continued to prevent large-scale military conflict between the major powers, it has failed to prevent aggression in the grey zone. From the Baltics to the Caucuses, Russia has repeatedly demonstrated how irregular tactics can achieve strategic objectives without fear of an unacceptable counteraction. Trends in national power, interdependence, and technology suggest Russia and other adversaries will continue to increase their ability to exploit the grey zone vulnerabilities. A deterrence policy focused solely on conventional and nuclear forces is no longer sufficient. To deter irregular tactics, the United States must develop a 21st-century deterrence strategy. This need will only grow as Russia tries to offset its military failures in

Ukraine. With Russian conventional forces weakened, Russia will increasingly rely on irregular tactics to attack its adversaries. This paper examines the declining relevance of traditional conventional and nuclear-focused deterrence strategies and argues that deterrence should be modified to remain relevant against 21st-century threats.

Keywords: deterrence, Russia, hybrid threats, irregular warfare, grey zone, national security.

Introduction

Soon after the defeat of Germany in World War II, the USA and the USSR found themselves in a global struggle for power and influence. In contrast to previous great power competitions, which often led to armed conflict, nuclear weapons changed the risk calculus for both sides. This had four key consequences. First, to decrease the likelihood of conflict and escalation, both the USA and USSR adopted irregular tactics.[1] Second, it pushed the competition into the grey zone below the level of traditional inter-state conflict.[2] Third, since combat operations between nuclear-armed adversaries could lead to their mutual annihilation, military force would now be primarily used for "coercion, intimidation, and deterrence." [3] Fourth, as can be seen in Vietnam and Afghanistan, it pushed armed conflict onto the competitors' proxies.

This led to the United States adopting a deterrence policy. Its adoption was a significant change for the military. As nuclear strategist Bernard Brodie noted: "thus far the chief purpose of our military establishment has been to win wars, from now on its chief purpose must be to avert them." [4] There are two traditional types of deterrence: deterrence by denial and deterrence by punishment. Deterrence by denial is based on an ability to deter actions by making them unlikely to succeed. Deterrence by punishment is the threat to impose costs—economic, military, political, or a combination—that are higher than the perceived benefits of aggression. Effective deterrence by denial or punishment are both predicated on the elaboration of clearly defined national interests ("red lines"), the capability to implement threatened actions, the credibility of will to execute them, and

[1] Irregular tactics exploit classical principles of strategy such as winning without fighting, measures short of war and salami-tactics. Contemporary examples include disinformation, cyberattacks, economic coercion, legal gamesmanship, and the use of proxies.

[2] Kathleen H. Hicks, "Russia in the Grey Zone," Commentary (Washington: Center for Strategic & International Studies, July 25, 2019), https://www.csis.org/analysis/russia-gray-zone.

[3] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 2008), 34. The goal of deterrence is to prevent an aggressor's potential course of action by convincing them that the costs or consequences of their action outweigh any potential gains. This definition is based on classic views of deterrence theory and practice.

[4] Andrew F. Krepinevich Jr., "The Eroding Balance of Terror: The Decline of Deterrence," *Foreign Affairs* (January/February 2019), https://www.foreignaffairs.com/eroding-balance-terror.

the ability to communicate with adversaries so that they understand the cost/benefits of a course of action.[5] Conventional and nuclear deterrence became the focal point for U.S. security for the next 50 years as the United States sought to achieve its strategic objectives while preventing a full-scale war.

Irregular Threats and Deterrence

Cold War deterrence was effective because the U.S. foreign policy kept strategic competition below the threshold of inter-state war. However, nuclear deterrence has long resulted in what Glenn Snyder described as a stability-instability paradox. "This holds that the more stable the nuclear balance, the more likely powers will engage in conflicts below the threshold of war." [6] This was true during the Cold War and remains true today. A 1981 State Department report highlighted irregular actions taken by the Soviet Union including "control of the press in foreign countries; outright and partial forgery of documents; rumors, insinuation, altered facts, and lies; use of international and local front organizations; clandestine operation of radio stations; exploitation of a nation's academic, political, economic, and media figures as collaborators to influence policies of the nation." [7] These efforts failed to achieve significant strategic impact due to the limitations of information technology and the bipolar geopolitical environment at the time. Today, because of changes in the global balance of power, the rise of a multipolar system, technology allowing states to directly target societal vulnerabilities, and interdependencies, states are much more vulnerable to irregular tactics. Russian interference in the 2016 U.S. presidential election and the 2020 SolarWinds data breach show that our adversaries can accomplish their strategic objectives at a low cost and with a limited risk of attribution or escalation.

