REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
8 April 2022	FINAL	

4. TITLE AND SUBTITLE

Competing and Winning: A Framework to Conduct Information Operations in the Gray Zone

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Spencer W. Schardein, USAF

Paper Advisor: Professor John M. Sappenfield, USMC

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)
Maritime Advanced Warfighting School
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Director, Maritime Advanced Warfighting School (MAWS)
686 Cushing Road
Newport, RI 02841-1207

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES
A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department and the Maritime Advanced Warfighting School (MAWS). The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC, the Department of the Navy, or the Department of the Air Force.

14. ABSTRACT

Competing and Winning: A Framework to Conduct Information Operations in the Gray Zone

Over the last two decades, China's continued exploitation of the space between competition and conflict, known as the gray zone, threatens international order and the rule of law. Although addressing China's malign activities in the gray zone will require an interagency approach, the U.S. military can leverage information operations to identify, expose, and counter Chinese gray zone actions. While the DoD lacks a gray zone doctrine and strategy, this paper utilizes existing joint doctrine to provide a framework for the joint staff to conduct information operations against Chinese gray zone activities. By establishing lines of effort based on Chinese gray zone trends, conceptualizing the information environment, identifying target audiences, and applying information-related capabilities, the joint staff gains an initial planning construct to integrate information operations with other gray zone military operations.

15. SUBJECT TERMS
Gray Zone, Information Operations, Gray Zone Framework, China Gray Zone, Information Warfare

16. SECURITY CLASSIFICATION OF: UNCLASSIFIED			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Director, MAWS
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED		26	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-6149

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE

Newport, RI

Competing and Winning: A Framework to Conduct Information Operations in the Gray Zone

By

Spencer Schardein

Maj/ USAF

Word Count: 4564

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Maritime Advanced Warfighting School.

The contents of this paper reflect my personal views and are not necessarily endorsed by the Naval War College, the Department of the Navy, or the Department of the Air Force.

Signature: _____

Date: 8 April 2022

Contents

List of Illustrations

Abstract

Competing and Winning: A Framework to Conduct Information Operations in the Gray Zone

Over the last two decades, China's continued exploitation of the space between competition and conflict, known as the gray zone, threatens international order and the rule of law. Although addressing China's malign activities in the gray zone will require an interagency approach, the U.S. military can leverage information operations to identify, expose, and counter Chinese gray zone actions. While the DoD lacks a gray zone doctrine and strategy, this paper utilizes existing joint doctrine to provide a framework for the joint staff to conduct information operations against Chinese gray zone activities. By establishing lines of effort based on Chinese gray zone trends, conceptualizing the information environment, identifying target audiences, and applying information-related capabilities, the joint staff gains an initial planning construct to integrate information operations with other gray zone military operations.

Introduction

In the post-Cold War era, the United States (U.S.) national security apparatus embraced the emerging status quo, which favored clear doctrinal delineations between war and peace. Over the last two decades, the Department of Defense (DoD) has predominantly focused on counterinsurgency and irregular warfare as the two primary national security concerns in the Global War on Terror (GWoT). With the 2018 *National Security Strategy*, the DoD has pivoted to address Great Power Competition (GPC) with peer and near-peer rivals, namely Russia and China, as the pacing-threat challenges to national security domestically and abroad. In this new era, the traditionally bipolar definitions of war and peace have given way to a broader "carrier concept" for the gray zone between competition and conflict.[1]

Over the last two decades, China has exploited the gray zone in the Indo-Pacific to avoid open conflict while making strategic advancements in all domains.[2] China's gray zone activities, coupled with its rapidly expanding military capacity, threaten to upend the rule of law and the ability to maintain a free and open Indo-Pacific. While the U.S. requires a whole of government approach to synergize effects against Chinese gray zone activities, the U.S. military's role is paramount to the government's effort due to the DoD's persistent presence throughout the Indo-Pacific. Currently, the joint force lacks a unified strategy and doctrine to address gray zone challenges; however, the joint force's use of information operations provides an impactful method to delegitimize and discourage China's malign activities.

The joint force requires a robust framework to conduct information operations to identify, expose, and counter Chinese gray zone actions. To begin planning for information

[1] Charles R. Burnett et al., *Outplayed: Regaining Strategic Initiative in the Gray Zone* (Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2016), 3.
[2] Burnett et al, 37.

operations, the joint force must first establish lines of effort and objectives for information operations to address functional trends of Chinese gray zone activities. Next, to further refine planning estimates, the information and influence relational framework provides an initial structure for the joint force to conceptualize the information environment and identify the target audience to apply information operations. Lastly, by selecting information-related capabilities to target designated audiences, the joint force is postured to integrate information operations against Chinese gray zone actions.

