CONNECTIONS
THE QUARTERLY JOURNAL

CONNECTIONS SPECIAL ISSUE

PARTNERSHIP FOR PEACE CONSORTIUM OF DEFENSE ACADEMIES AND SECURITY STUDIES INSTITUTES

HYBRID WARFARE AND THE NEED FOR INTERMEDIATE FORCE CAPABILITIES

EDITORS: PETER DOBIAS AND JOHN NELSON

SPRING 2022

Partnership for Peace Consortium of Defense Academies and Security Studies Institutes

This edition is supported by the United States government. The Consortium's family of publications is available at no cost at http://www.connections-qj.org. If you would like to order printed copies for your library, or if you have questions regarding the Consortium's publications, please contact the Partnership for Peace Consortium at PfPCpublications2@marshallcenter.org.

The Spring 2022 edition of *Connections: The Quarterly Journal* was published in August 2023 due to delays in publication. The content may reflect information and events more recent than the date indicated on the cover.

Dr. Raphael Perl
Executive Director

Sean S. Costigan
Editor-In-Chief and Chair, Editorial Board

ISSN 1812-1098, e-ISSN 1812-2973

CONNECTIONS

THE QUARTERLY JOURNAL

Vol. 21, no. 2, Spring 2022

Partnership for Peace Consortium of Defense Academies and Security Studies Institutes

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

https://doi.org/10.11610/Connections.21.2

Contents

Vol. 21, no. 2, Spring 2022

Editorial

Hybrid Warfare and the Need for Intermediate Force Capabilities 5
Peter Dobias

Research Articles

Twenty-first Century Threats Require Twenty-first Century Deterrence 11
Jim Derleth and Jeff Pickler

The Case for an Economic NATO 25
Ron Matthews

The 'Grey Zone' and Hybrid Activities 41
Peter Dobias and Kyle Christensen

Nonlethal Weapons and Intermediate Force: A Necessary Complement to Lethality 55
Susan LeVine

Developing a NATO Intermediate Force Capabilities Concept 67
John Nelson

How to Assess the Impact of Non-Lethal Weapons 85
Krista Romita Grocholski and Scott Savitz

Table of Contents

Gaming Intermediate Force Capabilities: Strategic Implications of Tactical Decisions 97
Peter Dobias, Kyle Christensen, and William Freid

Launching Narrative into the Information Battlefield 111
Suzanne Waldman and Sean Havel

NATO and Intermediate Force Capabilities: Why Human Effects Matter 123
Shannon Foley, Caitlin Jackson, Susan Aros & Anne Marie Baylouny

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

Peter Dobias, *Connections QJ* 21, no. 2 (2022): 5-9
https://doi.org/10.11610/Connections.21.2.00

Editorial

Hybrid Warfare and the Need for Intermediate Force Capabilities

Peter Dobias

Defence Research and Development Canada, https://www.canada.ca/en/defence-research-development.html

Abstract: NATO is faced with adversaries undertaking acts of aggression that deliberately stay below the lethal force threshold or aim to trigger a lethal response from NATO and incur costs to the Alliance such as undesired escalation, risks of collateral damage, including civilian casualties, or negative narratives. Examples of these activities range from dangerous aerial and maritime approaches, fomenting unrest and using refugees as a weapon, and even use of force short of lethal to intimidate opponents. Currently, the NATO responses are often limited to two extremes of mere presence or applying lethal force, thus ceding the initiative to the adversary. This issue contains a set of articles exploring intermediate force capabilities (e.g., non-lethal weapons, cyber, information operations, electromagnetic warfare, and strategic capabilities such as stability policing and use of special operation forces) and how they can address current NATO dilemma when operating below the threshold of lethal force.

Keywords: intermediate force capabilities, hybrid warfare, non-lethal weapons, human effects.

Analyses of the international security environment have increasingly drawn attention to what is often referred to as the gray zone.[1] A RAND study exploring hybrid warfare/gray zone challenges defined this part of the competition continuum as "an operational space between peace and war, involving coercive actions

[1] Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM* 7, no. 4 (November 2018): 31-47, https://ndupress.ndu.edu/Portals/96/Documents/prism/prism7_4/181204_Hoffman_PDF.pdf.

to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and non-military actions and the attribution for events." [2]

One of the challenges caused by the complexities of operating in such a security environment is that our adversaries, aware of NATO thresholds for employment of lethal force, can often operate with impunity below the level of armed conflict:

> Adversaries are undertaking acts of aggression that deliberately stay below the lethal force threshold or that ensure a lethal response from NATO would incur costs—undesired escalation, risks of collateral damage including civilian casualties, negative narratives, and other adverse strategic or political outcomes—to the Alliance.[3]

Examples of these activities range from dangerous aerial and maritime approaches, fomenting unrest and using refugees as a weapon, and even use of force short of lethal to intimidate opponents. The NATO responses are often limited to two extremes of mere presence or applying lethal force, thus ceding the initiative and narrative to the adversaries.

Recent Chinese behavior vis-à-vis the Philippines exemplifies this problem. As *Time* magazine stated

> From shining lasers at Philippine ships in February to firing water cannons at them over the weekend, China keeps testing the limits of aggression—dialing up the notch but carefully keeping short of an outright act of war—in disputed waters like the South China Sea. … by doing everything short of an armed attack, …, China can "chip away" at and "gradually erode" the Philippines' and other parties' "ability to respond in time and over time." [4]

This behavior reinforces the need for NATO countries to be able to counter hostile actions across the full spectrum of the use of force, not only in the lethal domain. Otherwise, adversaries benefit from what Kahn called "escalation dominance – a capacity, other things being equal, to enable the side possessing it to enjoy marked advantages in a given region of the escalation ladder." [5] In other words, they can bully NATO countries and their partners in order to achieve their objectives without escalating to lethal force; if NATO takes the bait and escalates, they can be portrayed as an aggressor.

---

[2] Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, CA: RAND, 2019), 8, https://doi.org/10.7249/RR2942.

[3] NATO Intermediate Force Capability Concept, Fourth Draft, Submitted to NATO Supreme Allied Command Transformation in December 2021.

[4] Chad de Guzman, China Is Testing How Hard It Can Push in the South China Sea Before Someone Pushes Back, *Time*, August 8, 2023, accessed August 15, 2023, https://time.com/6302515/china-philippines-south-china-sea-aggression/.

[5] Herman Kahn, *On Escalation: Metaphors and Scenarios*, 1st ed. (New Brunswick, NJ: Routledge, October 15, 2009).

In 1999, NATO developed a non-lethal weapons policy [6] aiming to expand the range of available military options to accomplish a mission while minimizing civilian casualties and damages to civilian infrastructure and materiel. However, the non-lethal weapons are only a subset of capabilities that can meet this objective. In response to the changing security environment, NATO endeavored to develop a broader concept of the use of force between mere presence and employment of lethal force. The resulting draft NATO concept defined Intermediate Force Capabilities [7] (IFC) as

> Active means below lethal intent that temporarily impair, disrupt, delay, or neutralize targets across all domains and all phases of competition and conflict.[8]

IFC include traditional non-lethal capabilities (kinetic, directed energy, and other), as well as cyber, information operations, electromagnetic warfare, and even strategic capabilities such as stability policing and the use of special operational forces short of lethal thresholds.

This issue's articles explore hybrid warfare and the need for IFC from a variety of perspectives. In the first article, Jim Derleth and Jeff Pickler discuss the increase in the use of irregular tactics by major state competitors in recent decades and argue that the deterrence focus on conventional and nuclear forces is no longer sufficient. They conclude that deterrence should be modified to remain relevant against 21st-century threats. Ron Mathews then examines the need for liberal democracies to respond to the growth of economic bullying, coercion, gunboat diplomacy, and geoeconomic pressure undertaken by Russia and China. This article concludes that the expansion of Russian and Chinese coercion represents a threat to the free world, requiring a more self-reliant long-term Western strategic, economic, security, and diplomatic posture, combined with economic support to poorer but strategically important nations. The third article, penned by Peter Dobias and Kyle Christensen, discusses the challenges of military operations in the gray zone, particularly the breakdown of deterrence below the lethal threshold, where NATO's adversaries often operate with impunity. Their article makes the case that IFC are precisely the kind of tools that provide effective means of response below the lethal threshold and that can shape the environment across domains up to the strategic level.

---

6 NATO, "NATO Policy on Non-lethal Weapons," October 13, 1999, accessed August 15, 2023, https://www.nato.int/cps/en/natohq/official_texts_27417.htm.

7 While not a doctrinal term, it is gaining traction across defense communities in the US and NATO. See e.g., Susan LeVine, "Beyond Bean Bags and Rubber Bullets: Intermediate Force Capabilities Across the Competition Continuum," *Joint Forces Quarterly* 100 (1st Quarter 2021): 19-24, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-100/jfq-100_20-25_Levine.pdf.

8 NATO ACT IFC Concept Development Workshop endorsed the definition in October 2021; also in NATO Research Task Group SAS-151, Intermediate Force Capabilities (IFC) Concept Development and Experimentation to Counter Adversary Aggression, NATO STO TR-SAS-151, December 2022.

The focus of the articles then shifts to IFC. Susan LeVine's article highlights the relevance of non-lethal weapons to the U.S. 2022 National Defense Strategy and NATO's 2022 Strategic Concept. She convincingly argues that IFC can strengthen deterrence, provide active or defensive measures to counter aggression below the level of armed conflict, and enable military operations among civilian populations in urban environments. John Nelson's article discusses the process of developing the draft NATO IFC concept through a series of wargames and workshops. His article concludes that NATO needs to develop, acquire, and effectively employ IFC across the continuum to win engagements both below and above the threshold of armed conflict, impose costs on the adversaries, and win the resulting narrative. Krista Romita Grocholski and Scott Savitz describe RAND's approach to assessing the strategic effects of non-lethal weapons through a logic model. They argue that a comprehensive logic model can be used to better characterize and communicate the impact of non-lethal weapons and actions at the tactical and operational levels and link these to strategic goals. Peter Dobias, Kyle Christensen, and William Freid then conclude this part of the discussion with a presentation of a novel approach to wargaming integrating various types of wargames across tactical, operational, and strategic levels to enable experimentation with the capabilities whose effects cross domain boundaries, including strategic and operational effects that are disproportional or not directly related to tactical performance.

Finally, the theme shifts to human factor considerations. In the first of this section, Suzanne Waldman and Sean Havel address the competition in the narrative battlefield and how it impacts outcomes on the physical battlefield. They conclude that it is vital for military institutions to internalize how the force as a whole is implicated in storytelling. Commanders who design operations need to understand that, increasingly, the stories that spread about their actions will impact far more people than the platforms or weaponry wielded in them. And lastly, Shannon Foley, Caitlin Jackson, Susan Aros, and Anne Marie Baylouny highlight shifts in the security environment with the implication that while lethality is absolutely necessary for NATO, it is no longer sufficient in typical military operations. They discuss how IFC can be effective tools to achieve desired changes in human behavior and conclude that NATO absolutely needs to recognize the power of IFC as a complement to lethal force, making it a necessary component of NATO planning and preparedness.

Disclaimer

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

About the Author

Dr. **Peter Dobias** is a Section Head for the Land and Operational Commands section of Defence Research & Development Canada, Centre for Operational Research and Analysis (DRDC CORA), Ottawa, Canada. He is responsible for operational research and strategic analysis support provided by five teams embedded with the Canadian Armed Forces' operational commands and the Canadian Army. Previously he led several teams in DRDC CORA and at U.S. Central Command. His research background includes analysis of complex adaptive and self-organized systems, deterrence and threat assessment, wargaming and constructive simulations, and strategic and operational mission assessment.
E-mail: Peter.Dobias@forces.gc.ca

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.

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

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

Ron Matthews, *Connections QJ* 21, no. 2 (2022): 25-39
https://doi.org/10.11610/Connections.21.2.02

Research Article

The Case for an Economic NATO

Ron Matthews

Rabdan Academy, Abu Dhabi, https://ra.ac.ae/

Abstract: This article examines the need for liberal democracies to respond to the growth of economic bullying, coercion, gunboat diplomacy, and geoeconomic pressure undertaken by Russia and China. The political call for an economic NATO-type international organization is growing louder following Russia's invasion of Ukraine and the resultant constraints imposed on food and energy supply, and China's bullying of the tiny NATO and EU state, Lithuania. This article chronicles examples of Russian and Chinese economic sanctions and the impact of China's geoeconomic diplomacy before identifying and explaining actual and potential western policy responses, especially the establishment of an Economic NATO.

Keywords: economic diplomacy, economic coercion, geoeconomics, economic NATO, Russia, China, geoeconomic threats.

Introduction

The Russia-Ukraine war is, first and foremost, a military catastrophe, but it has also generated seismic economic impacts that have had global consequences. Aside from the huge costs of the war, estimated at up to US $600bn for Ukraine alone,[1] there are the indirect effects, such as surging energy, fuel, and food prices, created by knock-on disruptions of global supply chains. Thus, if the international rule-based trading system is broken, then the globalization "holy grail" of liberal economics is under threat. The failure of markets to function smoothly because of protectionism and nationalism will cause the World economy to revert to 1930s "beggar-my-neighbor" policies. The beginning of this dangerous trend is evidenced by the nationalistic policies of developing countries, including

[1] Madeline Halpert, "Russia's Invasion Has Cost Ukraine Up to $600 Billion, Study Suggests," *Forbes*, May 4, 2022, https://www.forbes.com/sites/madelinehalpert/2022/05/04/russias-invasion-has-cost-ukraine-up-to-600-billion-study-suggests/.

Argentina, Egypt, India, Indonesia, Tunisia, and Turkey, which have acted to restrict or even halt exports of, respectively, pasta, vegetable oil, wheat, palm oil, vegetables, and beef, ramping up global inflationary pressure.[2] At the corporate level, building resilience into domestic supply chains is a rational step to minimize risk when international supply is uncertain, but the constrained national scale will further ratchet up prices. Developing nations suffering from rising energy costs and the loss of Ukrainian grain exports will suffer the most from this economic turbulence. Increasingly unable to participate in multilateral trade regimes, the poorer states will be attracted to bilateral trade and financing deals with countries like Russia and China, contributing to the geoeconomic fissures.

Of course, the contemporary international economy is a far cry from Adam Smith's classical theoretical paradigm. Rather than "perfect" markets, the reality is one of trade barriers, product differentiation, and imperfect market structures. Additionally, there are more insidious threats to free and open trade from anti-Western regimes, principally Russia and China. The US has sought to maintain a rule-based international order through efforts to negotiate the aborted US-EU free trade deal and the profoundly important Transatlantic Trade and Investment Partnership (TTIP). However, Washington's efforts have been undermined by its own unwillingness to open up US financial services and government procurement markets. An opportunity was missed because the TTIP was viewed as the chrysalis for what has been termed an economic NATO, enabling the West to continue to set the rules of the global economic game, increasingly threatened by anti-Western nations.[3] China, in particular, has been critical of these multilateral efforts, arguing they perpetuate Western domination of international trading flows.

The push for regulatory convergence has also been derailed by recent efforts of Russia and China to "weaponize" energy, food, and commodities to further their military, economic, and ideological goals. This process poses geoeconomic threats to Western interests in parallel with the risk of potential and actual military conflict. In response to these threats, the US Treasury Secretary, Janet Yellen, has proposed "friend-shoring" of supply chains,[4] and former NATO Secretary General Anders Fogh Rasmussen[5] and British Foreign Secretary Liz Truss

---

[2] Rajendra Jadhar, Maximilian Heath, and Nigel Hunt, "Food Export Bans, from India to Argentina, Risk Fueling Inflation," *Reuters*, June 27, 2022, https://www.reuters.com/markets/commodities/food-export-bans-india-argentina-risk-fueling-inflation-2022-06-27/.

[3] Simon Nixon, "To Ensure Security and Prosperity of the West, We Need an Economic NATO," *The Times*, June 30, 2022, https://www.thetimes.co.uk/article/to-ensure-security-and-prosperity-of-the-west-we-need-an-economic-nato-87vqd565j.

[4] Janet Yellen, "Remarks by Secretary of the Treasury Janet L. Yellen at the Brussels Economic Forum," *US Department of the Treasury*, May 17, 2022, https://home.treasury.gov/news/press-releases/jy0788.

[5] James Politi, "Former NATO Chief Calls for an Economic Version of Article 5 Defence Pledge," *Financial Times*, June 10, 2022, https://www.ft.com/content/1831d0f6-8ce0-47e2-9730-e73c0afe6e73.

have gone further by invigorating calls for an "Economic NATO."[6] The speech by the latter politician was particularly instructive, arguing that

> the assumption that economic integration drives political change – didn't work …We now need a new approach, one that melds hard security and economic security, one that builds stronger global alliances and where free nations are more assertive and self-confident, one that recognises geopolitics is back.

There is thus a recognition that the global rules-based order is crumbling, threatening both the economic security and prosperity of the West. The hallmark of the system is that all countries gain access to resources in an integrated global market protected by international law. NATO has done its job as a defense coalition, but is it the appropriate organization to address the parallel threats of state bullying, trade constraints, and economic diplomacy? This is likely a distraction from its principal military responsibility focused on collective defense, reflected in Article 5. The debate has therefore focused on a complementary trade-based NATO-type organization, possessing an "economic" Article 5, and comprising a broader geographical swathe of member countries that share the same democratic values. While Liz Truss asserts that geopolitics is back, it is rather geoeconomics that characterizes 21st-century diplomacy and statecraft. Accordingly, the purpose of this article is to identify and evaluate the nature of the geoeconomic threats Russia and China pose to the free world. This will be followed by an assessment of the various policy and institutional architectural options available to combat economic coercion and malign diplomacy.

Geoeconomic Threats

Conceptually, economic coercion has been around for generations but has only really entered into the international relations lexicon in the 21st century. It can take several forms, including diplomatic "bullying." Beijing, in particular, had developed a track record of engaging in this form of coercion, dating back to 2010 when it banned the import of Norwegian salmon after the Nobel peace prize was awarded to Chinese dissident Liu Xiaobo.[7] China's bullying again re-emerged in the recent 2020 David and Goliath dispute between Lithuania and China. Lithuania, a tiny Baltic state of just 2.8 mn people, was formerly under the Soviet sphere of influence. Shaped by its experience of repression, it was a proponent of liber-

[6] Rt Hon. Elizabeth Truss, "The Return of Geopolitics: Foreign Secretary's Mansion House Speech at the Lord Mayor's 2022 Easter Banquet," *Foreign, Commonwealth & Development Office*, April 27, 2022, https://www.gov.uk/government/speeches/foreign-secretarys-mansion-house-speech-at-the-lord-mayors-easter-banquet-the-return-of-geopolitics.

[7] Bill Hayton, "NATO Knows Asia Is Vital to Protecting Global Security," Report, *Chatham House*, June 28, 2022, https://www.chathamhouse.org/2022/06/nato-knows-asia-vital-protecting-global-security.

alism and human rights. Thus, the newly elected government was critical of Beijing's human rights record in Hong Kong and Tibet and expressed support for Taiwan's "freedom fighters." Indeed, in November 2021, the Taiwanese government was allowed to open a representative office in Lithuania's capital, Vilnius. Controversially, the office's nameplate read Taiwan rather than Taipei, a ploy used by other states to avoid offending China. This crossed a red line for Beijing, and its reaction was swift and brutal. Due to rising diplomatic tensions between the two states, China had already stopped operations of direct China-Lithuanian freight trains and closed credit lines for Lithuanian companies selling goods in China. However, now the Chinese Embassy in Vilnius was downgraded to *Charge d'affaires,* and Lithuania was obliged to reciprocate in China. In December 2021, China moved to block Lithuania's imports by delisting it as a country of origin, essentially banning customs clearance. The result was a 90 percent fall in shipments from Lithuania to China compared to December 2020.[8] Beijing then imposed secondary or indirect economic sanctions by pressurizing multinational companies in Lithuania's global supply chains to stop supplying goods to the Baltic state. In response, Taiwan and the US offered substantial trade credit deals, and the European Commission issued an Anti-Coercion Instrument against China, enabling potential countermeasures. Yet, Europe's reaction has been fragmentary, with German suppliers especially affected and pressuring Lithuania to reverse its stance.[9]

Russia has also recently employed economic coercion, which in this case might aptly be described as gunboat diplomacy. This statecraft tool was used in 19th-century conflicts to blockade enemy ports, depriving opposing forces of food and military resupply in order to force a surrender. Russia's naval blockade of Odesa and other Ukrainian ports on the Black Sea Coast was aimed at preventing grain from leaving the World's "breadbasket," thus cutting off a major source of revenue to bolster Ukraine's ailing economy. Moscow is in a position to exert extreme leverage as Ukraine and Russia's combined cereal exports account for almost one-third of the world's wheat and barley and more than 70 percent of its sunflower oil.[10] Putin's eventual agreement to allow "safe corridors" for these exports was likely due to extreme pressure from international organizations and client states in Africa and the Middle East, suffering badly from hunger and potential political instability due to the effects of global wheat scarcity and associated

[8] Dominique Patton and Andrius Sytas, "China Suspends Lithuanian Beef, Dairy, Beer Imports as Taiwan Row Grows," *Reuters*, February 10, 2022, www.reuters.com/world/china/china-suspends-lithuanian-beef-imports-taiwan-row-grows-2022-02-10.

[9] Judy Dempsey, "China's Bullying of Lithuania Spurs European Unity," *Carnegie Europe*, January 18, 2022, https://carnegieeurope.eu/strategiceurope/86208.

[10] Kelvin Chan and Paul Wiseman, "How the Russia-Ukraine War Triggered a Food Crisis," *National Observer*, June 20, 2022, https://www.nationalobserver.com/2022/06/18/news/how-russia-ukraine-war-triggered-food-crisis.

inflationary pressures. It has been estimated that around 400 million people, mostly located in the developing world, rely on Ukrainian food supplies.[11]

Yet another variant of economic coercion is retaliatory trade controls. These have gained currency over the last decade, having been used extensively by the West against rogue regimes such as Iran, Myanmar, and North Korea. The present sanctions against Russia are unprecedented, suggesting that trade controls are rapidly evolving into a significant method of statecraft to deter unacceptable arms proliferation, human rights abuses, and military adventures. However, sanctions can work both ways. Thus, linked to the Russia-Ukraine war, Moscow appears to be responding to western sanctions by slowing gas flows to Germany through the Nord Stream 1 pipeline. Maintenance work on the 759 miles pipeline is an annual event, but in 2022 it happened in July and then again in early August.[12] Gas flows were reduced by around 40 percent, and with the onset of winter, there is even the threat that Russia will stop gas flows altogether.[13] It is in a uniquely strong position to inflict serious multi-energy pain on the West. Not only is Russia the world's biggest natural gas exporter, accounting for 34 percent of European supplies of LNG alone, but its exports of coal account for 16 percent of the world's total, its 5 million barrels per day of crude oil represent 12 percent of global trade, and its 2.85 barrels per day of refined oil accounts for 15 percent of global trade.[14]

Similarly, China has sought to deter democracies from criticizing and otherwise working against its interests by applying reciprocal sanctions. This was made clear in the starkest terms by a Beijing spokesperson in 2021, who stated that "if [democracies] dare to harm China's sovereignty, security and development interests, they should be aware of their eyes being poked and blinded." [15] China is no longer supine, as evidenced by the recent testy politico-economic confrontation with Canada. In response to Canada's 2018 detention of Chinese citizen Meng Wanzhou, China retaliated by detaining two Canadian citizens just days later. As well as the arrest and trial of these two Canadian businessmen, Western companies, such as H&M, Zara, Burberry, and Nike, experienced boycotts of their goods

---

[11] Chan and Wiseman, "How the Russia-Ukraine War Triggered a Food Crisis."

[12] Kate Connolly, "Germany Braces for 'Nightmare' of Russia Turning off Gas for Good," *The Guardian*, July 10, 2022, https://www.theguardian.com/world/2022/jul/10/germany-russia-gas-flow-permanent-halt-nord-stream-1-maintenance; "Nord Stream 1 Pipeline to Shut Briefly in Latest Fuel Blow to Europe," *VOA News*, August 19, 2022, https://www.voanews.com/a/nord-stream-1-pipeline-to-shut-briefly-in-latest-fuel-blow-to-europe/6709144.html.

[13] Connolly, "Germany Braces for 'Nightmare' of Russia."

[14] Anne-Sophie Corbeau, "The Russian Invasion of Ukraine and the Global Energy Market Crisis," *Center on Global Energy Policy*, Columbia University, March 24, 2022, https://www.energypolicy.columbia.edu/research/qa/qa-russian-invasion-ukraine-and-global-energy-market-crisis.

[15] Jonas Parello-Plesner, "An 'Economic Article 5' to Counter China," *Wall Street Journal*, February 11, 2021, https://www.wsj.com/articles/an-economic-article-5-to-counter-china-11613084046.

in China.[16] Then, in August 2022, China reacted angrily to the Taiwan visit by Nancy Pelosi, the speaker of the US House of Representatives. Media headlines focused on China's military intimidation, especially its launch of multiple missiles toward Taiwan's North Eastern and South Western waters, including even ballistic missiles over the main island. Moreover, reportedly up to 66 Chinese fighter jets and 14 of its warships provocatively crossed the strategically significant median line in the Taiwan Straits.[17] China's suspension of 2,000 imported items from Taiwan was less publicized, halting mostly food products, such as citrus fruits, fish, and edible oils.[18]

A pattern is emerging of retaliatory Chinese trade controls. China's 2020-21 import bans on Australian goods and commodities drew an angry retort from US Secretary of State Antony Blinken, who singled out China's "blatant economic coercion of Australia" as an example of the urgent threats that democratic nations around the world face from increasingly assertive authoritarian regimes.[19] Canberra had irked Beijing not only by its call for an international inquiry into the origins of the coronavirus pandemic but also by its criticism of Beijing's ill-treatment of the Uighurs and its restrictions on democracy in Hong Kong. This then spiraled into a series of spying accusations, including claims of Chinese interference on Australian university campuses and counterclaims by Beijing that Australian universities were discriminating against Chinese students. However, behind the political rhetoric lies the economic leverage that China can exert. Trade disputes between the two countries have proliferated, including Beijing's decision to halt or severely restrict Australian exports, including coal, beef, wine, barley, timber, grapes, and seafood. By some measure, China is Australia's biggest trading partner, accounting for almost 33 percent of the latter's exports.[20] In particular, Australia's mining of iron ore is hugely dependent on China's big internal demand for steel production. Canberra, of course, also recognizes that regional strategic considerations impact its economic security and prosperity. It thus

---

16 Vanessa Friedman and Elizabeth Paton, "What Is Going on with China, Cotton and All of These Clothing Brands?" *The New York Times*, March 29, 2021, www.nytimes.com/2021/03/29/style/china-cotton-uyghur-hm-nike.html.

17 Joanna Walters, Martin Belam, and Samantha Lock, "Taiwan Says China Used 66 Planes and 14 Warships in Sunday's Drills – as It Happened," *The Guardian*, August 7, 2022, https://www.theguardian.com/world/live/2022/aug/07/china-taiwan-news-white-house-calls-chinese-drills-provocative-and-irresponsible-live.

18 "China Suspends 2,000 Food Products from Taiwan as Nancy Pelosi Visits," *Financial Times*, August 2, 2022, https://www.ft.com/content/ff15198f-cdc2-48fa-bed5-4a59bebbf01a.

19 Matthew Knott, "China's 'Blatant Coercion' of Australia Is a Lesson for the World, Says Antony Blinken," *The Sydney Morning Herald*, March 25, 2021, www.smh.com.au/world/north-america/china-s-blatant-coercion-of-australia-is-a-lesson-for-the-world-says-antony-blinken-20210325-p57duc.html.

20 Tony Makin, "Whither Australia-China Trade?" Australian Outlook, *Australia Institute of International Affairs*, June 16, 2020, www.internationalaffairs.org.au/australianoutlook/whither-australia-china-trade/.

watches with growing alarm China's efforts to spread its influence into Australia's "backyard," even extending to Antarctica. In this regard, Beijing has recently announced plans to build a large all-year-round airport 17 miles from its Zhongshan ice research station, located in East Antarctica within the 42 percent of the continent claimed by Australia.[21] Undoubtedly, the reported presence of sizable energy and mineral resources acts as a decisive pull factor.

China has also used retaliatory export bans on rare earth minerals, which it regards as a "strategic resource." These minerals are essential for the powerful magnets in electric-vehicle motors and also play a critical role in military systems, such as drones and missiles. Chinese leverage on the market is immense, not least because it possesses around 85% of the world's capacity to process rare earth ores, with the US alarmingly sourcing 80% of its rare-earth imports from China.[22] Thus, it is easy to see why Beijing might be tempted to weaponize these minerals if and when appropriate. In fact, it happened in 2010, when tensions arose over the Japanese-administered Senkaku Islands, claimed by China as the Diaoyu Islands, leading to Beijing imposing a trade ban on rare-earth exports to Japan. Similarly, China threatened to suspend rare-earth exports to the US in 2018, linked to the US defense contractor, Lockheed Martin, winning a contract to upgrade Taiwanese air defense systems, with further threats made in 2019 as the trade war between Washington and Beijing escalated. Yet more threats were made in 2022, following Washington's decision, over national security concerns, to intensify the trading ban on Huawei and around 70 of its affiliate enterprises. Only now, the Chinese are potentially seeking to ban not only the trade in exotic minerals but also the technologies that refine and purify the raw materials located upstream in the industry value chain. China is in a strong position to do this, given it controls around 50-60 percent of the mining market and about 90 percent of activities at the intermediate processing stage.[23] Beijing launched a new Export Control Law aimed at strengthening state control over the flow of strategic materials. In parallel, it announced the creation of a new state-owned enterprise, China Rare Earth Group. This newly created "megafirm" now controls 60-70 percent of Chinese rare earth production, which translates into 30-40 percent of the global supply.[24] In response to this industrial consolidation, a US Department of Defense official commented that the critical materials sector is a

[21] Barnard Lagan, "Beijing Challenges Australia for Slice of Antarctic Runways," *The Times*, May 6, 2021, https://www.thetimes.co.uk/article/cold-war-race-between-australia-and-china-for-all-year-antarctic-runways-s6kbcn8mx.

[22] Reuters Staff, "U.S. Dependence on China's Rare Earth: Trade War Vulnerability," *Reuters*, June 28, 2019, https://www.reuters.com/article/us-usa-trade-china-rare earth-explainer-idUSKCN1TS3AQ.

[23] Shunsuke Tabeta, "China Tightens Rare-Earth Regulations, Policing Entire Supply Chain," *Nikkei Asia*, January 16, 2021, https://asia.nikkei.com/Business/Markets/Commodities/China-tightens-rare-earth-regulations-policing-entire-supply-chain.

[24] Kristin Vekasi, "Chinese Rare Earth Consolidation a Cause for Concern," *EastAsiaForum*, March 30, 2022, https://www.eastasiaforum.org/2022/03/30/chinese-rare-earth-consolidation-a-cause-for-concern/.

"microcosm of the geopolitical and geo-competitive forces shaping the 21st-century."[25]

Coercion through Diplomacy

While economic diplomacy is an acceptable instrument of statecraft, embroidered into the 2013 launch of Beijing's "Belt and Road Initiative" (BRI)[26] is political and financial leverage, disturbingly similar to economic coercion. The BRI is a reincarnation of China's ancient "silk road" trade route to Asian and Western markets. Yet, the contemporary version has a broader global reach, reflected through digital and other 5G information and maritime tentacles. China's geoeconomic diplomacy represents a form of international statecraft aimed at satisfying its long-term trade, foreign policy, and strategic ambitions. The strategic thrust is to win the hearts and minds of the international community through politico-economic patronage and strategic influence. However, BRI is often categorized as checkbook diplomacy in the sense of providing non-concessionary financial incentives to support loanee country development goals. It is not *ad hoc* but forms part of a Grand Strategy designed to foster regional and global influence. At the core of this statecraft is an emphasis on non-interference in the internal affairs of recipient states, with an obvious appeal to democratically suspect and diplomatically beleaguered governments. China's economic diplomacy particularly targets investment into infrastructural sectors, such as ports and docks, having strategic implications.