---

[5] Elaborating upon these three key aspects of deterrence, capability is the means to influence behavior. Effective deterrence requires a range of capabilities to ensure any type of aggression will fail to achieve its objectives and/or has a credible risk of unbearable consequences for the adversary. Credibility is based on maintaining a level of believability that the stated deterrent actions will actually be implemented. Credibility requires having the capability to execute a variety of options and the willingness to employ them. Communicate means transmitting the intended message to the adversary one is trying to deter. Effective communication requires showing resolve to deny any benefits and/or impose costs on any adversarial actions.

[6] Glenn Snyder, *The Balance of Power and the Balance of Terror*, quoted in Michael Kofman, "Raiding and International Brigandry: Russia's Strategy for Great Power Competition," *War on the Rocks*, June 14, 2018, https://warontherocks.com/2018/06/raiding-and-international-brigandry-russias-strategy-for-great-power-competition/.

[7] "Soviet 'Active Measures': Forgery, Disinformation, Political Operations," Special Report No. 88 (Washington, DC: U.S. Department of State, Bureau of Public Affairs, October 1981), http://insidethecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20Forgery,%20Disinformation,%20Political%20Operations%20October%201981.pdf.

Notwithstanding these changes, the U.S. approach to deterrence remains largely the same as during the Cold War. It focuses on the use of conventional and nuclear forces to deter and, if necessary, defeat a peer adversary on the battlefield. The U.S. Army's current modernization efforts prioritize battlefield lethality, with billions of dollars poured into long-range precision fires, next-generation combat vehicles, future vertical lift platforms, the modernization of army network technologies, air and missile defense systems, and increasing the capability of individual soldiers' weapons. Training and exercises continue to focus on closing with and destroying a peer adversary through precision fires and maneuver. While capable and trained conventional and modern nuclear forces support deterrence, the last 15 years have shown that they do not deter cyberattacks, the use of proxies, disinformation campaigns, and other irregular tactics that dominate contemporary strategic competition. In contrast, our adversaries have incorporated changes in the strategic environment into their military strategies. For example, Russian Chief of the General Staff Gerasimov noted that the 'rules of war' have changed: "The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness." [8]

As Mark Galeotti noted in his book, *The Weaponisation of Everything*, "the world is now more complex and above all more inextricably interconnected than ever before… Wars without warfare, non-military conflicts fought with all kinds of other means, from subversion to sanctions, memes to murder, may be becoming the new normal." [9] This different strategic environment undermines our current deterrence strategy "…developments lead to an inescapable—and disturbing—conclusion: the greatest strategic challenge of the current era is neither the return of great-power rivalries nor the spread of advanced weaponry. It is the decline of deterrence." [10] This situation has numerous national security ramifications. Most importantly, it undermines conventional and nuclear deterrence and allows adversaries to act in the grey zone with impunity.[11] To change this situation, we need to change the cost-benefit calculus of Russia and other adversaries. In other words, we must develop an irregular threats deterrence strategy.

---

[8] Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," *Military Review* (January-February 2016): 30-38, 24, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf.

[9] Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War* (New Haven, CT: Yale University Press, 2022), 18.

[10] Krepinevich Jr., "The Eroding Balance of Terror."

[11] Sean Monaghan, "Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice," Hybrid CoE Paper 12 (Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats, March 31, 2022), 17, https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/.