Gray Zone Background

In the gray zone, "the uncomfortable conceptual no man's land for strategists and military planners," U.S. opponents deliberately seek opportunities to exploit the threshold of armed conflict and test the responsiveness of U.S. policy.[3] As the DoD lacks a doctrinal approach to gray zone operations, operational commanders and their staff must be deliberate in synergizing unified responses across components within Geographic Combatant Commands (GCCs) to avoid inadvertent escalation, yielding control of U.S. interests, or eroding redlines.[4] The gray zone has emerged as the fundamental competition space in GPC.

There are three intrinsic characteristics present in all gray zone contests. The first characteristic of gray zone contests is the inherent hybrid combination of adverse methods and strategic effects.[5] Gray zone operations thrive in a deliberately hybrid environment that affects all instruments of national power and all domains.[6] Hybridity allows gray zone operations to have more significant ambiguity between war and peace and complicates decision-making for

---

[3] Burnett et al, 37.
[4] Burnett et al, 37.
[5] Burnett et al, 4.
[6] Nathan P. Freier, "The Darker Shade of Gray: A New War Unlike Any Other," The Darker Shade of Gray: A New War Unlike Any Other | Center for Strategic and International Studies, September 12, 2014, https://www.csis.org/analysis/darker-shade-gray-new-war-unlike-any-other, 2.
.

political and military leaders. Furthermore, gray zone operations can avoid provoking established domain-specific redlines by obfuscating the cumulative effects of multiple adversarial lines of effort by intersecting multiple domains and instruments of power.

The second characteristic common in all gray zone contests is their direct and deliberate impediment to normalized military conventions.[7] Gray zone actions thrive outside traditional military frameworks by achieving wartime objectives without inciting a military response. Commanders and staffs have difficulty conceptualizing planning actions to address these "wicked" problems; thus, planning actions are often delayed or never implemented in time to respond to an adversarial action.[8]

The third characteristic present in all gray zone challenges is risk confusion, which delays U.S. military and political decision-making to counter the action.[9] The gray zone paralyzes risk analysis for U.S. decision-makers as both action and inaction carry similarly undesirable risks. If U.S. decision-makers respond to gray zone actions, political and military leadership must simultaneously factor in the potential risk of escalation or appeasement with near-peer rivals. China, one of the two most prominent proponents of gray zone activities, exploits this risk boundary to achieve de facto victories below the threshold of armed conflict.[10]

Information Operations Lines of Effort and Objectives

To begin planning for information operations, the joint force must first establish lines of effort (LOEs) and objectives for information operations to meet functional trends of Chinese gray zone activities. The Center for Strategic and International Studies, the leading U.S. think tank analyzing gray zone actions, identifies seven primary areas for coercive activities within the

[7] Burnett et al, 4.
[8] Burnett et al, 4.
[9] Burnett et al, 4.
[10] Freier, 3.

gray zone.[11] Known as the "Gray Zone Toolkit," these seven functional areas are information operations and disinformation, political coercion, economic coercion, cyber operations, space operations, proxy support, and provocation by state-controlled forces.[12] While China chooses to employ all seven tools against U.S. interests in the gray zone, provocation by state-controlled forces, economic coercion, cyber operations, and space operations are the four most commonly used and thus are best to focus against for military information operations.

LOE 1 – Identify and Counter Provocation by State-Controlled Forces

China's most blatant activity in the gray zone is its island-building campaign in the South China Sea (SCS), where China aims to erode the international order and norms.[13] In 2013, China began aggressive ocean dredging and developed artificial islands in the Spratly and Paracel Island chains.[14] The new landmasses and buildings covered 3,200 acres and included radar systems, surface-to-air missiles, and fighter aircraft suitable runways to project power forward in the SCS.[15] To assist in enforcing their actions, the Chinese relied on their Coast Guard and the People's Armed Forces Maritime Militia (PAFMM), disrupting the maritime fishing industry.[16] While China's actions were provocative in challenging existing sovereignty rights in the SCS, the U.S. response has thus far failed to employ information operations effectively to delegitimize China's actions.[17]

---

[11] Kathleen H. Hicks and Melissa Dalton, *By Other Means: Part II, Adapting to Compete in the Gray Zone* (Washington, D.C: Center for Strategic and International Studies, 2019), 2.
[12] Hicks and Dalton, 2.
[13] Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM: National Defense University* 7, no. 4 (January 1, 2018): pp. 30-47, 33.
[14] Alice Hunt Friend and Kathleen H. Hicks, *By Other Means: Part I, Campaigning in the Gray Zone* (Washington, D.C.: Center for Strategic & International Studies, 2019), 7.
[15] Friend and Hicks, 7.
[16] Friend and Hicks, 7.
[17] Friend and Hicks, 8.

