Modern Deterrence: 21st Century Warfare Requires 21st Century Deterrence

By Colonel Jeffrey W. Pickler

Introduction

After WWII, the United States and the Soviet Union found themselves competing for power and influence throughout the world. As the Soviet Union consolidated its control over the territory it occupied and the United States supported economic and political reform in Western Europe, a different type of war emerged. In contrast with previous wars which saw hundreds of divisions fighting across thousands of miles of battlefields, peace was now kept not only by the presence of large military formations, but also by the presence of nuclear weapons. The risk of escalation to a conflict greater in scope and scale than ever witnessed led to a 'Cold War,' with both countries competing below the threshold of traditional conflict. To help prevent the Cold War from becoming "hot," the United States adopted a policy of deterrence.

Deterrence is the "prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits."[1] Effective deterrence requires the capability, will, and ability to communicate to counter an adversary's activities through the threat of denial or punishment. Conventional and nuclear deterrence would be 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.

Most analysts agree that deterrence prevented a global war between the superpowers. However, deterrence did not end strategic competition between the United States and Soviet Union, it simply pushed it into areas which limited the risk of triggering an 'unacceptable counteraction.' While both superpowers used irregular warfare tactics to achieve strategic objectives, technological limitations consequently minimized the effectiveness and impacts of these tactics. This is no longer the case. The pace of technological change, an interconnected global network,

[1] Department of Defense, "Dictionary of Military and Associated Terms," *Joint Publication* 1-02 (8 November 2010): 70.

and a ubiquitous information environment provides an opportunity for states to achieve their strategic objectives below the threshold of conventional war. From the Baltics to the Caucuses, Russia has repeatedly demonstrated how sub-conventional actions can achieve strategic objectives, without fear of an unacceptable counteraction. Russia has incorporated changes in the global environment into a strategy in which cost, attribution, and risk of escalation are minimized. Therefore, a deterrence policy focused solely on conventional and nuclear forces is no longer sufficient for limiting Russian aggression.

In his reflections on deterrence in the 21st century, 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 a hybrid campaign to destabilize allies' societies."[2] Our current deterrence posture does not consider the 21st century operational environment. For deterrence to remain viable, it must be expanded to address conventional and sub-conventional attacks. This paper examines the declining relevance of traditional deterrence and makes recommendations to maintain its relevance for the 21st century.

The Evolution of Deterrence

American nuclear strategist Bernard Brodie famously wrote, "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."[3] Following WWII, the U.S. military began a massive demobilization. The country wanted a peace dividend following the nearly $4 trillion in military spending during World War II, which consumed 36% of the United States' GDP.[4] The United States compensated for a shrinking military through its monopoly on nuclear weapons and alliances such as the North Atlantic Treaty Organization (NATO), where "deterring Soviet expansionism"[5] was one of the primary reasons for its creation. These changes in the strategic environment led the United States to adopt a policy of deterrence based on a small conventional military, a strong alliance system, and a growing arsenal of nuclear weapons.

Deterrence theorist Thomas Schelling argued that deterrence is not about war, but the "art of coercion and intimidation."[6] Deterrence theory recognizes two basic approaches. Deterrence by denial is based on an ability to deter actions by making them either infeasible or unlikely to succeed. Deterrence by punishment threatens severe penalties, whether lethal, economic, or

---

[2] Alexander Vershbow, "Reflections on NATO Deterrence in the 21st Century," *Texas National Security Review* 4, no. 4 (Fall 2021): 133.
[3] 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.
[4] Stephen Daggett, "Costs of Major U.S. Wars," *Congressional Research Service Report for Congress* (2010), https://sgp.fas.org/crs/natsec/RS22926.pdf.
[5] "NATO Declassified: A Short History of NATO," *NATO* (2021), https://www.nato.int/cps/en/natohq/declassified_139339.htm.
[6] Liam Collins and Lionel Beehner, "Thomas Schelling's Theories on Strategy and War Will Live On," *Modern War Institute at West Point* (December 2016), https://mwi.usma.edu/thomas-schellings-theories-strategy-war-will-live/.

informational, should an attack occur.[7] Fundamental to both are clearly defined national interests, or 'red lines,' typically highlighted in national security documents and communicated by leadership. Schelling argued that an effective deterrence policy must combine the capability and willingness to win at all levels of escalation with a potential adversary, while maintaining open communication channels in order to deliver clear and direct messages to prevent unintended escalation.[8]