While China's geoeconomic strategy has been recognized in the literature,[27] analysts have focused solely on the investment and financial aspects, ignoring the BRI's strategic dimensions. China's brand of geoeconomic diplomacy is likely to prove more effective than either the long-term intangible benefits of Nye's soft power or the corrosive nature of hard power, whether via cyberattacks, quasi-military destabilization operations, gunboat diplomacy or, ultimately, the threat or actual use of military force. This perspective is underscored by David Shambaugh, who wrote that "China is constructing an alternative architecture to the postwar western order."[28] Beijing's geoeconomic diplomacy model is

---

[25] Vekasi, "Chinese Rare Earth Consolidation a Cause for Concern."

[26] Danielle Miller, "North American Critical Minerals Days: Rare Earths Day," *Adamas Intelligence*, October 19, 2021, https://www.adamasintel.com/north-american-rare-earths-day-2021-recordings/.

[27] Christian Dargnat, "China's Shifting Geo-economic Strategy," *Survival* 58, no. 3 (May 2016): 63-76, https://doi.org/10.1080/00396338.2016.1186980; Nicholas Kitchen, ed., *China's Geoeconomic Strategy*, IDEAS Reports – Special Report SR012 (London: London School of Economics and Political Science, June 2012), www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-Chinas-Geoeconomic-Strategy.pdf.

[28] David Shambaugh, "China's Soft-Power Push: The Search for Respect," *Foreign Affairs* 94, no. 4 (July/August 2015): 99-107, 100, http://www.jstor.org/stable/24483821. The *Sunday Times* mentions that the Chinese government plans to spend US $1 Trillion on overseas projects over the next 10 years, *Sunday Times* (April 2017).

more targeted and nuanced than its broader soft power approach, more durable than contingents of UN peacekeepers or warships on Gulf peacekeeping operations, and more practical in its impact than Confucius Centers. A historic tectonic geo-strategic shift appears to be underway, with China aiming to replace America as the world's dominant diplomatic power. President Xi hinted as much at Davos in early 2017, with a speech that represented a concerted strategy to achieve China's vision of the future global economic system at a time when the US is turning inward.[29]

The BRI aims at building roads, railways, ports, and other eco-strategic infrastructure. The scale of investment in the developing world is staggering. For example, there are reportedly 46 African ports where China has financial, construction, and operational involvement.[30] By mid-2017, more than 10,000 Chinese-owned companies were operating in Africa.[31] From a global perspective, in 2022, the BRI touches 147 countries,[32] 50 percent of the world's population, and a quarter of its GDP, via a multitude of investments financed through long-term loans.[33] Projecting forward, it has been estimated that by 2027, BRI spending will have reached $1.3 trillion, with more than 2,600 projects worldwide valued at $3.7 trillion.[34]

In Asia, China is pushing Thailand to agree on the construction of a 100 km Kra canal, on the scale of Panama, linking the South China Sea with the Bay of Bengal and thus bypassing thecrowded Strait of Malacca. For the West, the Kra canal exemplifies the common danger of the BRI acting as a vehicle for Beijing's potential acquisition of overseas infrastructural assets, contributing to a broadening and deepening of China's strategic influence. Moreover, Chinese asset acquisition comes with the danger of "debt traps." For instance, Beijing has built a new port at Kyaukpyu, Myanmar, and taken a 70 percent controlling stake after the host country defaulted on its repayments.[35] China has, therefore, potentially

---

[29] Lawrence Summers, "The US Must Work on Its Economic Relationship with China: Global Cooperation Matters More than Short-Term Gain," *Financial Times*, April 9, 2017, https://www.ft.com/content/abbeb10a-1b85-11e7-a266-12672483791a.

[30] Judd Devermont, Catherine Chiang, and Amelia Cheatham, "Assessing the Risks of Chinese Investments in Sub-Saharan African Ports," *CSIS*, June 5, 2019, https://reconasia.csis.org/assessing-risks-chinese-investments-sub-saharan-african-ports/.

[31] Frank Umbach, "How China's Belt and Road Initiative Is Faring," Report, *GIS*, April 8, 2022, https://www.gisreportsonline.com/r/belt-road-initiative/.

[32] Christoph Nedopil Wang, "Brief: China Belt and Road Initiative (BRI) Investment Report H1 2022," *Green Finance and Development Center*, July 24, 2022, https://greenfdc.org/china-belt-and-road-initiative-bri-investment-report-h1-2022/.

[33] Lily Kuo and Niko Kommenda, "What Is China's Belt and Road Initiative?" *The Guardian*, July 30, 2018, https://www.theguardian.com/cities/ng-interactive/2018/jul/30/what-china-belt-road-initiative-silk-road-explainer.

[34] Umbach, "How China's Belt and Road Initiative Is Faring."

[35] Yimou Lee and Thu Thu Aung, "China to Take 70 Percent Stake in Strategic Port in Myanmar – Official," *Reuters*, October 17, 2017, https://www.reuters.com/article/china-silkroad-myanmar-port-idUSL4N1MS3UB.

gained a naval base on the Indian Ocean side of the Malacca Strait chokepoint, projecting power across the Bay of Bengal.

The debtor nations view China's loans as an opportunity to earn high investment returns, but this invariably fails to happen. Sri Lanka's Hambantota Port project attracted huge Chinese investment but generated weak revenue streams. Combined with China's high-interest charges, it inevitably meant that Sri Lanka was forced into a dangerous debt trap. By 2017, the loans proved too costly to sustain, and a loan payment default occurred, obliging Beijing to call in its US1.4 billion debt.[36] With few cards to play, the Sri Lankan government signed a concessionary agreement for a contractual venture between the China Merchants Port Holdings Company Limited (CMPort), China's state-owned port company, and the Hambantota port. The agreement required the Sri Lankan government to service the debt by leasing the port infrastructure to the Chinese over a 99-year period. Colombo ceded 70 percent control of the Port to CMPort, with the Sri Lanka Ports Authority taking the remaining share.[37]

Policy Responses

China's expanding geoeconomic influence in Myanmar and Sri Lanka is but a microcosm of a broader trend affecting the Asian region. The massive inflows of Chinese funds have occurred because of an emerging strategic vacuum caused by ambivalent Western diplomacy. Recently, however, liberal democracies have begun to respond by launching essential policy initiatives. Firstly, there is the evolving "Quadrilateral Security Dialogue," comprising Australia, India, Japan, and the US. It is an informal security alignment that commenced in 2007 in response to China's rising strength in the Indo-Pacific Region. Although the Quad initially failed to generate diplomatic momentum, it was rejuvenated at the 2017 ASEAN summit, with the four nations recommitting to strengthening their security response to China. Significantly, at the second Quad Leaders' Summit in Tokyo in May 2022, there was confirmation that while maritime security is vital, Asian economic security is intertwined with defense capability.[38] A second policy initiative was launched in 2016 via the establishment of a NATO Asia-Pacific security framework. With Australia, the Republic of Korea, Japan, and New Zealand, NATO unveiled a partnership to defend the rules-based international order,

[36] Anjana Pasricha, "As Crisis-Hit Sri Lanka Counts Cost of Chinese Projects, India Moves to Recover Influence," *VOA News*, June 10, 2022, https://www.voanews.com/a/as-crisis-hit-sri-lanka-counts-cost-of-chinese-projects-india-moves-to-recover-influence/6611703.html.

[37] Lu Hai Liang, "Sri Lanka Hands over Port to China to Pay off Debt," *The National*, September 11, 2018, https://www.thenationalnews.com/world/asia/sri-lanka-hands-over-port-to-china-to-pay-off-debt-1.684606.

[38] "The 'Quad': Security Cooperation Among the United States, Japan, India, and Australia," *US Congressional Research Service*, updated July 25, 2022, https://crsreports.congress.gov/product/pdf/IF/IF11678/6.

forming part of the NATO 2030 Agenda.[39] The Asian (A-4) partners are all established democracies, have shared values, and are US Treaty allies, save for New Zealand, which has a close partnership with Washington. Regular discussions are now held by the North Atlantic Council and its A-4 partners. In fact, in April 2022, Finland, Georgia, Sweden, and Ukraine, along with EU representatives, met with the Foreign Ministers of the four Asia-Pacific countries to discuss the global implications of Russia's invasion of Ukraine.[40] A third initiative commenced in 2017 when Japan and India launched a program directly competitive to the BRI, the Asia-Africa Growth Corridor.[41] Then, in 2021, in a bid to capitalize on the Covid-induced delays affecting China's BRI program,[42] there was a US-Japan roll-out of an Indo-Pacific digital infrastructure program. This is a substantial 5G infrastructure investment initiative, forming part of a broader ambitious US-led alternative to China's BRI, involving more than 2,000 projects across multiple continents.[43]

Beijing has angrily responded to the West's strengthening of its Asian economic and military capacities, including the potential expansion and reenergizing of the "Asian NATO" initiatives, reflected by the 'Five' Power Defence Arrangement (Australia, Malaysia, New Zealand, Singapore, UK), 'Four' Quad (US-India-Japan-New Zealand Economic Agreement), 'Three' AUKUS (Australia, UK, US) submarine deal, and 'Two' bilateral alliances (US-South Korea, US-Japan).[44] The West's coordinated Asian response to China's Grand Strategy is impressive. It suggests the feasibility of consensus at the global level, whereby an international NATO-type body might assume the responsibility for addressing anti-coercion and diplomatic actions against Russia and China. Possibly the first reference to

---

[39] "Relations with Asia-Pacific Partners," *NATO*, July 12, 2022, https://www.nato.int/cps/en/natohq/topics_183254.htm.

[40] "Opening Remarks by NATO Secretary General Jens Stoltenberg at the Meeting of the North Atlantic Council in Foreign Ministers Session, with the Participation of Partners," *NATO*, April 7, 2022, https://www.nato.int/cps/en/natohq/opinions_194328.htm.

[41] Avinash Nair, "To Counter OBOR, India and Japan Propose Asia-Africa Sea Corridor," *The Indian Express*, May 31, 2017, https://indianexpress.com/article/explained/to-counter-obor-india-and-japan-propose-asia-africa-sea-corridor-4681749/.

[42] "China Says One-Fifth of Belt and Road Projects 'Seriously Affected' by Pandemic," *Reuters*, June 19, 2020, https://www.reuters.com/article/us-health-coronavirus-china-silkroad-idUSKBN23Q0I1.

[43] Richard Javad Heydarian, "US-Japan Roll out Digital Counter to China's BRI," *Asia Times*, April 20, 2021, https://asiatimes.com/2021/04/us-japan-roll-out-digital-counter-to-chinas-bri/.

[44] Pierre Haroche and Martin Quencez, "NATO Facing China: Responses and Adaptions," *Survival* 64, no. 3 (May 2022): 73-86, https://doi.org/10.1080/00396338.2022.2078047; "US Trying to Create Asian NATO with Blocs to 'Suppress' China: FM Wang Yi," *Business Standard*, March 7, 2022, https://www.business-standard.com/article/international/us-trying-to-create-asian-nato-with-blocs-to-suppress-china-fm-wang-yi-122030701343_1.html; Gerry Doyle, "Southeast Asian Defence Pact Can Help Region Manage Tensions, Members Say," *Reuters*, June 11, 2022, https://www.reuters.com/business/aerospace-defense/southeast-asian-defence-pact-can-help-region-manage-tensions-members-say-2022-06-11/.

an Economic NATO was made in 1956. Then, a scholarly paper highlighted the significance of economic warfare and the relevance of Article II in NATO's founding Treaty, which commits members to "seek to eliminate conflict in their international economic policies and [to] encourage economic collaboration between any or all of them."[45] Yet, the first tangible expression of this commitment came not from NATO but rather from the European Union through its 2021 launch of the Anti-Coercion Instrument. This new tool sought to counter third-country economic coercion through tailor-made proportional economic responses.[46] Then, in 2022, the Rasmussen Report (co-authored by Ivo Daalder), submitted for the June NATO Summit in Spain, looked to revive the idea of an Economic NATO.[47] The Report raised three salient points: that NATO 'is' the appropriate international organization to manage the "economic guarantee"; that tools in its economic armory should include the full spectrum of options, including direct sanctions, secondary sanctions, import tariffs, and though not mentioned, presumably also banking, financial services, and business investment; and that while such sanctions might lead to negative spill-overs on the countries imposing them, the upside is that this may act to consolidate the supply chains in democratic countries. In this sense, the Rasmussen Report signals that geo-strategic interests dominate economic interests, heralding a retreat on globalization, though more broadly, these two forces are inescapably interlinked.

A plethora of differing proposals to create an appropriate transnational anti-coercion body has begun to emerge, including a NATO for Trade,[48] a D-10 (G7 countries plus Australia, India, and South Korea) Club of Democracies,[49] and Germany's suggestion of an "Alliance of Democracies" to include the leading democracies in North America, Europe, and the Indo-Pacific. These regions make up roughly three-quarters of global GDP, the transatlantic partnership provides nearly 80% of official developmental aid worldwide, and the 20 highest-scoring countries in terms of soft-power influence are all democracies.[50] Their revealed socioeconomic capacities offer the West major leverage in addressing global

[45] Lincoln Gordon, "Economic Aspects of Economic Diplomacy – The NATO Experience," *International Organization* 10, no. 4 (November 1956): 529-543, 541.

[46] "EU Strengthens Protection Against Economic Coercion," *European Commission*, December 8, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6642.

[47] Alireza Ahmadi, "Against Russia and China, an 'Economic NATO' Is Not Enough," *The National Interest*, June 10, 2022, https://nationalinterest.org/feature/against-russia-and-china-%E2%80%98economic-nato%E2%80%99-not-enough-202874.

[48] Ahmadi, "Against Russia and China, an 'Economic NATO' is Not Enough."

[49] Patrick Wintour, "UK Plans Early G7 Virtual Meeting and Presses Ahead with Switch to D10," *The Guardian*, January 15, 2021, www.theguardian.com/world/2021/jan/15/uk-plans-early-g7-virtual-meeting-and-presses-ahead-with-switch-to-d10.

[50] Ash Jain, Matthew Kroenig, and Jonas Parello-Plesner, "An Alliance of Democracies: From Concept to Reality in an Era of Strategic Competition," *Atlantic Council*, December 7, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/an-alliance-of-democracies-from-concept-to-reality-in-an-era-of-strategic-competition/.

challenges. Yet, perhaps the most effective and expedient way forward is, as Liz Truss argues, to deploy the G-7,[51] which, with a membership representing half the globe – including the entire EU as a "non-enumerated member,"[52] is already positioned to defend the West's prosperity collectively. There is certainly the need for an economic equivalent of Article 5, and the G-7 represents a sound start in moving toward this goal. However, careful thought would need to be given to the following three factors: the nature of hostile actions triggering a collective response; whether the remit for a response would include non-economic considerations, such as human rights; and, finally, the need to ensure predetermined agreement on escalatory responses.[53] At the moment, the G-7 and NATO are working in tandem, and perhaps this is the logical short-term approach to be adopted, with the two organizations coordinating and representing a broad "coalition of the willing" to address global economic and military challenges. As for the long-term, it is likely that the institutional architecture will evolve, especially as President Biden is presently seeking to establish an ambitious global coalition that goes far beyond the G7 and NATO.[54]

NATO is not the only international organization capable of policing China's economic "grey zone" and hybrid coercion activities, and in the process also strengthening Western deterrence via resilience, denial, and punishment.[55] Other multilateral bodies, such as the World Trade Organisation and the United Nations, are possible candidates. Yet, their global membership is so large and includes either Russia or China as well as acolyte countries that decisive policy-making would be stymied. Moreover, if the purpose of Western sanctions is to deter or arrest aggressive military activities, then a more focused response might be preferable. What was once described as NATO's "economic arm," the Coordinating Committee for Multilateral Export Control (CoCOM), might fulfill this role.[56] Established in 1949 by the US and major allied states, it was intended to deny the USSR and Warsaw Pact countries access to strategic military components and dual-use technologies. An equivalent organization, called the China

---

[51] Truss, "The Return of Geopolitics."

[52] Bruce Stokes, "The World Needs an Economic NATO," *Foreign Policy*, May 17, 2022, https://foreignpolicy.com/2022/05/17/ukraine-war-russia-sanctions-economic-nato-g7/.

[53] Stokes, "The World Needs an Economic NATO."

[54] "US Working Towards Global Coalition Far Beyond G7, NATO: White House," *Business Standard*, June 10, 2022, https://www.business-standard.com/article/international/us-working-towards-global-coalition-far-beyond-g7-nato-white-house-122031500092_1.html.

[55] Fergus Hunter et al., "Countering China's Coercive Diplomacy: Prioritising Economic Security, Sovereignty and the Rules-based Order," Policy Brief Report No. 68 (Australia Strategic Policy Institute, February 22, 2023), https://www.aspi.org.au/report/countering-chinas-coercive-diplomacy.

[56] Richard T. Cupitt and Suzette R. Grillot, "COCOM Is Dead, Long Live COCOM: Persistence and Change in Multilateral Security Institutions," *British Journal of Political Science* 27, no. 3 (July 1997): 361-389, https://doi.org/10.1017/S0007123497000185.

Committee or ChinCom, was established in 1952 to similarly deny China access to strategic technologies. Following the implosion of the Soviet Union and the end of the Cold War, CoCOM was replaced in 1995 by the Wassenaar Arrangement, but its efficacy was hampered by two factors. Firstly, in the post-Cold War era, trade had become the priority, and economic sanctions undermined that goal. Moreover, Wassenaar's purpose was more nuanced than CoCOM, aimed at facilitating responsible trade rather than obstructing it. The second problem was that Russia was a member of Wassenaar.

The Russia-Ukraine war has catalyzed diplomatic momentum to replace CoCOM. Importantly, in April 2022, the US acted to strengthen the present Global Export Controls Coalition of democratic countries, including all EU states and other major players, such as the UK, Australia, and Canada, by imposing stringent technology and software export restrictions on the defense, aerospace, and maritime sectors of Russia and Belarus.[57] This was followed in May 2022 by a US-EU Trade and Technology Council launched to agree on a policy on limiting technology exports to Russia and thus curb aggressive military intent. Subsequent to these policies, there is now a need to harness and consolidate future efforts, and an integrated G-7 and NATO body is again a possible integrated institutional mechanism for coordinating action on strategic export control that will impact both Russia and China.[58] Tighter scrutiny of strategic military and dual-use technologies is urgently required, given that Russia's war machine is highly dependent on military systems sourced from Western states. A recent report by the London-based think tank RUSI provides a stark illustration. It found that some 317 of 450 unique microelectronic components in Russian military equipment deployed in Ukraine were manufactured in the US, with the remainder supplied from European and East Asian countries.[59]

Conclusions

The expansion of Russian and Chinese coercion represents a threat to the free world. The possession of scarce resources in the hands of states hostile to liberal democracies needs to be addressed through the creation of an appropriate international institution. As evaluated in the main body of this article, there is an urgent imperative to establish an economic Article 5 framework that will provide

[57] "Commerce Announces Addition of Iceland, Liechtenstein, Norway, and Switzerland to Global Export Controls Coalition," *US Department of Commerce*, April 8, 2022, https://www.commerce.gov/news/press-releases/2022/04/commerce-announces-addition-iceland-liechtenstein-norway-and.

[58] Chiara Albanese, "EU Analysis Suggests China May Send Tech Hardware to Help Putin," *Bloomberg*, March 25, 2022, https://www.bloomberg.com/news/articles/2022-03-25/eu-analysis-suggests-china-may-send-tech-hardware-to-help-putin.

[59] Andrew Macaskill, "Exclusive: Russian Weapons in Ukraine Powered by Hundreds of Western Parts, Report Says," *Reuters*, August 8, 2022, https://www.reuters.com/business/aerospace-defense/exclusive-russian-weapons-ukraine-powered-by-hundreds-western-parts-rusi-2022-08-08/.

a collective and coordinated response to malign Russian and Chinese statecraft. An Economic NATO-type body will be required, whether a newly formed global economic entity or through a formal coordinated policy mechanism between the existing G7 and NATO organizations. The body will need to address two separate but inter-spliced challenges facing the West. Firstly, there is a need to strengthen economic security through policies designed to deter Russian and Chinese trade restrictions on food, energy, investment, and exotic minerals. Secondly, there is a belated recognition among democratic nations for an appropriate geoeconomic and strategic framework to effectively engage Chinese economic diplomacy in an era characterized by Great Power Competition. Over recent years, the knee-jerk response in Western capitals has simply been to increase military resources, but that misses the point. A more self-reliant long-term Western strategic, economic, security, and diplomatic posture is required. The poorer but strategically important nations across the world prioritize development and prosperity just as much as defense and independence. Warships and fighters alone will not achieve this goal, so a diplomatic reset is essential. Yet, any new approach that emphasizes economic fundamentals will require diplomatic commitment and economic largesse. This will not be easy in a world increasingly featuring populist political sentiment and distracted by the specter of international recession.

Disclaimer

About the Authors

Ron Matthews is Chair in Defence and Security Capability, Rabdan Academy, Abu Dhabi. Visiting Professor in Defence Economics, Cranfield University at the UK Defence Academy. Former Chair in Defence Economics, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.
E-mail: rmatthews@ra.ac.ae

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

P. Dobias & K. Christensen,
Connections QJ 21, no. 2 (2022): 41-54
https://doi.org/10.11610/Connections.21.2.03

Research Article

The 'Grey Zone' and Hybrid Activities

Peter Dobias and Kyle Christensen

Defence Research and Development Canada, Centre for Operational Research and Analysis, 60 Moody Drive, Ottawa, Ontario, Canada, http://www.drdc-rddc.gc.ca

Abstract: Military operations in the grey zone (defined here as the space between peace and war where states are currently involved in a competition continuum) present a unique challenge for military planners. Potential adversaries—well aware of NATO's conventional lethal capabilities—have been using the space below the lethal threshold of conflict with impunity to further their objectives. To re-establish effective deterrence, it is imperative that NATO develops the ability to deny its adversaries the ability to act freely in this zone below conventional conflict. That requires imposing a cost on hostile actors acting below the lethal threshold of open conflict, across multiple domains, from the tactical through the operational to the strategic level. Intermediate Force Capabilities (IFC) are the kind of tools that provide effective means of response below the lethal threshold both tactically and operationally and can effectively shape the environment across domains up to the strategic level.

Keywords: grey zone, hybrid threats, non-kinetic, non-lethal, anti-access / area denial, A2/AD, competition continuum, threshold, conventional conflict, intermediate force capabilities.

Introduction

The Current Security Environment: Hybrid Threats and the Grey Zone

In recent years, studies of the international security environment have increasingly drawn attention to what is becoming understood as hybrid threats and the

grey zone.[1] A recent RAND study defined the grey zone as "an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and non-military actions and the attribution for events." [2]

In most respects, the "coercive actions" that blend military and non-military actions together are characterized as hybrid threats. Frank G. Hoffman defines hybrid threats as:

> [A] full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. Hybrid Wars can be conducted by both states and a variety of non-state actors. These multi-modal activities can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical and psychological dimensions of conflict.[3]

Hoffman's definition has gained wide appeal because it emphasizes not only the activities of a hybrid threat but the potential actors and their intent as well. It is also consistent with definitions of grey zone in that it involves all elements of state power, actions aimed deliberately below the level of state-on-state use of force, and typically synchronized and coordinated toward objectives in an organized manner.[4]

---

1 Terms such as irregular, asymmetrical, unconventional, unrestricted, non-linear, non-traditional, new generation, next generation, full spectrum, political warfare, lawfare, and pan- or multi-domain are also being used.

2 Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, CA: RAND Corporation, 2019), 8, www.rand.org/pubs/research_reports/RR2942.html.

3 Frank G. Hoffman, *Conflict in the 21st Century: Hybrid Wars* (Arlington, Virginia: Potomac Institute for Policy Studies, December 2007), 8, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf; and Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM* 7, no. 4 (2018): 30-47, https://www.jstor.org/stable/26542705.

4 Frank G. Hoffman, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," in *2016 Index of U.S. Military Strength: Assessing America's Ability to Provide for the Common Defense*, ed. Dakota L. Wood (Washington, DC: The Heritage Foundation, 2016), accessed September 10, 2020, www.heritage.org/sites/default/files/2019-10/2016_IndexOfUSMilitaryStrength_The%20Contemporary%20Spectrum%20of%20Conflict_Protracted%20Gray%20Zone%20Ambiguous%20and%20Hybrid%20Modes%20of%20War.pdf; U.S. Department of Defense, *Quadrennial Defense Review Report* (February 2010), https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf; and Hal Brands, "Paradoxes of the Gray Zone," *E-NOTES* (Foreign Policy Research Institute, February 5, 2016), accessed September 27, 2020, https://www.fpri.org/article/2016/02/paradoxes-gray-zone/.

Ultimately, the deliberate application of hybrid tactics, techniques, and capabilities is intended to create strategic, operational, and/or tactical dilemmas for an opponent. The aim is not so much to challenge an opponent in a head-to-head confrontation,[5] but rather to constrain the options available to them, thereby maximizing one's operational freedom of movement in the area between peace and war. Because the activities take place below the threshold of armed conflict, they paint opponents into a corner (i.e., tie a state's military, diplomatic, and political hands behind its back) by forcing it to either accept the emerging status quo or use force to resolve the dilemma. Remaining below the threshold of the use of force and avoiding head-to-head confrontations with an opponent has enabled weaker states to challenge stronger states because they no longer need to engage superior adversaries in a head-to-head confrontation.[6]

Operationalizing hybrid threats involves using all elements of state power and controlling their escalation/de-escalation both vertically and horizontally.[7] The most prominent examples of these approaches currently being undertaken are by Russia, China, and Iran.[8] Russia, China, and Iran conceptualize state interactions as a "continuum of conflict" or "competition continuum" in which the area between peace and war is simply an area of conflict by other means. Russia and China combine different elements of state power (economic coercion, political influence, unconventional warfare, information operations, and cyber operations) in ways to advance their interests and in ways that their opponents do not have an effective response.[9] Iran's approach focuses more on military and technological aspects; however, its overall strategic aim is the same: to constrain, deny, and challenge an adversary's access to geostrategically important

---

5 Andrew Krepinevich, Barry Watts, and Robert Work, *Meeting the Anti-Access and Area-Denial Challenge* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2003), https://csbaonline.org/uploads/documents/2003.05.20-Anti-Access-Area-Denial-A2-AD.pdf.

6 Institute of Defence and Strategic Studies, "Countering Anti-Access/Area Denial Challenges: Strategies and Capabilities," Event Report (Singapore: S. Rajaratnam School of International Studies, December 1, 2017), https://www.rsis.edu.sg/wp-content/uploads/2018/04/ER180424_Countering-Anti-Access.pdf.

7 Erik Reichborn-Kjennerud and Patrick Cullen, "What Is Hybrid Warfare?" *Policy Brief* (Oslo: Norwegian Institute for International Affairs, January 2016).

8 Reichborn-Kjennerud and Cullen, "What Is Hybrid Warfare?"; Peter Hunter, "Political Warfare and the Grey Zone," in *Projecting National Power: Reconceiving Australian Air Power Strategy for an Age of High Contest*, Special Report 142 (Barton, Australia: Australian Strategic Policy Institute, August 2019), https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-08/SR%20142%20Projecting%20national%20power.pdf; and James K. Wither, "Making Sense of Hybrid Warfare," *Connections: The Quarterly Journal* 15, no. 2 (2016): 73-87, http://dx.doi.org/10.11610/Connections.15.2.06.

9 Sydney J. Freedberg Jr., "Cyber Warfare in the Grey Zone: Wake up, Washington," *Breaking Defense*, April 9, 2019, https://breakingdefense.com/2019/04/cyber-warfare-in-the-grey-zone-wake-up-washington/.

areas. Although there are identifiable similarities between Russia's, China's, and Iran's activities in the grey zone, there are distinct differences as well.[10]

Strategic Competitors and Challengers in the Grey Zone

Russia – 'Strategy of Limited Actions'

Russia's approach to the grey zone has colloquially become known as the "Gerasimov doctrine." [11] In his 2013 article "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," General Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces, articulated that the very "rules of war" have changed: "The role of non-military 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." [12] The focus of conflict has shifted "…in the direction of the broad use of political, economic, informational, humanitarian, and other non-military measures… in coordination with the protest potential of the population… supplemented by military means of a concealed character, including… informational conflict and the actions of special operations forces." [13] The open use of force, usually under the pretext of peacekeeping, is resorted to only at a certain stage, primarily for the achievement of final success in a conflict.[14]

There has been considerable debate as to whether the Gerasimov doctrine is in fact an actual thing. Several scholars, including Michael Kofman, Roger N. McDermott, and Mark Galeotti, have voiced skepticism that the article penned by General Gerasimov is a doctrine laying out the Russian military's blueprint for actions in Ukraine and persistent competition with the West.[15] At worst, according to Galeotti, clinging to the inaccurate application of the Gerasimov doctrine

---

10 Morris et al., *Gaining Competitive Advantage in the Gray Zone*.

11 Ofer Fridman, " On the 'Gerasimov Doctrine:' Why the West Fails to Beat Russia to the Punch," *PRISM* 8, no. 2 (2019), accessed December 5, 2021, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Fridman.pdf.

12 Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," Translated by Robert Coalson, *Military Review* 96, no. 1 (January-February 2016): 23-29, 21, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2016/.

13 Gerasimov, "The Value of Science Is in the Foresight."

14 Gerasimov, "The Value of Science Is in the Foresight."

15 M. Kofman, "Russia's armed forces under Gerasimov, the man without a doctrine," *RIDDLE Russia* (4 January 2020), accessed September 10, 2021, https://www.ridl.io/en/russia-s-armed-forces-under-gerasimov-the-man-without-a-doctrine; R.N. McDermott, "Does Russia have a Gerasimov Doctrine?" *Parameters* Spring 2016; 46(1): 97-105.; and M. Galeotti, "I'm sorry for creating the 'Gerasimov Doctrine'," *Foreign Policy* (5 March 2018), accessed March 28, 2021, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

"limits and misdirects us in our attempt to grasp and thus combat" current Russian military thinking and planning.[16] Nevertheless, notwithstanding the myth of the Gerasimov doctrine's institutionalization in Russian military strategy and operational-level planning, the article highlights important conceptual global trends with regard to current strategic military thinking.

For example, the concepts and approaches discussed in the article highlight that modern "conflict" is waged through the use of a combination of elements of state power in an effort to achieve political objectives without having to resort to the use of overt military force (though the use of covert and paramilitary force is permissible), and this includes the use and manipulation of the information and technology spectrum.[17] As noted by Supreme Allied Commander Europe (SACEUR), General Philip Breedlove, Russia's campaign in Ukraine was "…the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare." [18]

In this way, Russia does not have to match the West's military superiority. It only needs to be operationally effective in specific areas or domains and maintain its presence in areas considered geostrategically important.[19] By integrating the different elements of national power, Russia can control the preparation of the competition continuum (i.e., formerly "preparation of the battlefield"), use deliberate escalation and de-escalation tactics, and exploit multiple domains of the conflict zone to its advantage.[20]

China – Active Defense

China's strategy with regard to competition in the grey zone can be identified in the concept of "active defense." The concept was first articulated by senior military leadership in the late 1930s and finally formed the basis for the People's Republic of China (PRC) military strategy in 1949.[21] According to the U.S. Department of Defense's (DoD) annual report to Congress on military and security developments involving the PRC, active defense adopts the principles of strategic defense in combination with offensive action at the operational and tactical lev-

[16] Galeotti, "I'm sorry for creating the 'Gerasimov Doctrine'."

[17] Gerasimov, "The Value of Science Is in the Foresight;" and Arthur N. Tulak, "Hybrid warfare and new challenges in the information environment," 5th Annual Information Operations Symposium, Honolulu, Hawaii, 20-22 October 2015.

[18] Wither, "Making Sense of Hybrid Warfare," 77.

[19] Institute of Defence and Strategic Studies, "Countering Anti-Access/Area Denial Challenges."

