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.

Acknowledgment

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

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