As the Eisenhower administration evaluated the strategic environment after the Korean conflict, it decided to codify the United States' deterrence strategy given the Soviet Union's superiority in conventional forces and our own growing nuclear arsenal. First communicated by Secretary of State Dulles in 1954, this new strategy communicated a threat of "direct, unrestrained nuclear response of massive scale in case of communist aggression, possibly aimed at the very centers of the enemy's economic life."[9] This view was formalized in National Security Policy Paper 162/2. It outlined the need to maintain "a strong military posture, with emphasis on the capability of inflicting massive retaliatory damage by offensive striking power."[10] This 'Massive Retaliation' strategy was based on 'deterrence by punishment,' allowing the United States to negate the Soviet Union's conventional numerical advantage by possessing the capability, and clearly communicating the will, to inflict an unacceptable cost should the Soviet Union or any other potential aggressor initiate any action which threatened our national interests.

As the Soviet Union achieved nuclear parity with the United States and both powers further developed their arsenals and capabilities, the U.S. was forced to reconsider the effectiveness of its deterrence policy. 'Massive Retaliation' changed to 'Mutually Assured Destruction (MAD),' but critics labeled MAD a geopolitical suicide pact which prevented national leadership's ability to control the escalation of all emerging crises.[11] Retired U.S. Army Chief of Staff Maxwell Taylor sharply criticized the United States' reliance on nuclear deterrence for deterring and responding to limited forms of war.[12] The strategic environment had again changed and the United States needed to change its military strategy to better facilitate deterrence. After President Kennedy's election in 1960, he established a 'flexible response' strategy that sought to provide a number of military and nonmilitary options to provocations. Flexible Response later evolved into Flexible Deterrent Options, which remains a component of contemporary military doctrine. It is defined in Joint Publication 5-0 as "preplanned, deterrence-oriented actions tailored to signal to and influence an adversary's actions."[13] The intent behind Flexible Deterrent Options is to leverage all elements of national power to de-escalate an emerging crisis and avoid provoking

[7] Richard J. Brown, "Understanding Deterrence," *RAND: Defence Studies* (2016): 196-197.
[8] Keir Giles, "What Deters Russia: Enduring Principles for Responding to Moscow," *Chatham House* (2021), https://www.chathamhouse.org/2021/09/what-deters-russia.
[9] Dimitrios Machairas, "Why Did the U.S. Adopt the Strategy of Massive Retaliation?" *Infinity Journal* (2013): 18-21.
[10] James S. Lay, Jr., *A Report to the National Security Council: Basic National Security Policy, NSC 162/2,* (1953).
[11] Peter Grier, "In the Shadow of MAD," *Air Force Magazine* (November 1, 2001), https://www.airforcemag.com/article/1101mad/.
[12] General Maxwell D. Taylor, *The Uncertain Trumpet* (1960), London: Harper & Brothers.
[13] Joint Publication 5-0: *Joint Planning*, Washington, DC: Department of Defense (2020), E-1.

full-scale combat. Both Flexible Response and Flexible Deterrent Options recognized that deterrence strategies must include more than the threat of nuclear annihilation, but neither adequately addressed sub-conventional threats.

Cold War deterrence was effective because the United States' strategy prevented large scale conflict between major powers and kept adversarial competition below the threshold of war. However, "effective nuclear and conventional 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."[14] This was true during the Cold War and remains true today. A State Department report from 1981 highlights actions taken by the Soviet Union in the Cold War including "control of the press in foreign countries; outright and partial forgery of documents; use of 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."[15] However, these efforts failed to achieve any significant strategic impact due to limitations of technology and the geopolitical environment at the time. Today, the strategic environment has again changed and these types of actions have far more effect on our national security. Russian interference in the 2016 U.S. Presidential Election and the 2020 SolarWinds data breach show that our adversaries can accomplish strategic objectives in the sub-conventional environment. Therefore, it is time to reevaluate our strategy to foster deterrence and ensure it remains relevant in the 21st century.