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

[21] M. Taylor Fravel, *Active Defense: China's Military Strategy since 1949*, Book 2 (Princeton University Press, April 2019).

els. It is rooted in the principle of avoiding initiating armed conflict but responding forcefully if challenged or keeping to the stance that "we will not attack unless we are attacked, but we will surely counterattack if attacked." [22]

While China's approach to active defense has remained generally consistent since 1949, the Chinese Communist Party (CCP) began issuing revised strategic military guidelines more regularly following the Cold War. In 1993, for example, Jiang Zemin directed the People's Liberation Army (PLA) to prepare to win "local wars" under "high-tech conditions." [23] Jiang revised the PLA's strategic military guidelines after observing the United States' overwhelming dominance during the 1991 Gulf War, a war the PLA acknowledges they would have been wholly unprepared to defend against.[24]

In 2004, Hu Jintao ordered the military to focus on winning "local wars under informatized conditions," and in 2014, Xi Jinping placed greater focus on fighting and winning "informatized local wars." [25] Again, these revisions were in response to the growing role and importance information operations (IOs) were having in places such as Iraq, Afghanistan, Syria, Ukraine, and elsewhere. Similar to Russian thinking about modern warfare, Chinese political and military leaders accepted that war itself had fundamentally changed. In effect, Beijing had to adopt an approach to warfare where a weaker country (i.e., China) could engage with and potentially defend itself in a high-tech conflict against the United States.[26]

In order to accomplish this task, Beijing continues with the modernization of its military, developing and building traditional military capabilities both in terms of sophistication and reach, that are key to not only "fighting and winning" modern "informatized" wars, but also contributing to China's activities in the grey zone. As such, conventional military power is essential for deterring external

---

[22] Fravel, *Active Defense: China's Military Strategy since 1949*.

[23] Gurmeet Kanwal, *China's New War Concepts for 21st Century Battlefields* (Institute of Peace and Conflict Studies, July 1, 2007), accessed December 5, 2021, www.ipcs.org/issue_briefs/issue_brief_pdf/1577903632IPCS-IssueBrief-No48.pdf.

[24] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999), https://www.c4i.org/unrestricted.pdf.

[25] M. Taylor Fravel, "China's New Military Strategy: 'Winning Informationized Local Wars'," *China Brief* 15, no. 13 (Jamestown Foundation, July 2015), accessed December 7, 2021, https://jamestown.org/program/chinas-new-military-strategy-winning-informationized-local-wars/.

[26] To highlight the point, the most recent DoD report to Congress on military and security developments involving the PRC states: "The PLA's evolving capabilities and concepts continue to strengthen the PRC's ability to "fight and win wars" against a "strong enemy" [a likely euphemism for the United States]." Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2021* (U.S. Department of Defense, November 2, 2021), https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF; and Liang and Xiangsui, *Unrestricted Warfare*.

powers from interfering in the internal affairs of China (particularly its core interests) and maintaining its ability to threaten the escalation of the use of conventional military force.[27]

However, senior PLA leaders have also emphasized the need to use coercive threats and/or violence below the level of armed conflict against states and other actors to safeguard China's sovereignty and national interests.[28] Beijing's aim is to pursue national goals through political maneuvering (diplomatic pressure, false narratives, and harassment) and displaying increasing levels of threats rather than engaging in risky and expensive head-to-head physical confrontations. Accordingly, the strategy involves using a multitude of means, both military and non-military, to strike at an enemy before and during a conflict.[29] It includes computer hacking, subversion of banking systems, markets, currency manipulation (financial war), media disinformation, urban warfare, and even terrorism.[30]

Most importantly, it is the interplay—or blending—of unconventional and traditional military tactics along with threats (implied or explicit) of the use of conventional military force that makes China's approach in the grey zone challenging. The most prominent example of this approach is displayed in the South China Sea, where Beijing has repeatedly and effectively integrated conventional and unconventional units (military, law enforcement, and militia) and tactics (blurring the distinction between military and constabulary activities) to achieve synergistic effects.[31]

China has utilized "irregular maritime forces," in this case, state-sanctioned fishermen-turned militia, that are neither ordinary merchant ships nor random fishermen. Andrew S. Erickson and Conor M. Kennedy have termed these irregular forces "maritime militia."[32] These paramilitary forces operate in pre-

---

[27] Liang and Xiangsui, *Unrestricted Warfare*; and *China's National Defense in the New Era* (The State Council Information Office of the People's Republic of China, July 2019), http://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

[28] Office of the Secretary of Defense, *Annual Report to Congress 2021*.

[29] Alessio Patalano, "When Strategy Is 'Hybrid' and not 'Grey': Reviewing Chinese Military and Constabulary Coercion at Sea," *Pacific Review* 31, no. 6 (2019): 811-839, https://doi.org/10.1080/09512748.2018.1513546.

[30] Wither, "Making Sense of Hybrid Warfare"; Fravel, "China's New Military Strategy."

[31] Liang and Xiangsui, *Unrestricted Warfare*; Patalano, "When Strategy Is 'Hybrid' and not 'Grey'."

[32] Andrew S. Erickson and Conor M. Kennedy, "Tanmen Militia: China's 'Maritime Rights Protection' Vanguard," *The National Interest*, May 6, 2015, https://nationalinterest.org/feature/tanmen-militia-china's-maritime-rights-protection-vanguard-12816; Andrew S. Erickson and Conor M. Kennedy, "Irregular Forces at Sea: Not 'Merely Fishermen' – Shedding Light on China's Maritime Militia," *Center for International Maritime Security*, November 2, 2015, accessed April 29, 2020, http://cimsec.org/new-cimsecseries-on-irregular-forces-at-sea-not-merely-fishermen-shedding-light-on-chinas-maritime-militia/19624.

planned roles and close coordination with other Chinese maritime forces (coast guard, the Maritime Safety Administration, and/or the PLA Navy).[33] The use of the maritime militia, acting as fishermen, creates a demand for the deployment of maritime forces (i.e., the threat of the use of force), in this case, the PLA Navy, to come to their aid. Invariably China has demonstrated a willingness to threaten and use force, albeit constrained, in support of its maritime militia to harass civilian and military vessels.[34] Using military and paramilitary organizations in this way in the grey zone makes it difficult for navies and coast guards in the region to respond to and/or counter China's activities in the region.[35]

Iran – A2/AD and Proxy Wars

Iran's exploitation of the grey zone involves the use of an anti-access/area denial (A2/AD) strategy in a direct confrontation and the use of proxies and irregular means (cyber, terrorism) to pursue their objectives through plausibly deniable activities.[36] A2 is defined as preventing or restricting a military force's ability to move into a theater of operations. AD is defined as preventing or denying the freedom of action of forces already in theater from using bases (permanent, maritime, mobile, or otherwise) for operations.[37] If A2 strategies aim at preventing a military force from entering into a theater of operations, AD strategies aim at denying them the freedom of action necessary to conduct operations when there.

Within the context of this strategy, Iran uses its naval, air, and missile forces, as well as paramilitary and other clandestine units, in an attempt to either control or deny others access to the Strait of Hormuz. Iran has developed/is developing a variety of weapon systems, including small boats (go fast), fast attack/missile-firing surface combatants, submarines, short-range unmanned aerial vehicles (UAVs), smart mines, long-range missile systems, precision-guided munitions, shore-based anti-ship missiles (ASMs) and anti-ship cruise missiles (ASCMs), over the horizon targeting systems, long-range strike aircraft, coastal defense artillery, surface-to-air missiles, and even ballistic missiles to swarm,

---

[33] Erickson and Kennedy, "Irregular Forces at Sea: Not 'Merely Fishermen'."

[34] ABS-CBN News, "PH Verifying Reported Chinese Harassment of Local Fishers," April 20, 2017, https://news.abs-cbn.com/news/04/20/17/ph-verifying-reported-chinese-harassment-of-local-fishers; and "South China Sea Incident Tracker," *CSIS iDeas Lab* (Center for Strategic and International Studies), accessed September 27, 2020, https://csis-ilab.github.io/cpower-viz/csis-china-sea/.

[35] Erickson and Kennedy, "Tanmen Militia."

[36] Ariane M. Tabatabai and Colin P. Clarke, "Iran's Proxies Are More Powerful Than Ever," Commentary, *TheRANDblog*, October 16, 2019, accessed December 5, 2021, www.rand.org/blog/2019/10/irans-proxies-are-more-powerful-than-ever.html.

[37] Andrew F. Krepinevich, "Why AirSea Battle?" (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2010), https://csbaonline.org/uploads/documents/2010.02.19-Why-AirSea-Battle.pdf; and Krepinevich, Watts, and Work, *Meeting the Anti-Access and Area-Denial Challenge*.

harass, interdict, control, deny, and attack military and civilian vessels in the region.[38] Recent evidence indicates Iran may even use advanced technologies such as satellite technology, global positioning system (GPS) spoofing, and cyber-attacks to facilitate its A2/AD strategy.[39]

Unlike the Gerasimov doctrine and active defense, Iran's exploitation of the grey zone is more narrowly defined in terms of a military and technological solution. However, the combined threat these layered systems pose can make transiting the Strait of Hormuz and conducting maritime operations challenging for naval forces.[40] In this way, similar to the Gerasimov doctrine and active defense, Iran does not have to be the strongest force in a confrontation; it just needs to be strong enough to prevent an adversary from gaining access to the theater of operations and/or conducting operations from within the region.[41]

One important aspect of Iran's A2/AD strategy is that it interlaces traditional elements (go fasts and ASMs) with high-tech elements (GPS spoofing) with covert and clandestine elements (commercial ships/vehicles to launch ASCMs, use of proxy forces). Iran will pursue this approach that mixes advanced technology, "maritime guerilla" tactics, and traditional maritime warfare to deny, control, and threaten passage through the Strait of Hormuz.[42]

---

[38] Defense Intelligence Agency, *Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance* (Washington, D.C.: U.S. Government Publishing Office, November 2019), https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/Iran_Military_Power_LR.pdf; Defense Intelligence Ballistic Missile Analysis Committee, *Ballistic and Cruise Missile Threat* (Wright-Patterson, OH: National Air and Space Intelligence Center, June 2017), https://irp.fas.org/threat/missile/bm-2017.pdf; and Farzin Nadimi, "The Counterintuitive Role of Air Defense in Iran's Anti-Status Quo Regional Strategy," Policy Analysis, PolicyWatch 2748 (The Washington Institute for Near East Policy, January 11, 2017), accessed April 29, 2020, https://www.washingtoninstitute.org/policy-analysis/counterintuitive-role-air-defense-irans-anti-status-quo-regional-strategy.

[39] Ian W. Gray, "Cyber Threats to Navy and Merchant Shipping in the Persian Gulf," *The Diplomat*, May 5, 2016, https://thediplomat.com/2016/05/cyber-threats-to-navy-and-merchant-shipping-in-the-persian-gulf/.

[40] Defense Intelligence Agency, *Iran Military Power*.

[41] Anthony H. Cordesman and Aaron Lin, *The Iranian Sea-Air-Missile Threat to Gulf Shipping* (Centre for Strategic and International Studies, February 2015), https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150219_Cordesman_IranAirSeaMissileThreat_Web.pdf.

[42] United States Institute of Peace, "Timeline: US-Iran Naval Encounters," *The Iran Primer*, August 29, 2016, updated January 22, 2018, https://iranprimer.usip.org/blog/2016/aug/29/timeline-us-iran-naval-encounters; International Crisis Group, "Strait of Hormuz," *Flashpoint*, April 23, 2020, accessed September 10, 2020, www.crisisgroup.org/trigger-list/iran-us-trigger-list/flashpoints/hormuz; Mark Gunzinger and Christopher Dougherty, *Outside-In: Operating from Range to Defeat Iran's Anti-Access and Area-Denial Threats* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2011), https://csbaonline.org/research/publications/outside-in-operating-from-range-to-defeat-irans-anti-access-and-area-denial.

A second important aspect of the Iranian approach to hybrid threats in the grey zone is its use of proxies. A recent study by the Center for Strategic and International Studies observed that:

> Tehran wields influence in the Middle East through its use of non-state partners, despite renewed U.S. sanctions against Iran and a U.S. withdrawal from the nuclear deal. Iran's economic woes have not contributed to declining activism in the region – at least not yet. If anything, Iranian leaders appear just as committed as ever to engagement across the Middle East using irregular methods.[43]

The size of Iran's partner proxy forces—trained, equipped, and coordinated by Iran—is estimated to be between 140,000 and 190,000. While these proxies actively support Iran's strategic goals, Tehran does not control them completely; this is by design. Iran has never tried to make these proxies completely dependent on itself. Instead, Iran has tried to help these groups become more self-sufficient, allowing them to integrate into their countries' political and economic processes and even build their own defense industries, thus reducing their reliance on Iran's supplies.[44] Nevertheless, Iran has used these proxies very effectively in its power struggle in the Middle East, both in its struggle with Israel and in its competition with Saudi Arabia.[45]

Overview of the Current Security Environment

Although exploitation of the grey zone (i.e., exploiting the space below the threshold of armed conflict) and A2/AD type activities are not new in and of themselves,[46] the prevalence of their use across a full spectrum of capabilities and domains by Russia, China, and Iran in recent years poses unique challenges for military planners. A review of Russia's and China's approach to grey zone activities reveals that Russia is generally more focused on messaging and information operations. China is less inhibited in the actual use of measured, albeit constrained, force. In terms of actual confrontation, Russia and China have used harassment tactics such as potentially risky low-altitude overflights of allied vessels at sea or close approaches to allied planes in the air. In contrast, though,

---

[43] Seth G. Jones, "War by Proxy: Iran's Growing Footprint in the Middle East," *CSIS Briefs* (Center for Strategic & International Studies, March 11, 2019), accessed December 5, 2021, https://www.csis.org/analysis/war-proxy-irans-growing-footprint-middle-east.

[44] Tabatabai and Clarke, "Iran's Proxies Are More Powerful Than Ever."

[45] Nakissa Jahanbani, " Reviewing Iran's Proxies by Region: A Look Toward the Middle East, South Asia, and Africa," *CTC Sentinel* 13, no. 5 (May 2020): 39-49, https://ctc.westpoint.edu/reviewing-irans-proxies-by-region-a-look-toward-the-middle-east-south-asia-and-africa/; and F. Gregory Gause III, "Beyond Sectarianism: The New Middle East Cold War," *Brookings Doha Center Analysis Paper*, no. 11 (July 2014), 11, www.brookings.edu/wp-content/uploads/2016/06/english-pdf-1.pdf.

[46] James Lacey, "Battle of the Bastions." *War on the Rocks*, January 9, 2020, https://warontherocks.com/2020/01/battle-of-the-bastions/.

China had demonstrated a willingness to use actual force through the use of its maritime militia, not only to harass and ram both civilian and military vessels but to open fire on them as well.[47] Similarly, even rogue countries such as Iran have demonstrated a willingness to use paramilitary assets to harass allied shipping in the Persian Gulf, Strait of Hormuz, and the Gulf of Oman.[48]

What is most important about these approaches to grey zone competition is that the hybrid tactics in the grey zone are synchronized, choreographed, and, to a large extent, planned and controlled. As articulated by Erik Reichborn-Kjennerud and Patrick Cullen, hybrid tactics in the grey zone are best understood by focusing on the various characteristics of an actor's capabilities, the ways they are employed, and to what effect.[49]

By employing all elements of power, the ability to escalate vertically and horizontally increases one's ability to create strategic effects. Not only does this assume a unity of effort among the different elements of national power, but it also assumes a certain degree of centralized operational command and control and strategic coordination between the elements.[50] Therefore, while it is important to increase lethality, it is argued here that it is also important to develop capabilities that would enable allied and coalition forces to respond to situations short of armed confrontation in a unified, calibrated, and synchronized manner.

Currently, NATO and its allies can do very little to deter adversaries from hostile activities below open conflict. Even when discussing conventional deterrence in the case of overt military aggression, there is a consensus that deterrence by punishment (i.e., increasing the cost to the adversary after the fact) will not be effective.[51] While deterrence by punishment still applies in cases of nuclear confrontation, one must argue that the rise of advanced conventional military capabilities/challenges, transnational terrorist and criminal networks, and digital-based threats has tipped the deterrence scales toward deterrence by denial (i.e., decreasing the perceived benefit to the hostile actor).[52] In general, deterrence requires clear signaling to the adversary of the capability and intent to respond if a certain threshold is crossed. One of the challenges in deterring hostile actions in the grey zone is that much of the conflict resides in the political domain where

---

[47] ABS-CBN News, "PH Verifying Reported Chinese Harassment of Local Fishers." See also "South China Sea Incident Tracker."

[48] For a full list of incidents in the Persian Gulf, Strait of Hormuz, and Gulf of Oman regions from May 1984 to January 2018, see United States Institute of Peace, "Timeline: US-Iran Naval Encounters;" and for an additional list of incidents from 15 June 2017 to 22 April 2020, see International Crisis Group, "Strait of Hormuz."

[49] Reichborn-Kjennerud and Cullen, "What Is Hybrid Warfare?" 2.

[50] Reichborn-Kjennerud and Cullen, "What Is Hybrid Warfare?"

[51] Michael Petersen, "The Perils of Conventional Deterrence by Punishment," *War on The Rocks*, November 11, 2016, https://warontherocks.com/2016/11/the-perils-of-conventional-deterrence-by-punishment/.

[52] Alex S. Wilner and Andreas Wenger, eds., *Deterrence by Denial: Theory and Practice* (Cambria Press, 2021), 1-2.

clear signaling of the thresholds for a lethal military response is often absent, goes unnoticed, or worse, is misperceived. This, of course, has conceptual and practical implications.[53]

A number of writers have identified the need to develop capabilities that deny adversaries the ability to act with impunity within the grey zone, thus avoiding a lethal confrontation with US and NATO.[54] Effective deterrence includes political, economic, and military means. Unfortunately, mere military presence, or the threat of lethal force, is often insufficient to deter malicious behavior, as demonstrated by the frequent provocative actions taken by adversary forces toward NATO units. Tactically and operationally—and paradoxically—not using force can also result in losses. This includes loss of access and mobility, loss of initiative, and even loss of NATO platforms and lives. By exploiting ambiguity, adversaries pose a dilemma: "over-reaction looks pre-emptive and disproportionate if clear responsibility for an attack has not been established, but the lack of a response leaves a state open to death by a thousand cuts." [55]

From this perspective, Intermediate Force Capabilities (IFC) have a great deal of applicability and relevance to coalition operations at both tactical and operational levels and across all domains. In an environment where adversaries (both state and possibly non-state) will attempt to exploit the operational space between war and peace and blur the line between military and non-military actions by attempting to keep engagements below the threshold of conventional conflict, it will be desirable to have a class of response options between doing nothing or employing lethal force. This is even more important because current response options can be politically unpalatable and allow an adversary to seize the initiative and maintain the moral high ground.

Thus, IFCs improve NATO's ability to address the challenges of hybrid threats in the grey zone. As identified in the NATO Warfighting Capstone Concept:

> Transposing non-physical domains, like cyber and space, and the pervasive information environment onto traditional warfighting domains (air, land and maritime) leads to a multidimensional battlespace: physical, virtual, and cognitive. Developing cohesive strategy in all operational domains in order to be

---

[53] Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverley Hills, CA: Sage Publications, 1977).

[54] Katie Crombe, Steve Ferenzi, and Robert Jones, "Integrating Deterrence across the Gray – Making It More than Words," *Military Times*, December 9, 2021, www.militarytimes.com/opinion/commentary/2021/12/08/integrating-deterrence-across-the-gray-making-it-more-than-words/.

[55] Bryan Clark, Mark Gunzinger, and Jesse Sloman, *Winning in the Gray Zone: Using Electromagnetic Warfare to Regain Escalation Dominance* (Center for Strategic and Budgetary Assessment, 2017), accessed December 5, 2021, https://csbaonline.org/uploads/documents/CSBA6305_(EMS2_Report)Final2-web.pdf; Andrew Mumford, "Ambiguity in Hybrid Warfare," Strategic Analysis 24 (NATO Hybrid CoE, September 17, 2020), https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-24-ambiguity-in-hybrid-warfare/.

effective within the multi-dimensional battlespace is the key to maintaining decisive advantage against any adversary.[56]

IFCs include a vast array of capabilities ranging from physical (e.g., directed energy non-lethal systems such as radio-frequency counter mobility), electromagnetic and cyber warfare, and information operations to the use of Special Forces[57] and Stability Policing. To be sure, it is important to have and maintain traditional lethal military capabilities to deal with situations in extremis. However, even if the use of lethal force is warranted and even desired, IFCs can be used to mitigate undesirable outcomes and thus decrease the political and narrative cost to NATO. For example, IFCs can be used to isolate targets and move them from socially or politically sensitive areas or areas where high collateral damage could present a problem.

Summary

NATO adversaries—well aware of NATO's conventional lethal capabilities, as well as NATO's threshold(s) for the use of lethal force—have been using the space below the lethal threshold of conflict with impunity to further their strategic objectives. This creates a strategic dilemma for NATO, where it finds itself unable to act in the space between the presence and the use of lethal force. Acting at either of these extremes can carry high operational and strategic costs. The IFC concept introduces a vast array of capabilities that can fill this space. To be sure, it is important to have and maintain traditional lethal military capabilities to deal with situations in extremis. However, as this strategic review shows, it is becoming increasingly important and necessary to develop capabilities that enable NATO and coalition forces to respond to complex hybrid threats in situations short of an armed confrontation.

[56] John W. Tammen, "NATO's Warfighting Capstone Concept: Anticipating the Changing Character of War," *NATO Review*, July 9, 2021, https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/.

[57] Keith Pritchard, Roy Kempf, and Steve Ferenzi, "How to Win an Asymmetric War in the Era of Special Forces," *The National Interest*, October 12, 2019, https://nationalinterest.org/feature/how-win-asymmetric-war-era-special-forces-87601.

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.

About the Authors

Peter Dobias – see the CV on p. 9 of this issue, https://doi.org/10.11610/Connections.21.2.00.

Kyle Christensen is a Strategic Analyst at Defence Research & Development Canada, Centre for Operational Research and Analysis (DRDC CORA), Ottawa, Canada. He is currently Director, Operational Research and Analysis (OR&A) at Canadian Joint Operations Command (CJOC). His previous research postings include NATO's Joint Analysis and Lessons Learned Centre (JALLC), Lisbon, Portugal; the Canadian Joint Warfare Centre (CJWC), Ottawa, Canada; and the Directorate of Maritime Strategy (DMS), National Defence Headquarters, Ottawa, Canada. His research background and interests include Arctic/ circumpolar security and defence, Asia-Pacific maritime security and defence, North Atlantic/NATO security, as well as wargaming and operational research and analysis. *E-mail*: Kyle.Christensen@forces.gc.ca

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

Susan LeVine, *Connections QJ* 21, no. 2 (2022): 55-66
https://doi.org/10.11610/Connections.21.2.04

Research Article

Nonlethal Weapons and Intermediate Force: A Necessary Complement to Lethality

Susan LeVine

Joint Intermediate Force Capabilities Office, https://jnlwp.defense.gov/

Abstract: This article updates a previous publication, "Beyond Bean Bags and Rubber Bullets: Intermediate Force Capabilities Across the Competition Continuum," highlighting the relevance of non-lethal weapons as intermediate force capabilities to the U.S. 2022 National Defense Strategy and NATO's 2022 Strategic Concept. Intermediate force capabilities can strengthen deterrence, providing active or defensive measures to counter aggression below the level of armed conflict, enable military operations among civilian populations in urban environments, and support establishing post-conflict safe and secure environments for transition to host nation governance.

Keywords: non-lethal weapons, intermediate force capabilities, deterrence, gray zone, protection of civilians, urban operations, mobility, infantry, stabilization, stability policing, maritime domain, land domain, NATO.

Introduction

The phrase *nonlethal weapons* often brings to mind capabilities such as bean bags, rubber bullets, pepper spray, and electric stun guns. These capabilities are used domestically by law enforcement and by the military, primarily for protection and security missions. Nonlethal weapons (NLW) technology, however, has advanced significantly over the past 20 years. Technological advancements, including the development of prototype-directed energy capabilities, could provide a variety of counter personnel and counter material effects without destruction. Could this new generation of capabilities provide senior leaders and operational commanders with intermediate force options that support the full spectrum of military objectives? If so, how do they fit in as a complement to the traditional lethality emphasis of military forces?

Evolution

The idea and military need for NLW are not new. In 1993, the U.S. National Security Strategy (NSS) identified nonlethal weapons as one of several key opportunities for the future defense arena. The NSS noted that, in peacetime, these future capabilities would be a deterrent, and in wartime, they would be essential to survival and success on the battlefield.[1] Interest in NLW continued to grow through the 1990s when then-U.S. Marine Corps Lieutenant General Anthony Zinni's efforts to make them available during operations in Somalia for the withdrawal of United Nations (UN) peacekeeping troops in Operation *United Shield* brought them into focus.[2] The situation was complex; the availability of NLW allowed the troops to make clear to local civilians that UN forces would be firm in maintaining order and apply minimal force as required. Subsequently, Congress directed the DOD to establish centralized responsibility for the development of NLW technology, leading to the designation of the Marine Corps as the DOD NLW executive agent, as well as to the publication of a DOD NLW policy directive.

The policy directive described NLW as a means to reinforce deterrence and expand the range of options available to commanders, including the ability to adapt and tailor escalation of force options to the operational environment, de-escalate situations to preclude the unnecessary application of lethal force, and enhance the effectiveness and efficiency of lethal weapons.[3] Nowhere does DOD policy imply that NLW are intended to make for a kinder or gentler military force or that they are limited to military law enforcement applications. The policy also emphasizes that NLW are not a prerequisite for the use of lethal force, nor are they guaranteed to have a zero percent chance of associated fatalities or significant injury. Rather, NLW are intended to provide a range of scalable options that offer an *intermediate* level of force to fill the gap between presence and lethal effects in those situations when it is desired to minimize risk to innocent civilians or the surrounding environment.

In 1999, NATO published a nonlethal weapons policy, agreed to by the North Atlantic Council, which is comprised of all the heads of state or government of NATO member nations.[4] The NATO NLW policy included many of the same at-

---

1 "National Security Strategy of the United States" (Washington, DC: White House, January 1, 1993), https://nssarchive.us/wp-content/uploads/2020/04/1993.pdf.

2 Anthony Zinni and Gary Ohls, "No Premium on Killing," *Naval Institute Proceedings* 122, no. 12 (December 1996), https://www.usni.org/magazines/proceedings/1996/december/no-premium-killing.

3 Department of Defense (DOD) Directive 3000.03E, "DOD Executive Agent for Non-Lethal Weapons (NLW) and NLW Policy" (Washington, DC: DOD, Incorporating Change 2, August 31, 2018), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300003p.pdf?ver=2018-10-24-112944-467.

4 "NATO Policy on Non-Lethal Weapons" (Brussels, BE: North Atlantic Treaty Organization, October 13, 1999, https://www.nato.int/cps/en/natohq/official_texts_27417.htm.

tributes of the U.S. policy. However, despite the policies and high-level endorsements and nearly 30 years later, NLW are minimally integrated within the military forces of the US or other NATO member nations. What has occurred over the last three decades is a steady pace of research with promising results on a wide range of technologies with applicability to NLW. Effects without destruction delivered at extended ranges, that last for greater durations and that are delivered from a variety of platforms are now possible. Notably, human effects research has accompanied technology development, providing the basis for risk of significant injury assessments that will enable confidence in use by the military. If used to its full potential, this new generation of nonlethal weapons—better described as a subset of intermediate force capabilities (IFCs)—could offer an array of options to senior leaders and commanders when the use of lethal force is either unnecessary or not desired. IFCs are an evolving construct that wholly includes nonlethal weapons and may also include other capabilities not intended to cause lethal effects.

Today's Binary Option: Lethal Force or No Force

The U.S. 2022 National Defense Strategy (NDS) acknowledges the challenges arising from dramatic geopolitical, technological, economic, and environmental change. It directs the DOD to act urgently to sustain and strengthen US deterrence, with the People's Republic of China as the pacing challenge in the Indo-Pacific and the Russia challenge in Europe as Defense priorities.[5] The binary peace-war framework that has historically been associated with the U.S. national security posture is evolving. The NDS recognizes that traditional military tools may not always be the most appropriate response to competitors' gray zone methods – coercive approaches that may fall below perceived thresholds for US military action.[6] While dominant lethality is absolutely essential as a means to deter and prevail in armed conflict, it has not been successful in deterring Chinese aggression in the Indo-Pacific nor Russian aggression in Ukraine. As our adversaries continue to conduct coercive and aggressive acts, the military remains trained and equipped to provide a binary response primarily – through the use of lethal force or no force at all. Intermediate force capabilities could provide active or defensive measures for the military to use as needed when a mission of presence is insufficient, or the use of lethal force is undesired or risks unnecessary escalation.

---

5 *2022 National Defense Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2022), https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

6 *2022 National Defense Strategy of the United States of America*, 12.

Deterring Aggression in the Maritime Domain

It is well documented that China is claiming and building defenses on disputed islands in the South China Sea, turning submerged reefs into artificial islands and generally attempting to dominate the region. According to a report by the Center for Strategic and Budgetary Assessments, the Chinese government uses a combination of civilian fishing vessels, coast guard ships, and maritime law enforcement troops to protect its island-building efforts. The report notes that because these vessels are unarmed, US naval forces cannot respond with military force without significantly escalating the confrontation.[7]

US interests in this increasingly contested region include freedom of navigation for its fleet and those of its allies and partners. China's civilian fishing fleet is emerging as a third element of its maritime forces.[8] There have been numerous incidents of nonmilitary Chinese surface vessels serving as government proxies and approaching US or allied vessels and behaving in a provocative fashion. These actions are largely unopposed as island-building continues while the world's most powerful and lethal military force watches without an appropriate counter. China's gray zone activities are similar to the actions of Russia during their 2014 illegal annexation of Crimea in which "little green men" (well-equipped forces without an identifiable uniform) were used to achieve a military objective of taking control of a region without an overt Russian military presence.

In an article titled "Maritime Hybrid Warfare is Coming," James Stavridis described a hypothetical future scenario in which nonattributable speedboats manned by "little blue sailors" attack dozens of Vietnamese fishing vessels, giving China an excuse to provide protection in the region and reaffirm its sovereignty over the South China Sea.[9] The point of the article was to highlight the need for the United States to analyze and fully understand how such hybrid warfare approaches translate to the maritime sphere, to highlight the importance of developing tactical and technological counters, and to train and exercise with US coalition partners against this threat.

Intermediate force capabilities are a potential technological counter to the maritime scenario described by Admiral Stavridis. Long-range acoustic hailers paired with translation devices could provide clear verbal warnings; eye-safe

---

7 Bryan Clark, Mark Gunzinger, and Jesse Sloman, *Winning in the Gray Zone: Using Electromagnetic Warfare to Regain Escalation Dominance* (Washington, DC: Center for Strategic and Budgetary Assessments, October 5, 2017), https://csbaonline.org/research/publications/winning-in-the-gray-zone-using-electromagnetic-warfare-to-regain-escalation.

8 Todd Crowell and Andrew Salmon, "Chinese Fishermen Wage Hybrid 'People's War' on Asian Seas," *Asia Times* (Hong Kong), September 8, 2018, www.asiatimes.com/2018/09/article/chinese-fisherman-wage-hybrid-peoples-war-across-asias-seas/.

9 James Stavridis, "Maritime Hybrid Warfare Is Coming," *Naval Institute Proceedings* 142, no. 12 (December 2016), https://www.usni.org/magazines/proceedings/2016/december/maritime-hybrid-warfare-coming.

dazzling lasers could deliver visual warnings and provide obscuring glare to personnel, windshields, and optics of approaching vessels or unmanned aerial systems; nonlethal "flash-bang" warning munitions could be fired directly in front of, or over, vessels instead of using a lethal shot across the bow. Next-generation high-power radio frequency-directed energy weapons could disrupt electronic controls and shut off vessel engines without harming occupants, and millimeter wave active denial-directed energy technology could physically, but nonlethally, repel personnel on approaching vessels. While many of these IFCs have had initial integration and testing and/or have been used in maritime exercises, they are not integrated or resourced at a level within DOD that they would be considered mainstream.

