

Stewards of the Status Quo

US Air, Space, and Cyber Imperatives in the Indo-Pacific Gray Zone

MAJ JOSEPH TOMCZAK, USAF

MAJ NICHOLAS TORROLL, USAF

MAJ BEDRI KALOSHI, ALBANIAN AIR FORCE

In 2019, the commander of US Indo-Pacific Command (USINDOPACOM), Admiral Phillip Davidson, testified before the Senate Armed Services Committee regarding the theater's command posture.¹ In his statement, Admiral Davidson stated that “[US] adversaries are pursuing their objectives between peace and war [and] USINDOPACOM must compete in the gray zone.”² As national security practitioners, we ask: What are the imperatives to enable this kind of competition within the gray zone? *Specific to air, space, and cyber power, the United States must apply new ideas, innovate new technology, and reorganize its forces to meet the imperatives of the gray zone.* Each of these imperatives is best understood through I. B. Holley's classic framework on the evolution of warfare as relating to either ideas, tools, or groups.³ This article interprets the framework as *application* (ideas), *technology* (tools), and *organization* (groups). First, the United States and its allies must leverage the full range of air, space, and cyber power in proactive ways to create dilemmas and uncertainty for the Chinese government and, if necessary, impose costs. Next, they must develop airpower technology focused on dispelling ambiguity, increasing attribution, and illuminating malign activity. And finally, the United States must orient a portion of its air, space, and cyber forces toward frustrating China's coercive gradualism.

Conceptualizing the Gray Zone

Nadia Schadow, the architect of the 2017 *National Security Strategy*, observes that the “space between war and peace is a landscape churning with political, economic, and security competitions that require constant attention.”⁴ Gray zone warfare occupies this space by melding the political, economic, and security aspects of strategic competition into what Hal Brands of Johns Hopkins University characterizes as “activity that is coercive and aggressive in nature, but that is deliberately designed to remain below the threshold of conventional military conflict and open interstate war.”⁵ In relation to security competition specifically, if a revisionist state wanted to increase its power relative to a status quo power, it would historically pursue that objective through conventional military force. However, nuclear deterrence, economic interdependence, and US conventional military

superiority have all pushed conflict down into the gray zone—where states are now less likely to pursue their political aims through traditional warfare.⁶

Globalization and the liberal world order, instead of creating a “global village” of interconnected and interdependent nation-states, inadvertently invited revisionist powers to manipulate the system in “insidious ways.”⁷ Patient practitioners of gray zone warfare seek gradual victories by nibbling at the edges of the status quo.⁸ When fought in the shadows, gray zone actions range from cyberattacks, electronic warfare, propaganda, political warfare, misinformation, economic coercion, and the use of proxy fighters.⁹ When fought in the open, gray zone forces remain ambiguous for as long as possible, quickly seize the objective once identified, and promptly “de-escalate and negotiate from a position of strength.”¹⁰ Understanding the conceptual framework of gray zone warfare will help shed light on America’s primary gray zone competitor—China.

China and Competition in the Gray Zone

Within the context of strategic competition with China specifically, “gray zone warfare” can be defined as a deliberate approach taken by a revisionist power to alter the geopolitical status quo commensurate with its national objectives, utilizing actions that frustrate the status quo power’s efforts to detect, attribute, and respond.¹¹ Hal Brands observes that the goal of a revisionist power in gray zone warfare is to “modify some aspect of the existing international environment” and to reap gains “normally associated with victory in war.”¹² The first step in understanding China’s intent in pursuing a gray zone warfare strategy is to understand the political aims it is trying to achieve. The Chinese Communist Party (CCP) embarked on an ambitious plan, the “Hundred-Year Marathon,” designed to transition communist China from “rule taker to rule maker” by 2049,¹³ requiring strategic patience and opportunistic dexterity.¹⁴ According to a 2016 study by RAND, the CCP’s pursuit of its own security architecture in the Indo-Pacific is meant to serve as a counterbalance—and as an eventual replacement for—the US alliance system in the region.¹⁵ Furthermore, the evolutionary transition from cultural revolution to peaceful modernization has led to an emboldened China proudly flying the banner of scientific socialism.¹⁶ Through gray zone warfare, the CCP is pursuing its strategic objectives by replicating Sun Tzu’s “acme of skill,” where the foe is subdued without a conventional fight.¹⁷ Ultimately, China will compete in the gray zone until it can win a “black and white victory.”¹⁸

