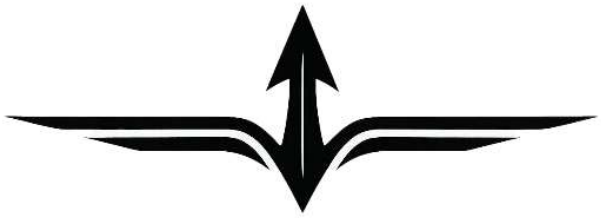
Chapter 4



Deterring Gray-Zone Warfare

Sam Mullins

"We have been handicapped…by a popular attachment to the concept of a basic difference between peace and war…and by a reluctance to recognize the realities of international relations—the perpetual rhythm of struggle, in and out of war. [2]

— George F. Kennan
U.S. Department of State *Policy Planning Memorandum No. 269*
May 4, 1948

Conceptualizing the Gray Zone

Throughout history, states have relied on a wide array of tools and techniques, ranging from disinformation and political interference

doi.org/10.71236/jphdcd10 |

to assassination and proxy warfare, to weaken adversaries and advance strategic objectives short of open war.[3] These so-called gray-zone tactics, hostile acts that "fall between the traditional war and peace duality,"[4] were visible during the Cold War but have risen to new prominence in the 21st century. Authoritarian and revisionist powers now exploit globalization and technology to expand influence, press territorial claims, and undermine the rules-based order, while avoiding more costly, direct confrontation with the United States.

China's coercion in the South China Sea and Russia's annexation of Crimea in 2014 are striking examples of this approach, visible tips of a steadily growing iceberg. In response, analysts have coined overlapping terms—*irregular warfare*, *hybrid threats*, *and malign influence*—all referring to hostile activities conducted below the threshold of conventional war yet outside accepted state behavior.[5]

Gray-zone tactics vary in form—some overtly aggressive and illegal, others more insidious or technically lawful—but share common traits: they are coercive, corrupting, covert, and/or deceptive.[6] Figure 4.1 illustrates this continuum, ranging from low-level, persistent non-kinetic activities to more aggressive, high-end coercion.[7]

By design, these tactics exploit ambiguity in attribution and intent, generating uncertainty, slowing decision-making, and enabling aggressors to secure objectives before defenders can respond. When states hesitate—fearing escalation or political costs—deterrence falters. The result, as seen in both Chinese and

Russian campaigns, is strategic gain without open conflict, incentivizing further use of gray-zone warfare.

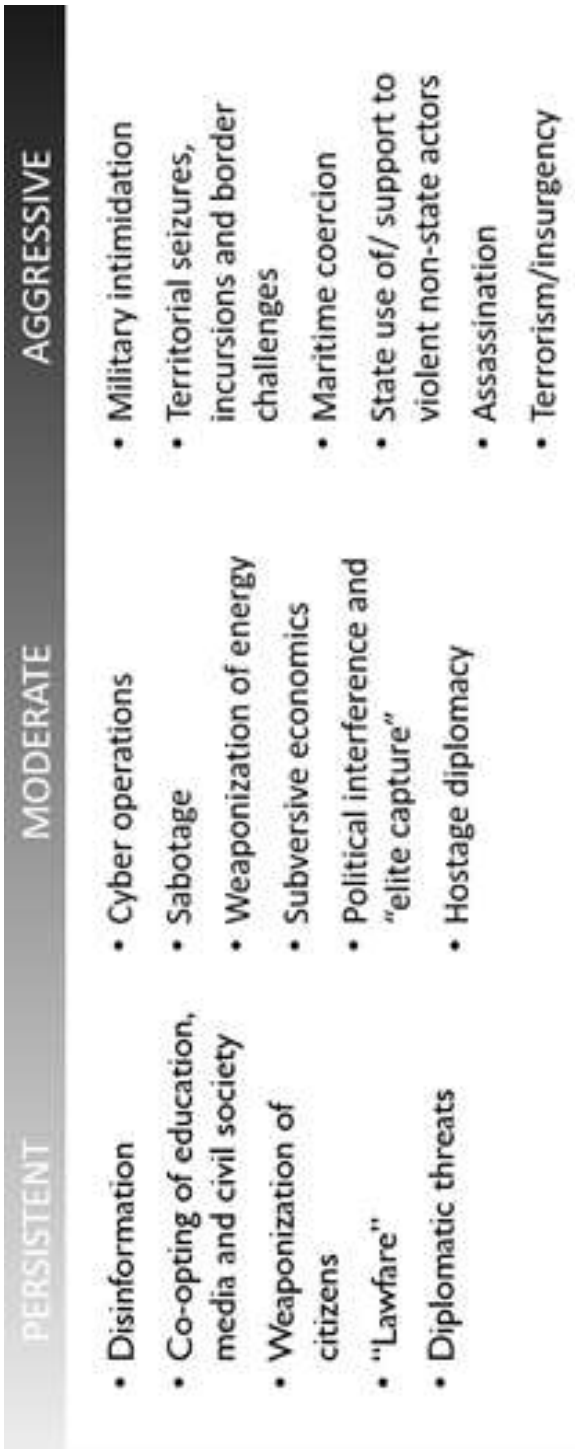


Figure 4.1: The Gray-Zone Continuum
Source: Dr. Sam Mullins' graphic, based on Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone* (2019)

For this volume, the analytical lens is deterrence. The central question, therefore, is not only what China, or other adversaries, do, but how these tactics degrade the three pillars of deterrence—capability, credibility, and communication—and how U.S. and allied actions can restore them short of war.

Winning Without Fighting

For the People's Republic of China (PRC), the concept of *winning without fighting*—competing below the threshold of war—has deep roots, dating back to Sun Tzu's *Art of War*. These ideas resurfaced with renewed intensity in the 1990s after the collapse of the Soviet Union and the Gulf War, when two senior colonels in the People's Liberation Army (PLA) published *Unrestricted Warfare*. They argued that the new principles of war were no longer limited to armed force but encompassed "all means…military and non-military…lethal and non-lethal…to compel the enemy to accept one's interests."[8]

Although not an official doctrine, this thinking reflected a growing emphasis on non-kinetic competition and the blurring of the distinction between peace and war in Chinese strategic circles. From 2001 onwards, the PLA's *Science of Military Strategy* introduced the concept of *peacetime-wartime integration*,[9] while senior leaders like General Zhang Youxia stressed that war "unfolds in all areas, at any time and space."[10] This logic underpinned the PLA's formal adoption in 2003 of the *three warfares*—public opinion, psychological, and legal warfare, which have been complemented by a steadily growing emphasis on the central

importance of information and cognition in warfare that began in the 1990s and pervades Chinese military analysis today.[11] Non-kinetic influence campaigns naturally extend beyond the PLA to encompass the United Front Work Department (UFWD), Propaganda Department, Ministry of State Security, and other organs, forming a whole-of-state enterprise.[12] The fact that the three warfares were adopted by the military, whose primary responsibility is warfighting, therefore speaks volumes to the importance of non-kinetic influence operations within the party-state as a whole.