The Role & Relevance of Deterrence in the Current Strategic Environment

The 2018 National Defense Strategy states that the Department of Defense's "enduring mission is to provide combat-credible military forces needed to deter war and protect the security of our nation."[16] This suggests that the same Cold War strategy will deter contemporary threats. However, as Mark Galeotti notes in his recent book, *The Weaponisation of Everything*,

> the world is now more complex and above all more inextricably interconnected than ever before. It used to be orthodoxy that interdependence stopped wars. In a way, it did – but the pressures that led to wars never went away, so instead interdependence became the new battleground. 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.[17]

[14] Michael Kofman, "Raiding and International Brigandry: Russia's Strategy for Great Power Competition," *War on the Rocks* (2018), https://warontherocks.com/2018/06/raiding-and-international-brigandry-russias-strategy-for-great-power-competition/.
[15] "Soviet 'Active Measures': Forgery, Disinformation, Political Operations," *Special Report No. 88,* (1981), U.S. Department of State Bureau of Public Affairs: Washington, DC.
[16] "Summary of the 2018 National Defense Strategy of the United States of America," Department of Defense, (2018): 1.
[17] Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War*, Yale University Press, (2022): 18.

This interconnectedness has changed the strategic environment and undermines our current deterrence strategy. "Taken together, these 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."[18]

Michael Kofman captured the Russian approach to war, noting "If war is not an option and direct competition is foolish in light of U.S. advantages, raiding is a viable alternative that could succeed over time. Therefore, Russia has become the guerilla in the international system, not seeking territorial dominion but raiding to achieve its political objectives."[19] Russia has spent years perfecting this 'raiding' which stands in stark contrast to how the United States approaches warfare. Russia is more effective in coordinating a whole-of-government approach and integrating all elements of national power to achieve their strategic aims. Its successful sub-conventional operations cover "the entire 'competition space,' including subversive, economic, information, and diplomatic means, as well as the use of military forces."[20] Their military continues to play a critical role as well, adapting their core doctrine to train and equip for these types of operations. Russian Chief of the General Staff Gerasimov noted that the "very '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."[21] This can be seen in Russia tactics, which in some cases, subordinate lethal operations to non-lethal operations.[22]

The United States' approach to deterrence remains largely the same as during the Cold War. The emphasis is on a conventional and nuclear deterrence model based on advanced weapons systems and capability developments to deter and, if necessary, defeat, a peer enemy on the battlefield. The U.S. Army's current modernization efforts prioritize battlefield lethality, with billions of dollars being 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 Soldier weapons.[23] Our Army's Combat Training Centers continue to train maneuver brigades against a peer threat on a battlefield, assessing each rotational unit's ability to close with and destroy an 'enemy force' through fire and maneuver. Division, corps, and theater-level Army warfighter exercises focus largely on each staff's ability to destroy a peer threat on contested terrain with mass and

---

[18] Andrew F. Krepinevich Jr., "The Decline of Deterrence as a Defense Strategy," *Foreign Affairs,* (Jan/Feb 2019), https://www.foreignaffairs.com/articles/2018-12-11/eroding-balance-terror?utm_source=tw&utm_campaign=daily_soc&utm_medium=social.

[19] Kofman, "Raiding and International Brigandry."

[20] Mason Clark, *Russian Hybrid Warfare,* Military Learning and the Future of War Series, Washington, DC, Institute for the Study of War, (2020): 8.

[21] 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,* (2016): 24.

[22] Sandor Fabian and Janis Berzins, "Striking the Right Balance: How Russian Information Operations in the Baltic States Should Inform U.S. Strategy in Great Power Competition," *Modern War Institute at West Point,* (April 2021), https://mwi.usma.edu/striking-the-right-balance-how-russian-information-operations-in-the-baltic-states-should-inform-us-strategy-in-great-power-competition/.

[23] "2019 Army Modernization Strategy: Investing in the Future," United States Department of Defense, (2019), https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf.

precision fires. These efforts facilitate conventional deterrence, but as the last 15 years have shown, they do not deter cyber-attacks, use of proxies, disinformation campaigns, and other forms of sub-conventional operations that dominate the current strategic environment. On the contrary, current training and procurement initiatives only serve to reinforce Russia's efforts to combat us where we are not investing our defense budget or focusing our training. As former CIA Director Leon Panetta noted, "[t]he next Pearl Harbor that we confront could very well be a cyberattack that cripples America's electrical grid and its security and financial systems."[24] This sentiment is echoed by many other former and current national leaders and reveals their concern that our current deterrence model will not protect U.S. national interests.

While conventional and modern nuclear forces continue to provide the foundation of our deterrence model, they are no longer sufficient. Contemporary deterrence requires both military and non-military capabilities to counter adversary tactics. Creating a strategy which deters potential adversaries through both punishment and denial will be crucial to facilitating 21st century deterrence. In the increasingly blurred lines between peace and war, we must be able to clearly articulate an unacceptable cost to sub-conventional threats aimed at destabilizing our society or threatening critical infrastructure, as we would against a conventional attack or nuclear threat. Deterrence will only remain credible if the United States has the capability and will to clearly communicate its willingness to punish or deny adversarial actions.[25] The strategic environment has again changed, and our strategy must change with it, in order for deterrence to remain relevant. Some countries, such as Finland, have updated their strategies for fostering deterrence as a result of changes in the operational environment.