Particularly disturbing is the fact that China continues to make strategic gains within the gray zone while incurring few (if any) costs from its coercive actions.¹⁹ By utilizing its so-called Three Warfares doctrine, which calls for manipulating legal, psychological, and media targets, China has in short order undermined international

institutions, unlawfully seized and militarized islands in the South China Sea, set up Air Defense Identification Zones over disputed islands, and subverted the international media—all “without firing a shot.”²⁰ Furthermore, the information domain now plays the “leading role” for Chinese strategy, while the domains of space and cyber are seen as the “commanding heights of strategic competition.”²¹ In cyberspace alone, China accounts for 90 percent of America’s cyberespionage instances.²² Furthermore, according to open-source reporting, China has hacked into 141 companies while stealing intellectual property valued at 0.87–2.61 percent of America’s GDP annually.^{23, 24} These actions may seem like minimal annoyances in their immediacy, but such threats accumulating over months, years, and decades could further China’s pursuit of regional hegemony and challenge the existing liberal world order.

US Strategic Considerations

Strategy is not only about setting political goals; it is about choices—often hard choices—that require prioritization.²⁵ However unpleasant it may sound to Western ears, America’s loss of deterrence toward China, closely coupled with an unwillingness to use compellence to reverse the gains already achieved, could be interpreted as appeasement. This dynamic does not mean that the United States needs to be lulled into playing a tit-for-tat gray zone game, one in which China always gets the first move. Short-sighted US actions with limited objectives constitute tactics masquerading as strategy. However, the United States does not need to entirely rethink the character of its deterrence posture toward China. Decades ago in another era, George Kennan designed his containment strategy against the Soviet Union during the Cold War to be “a long-term policy of firmness, patience, and understanding, designed to keep the Russians confronted with superior strength at every juncture where they might otherwise be inclined to encroach upon the vital interests of a stable and peaceful world.”²⁶

The gray zone as well as the means used within it may have changed the character of deterrence, but the nature of deterrence remains the same. As articulated by Henry Kissinger, “deterrence requires a combination of power, the will to use it, and the assessment of these by the potential aggressor.”²⁷ The White House’s March 2021 *Interim National Security Strategic Guidance* confirms that the United States will “develop capabilities to better compete and deter gray zone actions.”²⁸ Air, space, and cyber power offers attractive options for the United States to do so in concert with other instruments of national power. The options outlined below do not merely seek to increase US military power in the region; they are also designed to sever the connection between China’s actions and its political objectives by exploiting Beijing’s vulnerabilities. Strategic competition requires foresight, patience, and the will to confront this challenge.

Air, Space, and Cyber Application Imperatives

*The United States and its allies must leverage the full range of air, space, and cyber power in proactive ways to create dilemmas and uncertainty for the Chinese government and, if necessary, impose costs. As Michael Mazarr observes: “[T]he central strategic concept of gray zone strategies is to confront their targets with a conundrum.”*²⁹ The imperative for air, space, and cyber power in the gray zone is to create a presence of aircraft, satellites, and/or computer code that may appear limited and measured in application but through which the United States can gain an outsized advantage. Air, space, and cyber power can create a dilemma by presenting a situation in which the adversary becomes an aggressor for responding in an escalatory manner.³⁰ Just as China’s activities in the South China Sea are incremental actions specifically designed to be viewed as trivial in isolation, the United States can also employ air, space, and cyber tools in the Indo-Pacific in a way that does not provoke a Chinese response and is still viewed as legal under international law.