China's understanding of warfare continued to evolve in response to the "color revolutions" that took place in the former Soviet republics and the Arab world from 2003–2014. Echoing Deng Xiaoping's views on the student uprising at Tiananmen Square in 1989,[13] the Chinese Communist Party (CCP) came to see these events not as legitimate popular protests, but as U.S.-orchestrated "wars without gunpowder"—thus reinforcing its conviction that traditional boundaries between war and peace were eroding.[14] By the late 2010s, Chinese analysts spoke of "hybrid warfare" (a term they adopted from the West) not to describe their own methods, but to highlight U.S. and Russian practices—while portraying Beijing's actions as defensive.[15]

Yet the record is clear. From coercion in the South and East China Seas and across the Taiwan Strait, to elite capture and penetration of critical infrastructure abroad, China has made gray-zone tactics a defining feature of its foreign policy. This reflects a fluid understanding of the competition-conflict continuum and a conviction that the United States seeks to undermine CCP rule. Like Moscow,[16] Beijing sees itself as embroiled in a long-term strategic struggle that is more akin to war than peace.[17]

For U.S. and allied policymakers, this distinction is critical. Gray-zone aggression is not peripheral "political gamesmanship," but a deliberate form of strategic conflict designed to weaken deterrence by blunting capabilities, eroding alliance commitment, and confounding communication strategies. We may not be at war in the Clausewitzian sense, but defending the strategic edge in the Indo-Pacific requires adopting a wartime mindset that is attuned to the "perpetual rhythm of struggle, [both] in *and out* of war." [emphasis added].[18]

Gray-Zone Warfare in the Indo-Pacific

Gray-zone tactics are now a persistent feature of strategic competition across the Indo-Pacific. While gray-zone activity is not unique to Beijing, its use of these methods is especially wide-ranging and pervasive. This makes China the most consequential case for understanding gray-zone warfare in the region. The following sections provide an illustrative account of these activities.

Aggressive Tactics: Military Intimidation and Overt Coercion

At the aggressive end of the spectrum, China employs sustained military intimidation—patrols, exercises, missile tests, harassment, and unsafe maneuvers—combined with non-military pressure to alter the status quo. Nowhere is this clearer than Taiwan, where incursions into the island's air defense identification zone have surged from roughly 20 in 2019 to over 3,000 in 2024.[19] Large-scale exercises simulating blockades and invasions place immense strain on Taiwan's armed forces, probing readiness while imposing

fatigue.[20] Just as importantly, they serve as a form of psychological warfare, aiming to convince the Taiwanese public that resistance is futile.

China has applied similar tactics elsewhere. In the 2017 Doklam crisis, PLA roadbuilding on Bhutanese territory triggered a tense standoff with India.[21] In 2020, Chinese and Indian troops engaged in limited but deadly skirmishes along their disputed border.[22] Since then, Beijing has quietly expanded dual-use infrastructure projects across remote Himalayan regions, consolidating its existing territory and expanding its ability to project power beyond its borders.[23] In the maritime domain, China has leveraged its Navy, Coast Guard, and vast maritime militia to challenge Japan around the Senkaku Islands and steadily expand control in the South China Sea, disregarding internationally recognized exclusive economic zones of states like the Philippines and Vietnam.[24] These actions integrate quasi-civilian forces with island-building and increasing militarization,[25] giving China escalation control while leaving defenders with few options to respond. Physical initiatives are complemented by extensive application of the three warfares (informational, legal, and psychological measures), as well as political, economic, and other means discussed below.[26]

Moderate Tactics: Cyber, Economic, and Political Interference

China is particularly active in the cyber domain, where it views the boundary between peacetime and war as particularly blurred.[27] Taiwan alone faces tens of millions of attempted intrusions every month[28]—around 73 million in 2024, up from 18 million in 2019.[29]

Leaked data from a Shanghai-based contractor in 2024 further revealed Chinese espionage against more than a dozen states throughout Asia and beyond, including not only rivals, such as India, but even "all-weather friends" like Pakistan and Cambodia.[30] Chinese state-sponsored hackers have also repeatedly targeted the Association of Southeast Asian Nations.[31] Beyond espionage, Chinese actors are pre-positioning inside critical infrastructure in the United States, Singapore, and Pacific Island nations, creating options for disruption in a crisis.[32] Chinese operators have also been repeatedly linked to the cutting of undersea cables near Taiwan and in the Baltic Sea, leading to accusations of sabotage.[33]

Economic statecraft is another powerful gray-zone tool. Beijing routinely employs informal sanctions—such as tourism bans, import restrictions, and boycotts—to punish and coerce governments, companies, and individuals for policies or actions it disapproves of.[34] More strategically, the Belt and Road Initiative and related projects have secured Chinese access to ports, aviation hubs, energy facilities, telecommunications, and other infrastructure in strategic locations across South Asia and the Pacific, from Pakistan and Sri Lanka to Papua New Guinea and the Pacific Islands.[35] Whether state-owned or seemingly private enterprises, these assets create enduring vulnerabilities that can be exploited in various ways, including espionage, sabotage, and potential military positioning.

Besides the practical and military opportunities that economic projects can generate, perhaps first and foremost, the use of financial levers can be used to acquire political influence. Often this is achieved by winning over foreign elites, using political donations, financial inducements, and lavish trips to China.[36] The case of Australian Senator Sam Dastyari, who was forced to resign in 2018

after accepting payments from a Chinese billionaire later barred from the country, is emblematic of this approach.[37] Similar allegations of influence operations have surfaced in the United States, Canada, New Zealand, and across the Pacific.[38]

Persistent Tactics: Influence Operations, Disinformation, and Lawfare

Persistent gray-zone tactics are enduring and pervasive. Though their impact can be hard to measure, over time, they enable aggressors to shape the environment to their advantage. A central feature of China's approach involves the monitoring, co-optation, and mobilization of overseas ethnic Chinese communities. For example, the UFWD-affiliated Peaceful Reunification of China Association of New Zealand has organized political fund-raising and bloc voting, mobilized counter-protests during Chinese official visits, and facilitated access between selected community leaders and local politicians.[39] And while the proportion of the Chinese diaspora population that is knowingly involved in these efforts is likely to be only very small, the potential to exert political pressure in this way is significant.

Far from isolated, such efforts are global. The UFWD—described by Chinese leaders as a "magic weapon"—has affiliated organizations in more than 90 countries. Similar patterns of activity to those observed in New Zealand have been documented in Australia, Canada, Taiwan, and the United States.[40] In parallel, the UFWD, the Ministry of State Security, and other agencies also leverage diaspora networks for espionage and technology transfer, in support of China's Military-Civil Fusion strategy.[41] A 2023 U.S.

conviction of engineer Ji Chaoqun, who conspired with the Jiangsu Province Ministry of State Security to recruit Chinese-Americans for espionage, is illustrative.[42] A study of 204 espionage cases in the United States found that 41 percent involved private Chinese citizens, underscoring how the CCP seeks to exploit overseas populations.[43] Convictions, of course, are just the tip of the iceberg, and much remains unproven. In the Philippines, for instance, a sudden influx of Chinese students into northern Cagayan province in 2023 raised counterintelligence concerns because it coincided with Manila's decision to expand the Enhanced Defense Cooperation Agreement (EDCA) with Washington to include three new sites on Luzon.[44]

The Party also works to monitor and control overseas Chinese communities. It has sought monopolies over Chinese-language media abroad, mobilized political protests, pressured students to inform on each other, and intimidated families in China to silence dissent.[45] One Australian case saw parents threatened with prison unless they disowned their daughter overseas.[46] Such tactics export censorship and repression, undermining legally protected democratic norms and values in other states.