China and its proxies conduct these hybrid tactics largely unopposed. The use of IFCs would allow the military to push back against the provocative actions with a measured, deterrent response, denying US competitors unopposed gray zone operations or propaganda victories. Denying China the use of its proxy maritime militia would either diminish its subterfuge to harass the fleets of the United States and its partners or require China to be more overt through the use of its military assets. The latter would increase China's cost, time, and effort – reducing available resources to invest in pursuing lethality parity with the United States.

Protection of Civilians in the Land Domain

The Russian invasion of Ukraine and its indiscriminate use of force against civilians has united most nations of the world against the Russian aggression and has strengthened the NATO alliance. US and NATO strategic guidance highlights the importance of the protection of civilians in times of conflict. The 2016 NATO Policy for the Protection of Civilians recognizes that all feasible measures must be taken to avoid, minimize, and mitigate harm to civilians.[10] In 2022, DOD published an action plan to mitigate civilian harm during operations.[11]

Intermediate force capabilities could complement lethal systems during complex operations in urban environments, where multiple studies suggest that most future wars would take place and where interactions with civilians cannot be avoided.[12] How well prepared are US and NATO forces to maneuver to an objective in an urban environment which might be impeded either intentionally

[10] "NATO Policy for the Protection of Civilians," endorsed by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, July 8-9, 2016 (Brussels, BE: North Atlantic Treaty Organization, July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133945.htm.

[11] U.S. Department of Defense (DoD), *Civilian Harm Mitigation and Response Action Plan (CHMR-AP)* (Washington, DC: DoD, August 2022), https://media.defense.gov/2022/aug/25/2003064740/-1/-1/1/civilian-harm-mitigation-and-response-action-plan.pdf.

[12] Joe Lacdan, "Warfare in Megacities: A New Frontier in Military Operations," *Army News Service*, May 28, 2018, https://www.army.mil/article/205817/warfare_in_megacities_a_new_frontier_in_military_operations.

or unintentionally by civilian pedestrian and/or vehicular traffic? During peacetime, a host nation may provide local security for a convoy or a maneuver element. But in times of armed conflict, in enemy territory, how would the U.S. and/or NATO contend with this situation? To aid in clearing paths, selected armored vehicles, including tanks and personnel carriers, could be equipped with an IFC kit for the Common Remote Operator Weapon Station (CROWS). The CROWS is widely used on armored vehicles with lethal systems, such as the MK19 automatic grenade launcher and the M2 .50 caliber machine gun. The IFC kit would complement lethality by offering infantry and armor units a readily available escalation of force option that could be employed while under armor. For example, an acoustic hailer paired with a translation device, a bright white light, and an eye-safe dazzling laser integrated into the CROWS would provide clear warnings and visual suppression as convoys move through city streets. Future IFCs could include millimeter wave-directed energy to repel personnel and high-power microwave-directed energy to stop vehicles.

Scenarios such as unarmed civilians, including children, standing down a convoy by throwing rocks while cell phones livestream the scene across social media provide a true dilemma for military forces. The convoy commander could choose to win the engagement with lethal force but then quickly lose the war in information space. Intermediate force capabilities empower military forces with a proportional response to civilians who might interfere with the convoy's movement. In urban environments, the use of IFCs would support mission accomplishment and serve as a counter to adversaries who have little regard for civilian casualties or collateral damage and who would seek to exploit social media in an attempt to sway American and global public opinion against US and/or NATO forces.

Enduring Need: Stability and Security Operations

In his book *Decision Points*, President George W. Bush lamented the "one important contingency for which we had not adequately prepared," which was the descent of Baghdad into a state of lawlessness that included the looting of precious artifacts from Iraq's national museums. President Bush noted that the "damage done in those early days created problems that would linger for years. The Iraqis were looking for someone to protect them. By failing to secure Baghdad, we missed our first chance to show that we could." [13]

The looting described by President Bush illustrates the quandary faced by military forces armed almost exclusively with lethal weapons. While the use of lethal force on looters may have been legally permissible, US servicemembers killing Iraqi civilians that they had just liberated from a brutal dictator would have been detrimental to the mission. Alternately, a military force trained and equipped with IFCs would have had options to deter the looters, demonstrating

[13] George W. Bush, *Decision Points* (New York, NY: Crown Publishing Group, 2010).

the US commitment to maintain the security of the civilian populace to the host country—and the world—while minimizing civilian casualties.

The challenges in Iraq continued for years. In 2006, Lieutenant General Peter Chiarelli, USA, commanding general Multi-National Corps – Iraq, was convinced that US units' missteps were contributing to the insurgency and violence, particularly in the escalation of force incidents in which a perceived threat to coalition troops resulted in the death or injury of civilians. An associated study found that 81 percent of escalation of force incidents occurred during coalition force movement under conditions that gave soldiers and marines little time—often only seconds—to make life-and-death decisions on whether approaching Iraqis were a threat.[14]

Many of the escalations of force incidents occurred at checkpoints where US forces were primarily equipped with signal flares, traffic paddles, and lethal weapons. The results of a 2012 military utility assessment (MUA) conducted by the U.S. Army at Fort Benning, Georgia, indicated that increased availability of IFCs might have had a positive impact on checkpoint escalation of force incidents. The MUA evaluated the utility of IFCs at a snap vehicle checkpoint to stop cars that matched specific intelligence criteria.[15] The scenario was not a vehicle checkpoint typically seen at entrances to bases but a hasty one meant to be set up quickly by maneuver elements of an infantry unit instead of security forces and with no advance warning to the local populace. During the assessment, soldiers had a baseline capability set to warn approaching vehicles, and this did not include IFCs. An enhanced capability set equipped with IFCs was used later. Numerous iterations of multiple scenarios were conducted where the intent of approaching vehicles was unclear. When IFCs were used, vehicles were detected, hailed, warned, and stopped an average of 70 meters farther away. Additionally, vehicles were 80 percent more likely to stop prior to the use of lethal force, and the likelihood of civilian wounding decreased by 77 percent.

The IFCs used in these scenarios included acoustic hailing devices, green dazzling lasers, 40-millimeter and 12-gauge flash-bang warning munitions, and a lightweight vehicle arresting device. The baseline set consisted of signal flares, traffic paddles, and lethal weapons. Employed in a layered defense, the availability of these relatively low-cost IFCs increased the soldiers' ability to conduct threat assessments of oncoming cars, communicate with and signal to vehicles, de-escalate a potentially lethal scenario, and reduce civilian casualties. The MUA's results provide a quantitative look at the value of IFCs integrated across the joint force and not only in the law enforcement or security forces communities.

---

[14] Joel Rayburn and Frank Sobchak, eds., *The U.S. Army in the Iraq War: Invasion, Insurgency, Civil War 2003-2006,* Volume 1 (Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College Press, January 2019), 548, https://apps.dtic.mil/sti/pdfs/AD1066345.pdf.

[15] *Entry Control Check Point Military Utility Assessment Report* (Quantico, VA: Joint Intermediate Force Capabilities Office, 2012).

Lessons *Not* Learned?

The following are key questions for military forces: Have the lessons from post-conflict Iraq and Afghanistan been learned? Will future post-conflict security environments fare any better? A case study by the U.S. Army's Peace Keeping and Stability Operations Institute on the post-conflict environment following a hypothetical conventional war with North Korea in which South Korea and the United States prevail provides an illustrative example.[16] The study examined the aftermath of a kinetic battle, where a tremendously large—and most likely starving and frightened—population would endure. The following case study questions illustrate the challenges:

- How would the immediate security needs of the population be met, especially with several hundred rogue North Korean soldiers and police officers on the loose who have not surrendered, as well as a populace that is at best deeply suspicious of foreigners and at worst deeply terrified of them?
- How would refugee camps be secured? As some desperate North Koreans turn to crime (such as attacking World Food Program convoys), what would be the response?
- How are strategic communications conducted with a frightened population to reassure them that their immediate needs would be met and that foreign government personnel and forces should not be feared?

A force trained and equipped only with lethal weapons would be challenged in maintaining security and minimizing civilian casualties in this scenario. IFCs, integrated into conventional platforms along with lethal systems, afford military forces means to provide security at logistics hubs for the distribution of supplies, convoy protection, and protection of refugee camps and critical infrastructure. Information on the types of IFCs being employed could be readily communicated to the civilian population through an information operation and public affairs campaign, demonstrating the resolve to maintain security while also protecting the civilian population – the same approach employed by General Zinni in Somalia.

While the North Korea case study is theoretical, the events that unfolded in August 2021 during the US withdrawal from Afghanistan showcased the challenges of a military force dealing with a desperate civilian population. Chaos ensued as thousands of civilians approached Hamid Karzai International Airport (HKIA). The airfield perimeter was breached as hundreds rushed to aircraft parked on the tarmac. Scenes of civilians clinging to a C-17 taxiing down the runway exemplified the lack of security. US servicemembers and Afghan civilians

[16] Tamara K. Fitzgerald, *After the Fall of North Korea: A Post-Conflict Stability Operations Exercise*, Case Study 0617-03 (Carlisle Barracks, PA: U.S. Army Peacekeeping and Stability Operations Institute, n.d.), https://pksoi.armywarcollege.edu/index.php/after-the-fall-of-north-korea-a-post-conflict-stability-operations-exercise/.

were killed and seriously injured as crowds swelled the Abbey Gate entrance to HKIA and a suicide bomber detonated his payload.

There were many factors that contributed to the nature of events that unfolded at HKIA. Although nonlethal weapons alone undoubtedly would not have been a cure-all for the situation, the existence of longer-range nonlethal weapons integrated into platforms with military forces routinely trained to use them could have reinforced airfield and aircraft security. The few legacy nonlethal weapons that were available and used in an attempt to control the crowds, such as riot control agents and flash-bang munitions, were insufficient or even detrimental due to their short effective range and the nature of their associated nonlethal effects.[17]

As the tragic Afghanistan withdrawal fades in memory, the NDS notes that climate change and other transboundary threats may challenge the governing capacity in some countries while heightening tensions between others, risking new armed conflicts and increasing demands for stabilization activities.[18] Similarly, the 2022 NATO Strategic Concept states that climate change will profoundly impact Allied security as a crisis and threat multiplier, exacerbating conflict, fragility, and geopolitical competition.[19] It is fair to ask if lessons have been learned from stability operations in Iraq and Afghanistan. The establishment of NATO's Stability Policing Center of Excellence (SPCoE) in 2015 is an important step forward. Stability policing refers to actions that may be conducted by military forces—not just the military police—to establish safe and secure environments. One of the main findings from a recent SPCoE doctrine forum on the role of stability policing in countering hybrid threats was the suitability of intermediate force capabilities to avoid/minimize collateral damage.[20] Prudent investment by US and NATO member nations in training and equipping military forces with an appropriate mix of IFCs will be necessary to mitigate the long-term human and fiscal costs of extended stability operations and crisis response by quickly maintaining the safety and security of the population and enhancing the protection of civilians.

Mainstreaming Intermediate Force as a Complement to Lethality

DOD has benefited from a formalized NLW program for more than 25 years. Much has been accomplished in that time, including the fielding of NLW primar-

[17] "Hell at Abbey Gate: Chaos, Confusion and Death in the Final Days of the War in Afghanistan," *ProPublica* and *Alive in Afghanistan*, April 2, 2022, www.propublica.org/article/hell-at-abbey-gate-chaos-confusion-and-death-in-the-final-days-of-the-war-in-afghanistan.

[18] *2022 National Defense Strategy of the United States of America*, 6.

[19] "NATO 2022 Strategic Concept," adopted by the Heads of State and Government at the NATO Summit in Madrid, June 29, 2022, 6, www.nato.int/strategic-concept/.

[20] NATO Stability Policing Centre of Excellence, Doctrine Forum II Fact Sheet, September 19-22, 2022, https://www.linkedin.com/company/nato-spcoe/posts/?feedView=all.

ily in support of military security and law enforcement functions. Extensive research into new technologies has yielded promising results. These technologies are now approaching a stage where they and their associated systems and subsystems could be integrated into a wide range of military platforms for missions on land, sea, and air. The scope of these capabilities goes well beyond legacy law enforcement applications and is better described as intermediate force capabilities.

Over the past 20 years, NATO members have participated in formal systems and analysis studies on NLWs (IFCs) to evaluate measures of effectiveness, inclusion in concepts, and opportunities for future operations.[21] NATO has also conducted NLW (IFC) technology demonstrations, as well as maritime and land exercises.[22] The maritime exercise demonstrated that integrating NLWs into an escalation of force situations encountered during visit, board, search, and seizure missions increased the operational effectiveness of boarding teams to warn a vessel's crew, move people, deny access to an area, and suppress individuals. The land exercise demonstrated that integrating NLW into an escalation of force situations encountered during counterinsurgency missions increased the operational effectiveness of NATO forces in warning potential threats, supporting the threat assessment process, moving people, denying access to an area, and suppressing individuals.

Despite the apparent operational benefits, neither the United States nor other NATO member nations have prioritized the training and equipping of intermediate force capabilities. The deterrent and de-escalatory advantages that IFCs could provide in the gap between shouting and shooting and providing increased time/decision space are largely missing from U.S. and NATO concepts and doctrine. Further work is needed in concept development, the use of modeling and simulation to assess the contribution of IFCs to mission accomplishment, and routine inclusion of IFCs in wargames that address adversary aggression below the level of armed conflict and military operations in and around civilian populations. An updated lexicon should be developed that eliminates the cognitive bias of nonlethal weapons as tools solely for law enforcement, with updates to doctrinal publications to fully integrate the use of intermediate force as a complement to lethality. By doing so, IFCs could begin to be mainstreamed into operational planning, exercises, and mission-essential task lists, as well as in training and professional military education.

---

[21] *Analytical Support to the Development and Experimentation of NLW Concepts of Operations and Employment* (Brussels, BE: North Atlantic Treaty Organization, May 5, 2017).

[22] "Non-lethal Weapons: New Technologies to Save Lives," *NATO Newsroom*, October 2016, https://www.nato.int/cps/en/natohq/news_135772.htm.

Summary

Military forces trained and equipped with intermediate force capabilities would be better prepared to compete, fight and win across the spectrum of operations. The collective lethality of the US and NATO alliance provides a strong and necessary deterrent to adversaries. However, China's actions in the South China Sea and Russia's attack on Ukraine indicate that lethality alone does not deter aggression. Moreover, experience from operations in Iraq and Afghanistan has shown that lethality alone is insufficient to establish safe and secure environments in civilian populations.

As a complement to lethal weapons, intermediate force capabilities provide a means to assess potential threats, de-escalate situations, and increase the time and space to make decisions on the use of lethal force. Technology has significantly evolved beyond the traditional bean bags, rubber bullets, and tear gas of the last century, enabling a new generation of capabilities that can expand the competitive space and counter adversaries' strategies to exploit vulnerabilities that cannot be readily solved with lethal force alone. Sustained commitment by US and NATO civilian and military leadership is needed to mainstream these capabilities – from the infantry squad to the operational commander. With proper tools and training, our military will remain unbeatable across the entire spectrum of operations.

Disclaimer

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

About the Author

Susan D. LeVine is the Principal Deputy Director for Joint Integration and Outreach at the Joint Intermediate Force Capabilities Office (JIFCO), where she serves as senior advisor to the Director JIFCO on matters related to policy, strategy, and mainstreaming non-lethal weapons as intermediate force capabilities across the Joint Force and with Allies and Partners. Ms. LeVine is a "plank owner" at the JIFCO, coming from the Naval Surface Warfare Center Dahlgren Division in 1996 to support the stand-up and day-to-day execution of activities for the Commandant of the Marine Corps as the newly designated DoD Non-Lethal Weapons Program Executive Agent. Since that time, she has been involved in nearly all aspects of the DoD Non-Lethal Weapons Program, including technology development, policy formulation, developing Program roadmaps, coordinating Congressional matters, and serving as Chair of the NATO Joint Non-Lethal Weapons Capabilities Group. Ms. LeVine attended the University of South Carolina, receiving Bachelor's and Master's degrees in Physics, and was a fellow in the Massachusetts Institute of Technology Seminar XXI Class of 2015.

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

John Nelson, *Connections QJ* 21, no. 2 (2022): 67-84
https://doi.org/10.11610/Connections.21.2.05

Research Article

Developing a NATO Intermediate Force Capabilities Concept

John Nelson

Co-Chair NATO SAS-151, https://www.sto.nato.int

Abstract: NATO faces a military problem: adversaries are undertaking acts of aggression that deliberately stay below the lethal force threshold or that ensure a lethal response from NATO incurring costs—undesired escalation, risks of collateral damage including civilian casualties, negative narratives, and other adverse strategic or political outcomes—to the Alliance. Intermediate Force Capabilities (IFC)—active means (non-lethal weapons, particularly non-lethal directed energy, cyber, electronic warfare, information operations, and other effectors) beyond presence but below lethal thresholds—help solve this problem. SAS-151 and Allied Command Transformation developed and conducted wargames and IFC Concept Development Workshops that demonstrated the ways in which IFC improve NATO's ability to deter, counter, and defeat adversaries via: *Enhanced Engagement*: If fielded and incorporated into tactics, techniques, and procedures (TTPs), IFC can enable lethal engagements by isolating, stopping, or moving targets to positions of advantage, also, reversible (and in many cases unseen) effects allow for earlier employment, including potential autonomous/AI use of IFC where lethal capabilities would require human-in-the-loop; *Tempo/Initiative*: Instead of adversaries dictating the time and place of engagements, IFC help NATO gain/maintain the initiative by suppressing, imposing delays, and making adversaries reactive (even inactive); *Active means across the Competition Continuum*: NATO needs to develop, acquire, and effectively employ IFC across the continuum to win engagements, impose costs on the adversary, and win the narrative.

Keywords: Intermediate Force Capabilities, Non-Lethal Weapons, Non-Lethal Directed Energy, Cyber, Electronic Warfare, Information Operations, Concept Development & Experimentation

Introduction

What Motivates the Need for an IFC Concept?

Adversaries know NATO's lethal capabilities and the thresholds for their use. And they exploit this. They avoid direct symmetrical engagements, instead maneuvering below lethal thresholds, pursuing their aims observed but undeterred. Or, they act indirectly through proxies or intermediaries, blending in and engaging only at times and places of their choosing. They often complicate engagements, deliberately taking positions near sensitive locations (critical infrastructure, hospitals, buildings of historic or cultural importance, etc.) or near civilians to deny NATO an acceptable lethal response.

Current Hybrid and Grey Zone challenges[1,2,3] are a continuation of examples where adversaries exploit inadequate means, ways, or will to deter/counter, resulting in undesired outcomes, such as:

- *Bridge destruction impacts*[4]: Operation Deliberate Force, a NATO air campaign against the Bosnian Serb Army in August-September 1995, shortly preceded the Dayton Peace Accords. Bridges were carefully targeted to avoid casualties and collateral impact. Nonetheless, there were significant movement/ maneuver effects in subsequent NATO peace support operations and large economic and reconstruction costs in Bosnia and the region.
- *Restraint and own force casualties*[5]: Mazar-e-Sharif on April 1, 2011, is an apt example. In a normally peaceful area, an unexpected rush by a crowd toward the UN compound was met with no use of force. Local guards were disarmed (four were killed), and several UN officials (including LtCol Siri Skare, Norway's first female pilot) were captured and killed.

---

1 Bryan Clark, Mark Gunzinger, and Jesse Sloman, "Winning in the Gray Zone: Using Electromagnetic Warfare to Regain Escalation Dominance" (Center for Strategic and Budgetary Assessment, 2017), https://csbaonline.org/uploads/documents/CSBA6305_(EMS2_Report)Final2-web.pdf.

2 NATO SAS, "Addressing Obstacles to the Acquisition, Deployment, and Employment of Non-Lethal Weapons – Using Intermediate Force to Bridge the Gap between Presence and Lethal Force," Technical Report STO-TR-SAS-133 (Paris: NATO Science and Technology Organization, August 2020).

3 Andrew Mumford, "Ambiguity in Hybrid Warfare," Hybrid CoE Strategic Analysis Paper # 24 (Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats, September 2020), https://www.hybridcoe.fi/wp-content/uploads/2020/09/202009_Strategic-Analysis24-1.pdf.

4 "Bosnia, 1995 – Operation Deliberate Force: The Value of Highly Capable Proxy Forces" (Washington, D.C.: Brookings Institute, 2017).

5 "UN Remembers Personnel Killed in 2011 Mob Attack in Mazar-e-Sharif," *reliefweb*, April 1, 2013 (originally published by UN Assistance Mission in Afghanistan (UNAMA), Apr 2013), https://reliefweb.int/report/afghanistan/un-remembers-personnel-killed-2011-mob-attack-mazar-e-sharif.

- *Failure to deter*[6,7]: Russia's Crimea annexation and Eastern Ukraine incursions included a mix of overt and covert means—troop movements disguised with a snap exercise, distraction force ruses, use of "Little Green Men," civilians being used to obstruct Ukrainian responses, etc.—combined with an information campaign that targeted domestic, regional, and international audiences. Current approaches to deterrence have proved insufficient even for cases where there have been repeated provocations, with examples including years of Somali piracy, repeated fast attack boat runs at vessels in the Strait of Hormuz, and disruption of operations by manned/unmanned aircraft and simulated missile attacks in the Baltics, South China Sea, and elsewhere.

Hybrid/Grey Zone Challenges

NATO and its members face increasing challenges from adversaries undertaking acts of aggression designed to stay below the level that would trigger a lethal response. Exploiting this, adversaries pose a dilemma: "over-reaction looks preemptive and disproportionate if clear responsibility for an attack has not been established, but the lack of a response leaves a state open to death by a thousand cuts."

China has achieved territorial expansion in the South China Sea, leveraging an Informationized Warfare strategy that shapes the decision-making of a target's leadership—including through the civilian populace—to convince them not to fight.

Russia's New Generation Warfare seeks to create and make use of pro-Russian movements:

- fostering protests and conducting cyber activities to pressure the Baltic states;
- using civilians to block exit points from Ukrainian military installations (thereby denying freedom of movement/maneuver and trying to provoke the use of force to move those civilians);
- providing capabilities and technical assistance for others to use unmanned aircraft systems (UAS) and surface-to-air missiles that have been targeted at military and civil targets;
- invading (Georgia) or annexing (Crimea) territory.

[6] Michael Kofman et al., "Lessons from Russia's Operations in Crimea and Eastern Ukraine," Research Report (RAND Corporation, 2017), https://doi.org/10.7249/RR1498.

[7] ACO, *Protection of Civilians*, Handbook (NATO, Allied Command Operations, May 2020), https://shape.nato.int/documentation/protection-of-civilians-aco-handbook-.

NATO Recognition of These Threats and Challenges

> *NATO faces a dangerous, unpredictable, and fluid security environment, with existential challenges and threats from all strategic directions including state and non-state actors; near-peer military forces; cyber threats; space; terrorism; hybrid warfare; and information operations.*[8]

Many of these threats and challenges are highlighted in *Science & Technology Trends 2020-2040*[9] and *Allied Joint Doctrine* (AJP-01)[10]:

- Complications in detecting, deterring, and countering indirect approaches
- Increased connection between events overseas and the homeland
- Blurring across strategic, operational, and tactical levels
- Interconnectivity across air, land, sea, cyberspace, space, and the information environment
- Widely accessible technologies (automated/autonomous systems and weaponized information activities) proliferating and being used in novel ways.

Adversaries deliberately create and exploit uncertain situations including "targeting civilian populations, institutions, and critical infrastructure."[11]

- Acting not only directly but through proxies and intermediaries in order to achieve their goals but also to offer deniability
- Sub-threshold activities (hybrid warfare, lawfare, cyber, information operations, etc.) typically have asymmetries in the level of interest, ways and means employed, and escalation/de-escalation concerns that load predicaments and dilemmas on the Alliance:
  - ✓ Leading to a miscalculation that results in undesired escalation, even armed conflict
  - ✓ Making it difficult to gain and sustain the initiative
  - ✓ Ceding an advantage to adversaries: Russian and Chinese theories of victory emphasize seizing a decisive advantage in the early stages of conflict (initial period of war). Exploiting cyberspace, electromagnetic spectrum, and information technologies in recent conflicts has

[8] NATO STO, *Science & Technology Trends 2020-2040*.

[9] NATO STO, *Science & Technology Trends 2020-2040: Exploring the S&T Edge* (Brussels, Belgium: NATO Science & Technology Organization, 2020), https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

[10] NATO, "Framework for Future Alliance Operations," signed by General Curtis M. Scaparrotti, Supreme Allied Commander Europe, and by General Denis Mercier, Supreme Allied Commander Transformation (NATO, 2018).

[11] NATO, "Framework for Future Alliance Operations."

demonstrated that sub-threshold activity is a starting point for a conflict.[12]

- Positioning near sensitive locations or civilians to deny NATO an acceptable lethal response or impose costs—potential miscalculation, undesired escalation, establishment of a pretext for other adversary actions, risks of collateral damage and civilian casualties, altering the narrative, or other adverse outcomes—to the Alliance.

The 2021 NATO Summit[13] brought Heads of State and Government attention and direction:

> We face multifaceted threats, systemic competition from assertive and authoritarian powers, as well as growing security challenges to our countries and our citizens from all strategic directions. Russia's aggressive actions constitute a threat to Euro-Atlantic security; terrorism in all its forms and manifestations remains a persistent threat to us all. State and non-state actors challenge the rules-based international order and seek to undermine democracy across the globe. Instability beyond our borders is also contributing to irregular migration and human trafficking. China's growing influence and international policies can present challenges that we need to address together as an Alliance. We will engage China with a view to defending the security interests of the Alliance. We are increasingly confronted by cyber, hybrid, and other asymmetric threats, including disinformation campaigns, and by the malicious use of ever-more sophisticated emerging and disruptive technologies.

The Communiqué of the Brussels Summit further emphasized the need to respond to hybrid threats from state and non-state actors:

> In addition to its military activities, Russia has also intensified its hybrid actions against NATO Allies and partners, including through proxies. This includes attempted interference in Allied elections and democratic processes; political and economic pressure and intimidation; widespread disinformation campaigns; malicious cyber activities; and turning a blind eye to cyber criminals operating from its territory, including those who target and disrupt critical infrastructure in NATO countries. It also includes illegal and destructive activities by Russian Intelligence Services on Allied territory, some of which have claimed lives of citizens and caused widespread material damage.
>
> Our nations continue to face threats and challenges from both state and non-state actors who use hybrid activities to target our political institutions, our public opinion, and the security of our citizens. While the primary responsibility for responding to hybrid threats rests with the targeted nation, NATO is

[12] North Atlantic Treaty Organization (NATO), "Allied Joint Doctrine," AJP-01(F) (NATO Standardization Office (NSO), July 8, 2020).

[13] NATO, "Brussels Summit Communiqué," issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, June 14, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

> ready, upon Council decision, to assist an Ally at any stage of a hybrid campaign being conducted against it, including by deploying a Counter Hybrid Support Team. In cases of hybrid warfare, the Council could decide to invoke Article 5 of the Washington Treaty, as in the case of an armed attack. [14]

Moreover, at the Summit, the Heads of State and Government agreed to:

- "Enhance our resilience. Noting that resilience remains a national responsibility, we will adopt a more integrated and better-coordinated approach, consistent with our collective commitment under Article 3 of the North Atlantic Treaty, to reduce vulnerabilities and ensure our militaries can effectively operate in peace, crisis and conflict."
- "Enhance NATO's ability to contribute to preserve and shape the rules-based international order in areas that are important to Allied security."

The Essence of the Intermediate Force Capabilities Concept

IFC—active means (non-lethal directed energy, cyber, electronic warfare, information operations, and other relevant capabilities) delivering effects beyond Presence but below the threshold of Lethal Force—provide ways to address these threats and challenges and the stated military problem:

Military Problem: Adversaries are undertaking acts of aggression that deliberately stay below the lethal force threshold or that ensure a lethal response from NATO would incur costs—undesired escalation, risks of collateral damage including civilian casualties (CIVCAS), negative narratives, and other adverse strategic or political outcomes—to the Alliance.

IFC are not only a needed complement to lethal force but also a facilitator. Lethal force appropriately predominates in the Intervene stage. Even in this stage, however, IFC play an important role by suppressing targets or moving/ stopping/ separating/ isolating them to ensure targets are in positions for more effective lethal engagements.

IFC offer additional benefits in other stages—imposing costs, increasing decision and action space, helping to gain/maintain the initiative, shaping and expanding the engagement space with Multi-Domain effects, etc.—delivering effective actions and outcomes where rules of engagement or target restrictions would not permit lethal force or where use of lethal force would incur costs and negative consequences for the Alliance, its members, and/or partners.

[14] NATO, "Brussels Summit Communiqué," issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, June 14, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

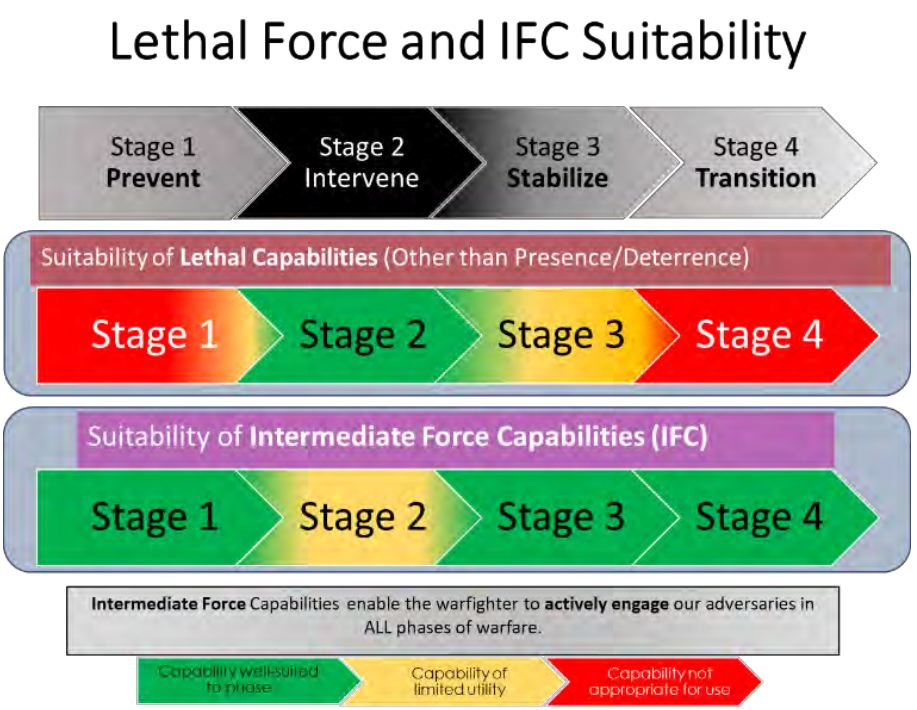

Figure 1: Utility of Lethal vs. Intermediate Force Capabilities.

Figure 2 depicts the ends, ways, and means associated with the draft NATO IFC Concept:

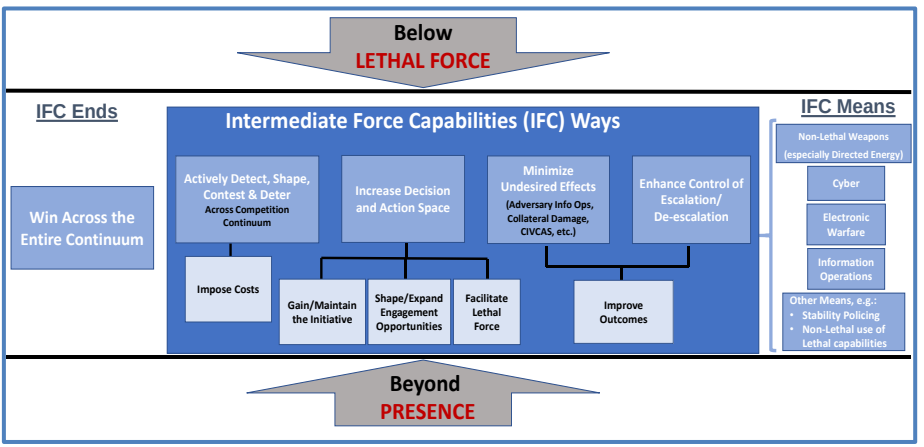

Figure 2: Ends, Ways, and Means Associated with the IFC Concept.