Flexible and Responsive Regional Deterrence

Conventional US military power underpins the traditional tools of statecraft used to maintain the status quo in the Indo-Pacific.³¹ However, China’s Anti-Access/Area Denial (so-called A2/AD) and long-range hypersonic weapons threaten the survivability and effectiveness of conventional forces, with the goal of denying US influence inside the first island chain. The distribution of conventional forces can be achieved through Agile Combat Employment, whereby aircraft can launch, recover, and rearm at forward locations such as partner forces’ airfields, civilian airports, and even long highways.³² By distributing forces throughout the Indo-Pacific and launching more sorties from sanctuary bases such as those in Australia and even India, the United States can increase its avenues of approach to the South China Sea and induce uncertainty into China’s air defense networks. Furthermore, the continued application of the Department of Defense’s (DoD) plans for Dynamic Force Employment in the region will ensure that deployments of aircraft carriers and bombers remain unpredictable to the adversary.³³ As part of this continual rotation, the US Air Force and US Space Force should institute requirements for airmen and guardians to participate in multinational exercises focused on the Indo-Pacific to encourage exposure to the region after two decades of American military involvement in the Middle East.

Operational Preparation of the Environment

US special operations forces are seasoned in the art of special reconnaissance and exploiting unique access and placement. In routine circumstances, Operational Preparation of the Environment (OPE) involves special operations forces conducting activities in a potential operating area to shape the environment.³⁴ In the gray zone, OPE provides US special operators access to create nonattributable disruptions to China's air and space infrastructure located outside Chinese borders. The United States must expand its thinking and actions beyond the Indo-Pacific geographical limits to hold critical Chinese infrastructure at risk anywhere on the globe. Critical to the US ability to surveil CCP-affiliated infrastructure outside the Chinese mainland is the support of host nations, requiring robust and parallel diplomatic efforts. Aviation foreign internal defense teams on officially sanctioned theater engagement missions with partner forces can provide access vectors in places such as Africa and South America in addition to the Indo-Pacific. By gaining unique access and placement on the ground, the US special operators can sow doubt in the integrity of China's air and space infrastructure to create what David Kilcullen characterizes as "internal challenges" designed for distraction.³⁵ The *Interim National Security Strategic Guidance* highlights the imperative for the United States to "maintain the proficiency of special operations forces" even during a shift to strategic competition by focusing on "unconventional warfare missions."³⁶ Using elite special operations forces to conduct OPE is one way in which the United States can capitalize on talents and capabilities honed since 2001 for countering violent extremist organizations.

Resilient Satellite Constellations and Information Operations

Space and cyber power enable the United States to further its political objectives in the information and cognitive domains. In 2020, the US Air Force partnered with SpaceX to test encrypted military internet connectivity using the company's Starlink satellite constellation.³⁷ Space-based internet has several implications for what air and space power can do within the gray zone battlespace. First, because the Starlink constellation will have 4,425 satellites (when fully operational by 2024), it renders Chinese antisatellite weaponry obsolete by saturating low-earth orbit with too many targets that can feasibly be destroyed with direct-ascent antisatellite weapons.³⁸ Next, the US military's encrypted internet communications will enable the connectivity required to conduct Joint All-Domain Command and Control (JADC2) to fuse real-time intelligence regarding Chinese activity across all domains.

Last, and most significant, space-based internet carries the potential to reach millions of Chinese citizens who currently consume information only behind CCP firewalls. One significant barrier to any deep-penetrating information operations in China is censorship controls placed on internet consumption, including software installed on Starlink receiver terminals. A coordinated effort by the international community to clandestinely insert unblocked receiver terminals into China could theoretically enable the United States to provide counternarratives to the CCP's misinformation. Unblocked Starlink receiver terminals in China offer a high-speed, high-bandwidth opportunity to circumvent CCP censorship, deliver Western narratives, and exploit Chinese vulnerabilities in the information domain in areas such as human rights abuses in Hong Kong, Xinjiang, and Tibet.