The CCP also increasingly uses disinformation to shape the information space and interfere in political and social issues. Taiwan is the primary target, with authorities reporting 2.16 million PRC-linked false or biased information items in 2024—a 60 percent increase from the previous year.[47] Chinese operations have at times triggered protests and allegedly shaped political outcomes on the island.[48] Globally, Beijing runs the "Spamouflage" (aka Dragonbridge) network, "the largest known cross-platform covert influence operation in the world,"[49] spanning thousands of

inauthentic accounts across dozens of platforms.[50] While its effectiveness has been limited so far, the scale and persistence of the effort reflect a learning adversary committed to long-term influence.

A final persistent tactic—and one of China's infamous "three warfares"—is lawfare. Beijing uses legal tools to legitimize its claims, reinforce its narrative, and lay the groundwork for further coercion.[51] The 2005 Anti-Secessionist Law thus bolstered the CCP narrative on Taiwan while providing a legal basis for the use of "non-peaceful means" in pursuit of "reunification."[52] This was expanded in 2024 when new provisions criminalized "Taiwan Independence Diehards" and authorized punishment even beyond China's borders.[53] Similarly, the 2021 Maritime Police Law empowered the Chinese Coast Guard to take "all necessary measures" in "sea areas under Chinese jurisdiction," a sweeping definition that includes the South and East China Seas far beyond China's recognized rights under the Law of the Sea.[54] These measures are not abstract legalisms; they provide pretexts for coercive actions at Second Thomas Shoal, the Senkaku Islands, and elsewhere, and are cited in official Chinese media[55]—illustrating how lawfare reinforces public opinion warfare at the low end of the spectrum, while also enabling and legitimizing escalation closer to the threshold of armed conflict.

The Challenge for Deterrence

Beijing's use of gray-zone warfare undermines deterrence in several ways. The risk of escalation means that the use of military force in response to most gray-zone aggression is rarely a credible option, meaning conventional deterrence fails. At the same time, China

seeks to erode deterrent capability by exhausting its opponents' military capacity while signaling its own growing strength. Moderate gray-zone tactics further expand opportunities for coercion, while creating strategic dependencies that weaken political resolve. Persistent tactics degrade deterrence over time by generating uncertainty and confusion, normalizing subversion, undermining cohesion, and preconditioning the environment for more aggressive action. Collectively, these dynamics blunt traditional punishments, while simultaneously undermining resilience, and thus also weakening deterrence by denial. The fundamental question that remains is how such low-cost, low-risk, yet high-reward activities can be effectively deterred.

Responding to Gray-Zone Aggression in the Indo-Pacific

Nations across the Indo-Pacific have adopted a variety of measures to counter Chinese gray-zone aggression, ranging from legal rulings to operational deployments. While uneven and often reactive, these responses illustrate both progress and gaps in building a credible deterrence posture.

Legislative Responses

Perhaps the most prominent legal pushback was the Philippines' 2016 case before the Permanent Court of Arbitration, which ruled that China's "nine-dash line" has no legal basis and that Beijing violated the Philippines' sovereign rights and its own environmental obligations under the United Nations Convention on the Law of the Sea.[56] Although China dismissed the ruling, the decision gave

Manila international legitimacy and rallied broader support—a reminder that lawfare can cut both ways.[57]

More broadly, legislation provides the foundation for defense in the gray zone. Recent examples include the U.S. Foreign Investment Risk Review Act (2018),[58] Taiwan's Foreign Infiltration Act (2019),[59] Australia's Foreign Influence and Transparency Scheme (2018),[60] Thailand's Cybersecurity Act (2019),[61] Singapore's Foreign Interference (Countermeasures) Act (2021),[62] and New Zealand's Crimes (Countering Foreign Interference) Amendment Bill (2024).[63] Collectively, these laws strengthen the detection and prosecution of foreign interference, harden critical infrastructure, and expand cyber defense.

Administrative Responses

Governments have also reorganized bureaucracies to better coordinate defenses against foreign interference. Australia has led the way, creating the Electoral Integrity Assurance Taskforce, the Counter Foreign Interference Coordination Centre (along with a National Counter Foreign Interference Coordinator), and the University Foreign Interference Taskforce, among other measures.[64] Similar initiatives, mostly aimed at countering disinformation and protecting the integrity of elections, have been introduced in New Zealand, Japan, South Korea, and Taiwan.[65] Meanwhile, the United States has enhanced the Committee on Foreign Investments in the United States, among other measures, but currently lacks a central, interagency coordinating body dedicated to assessing and responding to foreign interference.[66] Yet structures of this kind are incredibly important. Because gray-zone threats cross institutional

boundaries, coordination is essential and determines whether responses are fragmented or strategic.

Economic Responses

Economic resilience is another line of defense. Several states have tightened foreign investment screening, restricted the transfer of sensitive technology, and diversified supply chains to reduce dependencies. Japan's appointment of a Minister for Economic Security (2021) and passage of the Economic Security Promotion Act (2022) exemplify this trend.[67] Meanwhile, joint investments—such as U.S., Australian, New Zealand, and Japanese funding for electricity and internet infrastructure in Papua New Guinea—offer alternatives to Chinese projects and the vulnerabilities they bring.[68]

Economic punishment can be applied in the form of sanctions. Washington regularly imposes penalties on both Chinese state-owned enterprises as well as state-sponsored proxies involved in malign influence activities. By comparison, others have been more hesitant when it comes to sanctioning Chinese threat actors. However, in 2023, Japan issued sanctions against North Korean hackers, followed by sanctions against Chinese firms for supporting Russia's war in Ukraine.[69] Australia and New Zealand also recently applied sanctions against Russian cyber-attackers, thus paving the way for potential broader application.[70] Although threat actors have been remarkably resilient in the face of economic punishments so far, carefully targeted economic sanctions, applied multilaterally, may yet have a deterrent effect.

Operational Responses

Physical challenges to territory necessitate operational responses. Taiwan's daily sorties against PLA Air Force incursions and Japan's record-high coast guard patrols around the Senkaku Islands demonstrate resolve, though they also strain resources.[71] Freedom of Navigation Operations by the United States and its allies counter Beijing's unlawful maritime claims, while the Philippines' resupply missions to the grounded BRP *Sierra Madre* keep China from cementing control of Second Thomas Shoal.

Law enforcement plays a parallel role in containing gray-zone activities. The United States has indicted dozens of Chinese hackers and spies,[72] while Taiwan charged 64 people—mostly soldiers—for espionage in 2024.[73] Such prosecutions not only disrupt operations but also have important informational value by exposing gray-zone activity.