Integrated Deterrence

Adversaries use lethal and non-lethal irregular tactics to achieve their objectives. Examples include the use of proxies, threats to critical infrastructure, threats to citizens (assassination, harassment, kidnapping, etc.), and interference in democratic or governmental functions. Therefore, U.S. national security requires the ability to deter irregular threats. In the 2021 Interim National Security Strategic Guidance, President Biden pledged to "develop capabilities to better compete and deter gray-zone actions." [12] Since taking office, Secretary of Defense Austin noted that the United States needed a new way of approaching deterrence which would "impose costs where necessary, while using all of our tools to lower the risk of escalation with our adversaries and respond to challenges below the level of armed conflict." This new policy was called "integrated deterrence." [13]

Colin Kahl, the Undersecretary of Defense for Policy described integrated deterrence as informing "almost everything that we do… integrated across domains, so conventional, nuclear, cyber, space, informational, across theaters of competition and potential conflict [and] integrated across the spectrum of conflict from high intensity warfare to the gray zone." Integrated deterrence also includes the integration of all elements of national power. Kahl noted that while deterrence has been the focus of U.S. strategy since the Cold War, it has a different meaning as part of integrated deterrence: "we need to think about deterrence differently given the existing security environment, and the potential scenarios for conflict that we're trying to deter…The Department of Defense needs to have the capabilities and the concepts to deny the type of rapid fait accompli scenarios that we know potential adversaries are contemplating." [14]

While the components of integrated deterrence have yet to be fully elaborated, to deter irregular threats, this strategy should include both the ability to "punish" an aggressor state using irregular tactics and "deny" it the ability to significantly impact the target state.[15] Like traditional deterrence, integrated deterrence requires identifying and communicating "red lines" to adversaries.

---

[12] President of the United States, "Interim National Security Strategic Guidance" (Washington, D.C.: The White House, March 2021), https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

[13] Lloyd Austin, "Message to the Force" (Washington, D.C.: Office of the Secretary of Defense, March 4, 2021), https://media.defense.gov/2021/Mar/04/2002593656/-1/-1/0/SECRETARY-LLOYD-J-AUSTIN-III-MESSAGE-TO-THE-FORCE.PDF.

[14] Cited in Jim Garamone, "Concept of Integrated Deterrence Will Be Key to National Defense Strategy, DOD Official Says," *U.S. Department of Defense News*, December 8, 2021, www.defense.gov/News/News-Stories/Article/Article/2866963/concept-of-integrated-deterrence-will-be-key-to-national-defense-strategy-dod-o/.

[15] There are two prevalent irregular threat deterrence theories. One is deterrence by punishment and the other is based on deterrence by denial. See Dorthe Bach Nyemann and Heine Sørensen, "Going Beyond Resilience: A Revitalized Approach to Counter Hybrid Threats," Hybrid CoE Strategic Analysis 13 (Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats, January 2019),

These red lines should be based on the fact that a country cannot deter all irregular attacks. Instead, the focus should be on the most dangerous ones, understanding that this might also be an invitation to exploit vulnerabilities. After identifying the threats, states need to have the capability to punish an adversary. To do this, the guiding principle should be what does an adversary not want to happen? In other words, targeted states must be able to attack an adversary's vulnerabilities or core interests. Importantly, the countermeasures can either be "in kind"—countering cyber with cyber—or responses can be taken outside the domain in which the action occurred. An example could be threatening financial sanctions in case of a cyberattack.[16] For a smaller state, this could include collective punishment of an aggressor by an alliance (EU, NATO) of which it is a member.

The second component of an integrated deterrence strategy is the ability of target states to "deny" an adversary any benefits from an irregular attack. This can be done by improving societal resilience.[17] The European Union defines resilience as "the capacity to withstand stress and recover, strengthened from challenges." [18] Resiliency activities are generally low cost and fit within prevalent

https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-13-going-beyond-resilience-a-revitalised-approach-to-countering-hybrid-threats/ and Monaghan, "Deterring Hybrid Threats." This paper argues that an effective irregular threats deterrence strategy requires elements of both.

16 Vytautas Keršanskas, "Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats," Hybrid CoE Paper 2 (Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats, March 2020), 12, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf.