Air, Space, and Cyber Technology Imperatives

The United States and its allies must develop air, space, and cyber technology to dispel ambiguity, increase attribution, and illuminate malign activity. As Hal Brands observes, China undermines the established international order through “ambiguity and incrementalism.”³⁹ Chinese actions viewed by themselves might seem de minimis, such as the theft of intellectual property from US companies, but in the aggregate they serve to further China's revisionist strategic objectives.⁴⁰

Cyberspace Situational Awareness

One of the primary challenges the United States faces when confronting Chinese activity in the gray zone is closing the information gap between the CCP's version of events and reality on the ground. As Anthony Cordesman of the Center for Strategic and International Studies observes, “information is a powerful weapon against concealment and disinformation,” and the United States has several technological options to that end.⁴¹ To increase attribution for CCP activity, such as human rights abuses and COVID disinformation, the United States could exploit China's existing electronic surveillance state. China's ubiquitous use of facial recognition, social credit scores, and required cellular phone applications such as WeChat provides unique access to internal conditions and decision-making.⁴² Such exploitation could assist with ongoing US efforts to “name and shame” rogue Chinese hackers stealing intellectual property and to expose human rights abuses. Additionally, it would also provide more information so that the United States could choose to publicly release as part of a coordinated effort with partners and allies to illuminate a pattern of malign Chinese activity.⁴³ During conflict, access to the CCP's surveillance state network could potentially help the United States locate and target People's Liberation Army units by monitoring the

online behavior of Chinese military personnel. And finally, the exploitation of China's surveillance state could also allow the United States to measure the effectiveness of counternarrative efforts spread through the space-based internet.

Aircraft Optimized for Gray Zone Activity

While conventional aircraft designed for high-end operations in major war underpin US conventional deterrence in the region, they are generally expensive to operate, require longer runways, and carry with them the potential for increased escalation. A fleet of smaller, lighter, and cheaper aircraft could perform reconnaissance, logistics, and infiltration missions in the Indo-Pacific with a lower risk of detection.⁴⁴ Shorter runways and island beaches enable such aircraft to covertly insert or extract small teams, place sensors, collect signals from adversary activity without a noticeable military presence, and even carry weapons.⁴⁵ Both manned and unmanned aircraft with a civilian design could hide in plain sight among other aircraft at nonmilitary airports of partner nations. By effectively "flooding the zone" with a sustainable fleet to augment traditional conventional aircraft, the United States could force China to suffer from what David Kilcullen calls a "bandwidth problem."⁴⁶

Nonlethal Innovations to Confront Aggression

China's continual use of military assets to bolster its territorial expansion for economic advantage presents a quandary for US forces. If the United States does not protect the territorial and economic sovereignty of its partners and allies in the region, then it loses credibility. At the same time, if the United States responds kinetically, it risks escalation and appearing like the aggressor.⁴⁷ Chinese ships and aircraft routinely challenge freedom of navigation in places such as the South China Sea. Chinese aircraft have conducted provocative training missions off the coast of Borneo, where China and Malaysia have overlapping territorial claims.⁴⁸ Provocative actions such as these are designed to probe the responsiveness of US capabilities in the region and test the resolve of our alliances and partnerships. In these situations, nonlethal capabilities could allow the United States and its allies to enforce sovereignty and freedom of navigation while avoiding the dangers of escalation and the miscalculations that any loss of life could trigger.⁴⁹ Technological innovations such as directed energy, when used in a nonlethal manner, could be employed to disable a ship's powerplant or render an aircraft's onboard systems unusable. Deescalatory action with these tools could force vessels or aircraft to disengage from their malign activity and return to their ports or bases safely. Ultimately, nonlethal innovations increase the options available policy makers and commanders in the field when they are forced to confront provocative Chinese actions designed to elicit a response.