Overt operations are complemented by a variety of indirect, non-attributable, and asymmetric activities aimed at countering adversaries, while strengthening partners and allies.[74] U.S. Cyber Command's "defend forward" approach preempts attacks by persistently engaging adversary networks,[75] while Japan's 2025 Active Cyber Defense Law similarly authorized preemptive actions in cyberspace—indicating a growing realization that these capabilities are needed to effectively compete in the gray zone.[76] Yet as necessary as the various operational responses are, none of them has ultimately succeeded in deterring Chinese aggression.

Informational Responses

Finally, states are investing in awareness and narrative competition. Examples include New Zealand's annual *Security Threat Environment* report,[77] Australia's UFIT outreach to universities, and numerous public campaigns aimed at countering disinformation and foreign interference.[78] The Philippines has even produced a comic book, *Teacher Jun*, to educate children about maritime coercion in the West Philippine Sea.[79]

Informational responses also include "naming and shaming." Public indictments of hackers,[80] broadcasting of Chinese aggression at sea, and sustained documentation of harassment by Taiwan, Japan, and the Philippines all serve to establish legitimacy and mobilize international support.[81] While exposure alone has not curbed Beijing's behavior, it strengthens alliance cohesion and lays the groundwork for coordinated deterrence.

Restoring Deterrence in the Gray Zone

The preceding examples show that the United States and many of its Indo-Pacific partners have awakened to the scope of the gray-zone challenge and are taking steps to defend themselves. Encouraging as this is, the reality remains that China—and others such as North Korea—have been largely undeterred, continuing to press their aims with low-cost, high-reward tactics. How to blunt and ultimately deter these moves without sparking escalation remains an unresolved dilemma.

The following recommendations highlight ways that the United States and its allies can strengthen defenses and mount a more credible deterrent.

Thoroughly Assess and Publicly Identify the Threat

Significant progress has been made in exposing coercive gray-zone activity; however, progress has been uneven, and there is much more that can be done. To begin with, it is fundamentally important that nations develop comprehensive threat and vulnerability assessments—both classified and unclassified versions—that can be shared across government and with the public. These should draw on input from multiple agencies, civil society, and the private sector, and be willing to identify the sources of coercion by name. While some countries have indeed taken steps in this direction, it is unclear whether the threat and related vulnerabilities are fully understood, especially outside of the security sector. Moreover, many states still shy away from public attribution, which allows China to act with impunity.

Be Systematic, Yet Pragmatic

Ad hoc and reactive responses have proven ill-suited to the demands of gray-zone competition. Deterring such behavior requires more than isolated countermeasures; it demands a disciplined approach to competition that aligns assessment, decision-making, and action across time and across institutions.

A useful starting point is the recognition that gray-zone deterrence requires a structured way of aligning threats and vulnerabilities assessments, along with national priorities, response

options, and synchronization with partners—an approach articulated by the European Centre of Excellence for Countering Hybrid Threats.[82] The United States and its Indo-Pacific partners should study this approach and adapt it to their own strategic contexts and institutional constraints.

At the same time, strategic discipline requires realism. Not all gray-zone activity can be deterred, and attempts to do so indiscriminately risk strategic exhaustion. As Lyle Morris and his colleagues argue, high-end, *aggressive* gray-zone actions—those that approach the threshold of open conflict or threaten core interests—may be more susceptible to deterrence, while some *moderate* tactics may be dissuaded over time. By contrast, low-level *persistent* activities are unlikely to disappear and must instead be managed and mitigated.[83] Effective gray-zone deterrence, therefore, depends on differentiation: distinguishing what can realistically be deterred from what must be absorbed, disrupted, or blunted. Crucially, this must also involve a detailed assessment of the goals, interests, cost-benefit calculus, and vulnerabilities of the individual threat actor concerned, as well as the defending state's own resources and capabilities.

A systemic approach need not be rigid. On the contrary, the goal is pragmatic selectivity—focusing effort where deterrence is plausible, conserving resources where it is not, and ensuring that responses are proportionate, coordinated, and strategically aligned. In the gray zone, deterrence is less about eliminating hostile behavior than about shaping its cost, frequency, and effectiveness over time.

Improve Coordination

Current responses to gray-zone aggression are broad but often fragmented. Because gray-zone tactics deliberately cut across military, economic, informational, legal, and societal domains, they cannot be countered effectively by single agencies or siloed institutions. Meaningful deterrence, therefore, requires genuine whole-of-government coordination—including non-traditional partners—and, critically, alignment among allies and partners.[84] And yet, too often such coordination emerges only after a crisis is already underway.[85]

The United States and other Indo-Pacific nations must, therefore, examine and strengthen their coordination mechanisms now. Only integrated national and multilateral responses have a realistic chance of deterring China's gray-zone playbook. At the national level, this may require adapting existing institutional arrangements, or, where gaps persist, creating new coordinating bodies with clear authority and responsibility, such as Australia's Counter Foreign Interference Coordination Centre. International coordination presents additional political and legal challenges, but it is no less essential. The credibility of deterrence ultimately rests not only on U.S. power, but on the visible cohesion of a coalition that is willing and able to act decisively and in concert.

Accept Calibrated Risks

Most countermeasures employed today remain reactive and largely defensive, allowing the initiative to remain with the aggressor. While the risk of escalation is real—and ethical, legal, and reputational factors matter—effective deterrence cannot be built on

a zero-risk tolerance. Without credible denial strategies and at least the credible threat of punishment, adversaries will continue to push the boundaries with little fear of consequence.[86]

As Vytautas Keršanskas points out, "escalation is not inherently bad...[and] can be a necessary and appropriate part of deterrence."[87] This does not mean that the U.S. should "push the envelope" in response to all gray-zone provocation, but doing so on a carefully selected, case-by-case basis may compel would-be aggressors to back down.[88] Crucially, any strategy of limited escalation must be clearly communicated to adversaries in advance; otherwise, it is unlikely to alter their cost-benefit calculation.

Target Specific Perpetrators

Deterrence in the gray zone ultimately depends on altering the cost-benefit calculus of aggressors. While this often involves shaping the perceptions of the responsible state, much of that activity is carried out through proxies—quasi-state entities, private firms, and a cornucopia of other seemingly independent actors—whose personal incentives rarely align perfectly with those of the state.[89] Even individual officials working directly for the state have their own interests and motivations.

This creates opportunities for what Elizabeth Braw has termed "personalized deterrence."[90] Targeted indictments, financial sanctions, visa restrictions, exposure of corruption, and other individualized penalties can raise the personal costs of participation in gray-zone campaigns. Over time, such measures may shrink the pool of willing proxies and force key actors to reconsider both their

own roles and the broader strategy they are executing on behalf of the state.

Build Resilience—But Don't Depend on It

Resilience is indispensable but not sufficient. Gray-zone activity will persist, and societies must be able to absorb disruption, maintain core functions under pressure, and recover quickly from crises. In theory, whole-of-society resilience can contribute to deterrence by denial: if hostile actions consistently fail to achieve their intended effects, incentives for continued coercion diminish.

This logic underpins Singapore's long-standing *Total Defence* strategy and the work of Taiwan's rapidly maturing Whole-of-Society Defense Resilience Committee.[91] These models, alongside European experience, offer valuable lessons and should be adapted to local contexts across the Indo-Pacific.[92] Yet resilience must not become a substitute for deterrence by punishment. In Europe, overreliance on resilience has at times served as a way to avoid confrontation.[93] Indo-Pacific nations should avoid repeating that mistake by ensuring that resilience complements, rather than replaces, credible deterrent action.