Deterrence in Finland

Finland gained its independence from Russia in January 1918. Despite two separate invasions between 1939-1944, Finland successfully defeated the Soviet Union's attempt to bring them under communist control. Today, tens of thousands of Russians hold dual citizenship in Finland, and Russia repeatedly attempts to sow seeds of discord amongst the Finnish population to undermine their national identity and faith in their democratic government. Notwithstanding, Finland is one of only three nonaligned neighbors of European Russia who have not lost parts of their territory to Russia since the end of the Cold War.[26] The 833-mile border between Finland and Russia has remained stable in spite of Finland's military non-alignment and lack of NATO membership. Many analysts believe Finland has maintained its independence and territorial integrity despite its geographic location, economic, and military inferiority, due to its strategy of 'Total Defense.' This strategy helps deter Russian conventional provocative actions and sub-conventional tactics such as election interference, disinformation, and cyber-attacks.

---

[24] Lawrence J. Trautman, "Is Cyberattack the Next Pearl Harbor," *North Carolina Journal of Law & Technology, Vol. 18, 232,* (2016): 1.
[25] AMB Alexander Vershbow, "Reflections on NATO Deterrence in the 21st Century," *Texas National Security Review, Vol. 4, Iss. 4,* (2021): 133.
[26] Brigadier General Juha Pyykönen and Dr. Stefan Forss, *Deterrence in the Nordic-Batlic Region: The Role of the Nordic Countries Together with the U.S. Army*, Monographs, Books, and Publications: USAWC Press, (2019).

Finland's 'Total Defense' strategy is an integrated effort that works to educate its citizens and leaders, integrate government agencies with civil society organizations and businesses, and develop the necessary conventional and sub-conventional capabilities to protect national security. These efforts help ensure that all elements of society and government understand the threats and work together to mitigate them. Finnish conventional capability includes an active military which is comprised of approximately 23,000 service members, but its conscripted reserves total over 900,000 personnel.[27] It has advanced weapons systems and routinely conducts large scale exercises with NATO and non-NATO forces to coordinate large scale combat operations. They maintain a high state of readiness through their specialized 'readiness units,' which are led by professional soldiers and are meant to "respond rapidly to a threat, perhaps within hours [and] be deployed nationally [with] sufficient independent firepower and endurance to engage even a well-armed adversary."[28] This force structure ensures any invading military might accomplish initial gains, but will face a formidable defense in depth, capable of inflicting an unaffordable cost. These efforts, investments, and exercises demonstrate why Finland has one of the highest levels of military spending in Europe.[29]

Finnish sub-conventional deterrence initiatives focus on a whole of society approach by coordinating efforts across governmental and private entities, educating leaders and society on threats, integrating efforts to better deter those threats, and developing exercises to demonstrate capabilities across all domains. To counter Russian disinformation, Finland organized a 'Ministry of Defense Security Committee' to link government agencies and nongovernmental entities together in order to bypass typical bureaucratic problems in order to quickly share information, coordinate responses, and keep the Finnish population informed regarding known disinformation efforts.[30] This 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."[31] Finland's schools educate children to spot disinformation almost as soon as they learn how to read.[32] Media and technology literacy education efforts help ensure the entire Finnish society can delineate fact from fiction, fostering government legitimacy. Finland also developed a 'National Defense Course,' which educates participants on threats, security and defense policies, and their roles in national security. The course also promotes cooperation and

---

[27] "World Military Strength," accessed from Global Firepower, (2022), https://www.globalfirepower.com/country-military-strength-detail.php?country_id=finland&msclkid=5936cc0ac16a11ecbff5ab1e6c054587.
[28] Michael Peck, "Finland's Unique Defense Strategy Makes it Ready for Anything," *The National Interest* (September 2021), https://nationalinterest.org/blog/reboot/finlands-unique-defense-strategy-makes-it-ready-anything-193540.
[29] Michael Byers, "Why Finland doesn't fear the growling Russian bear next door," *The Globe and Mail* (March 2015), https://www.theglobeandmail.com/opinion/why-finland-doesnt-fear-the-growling-russian-bear-next-door/article23242595/.
[30] Macanzie Weiner, "What Finland Can Teach the West about Countering Russia's Hybrid Threats," *World Politics Review* (2018), https://www.worldpoliticsreview.com/articles/24178/what-finland-can-teach-the-west-about-countering-russia-s-hybrid-threats?msclkid=3da44264c1af11ecba0c6ce32e2b2e2d.
[31] Weiner, "Finland Can Teach the West."
[32] Edward Lucas, "NATO Leaders Have Much to Learn from Finland," *The Times* (April 2022), https://www.thetimes.co.uk/article/f9a282be-be7a-11ec-b4e3203ad1be3cbc?shareToken=1ec6e39d9aa30dfb09f22dfeb8e2e5fe.