Air, Space, and Cyber Organizational Imperatives

The United States must orient a portion of its air, space, and cyber forces to frustrate China's coercive gradualism. Those in the top tier of the US military establishment are deeply entrenched with planning the next generation of warfighting. The Third Offset Strategy, JADC2, and the All-Domain Operations Joint Warfighting Concept are designed to ensure that the United States regains its technological edge, fights from a shared situational awareness platform, and is able to operate in “information-based wars using enormous amounts of fast computer analysis across the land, air, sea, space and cyberspace domains.”⁵⁰ There is a comparative lack of discussion focused on how to organize for gray zone competition. The DoD is making progress in organizing air, space, and cyber forces for this competition, even if current efforts are piecemeal. Due to the importance of space, cyber, and information operations in both gray zone and high-end warfare, the time has come for the DoD and other government stakeholders to undertake a comprehensive mission portfolio and service responsibility review. The modern military has seen many organizational transformations, beginning with the National Security Act of 1947 and subsequent reorganization efforts in 1949, 1953, and 1958—culminating in the Goldwater-Nichols Act of 1986.⁵¹ Similarly, the US military establishment of the twenty-first century must evolve its organizational construct to account for the advent of new warfighting domains and the changed character of war—including gray zone warfare considerations.

Prioritized and Dedicated Space Cadre

The prioritization of space as a warfighting domain has spurred the United States into taking bold but necessary steps in professionalizing a dedicated space cadre. The creation of the US Space Force, a joint space development agency, and a Geographic Unified Combatant Command focused on space, will help ensure that the United States is organized to compete in this vital domain.⁵² Moreover, the United States will now have space professionals dedicated to organizing, training, and equipping space guardians, developing next-generation space capabilities, and remotely operating in the space and counterspace arena.

Cyber Organizational Transformation

Cyberspace has similarly been declared a warfighting domain but has yet to have its windfall organizational transformation. From 1998 onward, the DoD's cyber organizations have evolved into what is today the Unified Functional Combatant Command known as US Cyber Command (USCYBERCOM), with the Air Force, Marines, Navy, and Army acting as force providers as well as cyber

service components.⁵³ Currently, USCYBERCOM's Cyber Mission Forces have approximately 5,000–6,000 personnel spread across 133 teams supporting joint operations and combatant commanders. Not only are these forces considered to be in the low-density, high-demand category; the detachment of cyber professionals from the rest of the joint force inevitably results in cyber planning and operations remaining in relative obscurity.⁵⁴ The DoD's expertise in cyber is maturing, and the concern now is the rate of maturation and scale. Finally, without a dedicated cyber service providing both functional expertise and the organizing, training, and equipping role, cyber forces will remain reliant on the four services with cyber missions. A cyber service solves the prioritization dilemma because each service's primary mission domain takes precedence. However, the creation of a sixth military service could create additional bureaucratic hurdles and further inhibit the United States from responding to gray zone activity quickly. Therefore, given the relatively small size of the DoD's cyber and space cadres, it would be prudent to merge these professionals together into one service focused on remote warfighting in a digitally networked environment.

Information Environment Fusion

The USAF has subtly postured itself to compete in the gray zone with China. The activation of the Sixteenth Air Force took place in October 2019 and, with it, the Air Force's first operational unit dedicated to information warfare was created.⁵⁵ The Sixteenth is composed of 44,000 airmen spread across 10 wings and 178 squadrons, fusing the Air Force's global Intelligence, Surveillance, and Reconnaissance (ISR), electronic warfare, cyber, targeting, and information operations missions.⁵⁶ Placed squarely in the information environment, the mission of the Sixteenth Air Force is to “integrate information warfare by creating dilemmas for adversaries in competition, and if necessary, future conflicts.”⁵⁷ The Air Force perceives this unit to be on the front lines in the gray zone competition with China.⁵⁸ Additionally, given traditional airpower's inherent strengths as both a flexible military arm and deterrent force, the USAF should ensure that a robust complement of airpower is postured in the Indo-Pacific. With an adequate force posture, the Air Force could actively compete in the gray zone by conducting air policing in the East and South China Seas, ISR operations, and shows of force through exercises focused on adaptive basing and multilateral large-scale force employment.⁵⁹