IFC Ends: Win across the Entire Competition Continuum

RADM Tammen in his article[15] on the NATO Warfighting Capstone Concept (NWCC) stated: "The fundamental nature of war does not change. It always involves a clash of wills, violence, friction, fog, maneuvers or deception. At the same time, the character of warfare continues to evolve and become ever more pervasive with our competitors conducting activities that sit outside the 'normal' peace-crisis-conflict dynamic. Major shifts in warfare are often associated with technological innovation – from arrows to black powder to battle tanks to nuclear weapons to cyber and space systems today." IFC—non-lethal directed energy, cyber, electronic warfare, information operations, and other appropriate means—represent technological innovations essential to winning across the continuum.

Wargame results from IFC Concept Development and Experimentation are clear and compelling: *IFC help win engagements*, *impose costs on the adversary*, and *win the narrative* (all of which are essential).

These wargames[16,17,18,19,20,21] compared the same scenarios for the Baseline Case (only traditional—predominantly lethal—capabilities) versus IFC Case (with advanced IFC available as a complement). The following table presents a brief excerpt of results addressing actions and outcomes with respect to escalation/de-escalation considerations. The bottom line*: With IFC, NATO was able to achieve its objectives and to block adversaries and proxies from achieving theirs.*

---

15 Rear Admiral John W. Tammen, "NATO's Warfighting Capstone Concept: Anticipating the Changing Character of War," *NATO Review*, July 9, 2021, https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html.

16 Kyle D. Christensen, Maude Amyot-Bourgeois, George Nikolakakos, and Peter Dobias, "Use of Intermediate Force Capability Game Series: Game 1–NATO Naval Task Group in Port," Scientific Letter DRDC-RDDC-2020-L180 (Ottawa: Defence R&D – CORA, October 2020).

17 Kyle D. Christensen and Peter Dobias, "Use of Intermediate Force Capability Game Series: Game 2 – NATO Naval Task Group in Confined Waterway," NATO Technical Report, STO-TR-SAS151 (NATO SAS-151, March 3, 2021).

18 Kyle D. Christensen and Peter Dobias, "Wargaming the Use of Intermediate Force Capabilities in the Gray Zone," *The Journal of Defence Modeling and Simulation: Applications, Methodology, Technology*, published online April 20, 2021, 1-14, https://doi.org/10.1177/15485129211010227.

19 Kyle D. Christensen, Peter Dobias, Maude Amyot-Bourgeois, and B. Astles, "Use of Intermediate Force Capability Game Series: Game 4 – NATO Task Force in Land Wargame Scenario," NATO Technical Report, STO-TR-SAS151 (NATO SAS-151, October 2021), https://doi.org/10.14339/STO-TR-SAS-151.

20 Sean Havel et al., "Use of Intermediate Force Capability Game Series: Information Operations and Information Warfare Wargaming Scenario," draft report (NATO SAS-151, 2021).

21 Peter Dobias et al., "Use of Intermediate Force Capability Game Series: Game 5 – Noncombatant Evacuation Operation," draft report (NATO SAS-151, 2021).

Table 1. Sample Effects of Traditional and IFC Capabilities.

Baseline Case (Traditional capabilities only)	**IFC Also Available** (Traditional capabilities plus IFC)
"**In both scenarios, escalation spun out of control.**" • "The limited range of responses (i.e., doing nothing or using (Lethal) force) appeared to embolden the adversary to undertake more aggressive actions." • For the naval scenario, the tactical game resulted in missiles fired against friendly vessels and torpedoes fired by both friendly and adversary forces. • For the land scenario, friendly forces were pushed into using excessive force (including the use of CS gas against a crowd and firing high explosive rounds at civilian targets), which provided the impetus for the adversary to send forces across the border and fire missiles toward a joint Host Nation-NATO base.	"**IFC turned the strategic equation on its head in favor of friendly forces**." • "The adversary was also more restrained in their escalatory behavior." • "By the end of the tactical game, there was little to no response from the adversary to NATO's actions." • "IFC disrupted and degraded the hostile actions so that the damage was significantly less than in Option A (the Baseline Case). In both scenarios, rather than controlling the narrative and escalation, IFC appeared to take away the pretext/justification for the adversary's use of force and shifted the tactical initiative in favor of the friendly forces."

IFC Ways

The wargames [footnotes 16-21] drove insights with respect to the ways IFC solve the Military Problem:

➢ *Actively Detect, Shape, Contest, and Deter*

IFC help resolve ambiguity through active detection (including resolving ambiguity in intent); shape the environment to create more favorable conditions for further actions (including lethal if appropriate); and, finally, contest, deter or counter adversaries. This includes imposing material, financial, and/or social costs without the escalation associated with actions at the lethal force threshold. An example from the wargames was: "At the tactical level, during the naval scenario, the adversary's attempt to use force was hampered by NATO's use of IFC. IFC were able to deter unwanted behavior and/or degrade/disrupt the adversary's ability to use force. By the end of the tactical game, there was little to no response from the adversary to NATO's actions."

- *Increase Decision and Action Space*

IFC help gain/maintain the initiative, shape and expand the engagement space, and facilitate the use of lethal force at times and places dictated by NATO rather than by adversaries and their proxies. In the Baseline Case, the "adversary was generally able to maintain the initiative and demonstrate an aggressive stance toward friendly forces." Friendly forces were reactive, which often led to either uncontrolled escalation or a lack of friendly action, in both cases creating a situation favoring the adversary at the strategic level. In the IFC Case, NATO seized the initiative and decided when and how to use force, including lethal. "Consequently, the adversary force became more reactive in their actions during the naval wargame" and "By the end of the tactical game, there was little to no response from the adversary to NATO's actions."

- *Facilitate Lethal Engagements*

IFC can move/stop/separate/isolate/ suppress targets, enabling engagements at a position of advantage, increasing effectiveness, and reducing risks of unintended consequences. "The land game showed that the use of IFC to suppress and degrade adversary enabled more effective and targeted lethal response." Also, the land game showed IFC could be used to slow or stop targets, providing more efficient targeting (and more response time) with lethal engagements at the place and time of NATO's choice limiting the threat to civilians and critical infrastructure.

- *Minimize Undesired Outcomes*

Undesired outcomes may result from acts of omission or commission, and either may be grievous. Acts of omission may see adversaries achieve their aims observed but undeterred or see NATO suffer material losses (particularly in light of some adversaries' theories of victory leveraging sub-threshold activities to seize an early decisive advantage in conflict). Acts of commission may cause collateral damage and civilian casualties, harming NATO's interests. Relevant wargame results included: in the Baseline Case, "For the land scenario, the friendly forces were pushed into using excessive force… which provided the impetus for the strategic adversary to send forces across the border and fire missiles toward a joint Host Nation-NATO base." In the joint game the inaction and decision paralysis due to the lack of options in the Baseline Case led to a failure of the entire NATO operation. In the IFC Case, "friendly forces were able to use IFC to suppress hostile militia actions and were thus able to use lethal force more judiciously. Limited use of lethal force significantly reduced the number of civilian casualties and, more importantly, undermined the adversary's narrative." Both tactically and strategically, the adversary was put on the defensive.

- *Improve Control of Escalation/De-escalation*

One of NATO's core tasks is Crisis Management, which calls for "an appropriate mix of those political and military tools to help manage developing crises that have the potential to affect Alliance security before they escalate into conflicts."[22] IFC add tools for controlling escalation. Moreover, rather than a thin line separating Presence and Lethal Force, IFC offer an entire level in between. As demonstrated in the series of wargames, IFC can prevent escalation and lead to adversary de-escalation. In addition, IFC availability consistently resulted in improved outcomes with respect to NATO's objectives.

Millimeter Wave

Directed Energy
Vessel/Vehicle Stoppers

Figure 3: Examples of IFC as Means.

IFC Means

The working definition for IFC is "Active means below lethal intent that temporarily impair, disrupt, delay, or neutralize targets across all domains and all phases of competition and conflict." Various capabilities are consistent with this definition:

- *Non-Lethal Weapons (Especially Directed Energy)*

NLW are by their design IFC, providing means beyond Presence but below Lethal Force. The North Atlantic Council (NAC) issued a policy[23] defining NLW as "weapons which are explicitly designed and developed to incapacitate or repel personnel, with a low probability of fatality or permanent injury, or to disable equipment, with minimal undesired damage or impact on the environment." Key NLW Directed Energy capabilities include:

---

[22] NATO, "Active Engagement, Modern Defence," Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, adopted by Heads of State and Government at the NATO Summit in Lisbon, November 19, 2010, https://www.nato.int/cps/en/natohq/official_texts_68580.htm.

[23] NATO, "NATO Policy on Non-Lethal Weapons," October 13, 1999, www.nato.int/cps/en/natohq/official_texts_27417.htm.

- *Millimetre Wave* for long-range effects to compel the movement of individuals, deny areas and suppress targets, as well as for Counter-Unmanned Aircraft Systems (C-UAS) effects
- *High-Power Microwave (HPM)* and *High-Power Electro-Magnetics (HPEM)* for vehicle and vessel stopping, C-UAS, and other Counter Materiel applications
- *Low-energy lasers*, such as dazzling lasers, to warn and suppress individuals and sensors.

Counter-UAS

Low-Energy Lasers

Figure 4: Examples of non-lethal weapons.

Based on lessons from NLW use during NATO operations as well as results from wargames, formal military utility assessment exercises in the field, and previous NATO studies,[24,25] there are six areas where NLW contributions need to be included in concepts, all clearly and directly relevant to the draft IFC Concept:

1. Promote Compliance/Warn/Deter
2. Facilitate Engagement
3. Facilitate Manoeuvre
4. Defeat Threats Directly
5. Enhance Protection
6. Reduce CIVCAS/Collateral Damage.

➢ *Cyber*

Cyber capabilities also provide effective means beyond resence and below lethal force.

[24] NATO STO, "Analytical Support to the Development and Experimentation of NLW Concepts of Operation and Employment," Technical Report, STO-TR-SAS-094 (NATO Science and Technology Organization, 2017).

[25] NATO STO, "Addressing Obstacles to the Acquisition, Deployment, and Employment of Non-Lethal Weapons."

At the 2016 Warsaw Summit,[26] NATO recognised "cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea" stating: "This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances. It will support NATO's broader deterrence and defence: cyber defence will continue to be integrated into operational planning and Alliance operations and missions, and we will work together to contribute to their success." At the 2018 Brussels Summit,[27] the Heads of State and Government characterized threats and announced a Cyber Defence Pledge:

> We face a dangerous, unpredictable, and fluid security environment, with enduring challenges and threats from all strategic directions; from state and non-state actors; from military forces; and from terrorist, cyber, and hybrid attacks. Russia's aggressive actions, including the threat and use of force to attain political goals, challenge the Alliance and are undermining Euro-Atlantic security and the rules-based international order. Instability and continuing crises across the Middle East and North Africa are fuelling terrorism. They also contribute to irregular migration and human trafficking. The ongoing crisis in Syria has a direct effect on the stability of the region and the security of the Alliance as a whole. We face hybrid challenges, including disinformation campaigns and malicious cyber activities. … We have agreed how to integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, in the framework of strong political oversight. Reaffirming NATO's defensive mandate, we are determined to employ the full range of capabilities, including cyber, to deter, defend against, and to counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign.

- *Electronic Warfare*

Potential Electronic Warfare (EW) threats include systems that can detect, exploit, degrade, disrupt, destroy, and deceive communications, navigation systems, sensors, and weapons' control systems. Moreover, Directed Energy capabilities could attack personnel or materiel.

There is overlap among EW and other IFC, including cyber and Directed Energy, with some DE capabilities categorized as NLW (Millimetre Wave, HPM/HPEM, and low energy lasers as described previously) and others (higher energy lasers, HPM/HPEM/radio frequency, and particle beam capabilities) that would be categorized as EW but not as NLW.

EW activities and capabilities are diverse. They include sensing and protection measures such as emission control and electromagnetic hardening, security,

[26] NATO, "Warsaw Summit Communiqué," issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, July 8-9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[27] NATO, "Brussels Summit Declaration," issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, July 11-12, 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

intelligence collection, and countermeasures. They include measures to contest adversaries directly via Directed Energy applications (including laser, radio frequency, and particle beam capabilities), navigation warfare, or Electronic deception, intrusion, and jamming. EW effects range from temporary deception or disruption to more enduring degradation all the way to destruction, and as such most effects are consistent with IFC, while some destructive effects may cross to the level of lethal force.

- *Information Operations*

Recent operations have shown it is critical not only to win engagements but also to win the narrative. Adversaries will use information operations to advance their interests and harm NATO's. This battle for the narrative can have significant impact with respect to support from a Host Nation and its populace (affecting the mission as a whole and the status and security of forces), regional actors (and their willingness to provide proxies, base access, transit rights, financial support, etc.), and the international community (which may bring to bear their own diplomatic, informational, military or economic resources depending on their belief in the competing narratives).

Per the NATO Strategic Communications Centre of Excellence's *Strategic Communications Hybrid Threats Toolkit*[28]:

> The activities of potential adversaries need to be detected and monitored, to be able to assess when competition between states escalates into something more serious. Concurrently, an adversary's ability to restrict our own freedom of action must be denied. Responses will involve a range of government measures. These need to be coordinated so that they communicate with—and influence—the right target audiences, without risking undesired 2nd or 3rd order effects.

Information Operations are used to shape the information environment to achieve Alliance objectives and hinder adversaries from advancing their own objectives. Means may include:

- Strategic Communications
- Public Affairs
- Intelligence
- Civil-military operations
- Psychological operations and military deception

[28] Ben Heap, Pia Hansen, and Monika Gill, *Strategic Communications Hybrid Threats Toolkit: Applying the Principles of NATO Strategic Communications to Understand and Counter Grey Zone Threats* (Riga: NATO Strategic Communications Centre of Excellence, September 8, 2021), https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213.

- Cyber
- Electronic Warfare.

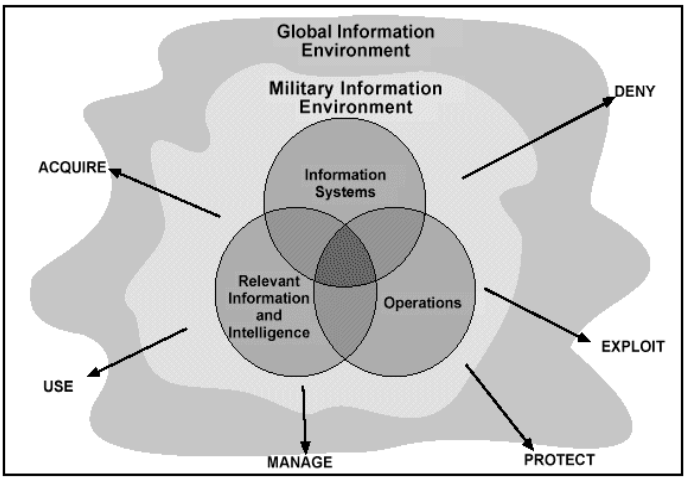

Figure 5: Information Environment and Operations.

➢ *Other Means Beyond Presence and Below Lethal Intent*

Capabilities develop over time or have functionality in addition to their original purpose. When such capabilities provide for effective action beyond presence while remaining below the level of lethal force, they can be legitimately considered Intermediate Force Capabilities. During IFC Concept Development & Experimentation, the Director and staff from the Stability Policing CoE highlighted Stability Policing's relevance to the IFC Concept:

- Stability Policing (SP) and policing in general mostly operate within the IFC remit, that is, between mere presence and the use of lethal force.
- SP can counter hybrid threats and act in grey zone confrontation below the threshold of conflict. The article "How to Win an Asymmetric War in the Era of Special Forces"[29] calls for new forms of deterrence and response, with the article emphasizing roles for Special Forces but also with clear opportunities for SP to address adversary exploitation of the target population:

  "Traditional deterrence, backed by large conventional formations and nuclear weapons, relies on the power to hurt an adversary by applying over-

[29] Keith Pritchard, Roy Kempf, and Steve Ferenzi, "How to Win an Asymmetric War in the Era of Special Forces," *The National Interest*, October 12, 2019, https://nationalinterest.org/feature/how-win-asymmetric-war-era-special-forces-87601.

whelming force if it crosses a red line for retaliation. Russia's New Generation Warfare and China's Unrestricted Warfare present challenges to traditional deterrence because they use "salami tactics" that avoid triggers for conventional retaliation... Deterring gray-zone coercion requires an unconventional approach, one that addresses the vulnerabilities that the adversary exploits in the target population, as well as augmenting capabilities that will nullify the aggressor's advantages."

- SP through reinforcement and capability building of Indigenous Police Forces can:
  - ✓ Expand the Alliance's reach into the policing/civil remit by Host Nation (HN) invitation to support HN national and societal cohesion/ resilience, build integrity amongst Justice Sector entities (law enforcement, judiciary, corrections), and increase support from the populace
  - ✓ Take action while reducing collateral damage risks (also key to provide support from the populace)
  - ✓ Add flexibility by applying authorities to arrest, seize illicit funds/ materiel, use tools combat forces cannot, and combat irregular actors through offensive cyberspace operations using Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVAs) if requested by the HN judicial authority.

The wargames highlighted the importance of area denial, area clearance, vehicle stopping, and protection of facilities and forces, with IFC making important contributions in each of these areas. Provided advance notice, Military Engineering (MILENG) can make relevant contributions in all of these areas. As such, MILENG represents another potential IFC means. Finally, wargames included the employment of Lethal capabilities to achieve Non-Lethal effects (warning shots and use against open terrain and infrastructure for counter-mobility). It should be noted even where the effects were Non-Lethal as intended, adversaries assessed (and changed) their escalation-of-force calculus very differently from other IFC.

Summary and Implementation Imperatives

NATO's *2030 Initiative*[30] and *Strategic Concept*[31] commit the Alliance to "prevent crises, manage conflicts and stabilize post-conflict situations" and "ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations." Given current and foreseen

[30] "NATO 2030: Making a Strong Alliance even Stronger," https://www.nato.int/nato2030/; NATO, "Brussels Summit Communiqué," issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, June 14, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

[31] NATO, "Active Engagement, Modern Defence."

threats, NATO needs IFC—active means (Non-Lethal Directed Energy, Cyber, Electronic Warfare, Information Operations, and other relevant capabilities) that deliver Multi-Domain effects beyond Presence but below the threshold of Lethal Force—to realize these commitments. In support of the NATO Warfighting Capstone Concept, IFC help win across the competition continuum, with concept experimentation (wargaming) highlighting IFC contributions that build through the stages of the "Framework for Future Alliance Operations"[32]:

Table 2. IFC Contributions through the Stages of "Future Alliance Operations."

Threats/Challenges across Stages	Ways IFC Address Threats/Challenges
Prevent Stage: Adversaries achieve goals directly or indirectly using military and paramilitary capabilities, proxies, insurgents, and/ or civil institutions and civilians, with threats and challenges spanning Physical, Information, and Cognitive Domains.	• Active means to detect, shape, deter, contest, and counter adversaries and proxies • Increase decision and action space • Manage escalation and promote de-escalation • Impose costs (direct costs and opportunity costs)
Intervene Stage: Adversaries deliberately complicate targeting by positioning near sensitive locations (critical infrastructure, hospitals, buildings of historical or cultural importance, etc.) or near civilians (blending in with the populace or intentionally using human shields).	• Facilitate Lethal engagements by using IFC to suppress/ move/ stop/ separate/ isolate targets • Take direct IFC action versus targets while minimizing collateral damage and CIVCAS risks • Win Engagements, Impose Costs, and Win the Narrative
Stabilize and Transition Stages: Adversaries seek to create and exploit friction with the Host Nation Government and populace, creating and leveraging incidents to advance their aims and harm NATO's.	• Avoid undesired outcomes adversaries can exploit • Provide means to gain/maintain the initiative and force adversaries and their proxies to be reactive

Wargames and IFC Concept Development Workshops also highlighted implementation imperatives:

- *Enhanced Engagement:* If fielded and incorporated into tactics, techniques, and procedures (TTPs), IFC can enable lethal engagements by

[32] "Framework for Future Alliance Operations."

isolating, stopping or moving targets to positions of advantage; also, reversible (and in many cases unseen) IFC effects allow for earlier employment, including potential autonomous/AI use of IFC where lethal capabilities would require human-in-the-loop.

- *Tempo/Initiative:* Provided IFC are available across the force and integrated into targeting, instead of adversaries dictating the time and place of engagements, IFC enable NATO to gain/maintain the initiative by suppressing, imposing delays, and making adversaries reactive (even inactive).
- *Win across the Competition Continuum:* NATO needs to develop, acquire, and effectively employ IFC across the continuum to win engagements, impose costs on the adversary, and win the narrative. Winning across the continuum will also require NATO to counter adversary employment of IFC.

Disclaimer

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

About the Author

John Nelson is an international defense analyst with more than 30 years of experience. He has led many high-level planning and analytical efforts, with examples including the analysis and re-design of the First Marine Expeditionary Force's (I MEF's) Planning/Decision/Execution/Assessment process, which significantly increased I MEF's planning horizon; development of the first in a series of interagency exercises (Emerald Express) on Peace Support Operations and Military Support to Civilian Authorities; development of theater-level contingency plans and organizational assessments for the Implementation Force/Stabilization Force (IFOR/SFOR) in Bosnia; leadership of American Systems work analyzing the insurgency in Iraq's Anbar Province for the Marine Corps Intelligence Activity. Leading roles in NATO studies include the Non-Lethal Weapons (NLW) Effectiveness Assessment (SAS-060) that won a 2008 NATO Scientific Achievement Award; a Capabilities-Based Assessment (SAS-078), which received Bi-Strategic Command (Supreme Headquarters Allied Powers Europe and Allied Command Transformation) endorsement; NLW in NATO and National Concepts (SAS-094) that won a 2017 NATO Scientific Achievement Award; and SAS-151's analysis, wargaming, and IFC Concept Development Workshops that developed a draft NATO IFC Concept. *E-mail*: john.nelson@americansystems.com

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

Krista Romita Grocholski & Scott Savitz
Connections QJ 21, no. 2 (2022): 85-95
https://doi.org/10.11610/Connections.21.2.06

Research Article

How to Assess the Impact of Non-Lethal Weapons

Krista Romita Grocholski and Scott Savitz

The RAND Corporation, https://www.rand.org/

Abstract: Assessing the tactical, operational, and strategic impact of non-lethal weapons is challenging, requiring different evaluative approaches from those used for lethal weapons. This article describes how a RAND team used a structure called a "logic model" to characterize what these systems and operations are intended to achieve and how they do so. The team then identified a set of metrics that collectively measured each element of the logic model. Additionally, the RAND team developed a diverse set of vignettes in which non-lethal capabilities were used and then qualitatively evaluated each metric in the context of each vignette using a set of standard criteria: how well the metric measured the corresponding element, how easily and quickly the value of the metric could be measured, and how consistently different individuals would likely assess the value of the metric in a particular situation. Based on this work, the logic model can be used to better characterize and communicate the impact of non-lethal weapons and actions at the tactical and operational levels and link these to strategic goals. Operators, planners, and commanders can also select specific metrics to measure the impact of these weapons and actions in real-world operations and wargames, enabling them to make better decisions on when and how to use them to achieve their goals.

Keywords: non-lethal weapons, impact, intermediate force capabilities, gray zone.

Introduction

Non-lethal weapons (NLWs) represent a diverse set of systems whose common feature is that they are intended to incapacitate rather than kill or destroy. For example, they include laser dazzlers that cause targets to experience intense glare, the Active Denial System (ADS) that emits millimeter-wave energy to cause

a temporary heating sensation, pepper balls that irritate eyes and airways, blunt-impact munitions such as rubber bullets and bean bags, and vessel-stopping technologies that entangle propellers. Generally, their effects are intended to be reversible. NLWs represent a subset of intermediate force capabilities (IFCs), which also encompass cyber, electronic warfare, and information operations. The term "IFC" is not doctrinal but is gaining traction in NATO circles. In this article, we focus on the NLW subset of IFCs.

At a time of increasing competition below the threshold of full-scale conflict, NLWs can play a role in addressing gray-zone operations: situations in which an adversary seeks to coercively change the situation without instigating a war.[1] They can be used to demonstrate resolve and counter coercion without inflicting casualties in ways that could cause unwanted escalation. NLWs can also be valuable in other contexts, such as clarifying individuals' intent in ambiguous situations or dispersing civilian crowds deliberately impeding military operations without causing permanent harm.

To inform decisions about how to acquire and employ NLWs, it is important to be able to measure their tactical, operational, and strategic impact. However, measuring the impact of NLWs requires a different methodology from more traditional approaches that do the same for lethal weapons. Lethal weapons are often assessed in terms of their ability to inflict a certain level of damage, whereas NLWs are valued for their ability to circumscribe it. Given this challenge, the U.S. Joint Intermediate Force Capabilities Office (JIFCO) asked a team from the RAND Corporation to conduct a study on how best to evaluate the impact of IFCs at multiple levels. In the remainder of this article, we describe that study, which we led, and the findings from it. While this analysis was centered on NLW usage within the U.S. Department of Defense (DoD), much of it can readily be applied in a NATO context.

Methodology

We began by reviewing over 150 documents and conducting 36 interviews with a variety of experts on NLWs. Based on this, we developed a structure called a "logic model" that linked the activities of NLWs with U.S. strategic goals via a series of intermediate steps. We refined the logic model based on expert feedback, then identified metrics that could be used to measure each item within the logic model. Next, we developed varied vignettes for NLW usage and evaluated the relative merits of the various metrics in the contexts of those vignettes. In addition, we further analyzed data from interviews and documents to identify

[1] According to a RAND report, "The gray zone is an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and nonmilitary actions and the attribution for events." See Lyle J. Morris, et al., *Gaining Competitive Advantage in the Gray Zone: Response Operations for Coercive Aggression Below the Threshold of Major War*, RR-2942-OSD (Santa Monica, CA: RAND Corporation, 2019), 8, https://doi.org/10.7249/RR2942.

broad themes and then developed a set of findings and recommendations regarding how best to evaluate and communicate the impact of NLWs.

Developing a Logic Model on the Impact of NLWs

Logic models can provide a structured way to relate specific processes or programs with high-level goals.[2] The logic model that we developed to characterize NLWs described how the following five categories related to one another:

- Inputs – items that are required for NLWs to be used, such as the systems themselves, doctrine, and training
- Activities – what NLWs actually do
- Outputs – the direct results of NLW usage
- Outcomes – higher-level effects of NLW usage
- Strategic goals – ultimate goals of the DoD.

The logic model consists of a series of elements distributed across each of these five categories (see Figure 1).

The inputs, listed in the leftmost column, include the systems themselves, the tactics, techniques, and procedures (TTPs) and concepts of operation (CONOPs) for using them, as well as doctrine, training, and sustainment capabilities. They also include the laws of war (LOW) and rules of engagement (ROE) that shape how NLWs may be used.

Activities, listed in the second column from the left, consist of things NLWs do. For example, these elements include hailing to communicate with other parties, disorienting them, impeding their mobility, or temporarily incapacitating them. Some NLWs can perform more than one activity at once, e.g., hailing can also help to reveal another party's intent based on how that party responds.

Outputs represent the direct results of NLW employment. Examples of these direct results include increasing time for decisions, impacting costs to US and adversaries, and minimizing collateral damage. The outputs are listed in the center column in Figure 1. Outcomes, listed in the column second from the right, are another level up and relate more to higher-level impacts of NLWs, such as managing escalation, enhancing perceptions of U.S. forces, and managing relationships with partner nations. Finally, strategic goals, listed in the rightmost column in Figure 1, are wide-reaching goals established by DoD leadership – specifically pulled from the 2018 National Defense Strategy unclassified summary.[3] While NLWs cannot be entirely responsible for the achievement of these higher-level goals, their use can contribute towards their fulfillment.

---

[2] See Scott Savitz, Miriam Matthews, and Sarah Weilant, *Assessing Impact to Inform Decisions: A Toolkit on Measures for Policymakers*, TL-263-OSD (Santa Monica, CA: RAND Corporation, 2017), https://doi.org/10.7249/TL263.

[3] Jim Mattis, "Summary of the 2018 National Defense Strategy: Sharpening the American Military's Competitive Edge" (Washington, D.C.: U.S. Department of Defense, 2018).

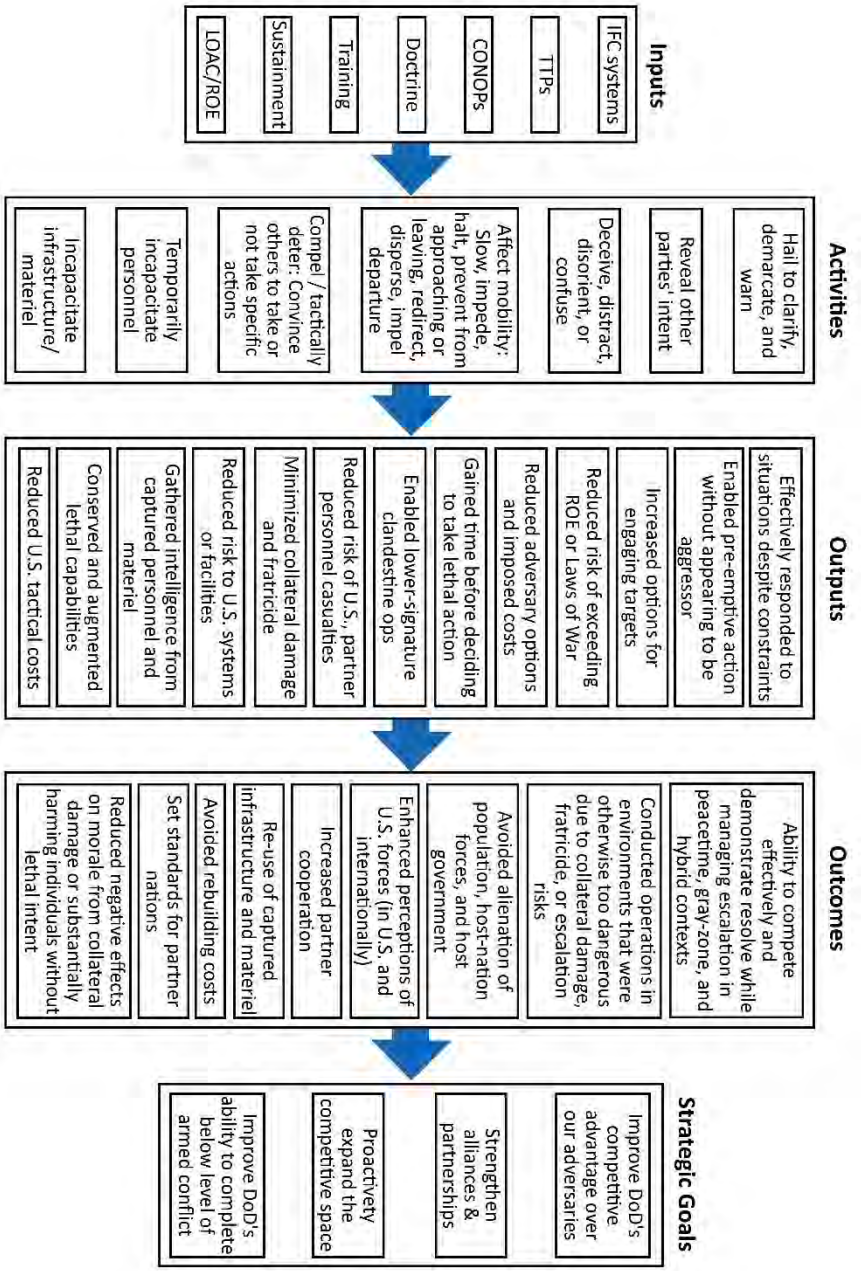

Figure 1: NLW Logic Model (Source: Krista Romita Grocholski et al., *How to Effectively Assess the Impact of Non-Lethal Weapons as Intermediate Force Capabilities*, Research Report RR-A654-1 (Santa Monica, CA: RAND Corporation, 2022), https://doi.org/10.7249/RRA654-1).