17 Tim Prior, "Resilience: The 'Fifth Wave' in the Evolution of Deterrence," Chapter 4 in *Strategic Trends 2018*, ed. Oliver Thränert and Martin Zapfe (Zurich: Center for Security Studies, 2018), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ST2018-06-TP.pdf); Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, Research Report RR-2942-OSD (Santa Monica, CA: RAND, 2019), https://www.rand.org/pubs/research_reports/RR2942.html; and Elizabeth Braw, *The Defender's Dilemma: Identifying and Deterring Gray-Zone Aggression* (Washington, D.C.: American Enterprise Institute, 2021), https://www.aei.org/the-defenders-dilemma/.

18 European Commission, "Joint Framework on Countering Hybrid Threats: a European Union Response," Joint Communication to the European Parliament and the Council (Brussels, April 6, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018&from=EN. While resilience has become a popular strategy in itself and has been used to rationalize various policy options, improving resiliency must be based on an assessment which identifies the sectors of society most vulnerable to irregular threats. Depending on the identified vulnerability, examples of resilience-building include improving cyber security, improving infrastructure, education against disinformation, diversifying resources, anti-corruption programs, etc.

"risk management" paradigms of national security.[19] Since the nature of irregular threats (ambiguous, hard to detect, difficult to attribute) makes deterrence by punishment difficult, it is crucial that states make themselves less vulnerable to them. A resiliency-based denial component of a comprehensive deterrence strategy allows states to make better use of scarce resources through the identification and mitigation of societal vulnerabilities. Resiliency also strengthens the foundations (communication, capability, and credibility) of a deterrence strategy. In summary, an integrated deterrence strategy should aim to prevent adversarial states from using irregular tactics while simultaneously mitigating their impact if used. This strategy would shrink the operational space for irregular actions and disincentivize their use.[20]

Creating a strategy that deters potential adversaries from using irregular tactics through both punishment and denial will be an essential feature of a 21st-century deterrence strategy. In the increasingly blurred space between peace and war, states must be able to clearly communicate to a potential aggressor that their conventional, nuclear, *and* irregular threats will not succeed. Deterrence will only remain credible if the United States and its Allies have the capability and will to clearly communicate their willingness to punish and deny adversarial irregular actions. There is currently a gap in the U.S. deterrence posture which needs to be addressed. The next section examines activities taken by allies and partners to improve their ability to deter irregular threats.

The Military Component of Integrated Deterrence

Because of the nature of irregular threats, an integrated deterrence strategy requires a whole-of-society approach that coordinates civilian[21] and military ele-

[19] Albin Aronsson, "The State of Current Counter-Hybrid Warfare Policy," Information note, Multinational Capability Development Campaign (MCDC), MCDC Countering Hybrid Warfare Project, March 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/803970/20190519-MCDC_CHW_Info_note_10-State_of_current_policy.pdf.

[20] Nyemann and Sørensen, "Going Beyond Resilience: A Revitalized Approach to Counter Hybrid Threats."

[21] In addition to traditional civilian entities involved with national security such as ministries of foreign affairs and interior, intelligence and security services, etc., it is crucial to include actors such as academics, non-government organizations, businesses, the media, and individuals. The latter often have the counter irregular threat knowledge, capabilities, and capacities that their government counterparts lack.

ments of national power across multiple domains. A growing number of countries have incorporated the concept of "Total Defense" [22] into their national security strategies to mitigate irregular threats.[23] Countries such as Finland, Sweden, and the Baltic states believe a Total Defense strategy is the best way to deter challenges across the threat spectrum.

Acknowledging that a whole-of-society approach is required to mitigate irregular threats, we will focus on the role of the military. In particular, actions taken by allied and partner militaries to educate their citizens, develop new capabilities, create relevant bureaucratic structures, and organize exercises that accurately reflect real-world threats and provide opportunities for societal organizations and individuals to integrate their counter-irregular threats capabilities and capacities.