Conclusion

This chapter examines the use of gray-zone tactics in the Indo-Pacific, assesses how states are responding, and identifies pathways for strengthening deterrence below the threshold of war. While the scale and diversity of gray-zone activity defy comprehensive treatment in a single chapter, the cases presented here illustrate both the scope of the challenge and the costs of insufficient response.

Gray-zone competition has re-emerged as one of the defining security challenges of our times. For decades, the CCP and like-minded regimes—including Russia, North Korea, and Iran—have deliberately blurred the distinction between peace and war, exploiting ambiguity to advance strategic objectives while avoiding direct confrontation. Recognizing this reality is a prerequisite for effective deterrence.

Not all forms of gray-zone activity can be eliminated, nor should deterrence be measured solely by the absence of provocation. Rather, success lies in shaping adversary behavior—restricting the space for subversive activities, raising the likelihood of failure, imposing meaningful and targeted costs, and controlling escalation dynamics, while preserving access, sovereignty, and alliance cohesion. Working together in this way, over time, Washington and its partners can reestablish deterrence and ultimately regain the strategic advantage in the contested space below the threshold of war.

Endnotes

1 The author is solely responsible for the views expressed in this publication, which do not necessarily represent the official policy or position of the Daniel K. Inouye Asia-Pacific Center for Security Studies, the U.S. Department of War, or the U.S. government.

2 George F. Kennan, *Policy Planning Staff Memorandum No. 269*, U.S. Department of State, May 4, 1948, https://history.state.gov/historicaldocuments/frus1945-50Intel/d269.

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

4 U.S. Special Operations Command, *The Gray Zone,* September 9, 2015, https://info.publicintelligence.net/USSOCOM-GrayZones.pdf.

[5] Joseph L. Votel et al., "Unconventional Warfare in the Gray Zone," *Joint Forces Quarterly*, 80, no.1, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf.

[6] U.S. Department of Homeland Affairs, "Defining Foreign Interference," accessed July 12, 2023, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/defining-foreign-interference; 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), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2942/RAND_RR2942.pdf.

[7] Morris et al., Gaining Competitive Advantage in the Gray Zone. Michael Pillsubury, The Hundred-Year Marathon: China's Strategic Strategy to Replace America as the Global Superpower (New York: St. Martin's Griffin, 2015).

[8] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999), 7, https://www.c4i.org/unrestricted.pdf.

[9] John Costello and Peter Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operations" in *China's Evolving Military Strategy*, ed. Joe McReynolds, (Washington, C: Jamestown Foundation, 2016), 187–88, Kindle.

[10] Seth Jones, Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare (New York: W.W. Norton, 2021), 143.

[11] B. A. Friedman, "Finding the Right Model: The Joint Force, the People's Liberation Army, and Information Warfare," *Journal of Indo-Pacific Affairs*, April 24, 2023, https://www.airuniversity.af.edu/JIPA/Display/Article/3371164; Elsa Kania, "Minds at War China's Pursuit of Military Advantage through Cognitive Science and Biotechnology," *Prism* 8, no. 3, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Kania_82-101.pdf; Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," *The China Brief* 16, no. 13, https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/; Peter Mattis, "China's 'Three Warfares' in Perspective," *War on the Rocks*, January 30, 2018, https://warontherocks.com/2018/01/chinas-three-warfares-perspective/; Koichiro Takagi, "New Tech, New Concepts: China's Plans for AI and

Cognitive Warfare," *War on the Rocks*, April 13, 2022, https://warontherocks.com/2022/04/new-tech-new-concepts-chinas-plans-for-ai-and-cognitive-warfare/.

12 Mattis, "China's 'Three Warfares' in Perspective."

13 Rush Doshi, *The Long Game: China's Grand Strategy to Displace American Order* (New York: Oxford University Press, 2021), 51, Kindle.

14 Global Times, "GT Investigates: US Wages Global Color Revolutions to Topple Govts for the Sake of American Control," December 2, 2021, https://www.globaltimes.cn/page/202112/1240540.shtml.

15 Nils Peterson, "The Chinese Communist Party's Theory of Hybrid Warfare," *Institute for the Study of War*, November 21, 2023, https://understandingwar.org/research/china-taiwan/the-chinese-communist-partys-theory-of/.

16 Oscar Jonsson, The Russian Understanding of War: Blurring the Lines Between War and Peace (Washington, DC: Georgetown University Press, 2019).

17 Doshi, *The Long Game,* 308–10, Kindle.

18 Kennan, Policy Planning Staff Memorandum No. 269.

19 Gerald C. Brown and Ben Lewis, "Taiwan ADIZ Violations," *Center for Strategic and International Studies*, n.d., accessed July 9, 2025, https://chinapower.csis.org/data/taiwan-adiz-violations/.

20 Derek Grossman, *The Chinese Communist Party's Gray Zone Tactics Against Taiwan*, (Washington, DC: Global Taiwan Institute, March 2025), https://globaltaiwan.org/wp-content/uploads/2025/03/OR_CCP-Gray-Zone-Tactics-Against-TW.pdf.

21 Sanjeev Milani and Fayaz Bukhari, "India, China Soldiers Involved in Border Altercation: Indian Sources," *Reuters*, August 15, 2017, https://www.reuters.com/article/us-india-china-idUSKCN1AV29F/.

22 Swati Gupta and Nectar Gan, "China and India accuse each other of firing shots as border tensions escalate" *CNN*, September 8, 2020, https://www.cnn.com/2020/09/08/asia/china-india-border-warning-shots-intl-hnk.

23 Muyi Xiao and Agnes Chang, "China's Great Wall of Villages," *New York Times*, August 10, 2024, https://www.nytimes.com/interactive/2024/08/10/world/asia/china-border-villages.html.

[24] Bonny Lin et al., *Competition in the Gray Zone* (Santa Monica, CA: RAND, 2022), https://www.rand.org/pubs/research_reports/RRA594-1.html; Rebecca Ratcliffe, "Confrontations in South China Sea Surge, Raising Fears a Miscalculation Could Lead to Conflict," *Guardian*, July 12, 2024, https://www.theguardian.com/world/article/2024/jul/12/south-china-sea-conflict-philippines-coast-guard; Masaaki Yatsuzuka, "How China's Maritime Militia Takes Advantage of the Grey Zone," *ASPI Strategist*, January 16, 2023, https://www.aspistrategist.org.au/how-chinas-maritime-militia-takes-advantage-of-the-grey-zone/.

[25] Asia Maritime Transparency Initiative, "China Island Tracker," accessed July 10, 2025, https://amti.csis.org/island-tracker/china/.

[26] Doug Livermore, "China's 'Three Warfares,' in Theory and Practice in the South China Sea," *Georgetown Security Studies Review*, March 25, 2018, https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/.