Partners and Allies in the Indo-Pacific

As Michael Green recently noted in *Foreign Affairs*, many countries in the Indo-Pacific struggle to resist China's attempted economic and military coercion.⁶⁰ Any air,

space, and cyber initiatives must involve close coordination with allies and partners in the region. These initiatives must seek to reaffirm common values among allies and partners without imposing undue costs and increasing risks for those nations.⁶¹ A model for this kind of coordination is the Pacific Defense Initiative (PDI), which funds deterrence-related security cooperation and allocates resources to defense infrastructure programs that can help make countries in the region more resilient in the face of Chinese economic pressure.⁶² In a departure from normal weapons and defense program procurement, PDI ensures investments in important programs that have no natural constituency, such as missile defense for Indo-Pacific countries. A similar model could be used to fund the needed air, space, and cyber imperatives in conjunction with partners and allies in the region.

Fortunately for the United States, nations throughout the Indo-Pacific region are increasingly viewing China as an imminent threat and are taking steps to balance the scales. While gray zone strategies can achieve significant short-term gains, the irony is that their reliance on long-term, patient, and gradual strategies can backfire.⁶³ China could very well end up isolated in its own backyard if its coercive tactics continually build resentment throughout the region. Furthermore, a clear benefit for the United States is that many of the nations throughout the region share the goal of a free and open Indo-Pacific that values sovereignty, economic growth, international law, and fair competition in accordance with the US State Department's 2019 vision.⁶⁴ The United States should take advantage of this to strengthen bilateral relationships and to build a flexible, resilient network of like-minded security partners.⁶⁵ These networks could look like what Michael Green calls "hub-and-spoke" between formal allies or "spoke-to-spoke" between nontraditional partners in the region such as Vietnam to increase connectivity.⁶⁶ While long-term allies such as Japan and Australia should form the backbone of any coalition, partnerships with nations such as Sri Lanka and Bangladesh should also be strengthened.

Conclusion

Traditional armed conflict in the Indo-Pacific between the United States and China is not inevitable. Air, space, and cyber power offers unique value to a whole-of-government approach to gray zone competition with the goal of maintain the status quo in the region. The United States must apply new ideas, innovate new technology, and reorganize its forces to meet the gray zone's imperatives. Each of these imperatives resides in I. B. Holley's classic framework of ideas (*application*), tools (*technology*), or groups (*organization*). These air, space, and cyber imperatives contribute to a larger effort to compete with China below the threshold of armed conflict. ❁

Maj Joseph Tomczak

Major Tomczak is a special operations pilot in the US Air Force, currently assigned as a student at the School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama. He is a graduate of the US Air Force Academy and the George Washington University's Elliott School of International Affairs.

Maj Nicholas Torroll

Major Torroll is an intelligence officer in the US Air Force, currently serving as the political-military affairs adviser to the commander, NATO Allied Air Command, Ramstein Air Base, Germany. He is a graduate of the University of Northern Colorado and the University of Oklahoma.

Maj Bedri Kaloshi

Major Kaloshi is a helicopter pilot in the Albanian Air Force, where he serves as a medical and casualty evacuation crew commander at Farka Air Base, Republic of Albania. He is a graduate of the Albanian Air Force Academy (*Shkollës së Aviacionit*).