In order for civil society to effectively contribute to Total Defense, they need to understand their role in it. The Finnish military hosts an annual "National Defense Course" to educate participants on the threat environment, security and defense policies, and their roles in fostering national security. The course also facilitates cooperation and networking among key business, government, and societal leaders.[24] To support their Total Defense strategy, Lithuania's military helped develop an education campaign that targets Russian disinformation. Using its Strategic Communications Command, Lithuania created a shared platform that identifies disinformation, debunks it with facts, and then distributes this information throughout society. This program plays a significant role in educating the public and deterring disinformation attacks by facilitating information sharing across trusted media platforms.[25]

In terms of new capabilities, Estonia uses its conscription to bolster cyber deterrence. By conscripting college-educated cyber specialists into the armed

---

[22] Total Defence is a whole of society approach to national security. It is intended to deter a potential adversary by raising the cost of aggression and lowering its chance of success. Total defense mobilizes all of a state's civilian and military resources so that an adversary is faced with national resistance if attacked or an ungovernable country if occupied. Total defense is not a new concept. It was the security posture of some non-aligned states during the Cold War. Key feature: institutionalized collaboration between government entities, civic organizations, the private sector, and the general public. As the current irregular threat environment includes both military and non-military challenges and the lines between war and peace have become blurred, an integrated approach to security is crucial. The direct involvement of civil society distinguishes total defense from traditional deterrence and defense.

[23] Tom Rostoks, "The Evolution of Deterrence from the Cold War to Hybrid War," in *Deterring Russia in Europe: Defence Strategies for Neighbouring States*, ed. Nora Vanaga and Toms Rostoks (London: Routledge, 2018), https://doi.org/10.4324/9781351250641.

[24] Braw, *The Defender's Dilemma*, 179.

[25] Benas Gerdziunas, "Lithuania: The War on Disinformation," *Deutsche Welle*, September 27, 2018, https://www.dw.com/en/lithuania-hits-back-at-russian-disinformation/a-45644080.

forces, Estonia dramatically improves its military cyber capabilities and strengthens its cyber infrastructure after the conscripts return to the civilian world.[26] This also provides Estonia with a trained and experienced cyber reserve force which is more proficient in dealing with cyber emergencies. The Estonian Armed Forces also sponsor a volunteer Cyber Defense Unit (CDU). It vets and grants members security clearances in order to provide additional capability and capacity against cyber threats.[27] Both of these programs provide expertise that improves deterrence against cyberattacks.

Deterring irregular threats also requires relevant bureaucratic structures. Finland's Ministry of Defense Security Committee links government agencies and non-governmental entities to bypass typical bureaucratic challenges in order to quickly share information, coordinate responses, and keep the Finnish population informed about irregular threats and attacks.[28] The Security Committee is comprised of approximately thirty specialists from across Finnish society and is focused on teaching civil servants and journalists about disinformation tactics through workshops and training sessions. The committee meets at least once a month to "ensure that vital information does not stay confined within various government agencies or in the private sector." [29] When Russian media outlets accused the Finnish government of abducting children with Russian backgrounds in custody battles between Finns and Russians, the committee was able to work with government officials to dispel this false narrative. This type of bureaucratic structure helps deter information attacks by improving the government's ability to identify them and boost the population's ability to disregard them.

While these examples show how a Total Defense strategy can improve deterrence against irregular threats, their effectiveness can only be determined through inclusive exercises. In contrast to U.S. experience, allies and partners have extensive experience integrating irregular threats and civilian entities (businesses, non-governmental organizations, etc.). For example, the Lithuanian military routinely executes whole-of-society exercises that allow various groups to prepare for and respond to irregular threats. These exercises have included representatives from the transportation, telecommunication, energy, infrastructure sectors, along with law enforcement and the military. Noteworthy, some exercises require coordination in a simulated non-cellular environment in which both

---

[26] Adi Gaskell, "How Estonia Is Using Military Service to Bolster Cybersecurity Skills," *Cybernews*, September 28, 2021, https://cybernews.com/security/how-estonia-is-using-military-service-to-bolster-cybersecurity-skills/.

[27] "Cyber Security in Estonia 2020" (Tallinn: Information System Authority, 2020), accessed December 21, 2021, https://www.ria.ee/sites/default/files/cyber_aastaraamat_eng_web_2020.pdf.