[27] China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020* (Montgomery, AL: CASI, 2022), 150, https://www.airuniversity.af.edu/CASI/Display/Article/2913216; Joe McReynolds, "China's Military Strategy for Network Warfare" in *China's Evolving Military Strategy*, ed. Joe McReynolds (Washington, DC; The Jamestown Foundation, 2017), 212, Kindle.

[28] Lin et al, Competition in the Gray Zone, 59.

[29] Grossman, Chinese Communist Party's Gray Zone Tactics, 7; Lin et al., Competition in the Gray Zone, 59.

[30] Matt Brazil, "Huge China Data Dump Disappears," *Spy Talk*, February 21, 2024, https://www.spytalk.co/p/a-chinese-snowden?utm_source=substack&publication_id=81003.

[31] Wired, "China Is Relentlessly Hacking Its Neighbors," February 28, 2023, https://www.wired.co.uk/article/china-hack-emails-asean-southeast-asia.

[32] Stephen Dziedzic, "China-backed APT40 Hacking Group Blamed for Cyber Attacks on Samoa," *ABC News*, February 11, 2025, https://www.abc.net.au/news/2025-02-12/china-backed-apt40-blamed-for-cyber-attacks-on-samoa/104927412; Cybersecurity and Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a; Aaron Tan, "Singapore Under Ongoing Cyber Attack From APT Group," *Computer Weekly*, July 21, 2025,

https://www.computerweekly.com/news/366627926/Singapore-under-ongoing-cyber-attack-from-APT-group.

33 Miranda Bryant and Pjotr Sauer, "Swedish Police Focus on Chinese Ship After Suspected Undersea Cable Sabotage," *The Guardian*, November 20, 2024, https://www.theguardian.com/world/2024/nov/20/sweden-denmark-undersea-cable-sabotage-navy-investigation; Koh Ewe and I-ting Chiang, "Taiwan Jails China Captain for Undersea Cable Sabotage in Landmark Case," *BBC News*, June 11, 2025, https://www.bbc.com/news/articles/cwy3zy9jvd4o.

34 Elisabeth Braw, *The Defender's Dilemma: Identifying and Deterring Gray-Zone Aggression* (Washington, DC: American Enterprise Institute, 2022), 56–82, Kindle.

35 Braw, *The Defender's Dilemma;* Clive Hamilton, *Silent Invasion: China's Influence in Australia* (Melbourne: Hardie Grant Books, 2018), 150–79, Kindle; Domingo I-Kwei Yang, *China's Dual-Use Infrastructure in the Pacific* (Sinopsis: 2025), https://sinopsis.cz/wp-content/uploads/2025/04/chinas-dual-use-infrastructure-in-the-pacific.pdf; Charlie Moore, "From Farms and Coal Mines to Airports and Water Supplies," *Daily Mail*, December 1, 2019, https://www.dailymail.co.uk/news/article-7725675; Michael Sullivan, "Cambodia Finishes Expansion of Main Naval Base, Largely Funded by China," *NPR*, April 7, 2025, https://www.npr.org/2025/04/07/nx-s1-5354692; Gonzalo Vázquez, "Gwadar Port and Chinese Dual Use Facilities," *Universidad de Navarra*, August 28, 2023, https://www.unav.edu/web/global-affairs/gwadar-port-and-chinese-dual-use-facilities.

36 Anne-Marie Brady, *Magic Weapons: China's Political Influence Activities Under Xi Jinping* (Washington, DC: Wilson Center, 2017), https://www.wilsoncenter.org/sites/default/files/media/documents/article/magic_weapons.pdf.

37 Tom Rabe, Kate McClymont, and Alexandra Smith, "Dastyari, ICAC and the Chinese 'Agent of Influence'," *Sydney Morning Herald*, August 29, 2019, https://www.smh.com.au/politics/nsw/dastyari-icac-and-the-chinese-agent-of-influence-20190829-p52m6e.html.

38 "A Guide to Foreign Interference and China's Suspected Influence in Canada," *The Globe and Mail*, May 22, 2022, https://www.theglobeandmail.com/politics/article-china-foreign-interference-canada-guide/; Brady, *Magic Weapons*; Angus Grigg and Nick McKenzie, "Chinese Aid Funded Alleged $1 Million Bribe to Former PNG

Leader, Somare," *Financial Review*, June 3, 2018, https://www.afr.com/world/asia/chinese-aid-funded-1-million-bribe-to-former-png-leader-somare-20180603-h10we3; Kirsty Needham, "Distribution of Chinese Funds by Solomon Islands PM Raises Questions," *Reuters*, August 24, 2022, https://www.reuters.com/world/asia-pacific/distribution-chinese-funds-by-solomon-islands-pm-raises-questions-2022-08-25/; Veerle Nouwens and Alexander Neill (Eds), *Malign Interference in Southeast Asia: Understanding and Mitigating Economic and Political Interference and Information Operations* (London: Royal United Services Institute for Defence and Security Studies, 2022), https://static.rusi.org/malign-interference-in-southeast-asia.pdf; Catrin Owen, "Yikun Zhang, the Millionaire at the Centre of the Political Donations Trial," *Stuff*, October 5, 2022, https://www.stuff.co.nz/national/crime/129949313; Cleo Paskal, "Micronesia's President Writes Bombshell Letter on China's 'Political Warfare'," *Diplomat*, March 10, 2023, https://thediplomat.com/2023/03/micronesias-president-writes-bombshell-letter-on-chinas-political-warfare/.

39 Brady, *Magic Weapons*, 16.

40 John Dotson, The Chinese Communist Party's Political Warfare Directed Against Taiwan, (Washington, DC: Global Taiwan Institute, 2020), 8 ; Alex Joske, The Party Speaks for You: Foreign Interference and the Chinese Communist Party's United Front System (Australian Strategic Policy Institute, 2020), 7, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2020-06/The%20party%20speaks%20for%20you_0.pdf?VersionId=gFHuXyYMR0XuDQOs.6JSmrdyk7MralcN; Clive Hamilton, China's Influence Activities: What Canada Can Learn From Australia (MacDonald-Laurier Institute, 2018), https://macdonaldlaurier.ca/files/pdf/201801026_Commentary_Hamilton_FWeb.pdf; Special Report on Foreign Interference in Canada's Democratic Processes and Institutions (Ottawa, ON: The National Security and Intelligence Committee of Parliamentarians, 2024), 16–34, https://www.nsicop-cpsnr.ca/reports/rp-2024-06-03/special-report-foreign-interference.pdf; Clive Hamilton and Mareike Ohlberg, Hidden Hand: How the Chinese Communist Party is Reshaping the World (London: Oneworld Publications, 2021), ch. 7.

41 Ibid.

42 Nicholas Yong, "Ji Chaoqun: Chinese Engineer Jailed for Eight Years for Spying in US," *BBC News*, January 25, 2023, https://www.bbc.com/news/world-asia-china-64408767.

[43] Center for Strategic and International Studies, *Survey of Chinese Espionage in the United States Since 2000* (Washington, DC: CISI, n.d.), https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000.