networking among key personnel.[33] Realizing the threat from cyber-attacks, Finland is a leader in cyber defense, recently placing first in an international cyber-defense competition.[34] Finland is also the home for the European Center of Excellence for Countering Hybrid Threats, or Hybrid CoE. The Hybrid CoE includes 31 partner countries from the European Union and NATO and is focused on hybrid threats emanating from Russia and nonstate actors. The Hybrid CoE's tasks "include research and analysis of hybrid threats, as well as organizing exercises to test crises-response tools related to cyber threat scenarios."[35] These efforts demonstrate Finland's understanding of how to effectively deter sub-conventional threats.

Finland's Total Defense is "a combination of deterrence, resilience, and defensive as well as offensive actions to constrain adversaries' hybrid activities in all situations."[36] Finland's conventional and sub-conventional capabilities clearly communicate a strong national will against all forms of aggression. Finland has a history of direct communication with Russia, understanding the need to clearly define boundaries and send "firm messages backed up by demonstrable seriousness about contingency planning."[37] On September 22, 2018, over 400 personnel from Finland's national police, border guard, and defense forces established a 'No Fly Zone' and raided 17 separate islands in western Finland owned by a Russian businessman. These islands are strategically located and, when seen within the greater context of sub-conventional threats, offered Russia a menu of options for potential operations.[38] More recently, when Finnish Prime Minister Sanna Marin was questioned regarding Russia's ultimatums against further NATO expansion, she responded "Finland decides on its own foreign and security policy. There are no two ways about this. We will not be blackmailed."[39] Finland's 2018 raids and Prime Minister Marin's remarks demonstrate to Russia and any other potential adversary Finland's capability and willingness to protect their national security. Many of these same initiatives can be incorporated into the United States European Command (EUCOM) to develop a more comprehensive, coordinated, and integrated deterrence model which clearly communicates the capability and will to deter all forms of Russian aggression.

Improving EUCOM's Ability to Facilitate Deterrence

The United States has previously adopted a number of strategies to foster deterrence in changing strategic environments. Today's strategic environment again requires change to facilitate deterrence. Our effective conventional and nuclear deterrence forms the foundation of

---

[33] Elisabeth Braw, *The Defender's Dilemma: Identifying and Deterring Gray-Zone Aggression*, AEI Press, Washington, DC, (2021): 179.
[34] Colin Demarest, "Finland wins NATO cyber defense competition," *Defense News* (2022), https://www.defensenews.com/cyber/2022/04/22/finland-wins-nato-cyber-defense-competition/.
[35] Weiner, "Finland Can Teach the West."
[36] Brigadier General Juha Pyykönen and Dr. Stefan Forss, Deterrence in the Nordic-Batlic Region: The Role of the Nordic Countries Together with the U.S. Army, Monographs, Books, and Publications: USAWC Press, (2019): 25.
[37] Keir Giles, "What Deters Russia: Enduring Principles for Responding to Moscow," *Chatham House,* https://www.chathamhouse.org/2021/09/what-deters-russia, (2021): 23.
[38] Mike Eckel, "Raids on Russia-Linked Island Properties Set Finland Abuzz," *Radio Free Europe* (September 2018), https://www.rferl.org/a/raids-on-reportedly-russia-linked-island-properties-sets-finland-abuzz/29509255.html.
[39] Pekka Vanttinen, "PM Marin: Finland 'will not be blackmailed' by Russia," *Euractiv* (January 2022), https://www.euractiv.com/section/politics/short_news/pm-marin-finland-will-not-be-blackmailed-by-russia/.