[28] Mackenzie Weinger, "What Finland Can Teach the West About Countering Russia's Hybrid Threats," *World Politics Review*, February 13, 2018, https://www.worldpoliticsreview.com/articles/24178/what-finland-can-teach-the-west-about-countering-russia-s-hybrid-threats.

[29] Weinger, "What Finland Can Teach the West About Countering Russia's Hybrid Threats."

military and civilian communication systems are degraded or inoperable.[30] Sweden's Total Defense 2020 exercise included more than sixty government agencies and non-governmental organizations. This exercise included multiple threat scenarios and provided opportunities for civilian organizations and government officials at the local, regional, and national levels to rehearse their responses to various types of irregular attacks, from a cyber denial of service attack to a proxy incursion.[31] Exercises like these improve deterrence by denial by demonstrating adversarial attacks will be ineffective.

EUCOM and Integrated Deterrence

Learning from Allies and Partners who have faced irregular threats for a number of years, the United States European Command (EUCOM) should incorporate similar actions into a comprehensive, coordinated, and integrated strategy to deter irregular attacks. As noted earlier, this type of strategy requires the integration of all components of national power. This section looks at ways EUCOM could educate its personnel, identify and integrate new capabilities, create relevant structures, and organize exercises to improve deterrence against what many consider the two most pervasive irregular threats: disinformation and cyber. These recommendations can be implemented quickly with little change to EUCOM's organizational structure. Even more importantly, they will foster subconventional deterrence by addressing specific vulnerabilities which Russia continues to attack with near impunity.

EUCOM currently rehearses its operational plans through strategic roundtables focused on Russia and chaired by the combatant commander. The EUCOM Commanding General noted that these roundtables "serve an important role in keeping our nation's senior-most military leaders synchronized both strategically and operationally on key issues related to global campaigning and competition." However, limiting participation to senior military and DoD officials, these strategic roundtables omit key stakeholders from industry and other governmental and non-governmental entities operating in Europe. Similar to Finland's Ministry of Defense Security Committee, these roundtables should include key regional non-military stakeholders, providing opportunities to give participants a more comprehensive understanding of Russian disinformation and cyber threats as well as identifying societal capabilities and capacities to help mitigate them. Reshaping elements of the Russia Strategic Roundtable into an educational event for stakeholders would bring unique perspectives and expertise to the group that would not otherwise be included in a military-only meeting.

---

[30] BNS, "Drills Will Allow Better Preparation for Hybrid Threats – Transport Minister," *The Lithuania Tribune*, February 28, 2018, https://lithuaniatribune.com/drills-will-allow-better-preparation-for-hybrid-threats-transport-minister/.

[31] Swedish Armed Forces, "Total Defence Exercise 2020," September 17, 2021, https://www.forsvarsmakten.se/en/activities/exercises/total-defence-exercise-2020/.

In terms of capability, U.S. cyber deterrence rests almost exclusively with the United States Cyber Command. Their deployment of "Cyber Squads" to Lithuania to "defend forward" against Russian aggression improves cyber deterrence but also demonstrates EUCOM's limited cyber capacity.[32] An initiative similar to Estonia's Cyber Defense Unit would help EUCOM improve its cyber deterrence capability by integrating civilian cyber experts. EUCOM could vet and grant security clearances to increase its capability and capacity against cyber threats. This would not only increase EUCOM's cyber deterrence but could also integrate cyber operations across planning and operations, providing the commander with more options to counter the multiple threats in the cyber domain.

Improved capabilities will have limited deterrent effect unless they are integrated into planning and operations. Lamenting the lack of an effective structure for integrating information operations, the U.S. Joint Staff Director for Command, Control, Communications, and Computers/Cyber, recently noted that "Combatant Commanders too often think of information operations as an afterthought. We understand kinetic operations very well. Culturally, we distrust some of the ways that we practice information operations (IO). The attitude is to 'sprinkle some IO on that.' Information operations need to be used—as commanders do in kinetic operations—to condition a battlefield." [33] To more effectively integrate information activities into military operations, an information warfare fusion cell that employs civilian and military experts should be created. This cell could help identify and counter disinformation. Currently, EUCOM's information experts are fragmented across the staff based on their specialty, tucked away in Sensitive Compartmented Information Facilities (SCIFs), given basement offices, or buried in a special staff section. Since information is a focal point of irregular attacks, expertise in information warfare cannot exist within a select few offices and hidden behind classification limitations. A fusion cell would allow EUCOM to improve its ability to more effectively identify and deter Russian information threats.