Connectivity Between Logic Model Elements

After constructing the logic model, we mapped the connectivity between individual elements of the logic model, which helps illuminate the ways in which the use of NLWs can create higher-level impacts. This also highlights which portions of the logic model are the most important to examine when it is applied to specific scenarios or goals. Figure 2 shows the completed connectivity mapping for the NLW logic model. In the figure, strong connections are indicated by thicker, darker lines than weaker connections (e.g., strong connection = bold line). Arrow colors are for clarity – all arrows coming from a particular element are the same color. Elements surrounded by a dark blue box are linked to strategic goals via strong connections.

By considering the mapping as a whole, we were able to identify patterns and develop some key insights. The density of the linkages between the logic model elements decreases as we move from left to right in Figure 2. For example, most activities have strong connections to most outputs, but fewer outcomes have strong connections to multiple strategic goals). This holistic view also allows us to see which elements of the logic model contribute most to the strategic goals, both via direct connections and through a series of strong linkages. All seven of the activities, nine of the thirteen outputs, and five of nine outcomes have strong links to the strategic goals. In assessing the impact of NLWs on the fulfillment of DoD-wide strategic goals, the elements encased by blue boxes are the most important.

Identifying Metrics to Evaluate the Logic Model

Having developed the logic model, we used it as a basis for identifying metrics that could be used to evaluate the impact of NLWs. We identified 97 unique metrics that collectively measured all 29 elements at the activity, output, and outcome levels. Some of the identified metrics were applicable to more than one logic model element, so we used those metrics multiple times, giving us an effective set of 115 metric-element pairings. We did not develop metrics for the inputs because those metrics would not relate to the effects of NLWs. We also did not develop metrics for the strategic goals, whose assessment is determined at a DoD-wide level and goes far beyond the scope of our study. Examples of the metrics we identified for three of the logic model's elements are shown in Table 1.

Overall, we found that:

- Activity metrics primarily related to which people or systems were affected by NLW usage and how they responded to it
- Output metrics generally related to providing the user with more time options, curtailing the adversary's options, and reducing tactical risks
- Outcome metrics most often related to reducing strategic and operational risks, influencing perceptions, maintaining morale, and reducing costs.

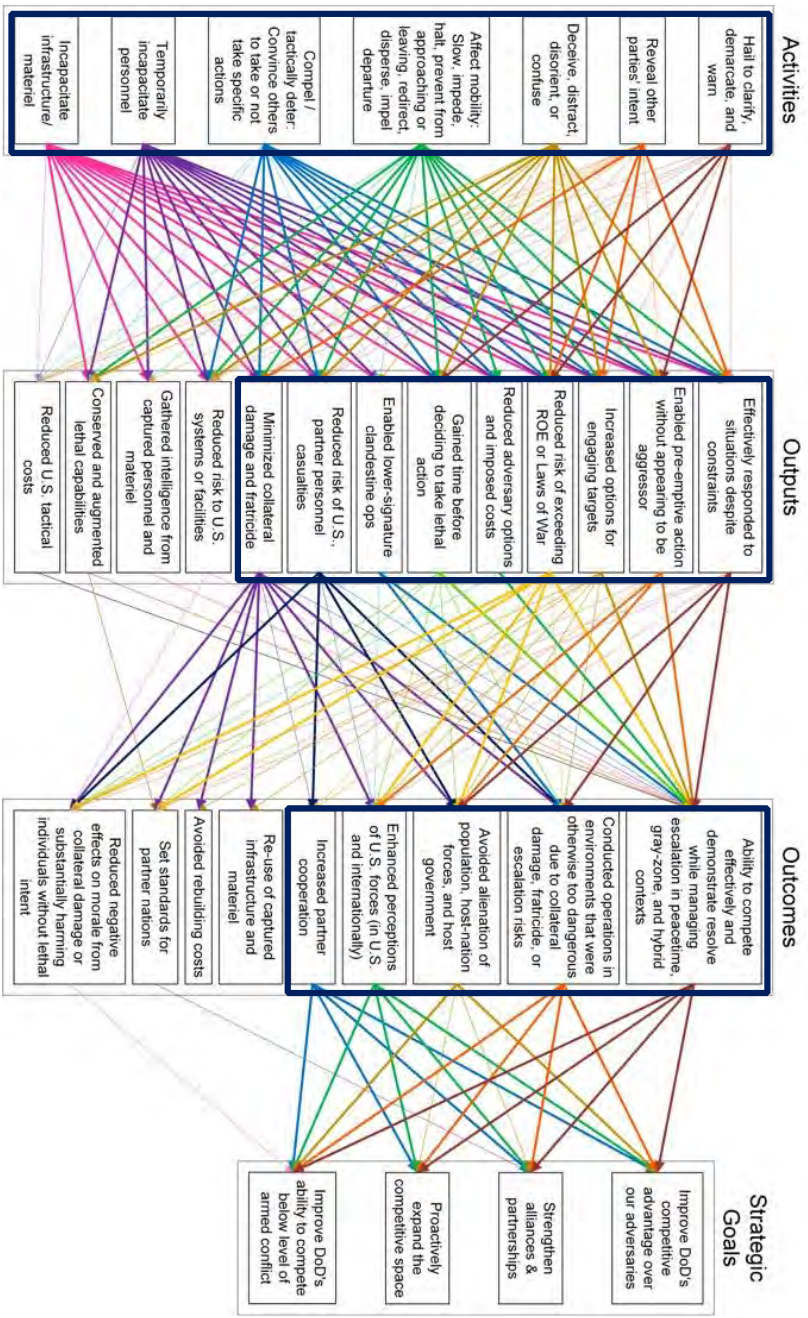

Figure 2: NLW Logic Model with Connectivity Between Elements (Source: Grocholski et al., *How to Effectively Assess the Impact of Non-Lethal Weapons as Intermediate Force Capabilities*).

Table 1. Examples of Metrics Associated with a Subset of Elements of the Logic Model (Source: Grocholski et al., *How to Effectively Assess the Impact of Non-Lethal Weapons as Intermediate Force Capabilities*).

Element Type	Element Description	Metric
Activity	Temporarily incapacitate personnel	Percentage of targeted population incapacitated by IFC
		Percentage of encounters in which non-targeted population is incapacitated by IFC
		Timeline between IFC use and incapacitation
		Duration of incapacitation
Output	Effectively responded to situations despite constraints	Percentage of tactical encounters in which use of IFCs was permissible, but lethal force was not
		Whether IFCs are allowed by ROE (Binary yes/no distinction)
		Degree to which targeted populations perceive IFCs as equivalent to lethal weapons
Outcome	Ability to compete effectively and demonstrate resolve while managing escalation in peacetime, gray-zone, and hybrid contexts	Percentage of incidents using IFCs that resulted in unwanted escalation divided by the percentage of incidents not using IFCs that resulted in an unwanted escalation
		Percentage of particular peacetime/gray-zone/hybrid incidents in which IFCs were used
		Percentage of incidents in which IFCs were used and commanders perceived them as contributing effectively
		Degree to which targeted populations perceive IFCs as equivalent to lethal weapons

Developing Vignettes

To ground the logic model and the associated metrics in the real world and to evaluate our metrics in a range of scenarios, we created and examined a total of thirteen vignettes featuring the use of NLWs. The vignettes encompass a range of circumstances and conditions. We ensured that they collectively included all combinations of possibilities with respect to the following criteria:

- *Whether the adversary sought to escalate the situation*. This provides some insights into the extent to which NLWs may be de-escalatory in situations where an adversary deliberately seeks to escalate the situation. It also provides comparisons between the de-escalatory capabilities of NLWs in situations with both escalatory and non-escalatory situations.
- *Whether withdrawal was feasible*. U.S. withdrawal can contribute to de-escalation of a situation, so we gauged both situations in which withdrawal was not possible and those in which it was.
- *Whether the narrative surrounding the incident was stable* (i.e., whether disinformation could radically change the narrative). Given that NLW usage can play an important role in shaping narratives, and those narratives can shape their ultimate impact in turn, it was important to explore both cases in which narratives from incidents were highly malleable and those in which they were not.

We assessed the values of each of these using a binary (yes/no) distinction and ensured that the thirteen vignettes included all eight possible combinations. We also designed the thirteen vignettes so that they collectively included all of the U.S. military services, took place in a range of locations around the globe, and spanned the air, sea, and land domains. Where possible, vignettes were based partly upon past events to enhance their realism. For example, one vignette involved a U.S. aircraft being intercepted and harassed by two military aircraft, so it sought to use NLWs to get them to back away without causing crashes or escalating the situation. This was based on a real-life incident in 2000, in which two Chinese aircraft intercepted a larger, slower U.S. aircraft, resulting in an accidental collision. A vignette involving U.S. marines securing an embassy against a rioting mob also reflected actual events in Bahrain in 2002, with the proviso that in the vignette, the marines could employ a range of NLWs. Similarly, an incident in which boats with unknown intent approached a U.S. destroyer was loosely based on the suicide boat attack that damaged the USS *Cole* in 2000. Still, in the vignette, NLWs provided additional options to protect the ship.

Our analysis of these vignettes confirmed that advanced NLWs (particularly directed energy) could have a substantial impact in a range of situations beyond their typical applications generally associated with law enforcement and crowd control (such as pepper spray). For example, in a gray-zone maritime standoff, advanced NLWs could help to demonstrate resolve without escalating the situation.

The vignettes also revealed the relative versatility of different classes of NLWs. We found that three types of systems were particularly versatile, with applicability in a majority of the vignettes, across a variety of contexts and domains. Both acoustic systems and laser dazzlers could be used to hail, deceive, distract, disorient, or confuse individuals. In addition, ADS could provide focused,

discriminating effects to tactically deter the other side, deny access, or compel movement. While these NLWs were especially versatile, a number of other NLWs also played important roles in specific vignettes. Having a panoply of NLWs available can ensure that the right ones are used for a particular situation.

Evaluating Metrics in the Context of Vignettes

We explored the vignettes using our logic model and metrics. The first step in this analysis was to determine which NLWs were applicable to the vignette. We then determined which elements of the logic model were relevant to the vignette itself and evaluated the associated metrics in the context of the vignette. The qualities of each metric (not the value of the metric) were evaluated using four standard criteria [4]:

- Validity – how well the metric measures the element
- Reliability – the degree to which multiple measurements will be consistent
- Feasibility – how easily the measurement can be made
- Timeliness – how quickly a measurement can be made.

This evaluation showed that most metrics were strongly applicable to the logic model elements and relatively straightforward to measure; however, only about half of the developed metrics were applicable to any particular vignette.

Themes Identified in Interviews

As part of our analytical process, our team conducted 36 interviews with experts and stakeholders from 25 organizations. Four broad themes came out of our analysis of these interviews:

1. *The two biggest barriers to NLW integration within DoD are cultural reticence and resource limitations*. Potential NLW users often have limited experience with their usage, contributing to limited confidence in them. They also sometimes do not understand the effects of these systems and/or perceive them as less useful than lethal systems. Competing training requirements often result in NLW training being de-emphasized.
2. *NLWs are often seen as logistically burdensome* in terms of space, power, and other requirements, so they are often not brought to locations where they could be useful.
3. *Opportunities for NLW usage beyond military policing and crowd control are not widely perceived*. The utility of NLWs in the competition below the threshold of war and many other contexts was not well-recognized.

[4] Savitz, Matthews, and Weilant, *Assessing Impact to Inform Decisions*.

4. *The above challenges are interrelated and mutually reinforcing*. For example, a lack of NLW usage due to training shortfalls and an aversion to supporting them logistically contributes to a lack of awareness and confidence regarding these systems, which lowers their priority in terms of both training and logistics.

Recommendations and Closing Remarks

Based on the results of our study, we made a series of recommendations to the U.S. Joint Intermediate Force Capabilities Office and DoD that could be potentially applicable to NATO and individual nations. First, the logic model, or a similar NATO-focused variant, can be used in a range of forums, including in discussions with senior leaders, in order to illustrate how NLWs can impact strategic goals. Second, to evaluate the impact of NLWs, it is necessary to gather data that can be used to calculate values for the metrics. This could be done using real events, wargames, and live exercises. Metrics that are associated with logic model elements with strong links to strategic goals and that are easy to measure should be assessed first.

Additionally, our study found that NLWs are often perceived negatively, which inhibits their larger adoption and use. To address and overcome this, we recommend that those seeking to leverage NLWs establish consistent and clear policies, concepts of operations, standardized training, and protocols to integrate non-lethal capabilities into tactics, techniques, and procedures. Additionally, the logic model, metrics, vignettes, and technology demonstrations can be used to inform non-specialists about the utility of NLWs. Finally, future NLW capabilities should be designed to reduce perceived and actual burdens on operators. Specifically, in order to appeal to potential users, future NLW development should prioritize making NLWs that are easy to carry, easy to maintain, and easy to learn how to use, even at the expense of other design tradeoffs. Moreover, the advanced NLWs that we had identified as particularly versatile in our vignette analysis—notably acoustic systems, laser dazzlers, and the ADS—are capabilities that should also be prioritized for future development.

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.

About the Authors

Krista Romita Grocholski is a physical scientist at the RAND Corporation and serves as co-program manager for the NOAA-funded Mid-Atlantic Regional Integrated Sciences and Assessments (MARISA) center. Her research at RAND has covered a wide range of topics, including emerging technologies, force generation and readiness modeling, assessing commercial space capabilities, climate adaptation and resilience, and assessing the impact of non-lethal weapons. Prior to RAND, Romita Grocholski completed her doctoral and master's degrees in observational astronomy at the University of Florida.
E-mail: kristarg@rand.org

Dr. Scott Savitz is a senior engineer at the RAND Corporation. Much of his research focuses on how to improve the effectiveness and resilience of operational forces through the use of new technologies and modified tactics. Recently, he has led analytical efforts to assess capability gaps in the European Arctic, the impact of non-lethal weapons, intelligence on threats to U.S. ports, and how the U.S., Japanese, and Brazilian militaries can invest in emerging technologies. Savitz has also led analyses on testing infrastructure requirements for autonomous systems, how to improve maritime domain awareness, how to measure the impact of efforts to counter hostile networks, and how the Coast Guard can prepare for future Arctic operations. He has previously led studies on how to effectively use unmanned surface vehicles, how to counter naval mine threats, and how the Coast Guard can make more informed asset allocation decisions. Previously, Savitz provided on-site analytical support for the Navy's mine warfare command and the U.S. Naval Forces Central Command. He has led exercise observation teams around the globe and supported the Navy in Bahrain from 2001-2003, addressing political-military, counter-terrorism, and chemical/ biological/ radiological defense issues. Savitz earned his bachelor's degree in chemical engineering from Yale University and master's and Ph.D. degrees in the same field from the University of Pennsylvania.
E-mail: ssavitz@rand.org

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

P. Dobias, K. Christensen & W. Freid
Connections QJ 21, no. 2 (2022): 97-109
https://doi.org/10.11610/Connections.21.2.07

Research Article

Gaming Intermediate Force Capabilities: Strategic Implications of Tactical Decisions

***Peter Dobias,*[1] *Kyle Christensen,*[1] *and William Freid* [2]**

[1] *Defence Research and Development Canada, Centre for Operational Research and Analysis, 60 Moody Drive, Ottawa, Canada, http://www.drdc-rddc.gc.ca*

[2] *Joint Intermediate Force Capabilities Office, U.S. European Command, Kurmacherstrasse Gebaude 2304, Stuttgart, Germany, https://jnlwp.defense.gov*

Abstract: This article reviews the development and tests of two Intermediate Force Capability (IFC) concept development hybrid wargames. The first wargame plays out a maritime Task Force's ability to counter hybrid threats in the grey zone. The second wargame examines the ability of a NATO Task Group, deployed to a third country to train local security forces, to counter a hostile militia trained and supported by a neighboring country. IFCs offer a class of response between doing nothing and using lethal force in a situation that would be politically unpalatable. As such, the aim of the wargame series is to evaluate whether IFCs can make a difference to mission success against hybrid threats in the grey zone. This wargame series was particularly important because it used traditional game mechanics in a unique and innovative way to evaluate and assess IFC's effects on strategic mission success. Specifically, the hybrid wargame series has demonstrated that IFCs have a high probability of filling the gap between doing nothing and using lethal force. IFCs have the potential to improve operational effectiveness by allowing for more restrained use of force to escalate/de-escalate a situation and increasing decision time and space for tactical decision-makers. Both counter-personnel and counter-materiel capabilities (including miniaturization) are needed to act effectively in the current hybrid threat environment.

Keywords: grey zone, hybrid threats, kriegsspiel, matrix, non-kinetic, non-lethal, wargaming.

Introduction

Hybrid Threats

In recent years, analysis of the international security environment has increasingly focused on hybrid threat tactics in the grey zone. The "grey zone" is defined in a recent RAND study as "…an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and non-military actions and the attribution for events."[1]

The goal of hybrid threat tactics in the grey zone is to create strategic, operational, and tactical dilemmas for an opponent while avoiding a head-to-head confrontation.[2] By keeping these activities below the threshold of interstate war, these tactics aim to force an opponent to either accept the emerging status quo or use force to resolve the dilemma (and thus become the aggressor themselves). Operationalizing hybrid threats involves all elements of state power. Russia, China, and Iran provide the most prominent examples of undertaking and implementing these approaches.[3] They consider state interactions as a "continuum of conflict" in which the area between peace and war is simply a conflict by other means. The implementation of these hybrid tactics differs between Russia and China on the one hand (relying on economic coercion, political influence, unconventional warfare, information operations, and cyber operations)[4] and Iran (military and technological aspects) on the other. The overall strategic aim,

---

1 Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM* 7, no. 4 (November 8, 2018): 30-47, https://cco.ndu.edu/news/article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/; 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 (Santa Monica, CA: RAND Corporation: 2019), 8, https://www.rand.org/pubs/research_reports/RR2942.html.

2 Andrew F. Krepinevich, Barry Watts, and Robert Work, *Meeting the Anti-Access and Area-Denial Challenge* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2003), 2-3, https://csbaonline.org/uploads/documents/2003.05.20-Anti-Access-Area-Denial-A2-AD.pdf.

3 Peter Hunter, "Political Warfare and The Grey Zone," in *Projecting National Power: Reconceiving Australian Air Power Strategy for an Age of High Contest*, Special Report 142 (Australian Strategic Policy Institute, August 2019), https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-08/SR%20142%20Projecting%20national%20power.pdf; Erik Reichborn-Kjennerud and Patrick Cullen, "What is Hybrid Warfare?" Policy Brief 1 (Norwegian Institute for International Affairs, January 2016), https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf; James K. Wither, "Making Sense of Hybrid Warfare," *Connections: The Quarterly Journal* 15, no. 2 (2016): 73-87, https://doi.org/10.11610/Connections.15.2.06.

4 Sydney J. Freedberg Jr., "Cyber Warfare in The Grey Zone: Wake Up, Washington," *Breaking Defense*, April 9, 2019, https://breakingdefense.com/2019/04/cyber-warfare-in-the-grey-zone-wake-up-washington/.

however, is similar: to challenge, constrain, or deny an adversary's access to geostrategically important areas.[5]

Intermediate Force Capabilities

While exploiting the space below the threshold of armed conflict and employing Anti-Access/Anti-Denial (A2/AD) type activities are not new in and of themselves,[6] the prevalence of their use by Russia, China, and Iran in recent years poses unique challenges for military planners. Although it is important to maintain lethal military capabilities in order to deal with these situations in extremis, it is becoming increasingly important to develop capabilities that would enable Allied forces to respond to situations below the threshold of lethal confrontation. Otherwise, coalition forces will be faced with the dilemma of either doing nothing or employing lethal force (either of these options may lead to potentially serious strategic outcomes) when responding to challenges posed by an adversary. The desirable class of response between these two extremes is what has become known as Intermediate Force Capabilities (IFC).

Early IFC development began in the mid-1990s—driven in part by the events that took place in Somalia—and, at that time, was focused on Non-Lethal Weapon (NLW) development. Efforts focused primarily on implementing existing systems to decrease the risk of casualties, such as rubber bullets/ bean-bag rounds, electro-muscular incapacitation devices (such as Taser™), water cannons, stun grenades, and even nets.[7] Most of these systems were aimed primarily at crowd control. In some cases, their use was legally restricted, e.g., while tear gas could be used by law enforcement, its use by front-line combat military forces was covered under the chemical weapon ban.[8]

However, the necessity for NLWs was highlighted again during the wars in Iraq and Afghanistan, particularly their need to evolve beyond simple crowd control and force protection measures and focus on decreasing civilian casualties.[9] In recent years the focus has shifted to broader IFC development in order to facilitate better and more comprehensive solution sets applicable in the grey zone. The fact that adversaries are exploiting this zone is driving the need to develop,

---

5 Morris et al., *Gaining Competitive Advantage in the Gray Zone*.

6 James Lacey, "Battle of the Bastions," *War on the Rocks*, January 9, 2020, accessed March 28, 2020, https://warontherocks.com/2020/01/battle-of-the-bastions/.

7 Joint Non-Lethal Weapons Directorate, "Intermediate Force Capabilities: Bridging the Gap Between Presence and Lethality," Executive Agent's Planning Guidance 2020 (United States: Department of Defense, March 2020), https://mca-marines.org/wp-content/uploads/DoD-NLW-EA-Planning-Guidance-March-2020.pdf.

8 Office for Disarmament Affairs, "1925 Geneva Protocol: Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare" (Geneva: United Nations, June 17, 1925), accessed March 28, 2021, https://www.un.org/disarmament/wmd/bio/1925-geneva-protocol/.

9 NATO Science and Technology Organization (STO), "Analytical Support to the Development and Experimentation of NLW Concepts of Operation and Employment," Technical Report STO-TR-SAS-094 (NATO STO, April 2017).

test, and implement IFCs. According to the Joint Intermediate Force Capabilities Office (JIFCO), "gray zone" competition dominates any conceptual "spectrum of warfare" and is ideally suited for IFC development.[10]

IFCs are intended to enable effective escalation management and control from tactical to strategic levels of operation and across all domains. Being able to control and manage escalation would allow coalition forces to gain and maintain the operational and strategic initiative and thus have a deterrence effect on a potential adversary. IFCs also encompass a much wider concept than NLWs. For example, IFC development explores a wide range of options for anti-personnel and anti-materiel options (including non-lethal directed energy systems). However, IFCs also include information operations, cyber, and electronic warfare capabilities (targeting an adversary's decision-making options in the cyber and information domains, for example).[11] Most importantly, IFCs do not come at the expense of the lethality of the overall force.[12] IFCs are a strategic risk mitigation investment that provides warfighters the tools to seize the initiative while competing below the level of armed conflict and, as such, enable more targeted and effective use of lethal force.

NATO R&D Response

Under the auspices of the NATO Science and Technology (STO) Systems Analysis Studies (SAS) panel, there has been a series of studies (SAS-035, SAS-060, SAS-078, and SAS-094) studying NLW options. Of these studies, SAS-078 led to a NATO Bi-Strategic Command NLW requirements list. This study also identified then-in-existence NLW capabilities and resulting gaps in NATO NLW capabilities/systems.[13] It was followed by the SAS-094 study that looked at the operational effects of NLWs during combat operations. The analysis of post-conflict operations identified opportunities for NLWs to extend the decision time and space for soldiers in an escalation of force incidents. NLWs were viewed as means to isolate and degrade targets to be engaged or to engage targets when the use of

[10] Wendell B. Leimbach Jr., "DoD Intermediate Force Capabilities: Bringing the Fight to the Gray Zone," Information Brief (Joint Non-Lethal Weapons Directorate), https://jnlwp.defense.gov/Portals/50/Documents/Resources/Presentations/IFCOverviewBrief_ColL_short.pdf.

[11] Joint Non-Lethal Weapons Directorate, "Strategic Plan 2016-2025: Science & Technology Joint Non-Lethal Weapons Program" (United States: Department of Defense, 2016), https://jnlwp.defense.gov/Portals/50/Documents/Resources/Publications/Government_Reports/JNLWP_ST_Strategic_Plan_FINAL_Distro_A.pdf.

[12] Joint Non-Lethal Weapons Directorate, "Strategic Plan 2016-2025," 1.

[13] NATO Research and Technology Organization (RTO), "Non-Lethal Weapons Capability-Based Assessment," RTO Technical Report RTO-TR-SAS-078 (AC/323(SAS-078)TP/461, December 2012).

lethal force would not be appropriate.[14] These observations were further reinforced by identical conclusions from two NATO Non-Lethal Technology Exercises executed in close collaboration with the SAS-094 study.[15]

The latest in this series of these studies, designated SAS-151, has the goal of exploring "Solutions Enabling Intermediate Force Capabilities (IFC)/Non-Lethal Weapons (NLW) Contributions to Mission Success." The research aims to build on the work of SAS-094 and examine and determine whether IFCs make a difference in mission success and to what extent. As a part of the overall methodology, SAS-151 elected to use a series of wargames to evaluate IFC effectiveness in the grey zone. These wargames were designed specifically to assess the strategic and operational effects of the tactical employment of IFCs in hybrid threat environments. The following sections briefly cover the design, implementation, and findings from two hybrid wargames that took place in September 2020 (assessing mission effectiveness of IFCs in naval task group operations) and April 2021 (assessing mission effectiveness of IFCs in a land /urban/ operation).

Wargaming and Intermediate Force Capabilities

At their core, wargames are tools for exploring and informing human decision-making in an environment with incomplete and imperfect information.[16] As such, they can be used to assess and/or generate innovative ideas, address defense problems of the future, and can be applied to all levels of warfare. There are a variety of different wargame types. The most common tabletop tactical games employ a kriegsspiel approach, while strategic games generally employ a matrix approach.[17] Nevertheless, in a strategic situation such as the one described here, where coalition forces must respond to hybrid threats in the grey zone and where tactical effects of various capability mixes can have dramatic strategic consequences both in terms of success and failure, neither a kriegsspiel game nor a matrix game would work in isolation.

A Kriegsspiel and a Matrix Game

Kriegsspiel games are generally effective at the tactical level. However, their normally compressed time scales and often limited scope preclude the development of strategic considerations. Even large-scale operational kriegsspiel games that

[14] NATO STO, "Analytical Support to the Development and Experimentation of NLW Concepts."

[15] NATO STO, "Analytical Support to the Development and Experimentation of NLW Concepts."

[16] U.S. Naval War College, *War Gamers' Handbook: A Guide for Professional War Gamers* (Newport, RI: U.S. Naval War College, November 2015), https://apps.dtic.mil/sti/pdfs/AD1001766.pdf.

[17] U.K. Ministry of Defence, *Wargaming Handbook* (London: Development, Concepts and Doctrine Centre, Ministry of Defence, August 2017), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641040/doctrine_uk_wargaming_handbook.pdf.

typically take place against a strategic backdrop do not consider changes to the strategic environment itself.[18] In contrast, matrix games can effectively model strategic decision-making and strategic implications of operational decisions. Still, because they are generally high-level and use generalized/ aggregate military capabilities, they are ill-suited to compare two or more tactical capability options. Therefore, the approach adopted by SAS-151 was to execute a modified/shortened version of a matrix game to assess the outcome of an initial tactical-level kriegsspiel engagement game. The kriegsspiel game itself was set up within the strategic and operational context of the matrix game that enabled changes in the strategic environment.[19] While the key components to a player's action and the key steps to a gameplay turn were retained, how they are used together to assess IFC effectiveness in the grey zone is a unique adaptation to these traditional games.[20]

Wargame Implementation

The hybrid wargame was initially intended as a tabletop wargame. However, with the advent of the SARS-CoV-2 virus (COVID-19) and the resulting travel restrictions imposed by many national governments, it was decided to design and execute the game online in a virtual environment. Several different web-based solutions were considered. The key constraint was that the proposed solution had to accommodate different user requirements – some players used personal computers while others used work/government/NATO computers. The gaming setup did not require significant login or joining instructions, was stable enough for prolonged gameplay, and was cost-effective. In the end, the SAS-151 Wargame Working Group settled on a combination of a simple video teleconferencing platform (WebEx(TM) was used due to easy availability for video) combined with Google Docs(TM)/Google Slides(TM) for team text chats and gameplay. Due to the complexity of the hybrid game setup, SAS-151 ran a full-scale test game to validate the methodology, scenarios, and online execution of the gameplay tools.

The naval scenario considered the harassment of coalition vessels by maritime militia, go-fasts and rigid-hull inflatable boats, other military vessels, and medium-sized unmanned aerial vehicles (UAV) by two aligned hostile countries.

---

[18] Matthew B. Caffrey Jr., "On Wargaming: How Wargames Have Shaped History and How They May Shape the Future," *The Newport Papers* 43 (U.S. Naval War College, January 2019), https://digital-commons.usnwc.edu/newport-papers/43.

[19] "International Safety Research, Summary Report 1: Vignettes, Scenarios and Tasks," *Force Protection Requirements for the Canadian Surface Combatant*, Report 7.06, CORA Task 019, ISR Report W7714-156105-T019 7.06, Version 2.0 (DRDC-RDDC-2017-C054, March 17, 2017).

[20] Kyle D. Christensen and Peter Dobias, "Wargaming the Use of Intermediate Force Capabilities in the Gray Zone," *The Journal of Defense Modeling and Simulation* (April 2021), https://doi.org/10.1177/15485129211010227.

These vessels impeded the NATO Maritime Task Force's navigation in a contested waterway and interfered with the Task Force's air operations. The adversaries could utilize harassment, swarming, and/or hit-and-run tactics in order to challenge the decision-making of the NATO Maritime Task Force Commander. Furthermore, the scenario presented players with a complex security situation that involved a very tense security environment. In effect, any miscalculation or excessive use of force could have significant strategic consequences. In the game, the two aligned hostile countries also waged an ongoing information operation campaign aimed at discrediting NATO and the Task Force's mission.[21]

The land scenario considered a NATO Task Group deployed to a third country to train local security forces. The combined Host Nation-NATO security force was confronted by a militia (trained and/or controlled by a neighboring country) attempting to expel NATO from the region. The militia used civilians as human shields and/or "influenced" crowds to limit NATO's freedom of action. Popular opinion in the Host Nation was largely opposed to NATO presence in the region. In addition, the neighboring country was massing forces at its border with the stated intent of protecting its ethnic minority population in the Host Nation. Consequently, any use of force could have significant strategic consequences for NATO forces in the region.[22]

Wargame Execution

Participants in the wargame included operational analysts, military personnel, strategic and regional analysts, and subject matter experts with expertise in IFCs. The participants were from multiple NATO countries (Belgium, Canada, Denmark, Germany, Italy, UK, US) and organizations (NATO Allied Command Transformation (ACT), Warfare in Confined and Shallow Water Centre of Excellence (COE), Military Police COE, and Littoral Warfare COE).

Two capability options were considered for each scenario:

- Option A. Baseline (no IFCs/legacy NLW systems such as FN-303 rifles), and
- Option B. Near Future IFCs (technology available now or expected to be operational within five years).

IFCs used in the games included Active Denial Systems (ADS), Laser Dazzlers, Long-Range Acoustic Devices (LRAD), and various mounted and handheld Anti-UAV Systems that can not only harass and warn but also interdict and incapacitate potential threats at a standoff distance. It was expected that this would give

[21] Kyle D. Christensen, and Peter Dobias, *Use of Intermediate Force Capability Game Series: Game 2 – NATO Naval Task Group in Confined Waterway* (NATO Science and Technology Organization, Pre-Released Technical Report, STO-TR-SAS-151 Annex F, March 2021).

[22] Maude Amyot-Bourgeois, Brittany Astles et al, *Use of Intermediate Force Capability Game Series: Game 3 – NATO Task Group in Land Wargame Scenario* (Pre-Released Technical Report, STO-TR-SAS-151 Annex G, October 2021).

the friendly forces more options to control (escalate/de-escalate) the situation and to take the strategic initiative.