deterrence, but their effectiveness is also what drove conflict into areas where deterrence did not exist. Our adversaries' sub-conventional actions now threaten national security and must be addressed. The upcoming National Defense Strategy notes this challenge and attempts to mitigate it through the concept of 'Integrated Deterrence.' The Undersecretary of Defense for Policy explained, "[i]n terms of integrated… we mean, integrated across domains, so conventional, nuclear, cyber, space, informational [and] integrated across theaters of competition and potential conflict [and] integrated across the spectrum of conflict from high intensity to the gray zone."[40] Deterrence in the 21st century will only be effective "if governments have a specific strategy for each actor they want to deter."[41] As we seek to better integrate all aspects of national power into deterrence, it is imperative that our deterrent policies are based on an adversary's strategic goals, interests, rationales, and vulnerabilities. Within EUCOM's operational environment, integrated deterrence should include allowing other government entities and business leaders to participate in EUCOM's planning, operations, and exercises, and developing information warfare capabilities that organize, educate, and train our personnel to defend against Russia disinformation and cyber activity. These recommendations can be implemented quickly and within EUCOM's current organizational structure, but most importantly, foster sub-conventional deterrence by addressing specific vulnerabilities within the operational environment where Russia continues to attack with near impunity.

EUCOM currently develops and rehearses its operational plans through strategic roundtables focused on Russia and chaired by the combatant commander. The EUCOM Commanding General stated 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."[42] Limited in participation to senior military and DoD officials, strategic roundtables omit key stakeholders from industry and other governmental and non-governmental agencies operating in Europe. Including these additional participants would provide a more comprehensive understanding of the threat and also unique perspectives and expertise that would not otherwise be included in a military-only attended meeting. Akin to Finland's Ministry of Defense Security Committee and its National Defense University, this recommendation would help develop a more thorough vulnerability assessment, educate participants on Russian sub-conventional tactics, and develop a whole of society approach to increase our understanding of the problem and develop capabilities to more effectively deter them. A challenge to this recommendation is the current classification level for the Russia Strategic Roundtable as 'Top Secret.' Incorporating participants without security clearances risks generalizing the discussion to a level that will not be beneficial to any participant. To mitigate

[40] Jim Garamone, "Concept of Integrated Deterrence Will Be Key to National Defense Strategy, DOD Official Says," *Defense News* (December 2021), https://www.defense.gov/News/News-Stories/Article/Article/2866963/concept-of-integrated-deterrence-will-be-key-to-national-defense-strategy-dod-o/.

[41] Vytautas Kersanskas, "Deterrence: Proposing a more strategic approach to countering hybrid threats," *Hybrid COE* (March 2020): 14.

[42] U.S. European Command Public Affairs, "USEUCOM Commander Hosts Russia Strategic Roundtable," U.S. European Command (October 2021), https://eucom-web-app.azurewebsites.us/pressrelease/41727/useucom-commander-hosts-russia-strategic-roundtable?msclkid=b49678fcc6e311ec86dc5b55bfa784ab.

this, efforts must be made to de-classify as much as possible, while also developing opportunities for those outside of the DoD to receive security clearances so these discussions continue to be worthwhile for all participants.

Another challenge for sub-conventional deterrence has been our inability to deter in the information space. The U.S. Government Accountability Office noted in 2021 that "DOD made little progress in implementing its information operations strategy and had challenges conducting information operations."[43] The current U.S. Joint Staff Director for Command, Control, Communications, and Computers / Cyber and Chief Information Officer, Lieutenant General Crall, recently stated "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. 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."[44] Indeed, there is still no DOD definition for Information Warfare, but the Congressional Research Service described it as "as a strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations."[45] EUCOM must develop an information warfare fusion cell that employs civilian and military experts to more effectively integrate information warfare into all of its operations. This cell will also educate and train our personnel and other leaders to better understand the threat and their role in the information space, including how to integrate offensive and defensive information warfare. Currently, these personnel are fragmented across the staff based on their specialty, tucked away in Sensitive Compartmented Information Facilities (SCIFs), basement offices, or within a special staff section. Russia has already demonstrated the effectiveness of integrating all elements of information warfare and EUCOM must do the same. Initiatives such as the recent deployment of a U.S. 'cyber squad' to Lithuania to defend forward against Russian aggression is a step in the right direction, but still demonstrates the current compartmentalization of cyber operations.[46] Expertise in information warfare cannot exist within a select few offices and hidden behind classification limitations or isolated named operations; all leaders need to gain experience, exposure, and opportunities to better understand information warfare capabilities and how best to integrate them into all operations. A EUCOM information warfare fusion cell would help educate all personnel, government agencies and private business leaders on information warfare.