Improved education, capabilities, and structures will have limited effect unless they are tested through exercises. EUCOM and its subordinate commands host nearly 30 exercises annually, focusing primarily on U.S., allied, and partner interoperability. These exercises foster conventional and nuclear deterrence by demonstrating military strength and U.S. commitment to alliances and partnerships. However, they do little to deter irregular aggression. This is because current exercises are focused on lethal operations, include no or limited irregular threats, and do not effectively integrate other government agencies, private industry, or non-governmental organizations. EUCOM should integrate irregular

---

[32] Colin Demarest, "US Cyber Squad Boosts Lithuanian Defenses amid Russian Threat," *C4ISRNET*, May 5, 2022, https://www.c4isrnet.com/cyber/2022/05/05/us-cyber-squad-boosts-lithuanian-defenses-amid-russian-threat/.

[33] Stew Magnuson, "U.S. Still Playing Catchup in Information Operations," *National Defense Magazine*, February 11, 2022, www.nationaldefensemagazine.org/articles/2022/2/11/still-playing-catch-up-in-information-operations.

threats into its exercise scenarios and incorporate a broad range of participants to assess our ability to defeat irregular attacks, especially in the cyber and information domains. This type of exercise would clearly communicate our ability and demonstrative our capability to identify and mitigate Russian irregular tactics, fostering deterrence.

Change is always a challenge, and military structures and organizations are especially resistant to it. Nevertheless, change is necessary to facilitate deterrence in the twenty-first century. Although Russia's invasion of Ukraine has returned the focus and conversation of warfighting to conventional and nuclear deterrence, this view is short-sighted. Russia's military is being decimated, and analysts believe it will be a number of years before it will be a lethal threat to NATO.[34] However, Russian strategic interests will not change, and Russia will continue to use irregular tactics against the United States and its allies and partners as it rebuilds its military capability. With the Russians fully engaged in Ukraine, EUCOM has a unique opportunity to improve its deterrence against irregular aggression.

Conclusion

A nuclear triad, strong alliance system, and technologically advanced military continue to deter Russian conventional and nuclear attacks against the United States. Nevertheless, a continuing increase in irregular attacks shows that the current U.S. deterrence strategy has failed to prevent them. In contrast to the Cold War, irregular tactics directly threaten national security by undermining deterrence and destabilizing society. Therefore, a deterrence policy focused solely on conventional and nuclear forces is no longer sufficient.

In his reflections on deterrence, former NATO deputy secretary general Vershbow noted that deterrence "requires effective, survivable capabilities and a declaratory posture that leave the adversary in no doubt that it will lose more than it will gain from aggression, whether it is a short-warning conventional attack, nuclear first use to deescalate a conventional conflict, a cyber-attack on critical infrastructure, or an irregular campaign to destabilize allies' societies." Our current deterrence posture does not fully consider changes in the operational environment. To improve national security, the United States needs a twenty-first century deterrence strategy to deter twenty-first century threats.

[34] Wesley Culp, "The Russian Military After the Ukraine War: On The Brink of Disaster?" *1945*, July 6, 2022, https://www.19fortyfive.com/2022/07/the-russian-military-after-the-ukraine-war-on-the-brink-of-disaster/.

Disclaimer

The views expressed are solely those of the authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

Connections: The Quarterly Journal, Vol. 21, 2022, is supported by the United States government.

About the Authors

Dr. **Jim Derleth** is a Professor of Irregular Warfare and the Course Director of the Seminar on Irregular Warfare/Hybrid Threats at the George C. Marshall European Center for Security Studies.
E-mail: James.Derleth @marshallcenter.org

COL **Jeff Pickler** currently serves on the staff and faculty of the George C. Marshall European Center for Security Studies.
E-mail: Jeffrey.Pickler@marshallcenter.org