Notes

1. ADM Philip S. Davidson, "Statement before the Senate Armed Services Committee on US Indo-Pacific Posture" (Washington, DC: US Senate, 2019).
2. Davidson, "Statement before the Senate Armed Services Committee," 15.
3. Irving Brinton Holley Jr., *Ideas and Weapons*, Air Force Historical Office (New York: Yale University Press, 1953).
4. Nadia Schadlow "It's a Gray, Gray World," *Naval War College Review* 73, no. 3 (Summer 2020): 140.
5. Hal Brands, "Paradoxes of the Gray Zone," National Security Program Report (Philadelphia: Foreign Policy Research Institute, 5 February 2016), 5.
6. Brands, "Paradoxes of the Gray Zone," 5.
7. Peter Pomerantsev, "Fighting While Friending: The Grey War Advantage of ISIS, Russia, and China," *The Atlantic*, 29 December 2015, 3.
8. Brands, "Paradoxes of the Gray Zone," 3.
9. Brands, "Paradoxes of the Gray Zone,"; and Robert Latiff, *Future War: Preparing for the New Global Battlefield* (New York, NY: Alfred A. Knopf, 2017), 21.
10. David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York: Oxford University Press, 2020), 163.
11. Professor Hal Brands of John Hopkins University in James R. Holmes and Toshi Yoshihara, "Deterring China in the 'Gray Zone': Lessons of the South China Sea for US Alliances," *Foreign Policy Research Institute*, 11 May 2017.
12. Brands in Holmes and Yoshihara, "Deterring China in the 'Gray Zone,'" 3.
13. Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt, 2015), 12.
14. Goeff Dyer, *The Contest of the Century: The New Era of Competition with China—and How America Can Win* (New York: Borzoi Book, 2014), 7.
15. Timothy R. Heath, Kristen Gunness, and Cortez A. Cooper, "The PLA and China's Rejuvenation: National Security and Military Strategies, Deterrence Concepts, and Combat Capabilities," RAND Corporation, 2016, <https://www.rand.org/>.

16. Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era" (Beijing, 18 October 2017), 3.
17. Sun Tzu, *The Art of War*, trans. Samuel Griffith (New York: Oxford University Press, 1963), 77.
18. Holmes and Yoshihara, "Deterring China in the 'Gray Zone,'" 6.
19. Holmes and Yoshihara, "Deterring China in the 'Gray Zone,'" 3.
20. Peter Pomerantsev, "Fighting While Friending: The Grey War Advantage of ISIS, Russia, and China," 2; Holmes and Yoshihara, "Deterring China in the 'Gray Zone,'" 3; and Thomas Christensen, *The China Challenge: Shaping the Choices of a Rising Power* (New York: W. W. Norton, 2015), 263.
21. M. Taylor Fravel, *Active Defense: China's Military Strategy since 1949* (Princeton, NJ: Princeton University Press, 2019), 231.
22. Pillsbury, *The Hundred-Year Marathon*, 221.
23. Dyer, *The Contest of the Century*, 26.
24. Joseph W. Sullivan, "From the Chartroom: The Cost of China's Intellectual-Property Theft," *National Review*, 10 July 2020, <https://www.nationalreview.com>.
25. Kilcullen, *The Dragons and the Snakes*, 15.
26. John Lewis Gaddis, *George F. Kennan: An American Life* (New York: The Penguin Press, 2011), 245.
27. Henry Kissinger, quoted in Holmes and Yoshihara, "Deterring China in the 'Gray Zone,'" 5.
28. President of the United States, *Interim National Security Strategic Guidance*, (Washington, DC: The White House, March 2021), 14.
29. Michael J. Mazarr, "Mastering the Gray Zone: Understanding a Changing Era of Conflict" (Carlisle Barracks, PA: United States Army War College Press, 2015), 61, <https://publications.armywarcollege.edu>.
30. Mazarr, "Mastering the Gray Zone," 61.
31. Mazarr, "Mastering the Gray Zone," 48.
32. Valerie Insinna, "The US Air Force Has Unconventional Plans to Win a War in the Asia Pacific," *Defense News*, 10 February 2020, <https://www.defensenews.com>.
33. Tyson Wetzel, "Dynamic Force Employment: A Vital Tool in Winning Strategic Global Competitions," *Real Clear Defense*, 18 September 2018, <https://www.realcleardefense.com>.
34. Joint Chiefs of Staff, Joint Publication 3-05, *Special Operations*, 22 September 2020.
35. . Kilcullen, *The Dragons and the Snakes*, 248.
36. President of the United States, *Interim National Security Strategic Guidance*, 14.
37. Grett Tingley, "The Air Force and SpaceX Are Teaming Up for a 'Massive' Live Fire Exercise," *The Drive*, 25 February 2020, <https://www.thedrive.com>.
38. Chris Horn, "Could Constellations of Mini-satellites Prevent the Splintering of the Internet?" *Irish Times*, 16 January 2020, <https://www.irishtimes.com>.
39. Brands, "Paradoxes of the Gray Zone," 6.
40. Anthony H. Cordesman and Grace Hwang, "Chronology of Possible Chinese Gray Area and Hybrid Warfare Operations," working draft CSIS Report (Washington, DC: Center for Strategic and International Studies, September 2020), 32, <https://csis-websiteprod.s3.amazonaws.com>.
41. Cordesman and Grace Hwang, "Chronology," 9.
42. Kilcullen, *The Dragons and the Snakes*, 245.
43. Cordesman and Hwang, "Chronology," 9.