This recommendation would also build better media and technology literacy across EUCOM's ranks and throughout its operational environment, which would have an immediate effect against

---

[43] Joseph W. Kirschbaum, *Information Environment: DoD Operations Need Enhanced Leadership and Integration of Capabilities,* Testimony before the Subcommittee on Cyber, Innovative Technologies, and Information Systems, Committee on Armed Services, House of Representatives, Washington, DC: Government Accountability Office, (2021).

[44] Stew Magnuson, "U.S. Still Playing Catchup in Information Operations," *National Defense Magazine* (February 2022), https://cset.georgetown.edu/article/u-s-still-playing-catch-up-in-information-operations/.

[45] Catherine A. Theohary, "Defense Primer: Information Operations," *Congressional Research Service* (December 2021), https://crsreports.congress.gov/product/pdf/IF/IF10771.

[46] Colin Demarest, "U.S. cyber squad boosts Lithuanian defenses amid Russian threat," C4ISRNET (May 2022), https://www.c4isrnet.com/cyber/2022/05/05/us-cyber-squad-boosts-lithuanian-defenses-amid-russian-threat/.

Russian disinformation efforts. Finally, the fusion cell must integrate respected and proven warfighters with operational experience into their ranks. This would ensure its members have a 'seat at the table,' where commanders and senior leaders within the organization espouse their value in front of the entire organization. These efforts will grow information warfare into a more capable, comprehensive, and integrated effort against Russian sub-conventional attacks. Separate, specialized commands and new initiatives such as the Army's 'Multi-Domain Task Force' aim to accomplish many of the same things noted above, but are too compartmentalized and specialized to be fully integrated into the military's entire operational framework. There are also similar challenges with regards to current classification levels of many of the Army's current information warfare initiatives. Effective information warfare can no longer be isolated to special operations, its own unique combatant command, or compartmentalized programs that require specific clearances to participate. This recommendation would allow EUCOM to develop this capability within its own command structure and more effectively deter Russia's current disinformation campaigns and cyber-attacks. A final challenge with regards to this recommendation is the U.S. military's reluctance to lead with information without gaining prior consent through various command channels. This reluctance does not allow our information warfare to move at the speed of relevance, which is the most important requirement within this domain. For this recommendation to be effective, EUCOM leaders must become more comfortable with the potential for operational missteps and be willing to underwrite mistakes in order to give the practitioners the confidence to continue the fight.

EUCOM and its subordinate commands host nearly 30 exercises in a calendar year, focusing primarily on U.S., allied, and partner interoperability.[47] These exercises demonstrate military strength and our commitment to alliances and partnerships, but do little to deter sub-conventional aggression. This is because the current exercises are focused on lethal operations and do not effectively integrate other government agencies, private industry, or non-governmental organizations in order to develop and rehearse our own sub-conventional capabilities outside of the military domain. In order for the above recommendations to foster sub-conventional deterrence, they need to be incorporated into an updated and more robust exercise program. Sweden's 'Total Defense 2020' exercise involves armed forces, government industry, and civil society to build capabilities and partnerships that will ensure Sweden is less vulnerable, more resilient, and capable of learning best practices to defeat conventional and sub-conventional aggression.[48] EUCOM should incorporate the recommendations from the restructured Russia Strategic Roundtable into its existing exercises and better develop, incorporate, and assess our ability to defeat sub-conventional attacks within an operational exercise framework.[49] These exercises could also serve as an opportunity to rehearse and evaluate the integration of

[47] Jim Garamone, "European Command Exercise Program Aims to Deter Russia," Defense News (June 2019), https://www.defense.gov/News/News-Stories/Article/Article/1864862/european-command-exercise-program-aims-to-deter-russia/.
[48] "Total Defence Exercise 2020," Swedish Armed Forces (2020), https://www.forsvarsmakten.se/en/activities/exercises/total-defence-exercise-2020/.
[49] Elisabeth Braw, "Countering Aggression in the Gray Zone," Op Ed for AEI (November 2021), https://www.aei.org/op-eds/countering-aggression-in-the-gray-zone/.

information warfare into the tactical, operational, and strategic levels of military operations. This would provide all participants experience on the effective use of information warfare. Ultimately, exercises such as this would clearly communicate our capability and will to deter and defeat all forms of aggression and improve the societal resilience required to facilitate sub-conventional aggression. The ongoing Russian invasion of Ukraine has also driven much of the current discussion on deterrence back into conventional capabilities and military power. This presents a perfect opportunity for the United States to gain ground in the sub-conventional environment and continue to refine our own capabilities. After Russia's actions in Ukraine are complete, many experts believe they will return to a robust sub-conventional campaign and will amplify their attacks against the United States and its allies as they seek to rebuild their conventional capability. This presents a unique opportunity to improve our deterrence against sub-conventional aggression.