Key Observations

Option A: Observations

Despite vast differences between the scenarios, the tactical situations developed similarly in both analyzed options. For example, in Option A, during the tactical kriegsspiel game, the adversary was generally able to maintain the initiative and demonstrate an aggressive stance toward friendly forces. In both scenarios, escalation spun out of control. For the naval scenario, the tactical game resulted in missiles fired against friendly vessels and torpedoes fired by both friendly and adversary forces. For the land scenario, the friendly forces were pushed into using excessive force (including the use of CS gas against a crowd and firing high explosive rounds at civilian targets), which provided the impetus for the adversary to send forces across the border and fire missiles toward a joint Host Nation-NATO base. In both cases, NATO's inability to constrain and control escalation gave a significant strategic initiative to the adversary. The adversary was able to exploit these tactical developments and use them very effectively in an information operations campaign and in diplomatic efforts to undermine coalition objectives and efforts in the game (as will be discussed later).

However, it must be noted that similar tactical outcomes resulted from very different approaches to counter tactical dilemmas encountered in both the naval and land games. In the naval game, friendly forces were generally passive and often resorted to doing nothing (or recording aggressive adversary actions). The limited range of responses (i.e., doing nothing or using force) appeared to embolden the adversary to undertake more aggressive actions. Even seemingly innocuous events, such as using small arms to down a UAV in order to recover a helicopter, had profound and significant consequences in the information space. In the land game, limited response options resulted in an early escalation of force against the crowd (use of rubber bullets and CS gas from the game opening) and rapid and excessive use of lethal force against the militia in the presence of civilians (use of high explosives to suppress the adversary's shooters). While this enabled the friendly forces to regain some freedom of action, it also gave the adversary the excuse to escalate further while successfully using information operations to paint the friendly force as aggressors. At no point in the Option A land game were the friendly forces able to control the cycle of escalation or put themselves in a position to de-escalate the situation.

In both scenarios, the adversary's assertive behavior carried over to the strategic matrix game. In the matrix game, the adversary was able to monopolize the narrative they created in the tactical game and painted friendly forces as belligerent and reckless, inept and incapable, and the cause for escalating tensions in the region. The naval game resulted in a neutral country that initially supported

NATO forces reconsidering its partnership with NATO. Similarly, in the land scenario, the adversary was able to use the excessive civilian casualties and damage to infrastructure to get a vote of non-confidence against the government supporting NATO's presence in the region. The neighboring country was even able to reinforce its international standing and justify its interference in the Host Nation. From this perspective, in both scenarios, Option A resulted in a strategic achievement for the adversary, with the adversary's position strengthened and NATO's position in the region weakened.

Option B: Observations

In both scenarios, the use of IFCs turned the strategic equation on its head in favor of friendly forces. At the tactical level, during the naval scenario, the adversary's attempt to use force was hampered by NATO's use of IFCs. IFCs allowed to discourage unwanted behavior and/or degrade/disrupt the adversary's ability to use force. By the end of the tactical game, there was little to no response from the adversary to NATO's actions. It appears the knowledge and presence of IFCs, in and of themselves, caused the adversary to consider the use of their own non-lethal options more seriously. The adversary was also more restrained in their escalatory behavior. In the land scenario, friendly forces were able to use IFCs to disrupt the initial hostile actions of the anti-government elements in the crowd. Just as important, friendly forces were able to use IFCs to suppress hostile militia actions and were thus able to use lethal force more judiciously. Limited use of lethal force significantly reduced the number of civilian casualties and, more importantly, undermined the adversary's narrative that NATO forces were belligerent and reckless.

However, it must be noted that the Option B wargame was not without its escalatory attempts or behaviors. In the naval game, the adversary directed warning shots at a NATO supply ship and one of the frigates (following verbal warnings to NATO vessels). These warning shots resulted in damage to the frigate. However, as the game progressed, and the adversary's attempts to elicit a forceful response from NATO (being more aggressive) were stymied by the IFCs. Consequently, the adversary force became more reactive in their actions during the naval war game. Similarly, in the land game, the militia was able to cause some damage to NATO and the Host Nation's forces, vehicles, and infrastructure using UAVs laden with explosives, RPGs, IEDs, and general-purpose machine guns. However, the use of IFCs disrupted and degraded the hostile actions, so the damage was significantly less than in Option A. In both scenarios, rather than controlling the narrative and escalation, IFCs appeared to take away the pretext/justification for the adversary's use of force and shifted the tactical initiative in favor of the friendly forces.

Most importantly, the change in the initiative in favor of the friendly forces caused a significantly different strategic outcome from the Option A scenario. In the naval game, the position of NATO in the region was strengthened, and a neutral country sought closer alignment with NATO. In the land scenario, while the

overall opposition to NATO within the region was not eliminated, it at least did not become any worse and remained manageable for the Host Nation government. Moreover, the outcome increased NATO's appeal as a regional partner and limited the international appeal of the adversary, particularly their objective to reduce or eliminate NATO's presence. The hostile country was unable to strengthen its position in either scenario. From this perspective, the availability of IFCs helped facilitate a strategic achievement for NATO.

One important aspect to note during the land game was that of the weight/size limits and, consequently, of mobility of IFCs. This was most apparent during the land scenario. While this was not really a concern in the naval game, in the land scenario, it would have been desirable to have, for instance, ADS (which was the most versatile and effective system in the game) mounted on vehicles or even on helicopters. It was noted that a mobile ADS would increase a convoy's operational effectiveness, even if at the cost of the system's range.

IFCs and Tactical Decisions: Space and Time in the Face of Dilemmas

As mentioned above, the most important tactical aspect of IFCs was that they expanded the NATO Task Force commander's decision time and space when faced with tactical dilemmas. In this specific case, these dilemmas were posed by the escalatory behavior and provocations of the adversaries. The IFCs gave NATO forces the ability to control the escalation, which eventually led to a shift in the dilemma to the adversary. Whereas without IFCs, friendly forces were either limited to doing nothing or reacting to hostile actions with significant lethal force, they were able to take the initiative with IFCs. In the end, it was the adversary who became reactive. For instance, in the naval game, the NATO commander was able to recover a helicopter in such a way that the initial attempt by hostile forces to interfere with the landing worked to strengthen NATO's narrative. Similarly, in the land game, the hostile elements in the crowd, as well as the militia, were forced to adopt a more passive-aggressive posture and "encourage" the crowd to block the road. This gave an opportunity to friendly forces to present themselves as providing aid to civilians affected by these hostile actions.

Being able to acquire greater time and space for decision-making reinforces findings and observations made during the two NATO Non-lethal Technology Exercises referenced earlier. At the time, it was determined that the availability of non-lethal capabilities gave tactical commanders critical decision time and space to choose courses of action that reduced collateral damage, resulted in fewer civilian casualties, and increased the probability of engaging actual threats.[23] Similar observations were made based on modeling ship force protection options against small boat swarms.[24]

---

[23] NATO STO, "Analytical Support to the Development and Experimentation of NLW Concepts."

[24] Peter Dobias and Cheryl Eisler, "Modeling a Naval Force Protection Scenario in MANA," *Operational Research and Management Science Letters* 1, no. 1 (2017): 2-7, https://www.orlabanalytics.ca/ormsl/archive/v1/n1/ormslv1n1p2.pdf.

IFCs and the Strategic Initiative

In both wargames, a shift in the tactical initiative led to a corresponding shift in the strategic initiative. Once NATO forces were able to shift the initiative in their favor at the tactical level, it was reflected in both the strategic narrative and NATO's relationship with allies at the operational level. The availability of IFCs prevented a situation where coalition partners questioned their continued support of the NATO mission (as happened during the Option A wargame). In fact, in the naval game, IFCs caused the exact opposite. During their planning, NATO allies consistently referred to staying close to and under NATO's protective IFC umbrella. One player summed up the effectiveness of IFCs as "No moves/ actions this turn. Stay under the protective umbrella of IFCs and watch the enemy impale themselves on the IFCs." In the land scenario, the presence of IFCs enabled NATO forces to limit the escalatory behavior of the Host Nation's security forces. In one of the turns, a Host Nation unit planned to use rubber bullets and CS gas. However, the use of ADS by NATO forces changed the tactical situation, and the Host Nation's security forces were no longer required to consider using escalatory courses of action or systems.

On the operational side, IFCs provided NATO forces with the time and space to plan ahead. In the naval scenario, as opposed to Option A, where the Naval Task Force was dispersed, not in control, and under increasing levels of threat or attack, the Task Force was in control in Option B, the threat level was diminishing, and most importantly, the NATO Maritime Task Force was growing in strength. Thus, during the war game, IFCs allowed the Maritime Task Force to preserve its power and freedom of action and maneuver. Within the scenario's strategic context, this was quite important. In the scenario, the adversary's Naval Task Force—a modern, capable fleet—was less than five hours away from the NATO Maritime Task Force. As a result of IFC availability, the NATO Task Force would be in a much better position to deal with the potential threat. Similarly, in the land scenario, the use of IFCs, particularly the vehicle stopper and laser dazzler, co-mounted on a remote weapon stations, enabled NATO and Host Nation forces to suppress/degrade the hostile militias and use lethal force very selectively and under less immediate pressure.

Another important key takeaway was that the adversary was less successful in turning innocuous events into profound and significant advantages. For example, the lack of video footage of NATO personnel using overt force hindered the adversary's information campaign. While the adversary still pursued an outright misinformation campaign during the strategic matrix game, their narrative had less or no supporting evidence, which led to their reliance on fake news.

Need for Strategic Narrative

There was one important observation that occurred in the naval scenario. Once NATO forces employed IFCs, more specifically ADS, the adversary resorted to calling it a "death ray" and used fake photos and videos of injuries to manufacture their claims. This put NATO on the defensive with regard to the narrative.

The NATO counter-narrative approach of speaking the truth and being transparent (i.e., offering test results, showing historic IFC use/testing, scientific studies, and demonstrations) did not appear to be overly effective during the war game. This post-fact approach may have challenges gaining acceptance not only in adversary populations (less surprising) but even in allied populations (more concerning). Unfortunately, the very nature of directed energy IFCs lends itself to a narrative of death or heat rays even when these articles attempt to present these capabilities in a positive light.[25] And in recent alleged examples of use, IFCs have been characterized as "cooking soldiers" and "burning you from the inside out.[26]

Summary and Future Research

The NATO SAS-151 maritime and land wargames have shown conclusively that IFCs provide an important capability set to manage escalation during conflict below the threshold of interstate war. In the analyzed scenarios, the IFCs allowed the coalition commander to resolve security dilemmas posed by the adversary's provocative, even escalatory behavior. This resulted in the friendly forces' ability to seize the initiative and forced the adversary to rely on misinformation and fake news. However, it was also observed that the adversary very effectively employed a "death ray" narrative concerning the IFCs, using fake news and falsified videos. This suggests that it will be important to be very transparent with safety trials prior to the deployment of such systems to pre-empt such a narrative should IFCs be employed.

The land wargame brought up issues of mobility (consequently, the weight/size limits of IFCs). For example, while ADS was very effective in both scenarios, in the land scenario, it would have been much more effective if it could be mounted on vehicles or even airborne.

The wargame results will be used for the NATO IFC concept development and additional gaming, where integrated modeling and simulations are already planned to help validate IFC effects and concepts. It is anticipated that a joint scenario can be used for concept refinement and validation and, at the same

[25] Benjamin Bissell, "The Navy's Scary New Death Ray," *Lawfare*, November 17, 2014, accessed December 1, 2020, https://www.lawfareblog.com/navys-scary-new-death-ray; Luke Fleet, "Dreaming of Death Rays: The Search for Laser Weapons," *Nature*, January 9, 2019, accessed December 1, 2020, https://www.nature.com/articles/d41586-019-00024-0.

[26] Tim Stickings, "China 'Used Secret Microwave Pulse Weapon to Cook Indian Soldiers Alive' and Force Them Into Retreat in Himalayan Border Battle," *Daily Mail*, November 17, 2020, accessed November 30, 2020, https://www.dailymail.co.uk/news/article-8957019/China-used-secret-microwave-pulse-weapon-Indian-soldiers.html; James Plafke, "China's New Microwave Pain Beam Burns You From the Inside Out," *Extreme Tech*, December 10, 2014, accessed December 10, 2020. www.extremetech.com/extreme/195671-chinas-new-microwave-pain-beam-burns-you-from-the-inside-out.

time, can help validate IFC effectiveness for other IFC categories (such as cyber and electronic warfare) across multiple domains.

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.

About the Authors

Peter Dobias – see the CV on p. 9 of this issue, https://doi.org/10.11610/Connections.21.2.00.

Kyle Christensen – see the CV on p. 54 of this issue, https://doi.org/10.11610/Connections.21.2.03.

Bill Freid began his military career as an infantry officer moving from platoon leader to anti-tank company commander. Mr. Freid then transitioned to Psychological Operations (PSYOP), where he supported the Green Berets during two deployments to Kandahar, Afghanistan. Mr. Freid was then a company commander for Tactical Psychological Operations Company. He again deployed to Kabul, Afghanistan, with NATO as the Media Director for the Combined Joint Psychological Operations Force. Upon his return, he was the executive officer for the 13th PSYOP battalion. Mr. Freid transitioned to be a civilian PSYOP planner at US European Command. He was then the non-lethal weapons planner for US European Command and a participant in the NATO Systems Analysis and Studies working group studying how to counter malign actors' activities in the grey zone. Currently, Mr. Freid serves as a PSYOP Planner at US Cyber Warfare Command.

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

S. Waldman & S. Havel, *Connections QJ* 21, no. 2 (2022): 111-122
https://doi.org/10.11610/Connections.21.2.08

Research Article

Launching Narrative into the Information Battlefield

Suzanne Waldman and Sean Havel

Defence Research and Development Canada, https://www.canada.ca/en/defence-research-development.html

Abstract: It has long been understood that competition in the narrative battlefield impacts outcomes on the physical battlefield. The impact of narrative only increases in our era of gray zone narrative warfare conducted via social media. Valid norms constrain democratic militaries from developing forms of narrative competencies that autocratic states have available for use – namely, those involving fictionalization, misattribution, and other forms of deception. To compete in the narrative battlefield, democratic militaries should enhance their capability for disseminating truthful, close-to-real-time, extended stories of military activities with real-world, value-based stakes, crafted using age-old formulas of characterization and plot to appeal to wide as well as targeted audiences.

Keywords: narrative, strategic communication, information operations.

Introduction

NATO and its member countries have been emphasizing the importance of developing and maintaining strategic narratives for nearly a decade on the grounds that activities in the narrative battlefield impact outcomes on the physical battlefield.[1] Lending coherence to the who, what, where, how, and why of foreign and military policies and actions, narratives influence how policies and actions

[1] Steven R. Cornyn, "NATO Strategic Comm and Narrative in Afghanistan," *COMOPs Journal*, June 21, 2012, https://csc.asu.edu/2012/06/21/nato-strategic-comm-and-narrative-in-afghanistan/.

are perceived by adversarial and allied strategic actors, along with the audiences from which these actors draw consent, support, and recruits.[2]

Narrative competition has heightened over the past two decades due to the dawn of social media and the breakdown of shared consensus-forming institutions.[3] Nowadays, amidst every event or situation, humans around the globe find themselves amidst narrative cacophony as different actors and groups "narrate" events or situations. Amidst this melee of discourse, those without firsthand knowledge become the target of narrative competition by other actors and groups—most of whom do not have firsthand knowledge either—making the case that the event or situation matches certain pre-set master narratives about how the world works, along with certain topic narratives about different actors and issues at play. Narrative competitiveness in this context amounts to the ability to create linkages between pieces of information more compelling that serve the purpose of advancing narratives for strategic benefit.

While some participants in narrative competition believe in the linkages they assert, narrative competitions can and often are co-opted by hostile actors attempting to spread and amplify certain interpretations of events purely because these play to their interests. Such actors exploit the associations created by narratives as influential psychological heuristics that reduce the individual ability and will to orient themselves cognitively. Essentially, they use stories to promote a feeling among individuals that they instantly understand events and contexts without having to research their unique features. Narrative deployed in this way has been called "adversarial narrative," or "narrative warfare" when conducted by organized or state interests against other states.[4] States and other organized entities conduct narrative warfare through black operations deploying fictionalized or decontextualized stories, fake accounts, bot networks to heighten the predominance of a desired narrative, and trolls to intimidate and ultimately silence actors advancing competing narratives.[5]

Though narrative warfare has powerful political and military effects on populations, democratic militaries have been hampered by valid norms as well as legacy structures from developing narrative warfare competencies relative to autocratic states and militaries. As fictionalizing events and inventing fake actors

---

[2] Thomas Elkjer Nissen, "Narrative Led Operations," *Militært Tidsskrift* (Danish Military. Journal) 141, no. 4 (January 2013): 67-77.

[3] Brad Allenby and Joel Garreau, eds., *Weaponized Narrative: The New Battlespace* (Washington, D.C.: Weaponized Narrative Initiative, Center on the Future of War, March 21, 2017), https://weaponizednarrative.asu.edu/file/272/download?token=kV886rEe.

[4] Paul Cobaugh, "A Five-Point Strategy to Oppose Russian Narrative Warfare," *medium.com*, April 25, 2018, https://medium.com/@paulcobaugh/a-five-point-strategy-to-oppose-russian-narrative-warfare-56e0006aab2a.

[5] Anthony Seaboyer, "Social Media Messaging for Influence in National Security," Technical Report DRDC-RDDC-2016-C257 (Toronto, ON: Toronto Research Centre, Defence Research and Development Canada, January 1, 2016), https://cradpdf.drdc-rddc.gc.ca/PDFS/unc250/p804652_A1b.pdf.

and media sources to disseminate the spurious accounts of them is, and should be, ethically off the table for democracies—at least in most cases—the outstanding question remains, what can democratic militaries do to compete effectively and legitimately in the high stakes narrative battlefield?

Building Resilience to Narrative Manipulation

Clearly, the best-case scenario is for democratic governments to build resilience among audiences to disinformation and other forms of narrative manipulation. Education about disinformation and instilling wider media literacy is an important facet of citizenship that militaries, along with other governmental agencies, should encourage both domestically and internationally. Numerous resources have been developed to assist in this regard.[6] However, given the intense psychological power and emotional appeal of stories and narratives, educating the public to recognize adversarial narrative practices and motivating them to resist their influence is likely to achieve slow—possibly generational—gains at best.[7] Accordingly, the authors believe militaries need to investigate and refine other means of enhancing their competitiveness in the narrative environment.

Enhancing Narrative Competitiveness

A fundamental improvement militaries could make that would give them greater effectiveness in narrative competition would be to cultivate their ability to tell their stories in more impactful ways. Many military actions and activities have inherent features that could permit them to be turned into appealing stories, including high dramatic and value-driven stakes, exotic settings, and often also brave or ingenious individuals. However, military organizations neglect to emphasize these features of their activities in their communications. Understandably, they maintain an objective and impersonal style of information delivery to foster a sense of transparency and avoid imputations of propaganda.[8,9]

Yet research suggests institutional trustworthiness is also grounded in other values such as benevolence and integrity, which may be easier to communicate

---

6 See Cherilyn Ireton and Julie Posetti, eds. (UNESCO), *Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training* (UNESCO, 2018).

7 Christoph Eisemann and Christoph Pimmer, "Educational Approaches to Address Fake News: Preliminary Insights from a Systematic Review," in Proceedings of the IADIS International Conference Cognition and Exploratory Learning in the Digital Age 2020, ed. Demetrios G. Sampson, Dirk Ifenthaler and Pedro Isaías (Lisbon, November 2020), https://www.researchgate.net/publication/344217167_Educational_approaches_to_address_fake_news_preliminary_insights_from_a_systematic_review.

8 Government of Canada, Treasury Board Secretariat, "Policy on Communications and Federal Identity," 2019, https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=30683.

9 Robert T. Davis II, "The US Army and the Media in the 20th Century," Occasional Paper 31 (Fort Leavenworth, Kansas: Combat Studies Institute Press, US Army Combined Arms Center, 2009), https://apps.dtic.mil/sti/pdfs/AD1118120.pdf.

through more emotive communicative approaches.[10] Further, purely neutral styles of communication are unlikely to stand out in the narrative melee of social media, leaving a vacuum for other, less principled actors to take up influential roles.

In short, if militaries want their accounts of events to take up more role in the social media landscape of narratives and assume higher levels of trustworthiness among audiences, they may need to update their communication approach. One proposed way to do so is to re-envision themselves from being sources of information, sending out fact-based messaging for consumption by rational actors, to storytellers supplying stories that can appeal on different levels to different types of audiences.[11]

Narrative Intelligence

The first requirement for developing more impactive narratives is to develop a narrative intelligence capability. Stories do not exist in a vacuum; one can enter into, update, and adapt stories selected amongst larger webs, thus changing cultural discourses and minds along the way. Accordingly, a distinctly narrative intelligence would be oriented to identifying and understanding the types of narrative already favored by key audiences, along with stories on military-relevant themes circulating at any given time among those audiences. Narrative intelligence is a close cousin of the cultural intelligence militaries have long been called on to assemble to win the "hearts and minds" of audiences[12] and would help ensure stories told by militaries have a chance of resonating with audience concerns, interests, and tastes.

The good news is that AI-driven tools are in development that will be able to detect and cluster narratives on traditional and social media according to common threads amongst them, along with sentiments they feature and the social networks they are popular amongst.[13] By structuring the big data of the public

[10] Roger C. Mayer, James H. Davis, and F. David Schoorman, "An Integrative Model of Organizational Trust," *The Academy of Management Review* 20, no. 3 (1995): 709-734, https://doi.org/10.2307/258792.

[11] Jan K. Hanska, "Narrative Approach to the Art of War and Military Studies: Narratology as Military Science Research Paradigm," *Journal of Military Studies* 5, no. 1 (June 2014): 1-19, https://doi.org/10.1515/jms-2016-0186.

[12] Christopher Paul, Colin P. Clarke, Beth Grill, and Molly Dunigan, *Paths to Victory: Lessons from Modern Insurgencies* (Santa Monica, CA: RAND Corporation, 2013), https://www.rand.org/pubs/research_reports/RR291z1.html.

[13] Bruce Forrester, Shadi Ghahar-Khosravi, and Suzanne Waldman, "Machine Learning-Enabled Narrative Search in the Information Environment," MP-SAS-OCS-ORA-2021-AIML-02-4, 15th NATO Operations Research and Analysis Conference, October 18-20, 2021 (Paris: NATO Science and Technology Organization, October 2021), https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-OCS-ORA-2021/MP-SAS-OCS-ORA-2021-AIML-02-4.pdf.

information environment, such tools can help militaries makes sense of narrative-lay-of-the-land and how they can effectively engage in it.[14] We propose using a pyramid-like narrative model for processing data on stories circulating among groups to facilitate a broader understanding of the narratives they favor on various topics and underlying master narratives that structure their perspectives.

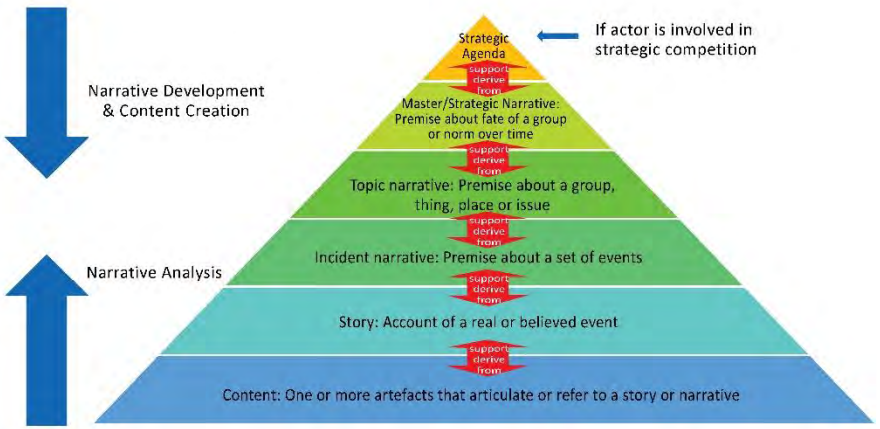

Figure 1: Narrative Analysis and Design Model.

Narrative Design

The narrative model can also help curate and design content that can speak to—and sometimes nudge—audience perspectives in ways that can create common ground. The hardest part of communicating via narrative is designing content that will meaningfully convey favored narratives to specific real audiences. Narratives take the form of claims either about topics ("vaccines are more harmful than the diseases they prevent") or events ("COVID-19 was made in a lab"). Audiences are typically induced to adopt narratives not by logically encountering them in the form of claims but by repeatedly encountering stories that testify to them, e.g., testimonies of people getting sick from vaccines or supposed witness accounts of cover-ups at the imputed laboratory. The most effective narrative communicators thus primarily message not narratives in themselves but stories and actions that testify to the validity of those narratives.

[14] Suzanne Waldman et al., "Enabling Narrative Sensemaking in the Information Environment: An Evaluation of Commercially-Available Media and Social Media Monitoring and Analysis Tools for Enabling Situational Awareness of Military-Relevant Narratives in the Information Environment," Technical Report DRDC-RDDC-2021-R093 (Toronto, ON: Toronto Research Centre, Defence Research and Development Canada, April 2021).

Given that many militaries are already committed to the idea of strategic narrative, they are in an excellent position to excel at this type of narrative communication if they have the will and skills to do so. It is a Strategic Communications commonplace that military operations should be guided and justified through the use of strategic narrative.[15] Yet militaries need to put much more thought into how strategic narratives can be effectively communicated to audiences through telling and enacting stories that would make these narratives meaningful and convincing. We propose three main interconnected vehicles for militaries to achieve narrative effects, namely (1) by telling stories about relevant situations that interpret them via narratives; (2) by initiating actions that bear out narratives; and (3) by initiating messaging about their actions that narrates how these actions are congruous with them.

Figure 2: The Three Modes of Operationalizing Narrative Effects.

A narrative-driven strategy or operation should be designed to cycle seamlessly among these vehicles as it uses its communication capabilities to provide stories to audiences demonstrating what it sees is happening along with the solution it has identified, faithfully embodying that solution in kinetic and other types of action, and then using additional detailed stories to explain to audiences how those actions created the desired results.

Moving on to how to craft the stories that are a key part of this cycle, theorists of storytelling ('narratology') tell us that impactive stories are not simply

[15] NATO MC 0628 (Final), "NATO Military Policy on Strategic Communications," July 26, 2017.

accounts of events.[16] Rather, good stories demonstrate at least four features, abbreviated as PAIV: *Plot* locating the phase of the narrative in play and anticipating where it is going—are we in the calm before the storm or the darkness before the dawn; *Archetypes* consisting of formulaic and structurally opposed characters involved in the action; *Imagery* that makes situations tangible to audiences; and *Values* being tangibly reinforced or defended. The good news is that military stories tend to be dramatic with high-value stakes and inherently offer a range of PAIV features. Still, storytelling and story-crafting are needed to bring these features out more strongly by turning military events into gripping stories with compelling characters and natural plots with ups and downs and twists and turns.

When not involved directly in action, good plotting means moving beyond the static representations of military gear that so often predominate in military social media. Instead, military messaging should continuously locate where they see themselves in the larger "plot" of their strategic agendas. How are service members protecting or advancing what is valued, on behalf of whom, and to what end? Literary theory tells us that two core plots that underpin action are comedies and romances or, respectively, preservation of a basically good condition despite bumps and transformation of a basically bad condition into a good one through radical purging.[17] The type of operations a military is engaged in can be compellingly communicated by drawing on the formulaic features of these types of plots. Comedies, for their part, tend to employ relatable characters, clever teams and schemes, and humiliating dismissals of ill-doers, whereas romances tend to feature more ambivalent heroes, uncertain and perilous quests and encounters, and dramatic and violent reversals.

Stories also need characters, which could be more determinately created with text and images showing individual commanders and force members as archetypal figures engaged in compelling military actions for meaningful purposes. Individually naming these featured members is optional but would be helpful for attracting the kinds of "parasocial relationships" among audience members and key to sparking their involvement and loyalty.[18] As discussed, especially relatable or attractive individuals make excellent comic heroes, whereas exceptionally perseverant or intellectual members stand out as romantic figures. Casting negative archetypes is likely to be a stickier point, as there is understandable political reticence about naming villains in under-the-threshold circumstances. Still, for

[16] Mark A. Finlayson and Steven R. Corman, "The Military Interest in Narrative," *Sprache und Datenverarbeitung* 37, no. 1-2 (2013): 173-191, https://users.cs.fiu.edu/~markaf/doc/j2.finlayson.2013.sdv.37.173_archival.pdf.

[17] Northrop Frye, *Anatomy of Criticism: Four Essays* (Princeton University Press, 1957), https://doi.org/10.2307/j.ctvct0080.

[18] Riva Tukachinsky, Nathan Walter, and Camille J. Saucier, "Antecedents and Effects of Parasocial Relationships: A Meta-Analysis," *Journal of Communication* 70, no. 6 (December 2020): 868-894, https://doi.org/10.1093/joc/jqaa034.

the purpose of creating drama, the presence of threatening actors justifying military actions should be hinted at, at the very least.

All these characteristics are illustrated in the following picture, aptly found in the "Great Military Pics" Twitter handle. This picture implicitly encapsulates P-plot of menace being held off, A-archetype of a protector defending innocents, I-imagery of munitions being used to hold the line "between a rock and a hard place," and V-values of security and freedom from terror. While not every military tweet can be this dramatic, this one offers an example of the kind of *in media res* action and evocative contrasts to which military storytelling should aspire.

Figure 3: Posting by "Great Military Pics" Twitter account, 2013 (source unknown).

Case: Sviatlana Tsikhanouskaya

As the above picture suggests, the best storytelling in the political-military milieu comes from making the most of circumstances that arise by broadcasting exciting as well as relatable events, demonstrating how these events are connected to the values, and giving platforms to interesting and evocative real-life individuals with the potential of emerging as characters capable of drawing audiences into causes.

A contemporary example of a captivating and high-stakes political story with strong characterization and plot was that of Belarusian leader-in-exile Sviatlana Tsikhanouskaya. In 2020, Tsikhanouskaya ran for President "out of love"—after her husband was arrested for planning to do so—to free him from prison. Losing the official vote, Tsikhanouskaya fled to Lithuania to rally support as Belarus's legitimate leader-in-exile. She was taken on as a cause celebre by European and

allied circles, perhaps in part because her story revived a classic comedic (which is not the same as funny) plot structure going back to the Roman period, in which courageous young people struggle against decadent old tyrants to build a world in which they can love freely.

Figure 4: Tweet of Sviatlana Tsikhanouskaya, August 7.

This story also demonstrates how impactive stories are fuelled by the actions of classic characters – that is, of "archetypes." The attractive Tsikhanouskaya plays her part well as a relatable, enterprising comic heroine, expressing herself on social media using plain, emotive, value-driven language. In contrast, the incumbent President Lukashenko is easy to peg as a corrupt but blundering tyrant, yet another archetypal character of Roman comedy.[19]

True to form, a review of the social media data suggests that most of the drama in the story has been generated through absurd overreaches by the Lukashenko government. These included bringing down an international jet to arrest yet another young activist couple and having Olympics coaches pressures a female sprinter to return home to face consequences for social media candour, leading to her defection at the airport where she cleverly employed Telegram and Google Translate. Social media data also shows that these actions did not purely speak entirely for themselves, but were ably amplified by Sviatlana Tsikhanouskaya's campaign team to reach international notoriety.

[19] Frye, *Anatomy of Criticism*.

Figure 5: Search Results from Predata Platform Showing Attention to Sviatlana Tsikhanouskaya Peaking in 2021, the Day the Lukashenko Regime Brought Down RyanAir Flight 4978.

While we cannot be sure if affairs in Belarus will achieve the traditional comic outcome—an inclusive society where young people can love freely [20]—the story is being skilfully told to make important strategic audiences around the world pull for that ending.

Conclusion

Enhancing narrative competence will require militaries to advance several interconnected capabilities. These include expertise in curating and communicating stories that incorporate a plot, characterization, and imagery and delivering through natural voices along communication paths that will encourage organic spread through key audiences.