[44] Elvira Ramirez-Cohn, "Fears Over 'Influx' of Chinese Students in Strategic Area" *University World News*, April 22, 2024, https://www.universityworldnews.com/post.php?story=20240422132616250

[45] Brady, *Magic Weapons*, 35–39; Hamilton, *Silent Invasion*, 62–67; Hamilton and Ohlberg, *Hidden Hand*, chapter 9; Poppy Wood, "'I No Longer Trust Anyone': The Chinese Student Seized for Speaking out in Britain," *Yahoo News*, March 25, 2025.

[46] Tom Canetti, "In Australia, Pro-Democracy Students Aren't Safe From China's Reach" *Foreign Policy*, January 6, 2023, https://foreignpolicy-com.eu1.proxy.openathens.net/2023/01/06/australia-china-protests-ccp-xi-jinping-democracy-diaspora/.

[47] Christopher Bodeen, "Taiwan Says China is Redoubling Efforts to Undermine Democracy with Disinformation," *Associated Press*, January 3, 2025, https://apnews.com/article/taiwan-china-disinformation-3f05dac36399bf672a702100147bf8fa.

[48] Dotson, *The Chinese Communist Party's Political Warfare Directed Against Taiwan*, 8; Scott W. Harold, Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung, *Chinese Disinformation Efforts on Social Media* (Santa Monica, CA: RAND, 2021), 68–69, https://www.rand.org/pubs/research_reports/RR4373z3.html; Paul Huang, "Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate," *Foreign Policy*, June 26, 2019, https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/.

[49] Guy Rosen, "Raising Online Defenses Through Transparency and Collaboration," Meta, August 29, 2023, https://about.fb.com/news/2023/08/raising-online-defenses/.

[50] Zak Butler, "Google Disrupted Over 10,000 Instances of DRAGONBRIDGE activity in Q1 2024," Google Threat Analysis Group, June 26, 2024, https://blog.google/threat-analysis-group/google-disrupted-dragonbridge-activity-q1-2024/; Ben Nimmo et al., *Second Quarter Adversarial Threat Report* (Meta: August 2023), 11–19, https://transparency.meta.com/metasecurity/threat-reporting/.

[51] Kania, "The PLA's Latest Strategic Thinking on the Three Warfares"; Doug Livermore, "China's 'Three Warfares' in Theory and Practice in the South China Sea," *Georgetown Security Studies Review*, posted March 25, 2018; Mattis, "China's 'Three Warfares' in Perspective."

[52] Bonny Lin and I-Chung Lai, *Employing "Non-Peaceful" Means Against Taiwan: The Implications of China's Anti-Secession Law* (Washington, DC: Center for Strategic and International Studies, 2024), https://www.csis.org/analysis/employing-non-peaceful-means-against-taiwan.

[53] Lin and Lai, Employing "Non-Peaceful" Means Against Taiwan.

[54] Raul (Pete) Pedrezo, (2021) "Maritime Police Law of the People's Republic of China," *International Law Studies* 97 (2021), 465–77, https://digital-commons.usnwc.edu/ils/vol97/iss1/24; Raul (Pete) Pedrezo, "China Coast Guard: Beijing's Tool for Intimidation," *KIMS Periscope*, no. 236 (Korea Institute for Maritime Strategy, n.d.), https://en.kims.or.kr/issubrief/kims-periscope/peri236/.

[55] Yuyuan Tantian, "How Should We Understand the New Statement by the China Coast Guard Regarding 'Boarding and Inspecting' Philippine Vessels?" *CCTV News*, June 19, 2024, https://news.cctv.com/2024/06/19/ARTIEfP0ydAJv1CloyUXXbNQ240619.shtml (translated from the original Chinese).

[56] Permanent Court of Arbitration, *The South China Sea Arbitration (The Republic of the Philippines v. The People's Republic of China)*, (The Hague, July 12, 2016), https://pcacases.com/web/sendAttach/1801.

[57] "Philippines Welcomes G7 Backing in South China Sea Dispute," *Philstar*, April 21, 2024, https://www.philstar.com/headlines/2024/04/21/2349389/philippines-welcomes-g7-backing-south-china-sea-dispute.

[58] U.S. Department of the Treasury, *Summary of the Foreign Investment Risk Review Modernization Act of 2018*, n.d., https://home.treasury.gov/system/files/206/Summary-of-FIRRMA.pdf.

[59] Mainland Affairs Council, "Legislative Yuan Passes Anti-Infiltration Bill to Strengthen Defense for Democracy and Preserve Stable and Orderly Cross-Strait Exchanges," *MAC Press Release* no. 101, December 31, 2019, https://www.mac.gov.tw/en/News_Content.aspx?n=A921DFB2651FF92F%26sms=37838322A6DA5E79%26s=88E5E1EF1343B1B8.

[60] Attorney-General's Department (Australia), "Foreign Influence Transparency Scheme," n.d., https://www.ag.gov.au/integrity/foreign-influence-transparency-scheme.

[61] "Thailand's Cyber Security Maintenance Act of 2019," *DigWatch*, May 2019, https://dig.watch/resource/thailands-cyber-security-maintenance-act-of-2019.

[62] Ministry of Home Affairs (Singapore), "Provisions in the Foreign Interference (Countermeasures) Act for Countering Foreign Interference via Local Proxies," December 12, 2023, https://www.mha.gov.sg/mediaroom/press-releases/provisions-in-the-foreign-interference-countermeasures-act-for-countering-foreign-interference-via-local-proxies/.

[63] Ministry of Justice (New Zealand), "Countering Foreign Interference," n.d., https://www.justice.govt.nz/justice-sector-policy/key-initiatives/countering-foreign-interference.

[64] "Development of University Foreign Interference Taskforce - Guiding Framework," *Department of Education*, August 29, 2019, https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/development-university-foreign-interference-taskforce-guiding-framework.

[65] Emily Feng, "Taiwan Deals with Lots of Misinformation, and It's Harder to Track Down," *NPR*, January 11, 2024, https://www.npr.org/2024/01/11/1216340756/taiwan-election-disinformation-social-media-ptt; "KCC to Launch Task Force on Stamping out Fake News," *KBS World*, September 6, 2023, https://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=180304; Yuta Kimura, "Protecting Japan's National Security From Information Operations," *Australian Strategic Policy Institute*, July 5, 2024, https://www.aspistrategist.org.au/protecting-japans-national-security-from-information-operations; Department of the Prime Minister and Cabinet (New Zealand), "Multi-Stakeholder Group to Strengthen Resilience to Disinformation," June 19, 2024, https://www.dpmc.govt.nz/our-programmes/national-security/strengthening-resilience-disinformation/multi-stakeholder-group-strengthen-resilience-disinformation.

[66] U.S. Department of the Treasury, "Treasury Issues Final Rule Expanding CFIUS Coverage of Real Estate Transactions Around More Than 60 Military Installations," November 1, 2024, https://home.treasury.gov/news/press-releases/jy2708.

[67] "Japan's Economic Security Promotion Act and the Implications for Businesses," *Strategic Comments* 28, no. 8 (2022), viii–ix, https://doi.org/10.1080/13567888.2022.2157625.

[68] "US and Its Allies Pledge Power to PNG to Counter China's Influence in Pacific," *The South China Morning Post*, November 18, 2018, https://www.scmp.com/news/asia/australasia/article/2173801/us-and-its-allies-pledge-power-png-counter-chinas-influence.