The Hybrid CoE in Finland recently published a deterrence proposal regarding hybrid threats, stating that successful deterrence "in the form of a decision not to pursue intended action, is induced in the mind of the hostile actor, meaning both public and private communication plays an important role in shaping the perception."[50] President Biden's recent remarks on our "sacred obligation under Article 5 to defend each and every inch of NATO territory with the full force of our collective power"[51] coupled with his decision to expeditiously declassify U.S. intelligence regarding Russia's planned invasion of Ukraine[52] are examples of effective communication. However, we must do more. We must also communicate tangible resolve and a willingness and capability to implement forceful solutions against all forms of Russian aggression.[53] These recommendations will improve sub-conventional deterrence and can be accomplished within EUCOM's current organizational structure. By better developing a whole of society approach to the Russian threat, integrating information warfare into all aspects of our operations, and effectively exercising our capabilities, we communicate to Russia and other adversaries that the United States has the necessary capability and will to deter aggression.

Conclusion

Our nuclear triad, strong alliance system, and technologically advanced military continue to deter Russian conventional attacks against the United States and NATO allies. However, as NATO Secretary General Stoltenberg recently noted "[h]aving a strong military is fundamental to our security. But our military cannot be strong if our societies are weak. So our first line of defense must be strong societies."[54] By developing a whole of society approach where leaders from all

[50] Vytautas Kersanskas, "Deterrence: Proposing a more strategic approach to countering hybrid threats," Hybrid COE, (March 2020): 18.
[51] President Joseph R. Biden, *Remarks by President Biden on the United Efforts of the Free World to Support the People of Ukraine,* Warsaw, Poland (March 26, 2022).
[52] Jake Harrington, "Intelligence Disclosures in the Ukraine Crisis and Beyond," *War on the Rocks* (March 1, 2022): https://warontherocks.com/2022/03/intelligence-disclosures-in-the-ukraine-crisis-and-beyond/?msclkid=7fdcbb3cc6fe11eca924275f1b11a121.
[53] Keir Giles, "What Deters Russia: Enduring Principles for Responding to Moscow," Chatham House, https://www.chathamhouse.org/2021/09/what-deters-russia, (2021).
[54] Elisabeth Braw, "The Importance of National Resilience in Deterrence," *Transatlantic Futures: Towards #NATO2030,* (2020): 92-93.

sectors within the United States work together to better identify, understand, and mitigate Russian sub-conventional aggression, deterrence will be strengthened. The United States has repeatedly demonstrated its ability to change strategies with the strategic environment to foster deterrence. These recommended changes continue that tradition and reinforce deterrence so that the United States will remain relevant in the 21st century and facilitate international stability for years to come.

About the Author

COL Jeffrey W. Pickler commissioned in June 2001 as a Second Lieutenant in the Field Artillery from the United States Military Academy. He has served in a number of leadership positions with the 82nd Airborne Division, 2nd Ranger Battalion, the 173rd Airborne Brigade Combat Team, 25th Infantry Division, and 4th Infantry Division. He has a Masters in Organizational Psychology and Leadership from Teacher's College, Columbia University. He has served on the staff at the United States Military Academy at West Point and within the Office of the Chairman of the Joint Chiefs of Staff. He recently completed his War College Fellowship at the George C. Marshall European Center for Security Studies.

The George C. Marshall European Center for Security Studies *in Garmisch-Partenkirchen, Germany is a German-American partnership and trusted global network promoting common values and advancing collaborative geostrategic solutions. The Marshall Center's mission to educate, engage, and empower security partners to collectively affect regional, transnational, and global challenges is achieved through programs designed to promote peaceful, whole of government approaches to address today's most pressing security challenges. Since its creation in 1992, the Marshall Center's alumni network has grown to include over 15,000 professionals from 157 countries. More information on the Marshall Center can be found online at www.marshallcenter.org.*

Marshall Center ***Security Insights*** are analytical articles that identify, explain, and put into context significant current and emerging defense and security issues. The series is aimed at the needs of political decision makers and others who are looking for concise summaries and analyses of important contemporary security topics. ***Security Insights*** are generally authored by Marshall Center faculty and staff.

The articles in the ***Security Insights*** series reflect the views of the author and are not necessarily the official policy of the United States, Germany, or any other governments.