44. Kilcullen, *The Dragons and the Snakes*, 248.
45. Mike Pietrucha and Jeremy Renken, "Blurring The Lines Part III: Airpower Applications In The Gray Zone," *War on the Rocks*, 18 April 2019, <https://warontherocks.com>.
46. Kilcullen, *The Dragons and the Snakes*, 249.
47. Mazarr, "Mastering the Gray Zone," 71.
48. AFP News, "China Says Military Flight Off Malaysia Was Routine Training," *France 24*, 6 February 2021, <https://www.france24.com>.
49. Michael O'Hanlon, "China, The Gray Zone, and Contingency Planning at the Department of Defense and Beyond," CSIS Report (Washington, DC: Center for Strategic and International Studies, September 2019), 7, <https://www.brookings.edu>.
50. Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W.W. Norton, 2018), 59; Theresa Hitchens, "J6 Says JADCS Is a Strategy; Service Posture Reviews Coming," *Breaking Defense*, 4 January 2021, <https://breakingdefense.com>.
51. James R. Locher III, *Victory on the Potomac: The Goldwater-Nichols Act Unifies the Pentagon* (College Station: Texas A&M University Press, 2002), 29.
52. Everett C. Dolman, "Space Force Déjà Vu," *Strategic Studies Quarterly* 13, no. 2 (Summer 2019): 16.
53. United States Cyber Command, "US Cyber Command History," <https://www.cybercom.mil>.
54. Lt Gen Charles L. Moore, "Cyber Security" (Lecture, Air Command and Staff College, Maxwell AFB, 14 December 2020).
55. "Sixteenth Air Force (Air Forces Cyber)," 27 August 2020, <https://www.16af.af.mil>.
56. Lt Gen Timothy Haugh, "16th Air Force, AF Cyber, & Joint Force-HQ-Cyber" (Interview, Aerospace Nation, Mitchell Institute of Aerospace Studies, 15 July 2020).
57. "Sixteenth Air Force (Air Forces Cyber)."
58. Haugh, interview.
59. Patrick Mills et al., "Building Agile Combat Support Competencies to Enable Evolving Adaptive Basing Concepts," RAND Corporation, 2020, <https://www.rand.org>.
60. Michael Green, "Can America Restore Its Credibility in Asia?" *Foreign Affairs*, 15 February 2021, <https://www.foreignaffairs.com>.
61. Green, "Can America Restore Its Credibility in Asia?"
62. Green, "Can America Restore Its Credibility in Asia?"
63. Mazarr, "Mastering the Gray Zone," 88–89.
64. Michael R. Pompeo, "A Free and Open Indo-Pacific: Advancing a Shared Vision," (Washington, DC: US Department of State, 2019), 5.
65. Pompeo, "A Free and Open Indo-Pacific," 8.
66. Green, "Can America Restore Its Credibility in Asia?"

Disclaimer

The views and opinions expressed or implied in *JIPA* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Department of the Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government or their international equivalents.