[69] "Japan Sanctions China-Based Firms Accused of Supporting War in Ukraine" *Al-Jazeera*, June 21, 2024, https://www.aljazeera.com/economy/2024/6/21/japan-sanctions-china-based-firms-accused-of-supporting-war-in-ukraine; Meg Kinnard and Mari Yamaguchi, "Japan Sanctions 3 Groups and 4 Individuals for Supporting North Korea's Missile Program," *Quartz*, August 31, 2023, https://qz.com/japan-sanctions-3-groups-and-4-individuals-for-supporti-1850795527.

[70] Daryna Antoniuk, "New Zealand Sanctions Russian Military Hackers Over Cyberattacks on Ukraine," *The Record*, September 15, 2025, https://therecord.media/new-zealand-russia-gru-ukraine; Department of Foreign Affairs and Trade (Australia), "Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Regulations 2021," December 21, 2021, https://www.dfat.gov.au/news/news/autonomous-sanctions-amendment-magnitsky-style-and-other-thematic-sanctions-regulations-2021; Australian Department of Defence, "Further Cyber Sanctions in Response to Medibank Private Cyberattack," February 12, 2025, https://www.minister.defence.gov.au/media-releases/2025-02-12/further-cyber-sanctions-response-medibank-private-cyberattack; Kinnard and Yamaguchi, "Japan Sanctions 3 Groups and 4 Individuals for Supporting North Korea's Missile Program."

[71] Brian Mcelhiney and Keishi Koja, "China Sets Record for Coast Guard Vessels Spotted Near Japanese Islets," *Stars and Stripes*, January 7, 2025, https://www.stripes.com/theaters/asia_pacific/2025-01-07/senkaku-islands-china-japan-16401727.html.

[72] U.S. Department of Justice, "Fact Sheet: Disruptive Technology Strike Force Efforts in First Year to Prevent Sensitive Technology from Being Acquired by Authoritarian Regimes and Hostile Nation-States," February 16, 2024, https://www.justice.gov/archives/opa/pr/fact-sheet-disruptive-technology-strike-force-efforts-first-year-prevent-sensitive.

[73] "Taiwan Reports 'Significant Rise' in Suspected Chinese Espionage," *Reuters*, January 12, 2025, https://www.reuters.com/world/asia-

pacific/taiwan-reports-significant-rise-suspected-chinese-espionage-2025-01-13.

74 Office of the Under Secretary of Defense for Policy, *DOD Instruction 3000.07: Irregular Warfare*, September 29, 2025, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/300007p.PDF?ver=lRJ36mSworhF2PKZnXE-zA%3D%3D.

75 U.S. Cyber Command Public Affairs Office, "CYBER 101: Defend Forward and Persistent Engagement," U.S. Cyber Command, October 25, 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement.

76 Tova Dvorin, "Japan's New Active Cyber Defense Law: What It Means for Cyber Resilience and AEV," *Safebreach*, June 12, 2025, https://www.safebreach.com/blog/japan-active-cyber-defense-law/.

77 Tess McClure, "New Zealand Intelligence Report Accuses China of 'Foreign Interference'," *The Guardian*, August 11, 2023, https://www.theguardian.com/world/2023/aug/11/new-zealand-intelligence-report-accuses-china-of-foreign-interference; *New Zealand's Security Threat Environment 2025* (Auckland: New Zealand Secret Intelligence Service, 2025) https://www.nzsis.govt.nz/our-work/new-zealands-security-threat-environment/security-threat-environment-2025.

78 National Center of Incident Readiness and Strategy for Cybersecurity (Japan), "Commitment to a Free, Fair and Secure Cyberspace," n.d., https://www.cyber.go.jp/eng/index.html; "Shields Up!" *Cybersecurity and Infrastructure Security Agency*, undated, https://www.cisa.gov/shields-up; Critical Infrastructure Security Centre (Australia), "Trusted Information Sharing Network," March 6, 2024, https://www.cisc.gov.au/how-we-support-industry/partnership-and-collaboration/trusted-information-sharing-network.

79 Jim Gomez, "Philippines Launches Comic Book to Counter China's Disinformation," *National Post*, January 24, 2025, https://nationalpost.com/news/philippines-launches-comic-book-to-counter-chinas-disinformation.

80 U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014, https://www.justice.gov/archives/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[81] Richard Javad Heydarian, "South China Sea: The 'Transparency Initiative' Success is Plain to See," *The Interpreter*, September 9, 2024, https://www.lowyinstitute.org/the-interpreter/south-china-sea-transparency-initiative-success-plain-see; Yimou Lee and Ben Blanchard, "Exclusive-Taiwan Estimates China Spent 40% More on Pacific Drills Last Year to Hit $21 Billion," *Yahoo News*, August 28, 2025, https://ca.news.yahoo.com/exclusive-taiwan-estimates-china-spent-022048204.html; Ministry of Foreign Affairs of Japan, "Trends in China Coast Guard and Other Vessels in the Waters Surrounding the Senkaku Islands, and Japan's Response," August 1, 2025, https://www.mofa.go.jp/region/page23e_000021.html.

[82] Vladimir Rauta, *Countering State-Sponsored Proxies: Designing a Robust Policy* (Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2025), https://www.hybridcoe.fi/wp-content/uploads/2025/02/web_Hybrid_CoE_Paper-23_rgb.pdf.

[83] Morris et al, Gaining Competitive Advantage in the Gray Zone.

[84] Viktorija Rusinaitė, *Turning Strategy into Praxis: Lessons in Hybrid Threat Deterrence* (Helsinki: Hybrid Threats Centre of Excellence, 2025) https://www.hybridcoe.fi/publications/turning-strategy-into-praxis-lessons-in-hybrid-threat-deterrence/.

[85] Rusinaitė, Turning Strategy into Praxis.

[86] Rusinaitė, Turning Strategy into Praxis.

[87] Vytautas Keršanskas, *Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats* (Helsinki: Hybrid Threats Centre of Excellence, 2020), 11, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf.

[88] Morris et al, Gaining Competitive Advantage in the Gray Zone.

[89] Elizabeth Braw, "Countering Aggression in the Gray Zone" *PRISM* 9, no. 3 (2021), 62–75; Sam Mullins, *The Role of Non-State Actors as Proxies in Irregular Warfare and Malign State Influence* (Arlington, VA: Irregular Warfare Center, 2024), https://irregularwarfarecenter.org/wp-content/uploads/The-Role-of-Non-State-Actors-as-Proxies-in-Irregular-Warfare-and-Malign-State-Influence.pdf.

[90] Braw, "Countering Aggression in the Gray Zone," 62–75.

[91] Singapore Government, "About Total Defence," July 14, 2025, https://www.totaldefence.gov.sg/about/; Office of the President, Republic of

China (Taiwan), "Whole-of-Society Defense Resilience Committee," n.d., https://english.president.gov.tw/Page/670.

92 Marc Ablong, *National Resilience: Lessons for Australian Policy From International Experience* (Canberra: Australian Strategic Policy Institute, 2024), https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2024-02/National%20resilience.pdf.

93 Rusinaitė, Turning Strategy into Praxis.