These capabilities also include OSINT and analytic capabilities for understanding the narrative cultures of audiences in the information environment, including master narratives, favored plots, and characteristic stories that express their worldviews and aspirations. As an example, comedies such as the one being performed by Sviatlana Tsikhanouskaya tend to be favored by optimistic progressives who believe problems might solve themselves if only vested interests were cleared away. Another example of such an optimistic, progressive leader is Greta

[20] Frye, *Anatomy of Criticism*.

Thunberg, the young environmentalist who advocates for reduced influence by fossil fuel companies to facilitate wind and solar power development. Not coincidentally, Thunberg attended a rally for Tsikhanouskaya last May in Sweden – thereby spreading the cause of Belarusian resistance among her own networks. Militaries and other institutions could learn well how to harness sympathetic influencers in such an effective way.

Figure 6: Tweet of CNN Journalist Bianna Golodryga Retweeting Sviatlana Tsikhanouskaya's Senior Advisor on the Belarusian Regime's Mistreatment of Olympics Sprinter Krystsina Tsimanouskaya, August 1, 2021.

Narrative competence should also provide means to understand adversarial narratives and anticipate the inferences they may draw. In contrast with relatively light-hearted comic narratives preferred by optimists, alienated communities and individuals—the likes of revolutionaries as well as conspiracists—tend to be drawn to darker romance narratives of ambivalent heroes determined to enter "the belly of the beast" of elite power and slay their ways out.[21] One can find such violent romance narratives at the basis of many of the darker political fantasies around us occasionally acted out in the real world. Moreover—as the

[21] Frye, *Anatomy of Criticism*.

Predata results above show—one's own side's actions can be the biggest amplifiers of one's adversaries' narratives. To avoid playing into adversarial romances of ordinary folks standing up to corrupt elites, militaries and other institutions might consider spurning common bureaucratic photo ops of leaders in handshaking events and boardrooms. Instead, such institutions would do better to focus narrative attention on everyday heroes inside and outside their organizations who evince values of sincerity and benevolence, which are essential for building trust.[22]

But the narrative understanding that most needs to be internalized among military institutions is how the force as a whole is implicated in storytelling. Commanders who design operations need to understand that, increasingly, the stories that spread about their actions will impact far more people than the platforms or weaponry wielded in them. Operators need to understand that cracks in their operational narrative will inevitably be exploited by adversaries. Communicators need to understand that a keen plot, relatable characters, and plain language appeal to everyone. In contrast, postings featuring primarily gear and jargon speak to almost nobody beyond the institution itself, reinforcing cultural silos rather than paving paths beyond them for military values to be advanced. In the old-is-new era of narrative, no one is off the hook from telling stories – or from knowing the stories they are enabling others to tell about them.

Disclaimer

About the Authors

Suzanne Waldman is a Defence Scientist at Defence Research and Development Canada.
E-mail: suzanne.waldman@ecn.forces.gc.ca

Sean Havel is a co-op student at Defence Research and Development Canada.
E-mail: sean.havel@ecn.forces.gc.ca

[22] D. Harrison McKnight and Norman L. Chervany, "What is Trust? A Conceptual Analysis and an Interdisciplinary Model," in *Americas Conference on Information Systems, AMCIS 2000 Proceedings*, 382, https://aisel.aisnet.org/amcis2000/382.

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

S. Foley, C. Jackson, S. Aros & A. Baylouny
Connections QJ 21, no. 2 (2022): 123-134
https://doi.org/10.11610/Connections.21.2.09

Research Article

NATO and Intermediate Force Capabilities: Why Human Effects Matter

Shannon Foley,[1] Caitlin Jackson,[1] Susan Aros,[2] and Anne Marie Baylouny [2]

[1] *Joint Intermediate Force Capabilities Office, U.S. Department of Defense, https://jnlwp.defense.gov/*

[2] *Center for Modeling Human Behavior at the Naval Postgraduate School, https://www.nps.edu/cmhb*

Abstract: On February 24, 2022, when Russia invaded Ukraine, the international order changed as sharply and abruptly as it did on the morning of the September 11, 2001, terrorist attacks when the North Atlantic Treaty Organization (NATO) invoked Article V for the first time in NATO's history. As a result of Russia's invasion, NATO's demand for deterrence capabilities—with the hope that Article V is never again necessary to exercise—is more urgent now than at any time in the 21st century. Because lethality is absolutely necessary but not sufficient, NATO must develop and maintain capabilities that complement lethal force with intermediate force options to complete the deterrence equation across the entire competition continuum.

Intermediate Force Capabilities (IFCs) can deliver immediate value to NATO countries, providing leaders and policymakers with Non-Lethal Weapons (NLW) options that can deter enemy actions, as necessary, below the level of lethal combat operations. IFCs, a term introduced into the U.S. Department of Defense in 2020 to define capabilities that bridge the gap between presence and lethal effects, encompass NLWs as well as other additional capabilities and technologies that have utility below the level of armed conflict.

Keywords: intermediate force capabilities, non-lethal weapons, simulation, agent-based, modeling, security forces, gray zone.

Introduction

On February 24, 2022, when Russia invaded Ukraine, the international order was impacted sharply and abruptly. Russia's invasion put the North American Treaty Organization (NATO) on center stage. As a contribution to international security, NATO's deterrence capabilities take many forms. From nuclear weapons to cyberattacks, to be effective, deterrence must be scalable across a conflict spectrum that includes non-kinetic actions. Because lethality is certainly necessary but not sufficient, NATO must develop and maintain capabilities that complement lethal force with intermediate force options. Intermediate capabilities complete the deterrence equation across the entire competition continuum.

Both NATO's 2030 Strategic Concept and responses following the Russia-Ukraine war envisage deterrence measures that can be scalable across the spectrum of conflict.[1] Often called a competition continuum, the "gray zone" refers to aspects of strategic and operational campaigning that are below the level of a lethal armed conflict between opposing and irreconcilable wills. Gray zone warfare, also called hybrid warfare, includes aspects of irregular warfare.

In addition to gray zone warfare, there are also phases of political conflict other than lethal dominance. Lethal domination is not the only phase of warfare. It also involves shaping the upcoming conflict, deterrence, initiative seizing, stabilization, and the enablement of civil authority. Lethal weapons are singularly insufficient to achieve the goals of these five other phases, especially in this modern age when political conflicts are held in the public eye.[2] Intermediate Force Capabilities (IFCs) can deliver immediate value to NATO countries, providing leaders and policymakers with Non-Lethal Weapons (NLW) options that can influence enemy actions, as necessary, below the level of lethal combat operations.

Intermediate Force Capabilities

IFCs, a term introduced into the U.S. Department of Defense (DoD) in 2020 to define capabilities that fill the span from presence and lethal effects, encompass NLWs as well as other additional capabilities and technologies that have utility below the level of armed conflict. IFCs include weapons, devices, and munitions used to slow, stop, and/or divert an adversary's actions.[3] They bridge the tactical

---

1 Susan LeVine, "Beyond Bean Bags and Rubber Bullets: Intermediate Force Capabilities Across the Competition Continuum," *Joint Forces Quarterly*, no. 100 (2021): 19-24, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2497112/beyond-bean-bags-and-rubber-bullets-intermediate-force-capabilities-across-the/.

2 Krista Romita Grocholski et al., *How to Effectively Assess the Impact of Non-Lethal Weapons as Intermediate Force Capabilities*, Research Report RRA654-1 (Santa Monica, CA: RAND Corporation, 2022), https://doi.org/10.7249/RRA654-1.

3 Wendell B. Leimbach Jr., "DoD Intermediate Force Capabilities: Bringing the Fight to the Gray Zone," PowerPoint presentation available upon request, Joint Intermediate Force Capabilities Office.

and strategic gaps between presence and lethal effects while minimizing casualties and collateral damage. IFCs include legacy law enforcement NLWs and leap-ahead technology, now available to provide a new generation of capabilities with extended ranges and durations of effects against personnel and materiel to support missions across the competition continuum framework of the National Defense Strategy. IFCs provide a range of scalable options that offer an appropriate level of force when it is desired to minimize risk to innocent civilians or the surrounding environment.[4]

IFCs benefit the Joint Force and NATO operations. IFCs support efforts to partner, persist and operate forward by giving Commanders effective and tailorable counters to gray zone tactics. IFCs' discriminate and relatively reversible effects, which are neither likely nor intended to cause death or serious injury, also reduce the risk of escalating a conflict and conserve valuable lethal weapons for use elsewhere.[5] IFCs complement lethal force by helping service members to discern uncertain situations, isolate targets, enhance force protection, and mitigate the risk of collateral damage or casualties. IFCs afford service members engaged in irregular warfare within the ground, maritime, and air domains more deter/defeat options. Overall, these adaptive measures enhance the Joint Force's adaptability and capability to survive asymmetric, unpredictable events. At a minimum, IFCs can provide a low-risk, non-lethal means of supporting our partner-building capacity with the host nation and allied security forces.[6]

Because IFCs can offer discriminate and reversible effects without causing unnecessary destruction or loss of life, they can support NATO's strategic objectives without unintentionally initiating, escalating, or prolonging hostilities. IFCs strongly align with the NATO 2030 Strategic Concept and represent a suite of capabilities that respond effectively to the demand signals for new risk management protocols following Russia's unprovoked attack on Ukraine. IFCs will enable NATO's senior leaders to expand decision time and space, providing options to validate that a perceived hostile action is, in fact, hostile while simultaneously bridging the gap from presence to lethal effects without reducing the overall force design of lethality.

Non-Lethal Weapons

As a subset of IFCs, NLWs provide operating forces needed capabilities to clear personnel, control group movements, target selected individuals, and secure without destroying. NLWs are designed and primarily employed to incapacitate personnel or materiel immediately, minimizing fatalities, significant injuries to personnel, and collateral damage. DoD Directive 3000.3E establishes that NLWs

[4] Leimbach Jr., "DoD Intermediate Force Capabilities: Bringing the Fight to the Gray Zone," 3.

[5] Stacia A. Hylton, "Use of Force," U.S. Marshals Service Policy Directives, accessed July 23, 2019, https://cops.usdoj.gov/pdf/use-of-force.pdf.

[6] Hylton, "Use of Force," 3.

aim to achieve effects that "minimize the probability of producing fatalities, significant or permanent injuries" yet also are not required to "eliminate risk of those actions entirely." While NLWs are not required to have a zero probability of producing fatalities or permanent injuries[7], NLW developers are required to characterize (in requirements as well as test and evaluation) both injury potential and weapon effectiveness against the target.[8] When developing new NLW systems or deciding to employ an existing one, knowledge of the potential of the system to cause unintended injury is an important component. Like other weapon systems, NLWs must also establish reliability and effectiveness metrics to determine the extent to which the intended effect is achievable. For NLW, the human effects aspects of effectiveness and injury potential are frequently the most important constraints bounding the developmental trade space.

Human Effects and Reversibility

Human effects are the physical impact on, or behavioral response of, a human resulting from a stimulus or a set of stimuli. The human effects characterization process ensures the development and fielding of non-lethal weapons capabilities that meet the escalation of force needs of Warfighters and enable confidence in the effectiveness and understanding of the risks. Additionally, human effects knowledge can support operational commanders by informing the development of non-lethal weapons tactics, techniques, procedures (TTPs), and training.[9]

U.S. DoD Instruction (DoDI) 3200.19 defines the policies, responsibilities, and procedures for the characterization of the human effects of non-lethal technologies and systems. Human effects characterization is the formal process for describing the compendium of physiological- and behavioral-effects knowledge associated with a given NLW. The Instruction establishes the risk of significant injury (RSI) as the metric used to describe the reversibility of NLW effects as it relates to humans. RSI is specifically the likelihood, or probability, of a NLW directly causing injuries that are permanent, including death, or requiring greater than Limited First Responder Capability (LFRC) (including self-aid, buddy-aid, and combat lifesaver skills) in order not to be permanent. A permanent injury is formally defined in DoDI 3200.19 as "physical damage to a person that permanently impairs physiological function and restricts the employment or other activities of that person for the rest of his or her life." When injuries are not permanent and do not cause death, the LFRC distinction is used to draw the line between

[7] Department of Defense Directive 3000.3, "DoD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy," April 25, 2013, Incorporating Change 2, August 31, 2018, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300003p.pdf?ver=2018-10-24-112944-467.

[8] Department of Defense Instruction (DoDI) 3200.19, "Non-Lethal Weapons (NLW) Human Effects Characterization," May 17, 2012, Incorporating Change 1, September 13, 2017, https://irp.fas.org/doddir/dod/i3200_19.pdf.

[9] DoDI 3200.19, "Non-Lethal Weapons (NLW) Human Effects Characterization," 8.

the categories of "significant" and "not significant." An injury that requires greater than LFRC in order not to be permanent is considered significant.[10]

Furthermore, DoDI 3200.19 requires that for any non-lethal technology or system, RSI must be identified by the combat developer (the command or agency that formulates doctrine, concepts, organization, material requirements, and objectives; representing the user community role in the material acquisition process).[11] The purpose of RSI is to assist in materiel development and provide Commanders with the level of risk associated with the intended use of the NLW. Warfighters, through combat developers, determine this risk based on a concept of operations for a non-lethal capability. This determination is deliberative, driven by the intended mission use, and informed by human effects experts. RSI is, therefore, the build to DoD specification for non-lethality. Describing the trade space between the risk of significant injury and effectiveness is central to NLWs' development.

Capabilities for Commanders

NLWs provide Commanders options for escalation and de-escalation of force, making them more effective in situations in typical recent operations. The characterization of human effects for NLW has become more defined and advanced, building on knowledge and lessons learned. Today, it is guiding NLW development in its earliest stages, focused first and foremost on warfighter needs as expressed by combat developers. Thus, continually improving the human effects characterization process is key to improving NLWs and IFCs.

Combatant Commands use defined Standing Rules of Engagement (ROE) and interpret them for their unique application. Task Force Commanders take Standing ROEs (as interpreted) and apply them in a way that is permissibly more conservative but not more lenient than the Standing ROEs. The Joint Intermediate Force Capabilities Office (JIFCO) maintains Combatant Liaison Officers at each of the geographic Combatant Commands to facilitate this process. Additionally, a better understanding of relationships between IFCs, ROE, and effectiveness is needed. It is important to emphasize that the physiological effects that NLW stimuli produce on targeted personnel are not the end goal of NLWs. Commanders require an understanding of how to employ a suite of NLWs to effect predictable behavioral changes in these targets. To do this requires a mapping of physiological effects to behavioral outcomes.

Behavioral Effects

The nature of NLWs is to influence human behavior. NLWs tend to correspond to two major categories: counter-personnel and counter-materiel weapon systems. Counter-personnel NLWs aim to incapacitate, deter, distract, suppress, or

[10] DoDI 3200.19, "Non-Lethal Weapons (NLW) Human Effects Characterization," 8.

[11] DoDI 3200.19, "Non-Lethal Weapons (NLW) Human Effects Characterization," 8.

move a human-targeted individual. This can be done through various means: sound and light, pressure waves, directed energy, malodorants, electro-muscular stimulation, and more. In these cases, a physical stimulus is delivered, a physiological response is caused, and ultimately a change in behavior is the result. For example, when a flashbang grenade is used, a loud sound, a bright light, and a pressure wave impact the human target; the person feels the physiological effects and has some cognitive and emotional reactions. These effects can cause the person to change their behavior. The extent that their behavior has been modified is one measure of the effectiveness of the weapon system. Behavioral effectiveness can be difficult to measure because humans can think, feel, and behave in a dynamic interaction with each other and their environment. Sometimes the focus is on measuring the physiological effect in place of the behavioral change because it is easier to measure and can offer other scientific advantages. For example, when a Human Electro-Muscular Incapacitation (HEMI) device is employed, the physiological effect of skeletal muscular incapacitation is so strong that behavioral control is no longer under the targeted human's volition. In this case, the physiological effect is a suitable effectiveness measure approximating behavioral change. For other NLWs, though, the physiological effect fails to capture the true consequence of the NLW. Additionally, NLWs are sometimes used in a scenario with multiple people or in a crowd situation. Whether the scenario involves one individual, multiple individuals, or a crowd, understanding human behavior is central to understanding NLW system effectiveness.

Beyond system effectiveness, understanding and ultimately being able to predict human behavior is important for better tactical and mission effectiveness. The continuum for applying knowledge of human behavior is broad. How we employ systems is just as important as the technology itself. This includes the full range of systems engineering (e.g., was the light beam the right color to be a warning?), but also, more broadly TTPs (e.g., were the tactics of employing the system effective?), RoE (Rules of Engagement – e.g., did the way we engaged allow for effective system employment?), cultural considerations (e.g., does the local culture influence the system's potential effectiveness?), and foundational psychology (e.g., did the extreme heat contribute to escalated tensions?). When the focus is on behavioral change and effective outcomes, then the full range of contributing factors needs to be considered. Likewise, a full range of creative and innovative solutions is possible. Often these innovative solutions offer a parsimonious solution as well. For example, if we know that extreme heat can make tempers flare, then perhaps tents and fans at a checkpoint or food distribution event would prevent aggressive escalation. Or, from basic psychology, if cameras are readily emplaced with signage highlighting their presence, perhaps aggressive escalation is prevented by reminding people of their personal identity and place in society (as well as knowing they could be identified and held accountable for their actions). Something as simple as a sign that clearly states a message can be extremely effective at very little cost – in this case, the challenge is not high-tech or expensive but having the awareness and foresight to know that such a

sign is needed. When we focus on the goal of changed behavior, a myriad of solutions presents themselves.

What We Know About Crowds

We now know that many old ideas about crowds do not correspond to the data.[12] Crowds are not homogenous, participants are not identical in motivation or behavior, and individuals neither lose their individuality nor benefit from some universal sense of anonymity. Rather, crowds are composed of small groups of people, "companion clusters," who arrive, remain, and leave together.[13] Nor are crowds uniquely distinguished by violence.[14] Among the myriad crowds that gather every day for concerts, celebrations, or socializing, very few end in violence. Crowd participants can be influenced by or "catch" the emotions and behavior of others in the crowd, but this effect is conditional. The social identification of the individual determines this effect along with proximity.[15]

Research has also determined that security forces' loss of legitimacy is often caused by a perceived mismatch between the severity level of a deployed weapon and the hostility level of those impacted.[16] The resulting fear and anger from this and a few other processes can have dramatic effects on crowd behavior. Instead of losing their identities, crowd participants under these dynamics join into shared or new social identities that can pass emotions and create particular crowd dynamics.[17] Threat and fear are two central emotions that have been linked to the outbreak of violence and can knit together disparate groups

---

[12] Clark McPhail, *The Myth of the Madding Crowd*, 1st Edition (Routledge, September 2017).

[13] Benjamin Cornwell, "Bonded Fatalities: Relational and Ecological Dimensions of a Fire Evacuation," *The Sociological Quarterly* 44, no. 4 (September 1, 2003): 617-638, https://doi.org/10.1111/j.1533-8525.2003.tb00528.x.

[14] John M. Kenny et al., "Crowd Behavior, Crowd Control, and the Use of Non-Lethal Weapons," Human Effects Advisory Panel Report of Findings (University Park, PA: Institute for Non-Lethal Defense Technologies Applied Research Laboratory, The Pennsylvania State University, January 1, 2001, https://live-cpop.ws.asu.edu/sites/default/files/problems/spectator_violence/PDFs/HEAP.pdf

[15] Fergus G. Neville et al., "Self-Categorization as a Basis of Behavioural Mimicry: Experiments in The Hive," *PLOS ONE* 15, no. 10 (October 30, 2020): e0241227, https://doi.org/10.1371/journal.pone.0241227; Clifford Stott, John Drury, and Steve Reicher, "On the Role of a Social Identity Analysis in Articulating Structure and Collective Action: The 2011 Riots in Tottenham and Hackney," *The British Journal of Criminology* 57, no. 4 (July 2017): 964-981, https://doi.org/10.1093/bjc/azw036.

[16] Clifford Stott et al., "Patterns of 'Disorder' During the 2019 Protests in Hong Kong: Policing, Social Identity, Intergroup Dynamics, and Radicalization," *Policing: A Journal of Policy and Practice* 14, no. 4 (December 1, 2020): 814-835, https://doi.org/10.1093/police/paaa073.

[17] Susan Aros, Anne Marie Baylouny, Deborah E. Gibbons, and Mary McDonald, "Toward Better Management of Potentially Hostile Crowds," in *2021 Winter Simulation Conference (WSC)*, Phoenix, AZ, December 12-15, 2021, 1-12, https://doi.org/10.1109/WSC52266.2021.9715452.

in the crowd, generating a larger group with a stronger sense of self-efficacy. This larger group can pursue confrontational courses of action bolstered by numbers.[18] However, these individuals do not lose their individuality and retain agency: some can and do leave the group if it does not match their view of the social identity. Therefore, while we can model it as an aggregate group, we must maintain the possibility of departure from group acts.

Behavioral Effects Science and Technology

The JIFCO has conducted ongoing research on the effects of IFCs on human behavior. Past and ongoing research is focused on two salient aspects: how human behavior can generally be influenced by IFCs, and the effects that each specific type of IFC will have on human behavior when employed. The elements of IFC and NLWs' human effects research involve identifying how human behavior can be influenced by IFCs, and the effects that each specific type of IFC will have on human behavior when employed relative to the goals of the mission.

In recent years the JIFCO has sponsored the development of an agent-based modeling capability (Workbench for refining Rules of Engagement against Crowd Hostiles – WRENCH) for these specific purposes. Simulation and experimentation using WRENCH will allow exploration of the possible NLW and ROE combinations to inform future NLW policy.

The Future of NLW Behavioral Effectiveness

Between systems engineering applications, tactical effectiveness, and mission effectiveness, understanding human behavior and being able to apply that knowledge is key. The objective of establishing a more robust agent-based crowd modeling simulation is to better understand the consequences of the use of NLW in crowd behavior. Responses of crowds to the use of IFCs are complex and difficult to predict; aspects of identity and group dynamics influence crowd response often unexpectedly. Agent-based crowd modeling and simulation has some science and technology challenges to work through. For example, aggregate behavior is a result of non-linear feedback processes, and crowds define a complex behavior system continuously evolving and operating at multiple scales simultaneously. It is essential to understand the motivating drivers of individual and social identity group behavior and how they change. How realistically the model represents the realities of things, such as identities, emotions, and social regularities, will determine its usefulness.

---

[18] Randall Collins, "The Micro-Sociology of Violence," *British Journal of Sociology* 60, no. 3 (2009): 566-576, https://doi.org/10.1111/j.1468-4446.2009.01256.x; Anne Nassauer, "Situational Dynamics and the Emergence of Violence in Protests," *Psychology of Violence* 8, no. 3 (2018): 293-304, https://doi.org/10.1037/vio0000176; Norbert L. Kerr, "Illusions of Efficacy: The Effects of Group Size on Perceived Efficacy in Social Dilemmas," *Journal of Experimental Social Psychology* 25, no. 4 (July 1, 1989): 287-313, https://doi.org/10.1016/0022-1031(89)90024-3.

WRENCH models key physical, psychological, and social aspects of individuals and social identity groups that comprise a population in which crowds may form. Individuals have a dynamic interaction with their environment. When something changes, they can have immediate flashes of emotion. Those emotions can result in heightened action readiness which may or may not result in an immediate behavioral response since action readiness is a precursor for behavior but is not a determinant.[19] Social contagion, a subtle influence of others in physical proximity, can also affect emotions. In addition to immediate emotional responses to an experience, emotion is known to be affected by cognitive interpretation of that experience. As discussed above, interpretations of actions of forces as being appropriate or excessive can affect fear and anger and contribute to changes in beliefs about the legitimacy of the forces. These emotional and cognitive processes heavily influence hostility levels. Many other factors come into play in driving behavior, such as the physical needs and injury levels of the individual, their personal goals or objectives, their sense of personal potency, and their social needs.

Social identities and social identity groups (SIGs) further influence crowd behavior. Individuals have social identities and may choose to join with others who have common identity(s) into a SIG that stays together and influences each other. In some cases, family membership will define a SIG, and other SIGs will form based on other social identities. These groups are not merely a sum of their component individuals, nor do they subsume the individuals into a single cohesive group. When a group forms, the individuals within retain their ability to react to the environment individually while also being influenced by the group. For modeling purposes, when a SIG first forms, it will initially take on the aggregate characteristics of the individual members, but as the members continue to react and adjust to their environment over time, the SIG changes more slowly; changes in individual members of a group do not instantly alter the group as a whole. The result is dynamic SIGs and individuals. Generally, people in a group will tend to stay in a group, but if an individual changes their objectives to the point where their objective, emotions, or beliefs differ drastically enough from the group, they may leave the group. Crowds demonstrate such dynamic changes as people and companion groups leave while others join. There are different motivators to join with others, such as shared objectives, fear, or the desire to protect someone. And just like individuals can group together, smaller SIGs can join with other smaller SIGs to create much larger groups while still retaining their own agency.

Within WRENCH, a security force interacts with the population. If a potentially hostile crowd forms, the force members will use IFCs according to the specified ROEs to manage the crowd, with required lethal oversight. Within WRENCH, the ROEs also include some information on TTPs. There are varying types of IFCs that can be issued to the force members and a variety of ROEs that can be used.

[19] Nico H. Frijda, Peter Kuipers, and Elisabeth Ter Schure, "Relations among Emotion, Appraisal, and Emotional Action Readiness," *Journal of Personality and Social Psychology* 57, no. 2 (1989): 212-228, https://doi.org/10.1037/0022-3514.57.2.212.

Custom ROEs can also be defined. This allows the testing to explore the effects of a variety of IFCs, alone or in combination, under different ROEs. Different force configurations can also be specified, along with differing stances toward the population.

Since different types of crowd characteristics will change the expected crowd response,[20] WRENCH has functionality allowing the specification of a variety of population characteristics. These include not only population size, demographics, and initial SIG configurations but also numerous different attributes that could affect crowd response. The general stance of the population toward the forces and initial emotions, objectives, and beliefs can be configured along with other culture-specific details such as desired personal space.

The vision for the WRENCH simulation program is to gain insights into the operational and strategic implications of incorporating various NLWs into the force continuum under different ROEs. In the near term, the effects of using different TTPs for existing NLWs will be explored. Interactive engagement with WRENCH will increase understanding of the potential benefits of using different NLWs and ROEs in a variety of operational environments. Large-scale simulation and experimentation using WRENCH can help explore the possible NLW and ROE combinations and could inform future NLW policy. The JIFCO human effects team's research aims to offer demonstrative, foundational illustrations for NATO wargaming, planning, and employment of IFCs with a direct, immediate, and predictable impact.

Intermediate Force and NATO

Over the last 20 years, NATO has quietly and steadily built a strong foundation to begin the mainstreaming of intermediate forces. NATO—via the Science & Technology Organization and the Main Armaments Groups—has sponsored multiple initiatives, including a capabilities-based assessment. In addition, NATO Headquarters Emerging Security Challenges Division has supported several technology demonstrations and assessments. The NATO Industrial Advisory Group has conducted studies on non-lethal effects range extension, low-collateral damage effectors to counter small unmanned aerial systems, and the feasibility of scalable directed energy weapons from aircraft.

Under the NATO Army Armaments Group, the Joint NLW Capability Group is a permanent standing activity for standardization and related topics, including recent engagements with the NATO doctrine community on the doctrinal implications of IFCs. What is needed now—particularly in response to Russia's invasion of Ukraine, the prevalence of gray zone warfare, and NATO's enduring relevance on the world stage—is the strength of recognition by NATO and national

[20] Kathryn M. Zeitz et al., "Crowd Behavior at Mass Gatherings: A Literature Review," *Prehospital and Disaster Medicine* 24, no. 1 (January-February 2009): 32-38, https://doi.org/10.1017/s1049023x00006518.

leadership in the power of intermediate force as a complement to lethal force, making it a necessary component of NATO planning and preparedness.

Disclaimer

About the Authors

Dr. **Shannon Foley** is a human effects scientist and subject matter expert at the Joint Intermediate Force Capabilities Office (JIFCO), Quantico, VA, since 2013. She directs and manages the JIFCO's human effects R&D portfolio, the goal of which is to develop an understanding of dose-response relationships, human behavioral characterization, and create models, surrogates, and test targets to support the development, acquisition, and fielding of non-lethal weapons. Dr. Foley serves as a human effects subject matter expert on Joint and Service-led combat development, materiel development, and Department of Defense (DoD) Acquisition program integrated product teams. Supporting the DoD since 2006, she was a human systems engineer at the Naval Surface Warfare Center Dahlgren Division, and previously worked as a DoD industry partner. Dr. Foley holds a Ph.D. and M. Phil in cognitive neuroscience from The George Washington University.

Ms **Caitlin Jackson** is a human effects scientist in support of the JIFCO and Human Effects R&D portfolio. Since 2015 she has supported the JIFCO as a DoD contractor, in the past three years providing scientific analysis and program management support in the subject area of human effects. She has a BA in Biology from the University of North Carolina and MSc in Conservation Biology from the Victoria University of Wellington.

Dr. **Susan Aros** is a research assistant professor in the Naval Postgraduate School's Department of Defense Management and Director of NPS's Center for Modeling Human Behavior. Her current research focuses on modeling human behavior and identity dynamics of crowds in security contexts using agent-based simulation modeling. She received her Ph.D. in Information, Risk, and Operations Management from the University of Texas at Austin. She also holds an MEng in Operations Research and Industrial Engineering from Cornell University, an MA in Spiritual Formation and Soul Care from Biola University, and a BA in Psychology from Cornell University.
E-mail: skaros@nps.edu

Dr. **Anne Marie Baylouny** is a Professor of National Security Affairs at the Naval Postgraduate School and Director of NPS's Center for Modeling Human Behavior. She specializes in refugees, the dynamics of protest, and Middle East politics. She currently works on developing a theory-backed computer simulation for interactions between diverse types of crowds and security forces using less-lethal weapons. Baylouny received her Ph.D. in Political Science from the University of California, Berkeley, and is an affiliated scholar with the Abbasi Program in Islamic Studies at Stanford University.
E-mail: ambaylou@nps.edu

Connections: The Quarterly Journal
Submission and Style Guidelines

Connections accepts manuscripts in the range of 2,000 to 5,000 words, written in a lucid style for a target audience of informed defense and security affairs practitioners and academics. All manuscripts should be submitted to the *Connections* editorial office electronically at PfPCpublications2@marshallcenter.org or uploaded to the journal website via https://connections-qj.org. They should feature the author's name, current institutional affiliation, and a provisional title at the top of the first page, and should include footnotes where necessary. Additionally, authors should provide a manuscript abstract and keywords.

Preferred themes for future journal editions include:

- Ukraine War
- Post Conflict Management
- Countering Hybrid Warfare
- Bolstering the North Atlantic Alliance
- Competition for Resources and Its Impact on Security
- Non-State Actors in Cyber Space
- Emerging and Disruptive Technologies
- Digital Transformation and Security
- Defense Institution Building
- Reducing Corruption and Building Integrity
- Enhancing Defense Education

For questions on footnotes and references, please refer to the Chicago Manual of Style, at http://www.chicagomanualofstyle.org/tools_citationguide.html.

Unsolicited manuscripts are accepted on a rolling basis at the discretion of the PfPC Editorial Board.

NATO is faced with adversaries undertaking acts of aggression that deliberately stay below the lethal force threshold or aim to trigger a lethal response from NATO and incur costs to the Alliance such as undesired escalation, risks of collateral damage, including civilian casualties, or negative narratives. Examples of these activities range from dangerous aerial and maritime approaches, fomenting unrest and using refugees as a weapon, and even use of force short of lethal to intimidate opponents. Currently, the NATO responses are often limited to two extremes of mere presence or applying lethal force, thus ceding the initiative to the adversary. This issue contains a set of articles exploring intermediate force capabilities and how they can address current NATO dilemma when operating below the threshold of lethal force.

For all information regarding
CONNECTIONS, please contact:

Partnership for Peace – Consortium
Managing Editor – LTC Ed Clark
Gernackerstrasse 2
82467 Garmisch-Partenkirchen, Germany
Phone: +49 8821 750 2259
E-Mail: PfPCpublications2@marshallcenter.org

ISSN 1812-1098
e-ISSN 1812-2973