The DoD's *Asia-Pacific Maritime Security Strategy* identifies three primary maritime objectives, "safeguard freedom of the seas; deter conflict and coercion; and promote adherence to international law and standards."[18] While direct military operations to force China's return to the status quo likely risk significant escalation, the objective of information operations is to delegitimize further Chinese expansion efforts in the SCS.[19] By reinforcing adherence to international law and standards and messaging U.S. commitment to safeguarding freedom of the seas, the joint force can apply information operations in concert with freedom of navigation and security assistance operations to strengthen the deterrence of Chinese actions.

LOE 2 – Identify and Expose Chinese Economic Coercion

China employs economic coercion in the gray zone through various means and in multiple domains. China's chief method of economic coercion is Xi Jinping's Belt and Road Initiative (BRI).[20] While some aspects of the BRI exist due to China's surplus in domestic industrial capacity, China also leverages the BRI to shape opinions of other countries' interests and engages in debt-trap diplomacy to acquire foreign land for dual-use military developments.[21] In 2018, China forced Sri Lanka to surrender the Port of Hambantota after failing to make debt payments.[22] Eight other countries also risk losing infrastructure due to China's predatory lending.[23] China is also pursuing the Digital Silk Road initiative to market key Chinese technology; however, this initiative has also come under scrutiny for its malign motives.[24] In

---

[18] U.S. Department of Defense. *The Asia-Pacific Maritime Security Strategy: Achieving U.S. National Security Objectives in a Changing Environment*. Washington, D.C., 2015, 1.
[19] Michael J. Green et al., Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence (Washington, D.C.: Center for Strategic & International Studies, 2017), 119.
[20] Friend and Hicks, 8.
[21] Friend and Hicks, 8.
[22] William C. Pacatte, "Be Afraid? Be Very Afraid? — Why the United States Needs a Counterstrategy to China's Belt and Road Initiative," *Defense360*, October 19, 2019, 4.
[23] Pacatte, 4.
[24] Friend and Hicks, 9.

2019, the U.S. banned the Chinese 5G company Huawei due to concerns that its technology was a cover for Chinese espionage and intelligence gathering.[25]

The joint force can employ information operations to identify and expose Chinese malign economic actions within the Indo-Pacific. The 2018 *National Defense Strategy* stipulates that a critical focus area of the DoD is to support the interagency objective to counter coercion and subversion.[26] The joint force can leverage its persistent presence in the region to assist in identifying dual-use infrastructure under the BRI umbrella. Furthermore, in areas of contested access, U.S. Special Operations Forces (SOF) can further assist in identifying and exposing Chinese malicious economic activity. One key SOF initiative is exploring the use of human-machine teaming and swarming data collection to source indicators of Chinese intentions to build dual-use infrastructure. By leveraging commercial off-the-shelf decryption exploitation, SOF operators have been able to identify open-source Chinese indicators to build dual-use infrastructure under the BRI umbrella two years prior to the project breaking ground.[27] By applying this technology with targeted information operations, the joint force can expose Chinese malign economic coercion and set conditions to discourage further action.

LOE 3 – Expose and Counter Chinese Malign Cyber Operations

China is the most malicious of gray zone actors within the cyberspace domain. Through non-attributional cyber operations, China targets other states' infrastructure, conducts espionage, and disrupts political processes with impunity.[28] By accessing U.S. government networks and stealing intellectual property, China has kept pace and, in some areas, surpassed U.S.

---

[25] Friend and Hicks, 9.
[26] James Mattis. *Summary of the 2018 National Defense Strategy of the United States of America*. Washington D.C., 2018, 5.
[27] Major Joshua K. Martin (HAF A5/7S), email interview with the author, February 2022.
[28] Friend and Hicks, 8.

technological developments. In recent years, China has launched denial-of-service (DoS) attacks and attempted to infiltrate U.S. companies such as General Electric, Boeing, and T-Mobile.[29] Although cyber operations slowed in 2015, in the wake of more recent economic sanctions, China has resumed cyber operations with a greater degree of sophistication to complicate attribution.[30] While the traditional U.S. military response has been to increase security measures to protect critical data systems, limited information operations have successfully deterred Chinese actions.

In 2015, in response to Chinese cyber operations, the U.S. Cyber Command (CYBERCOM) was able to identify the origins of several Chinese cyber-attacks. In response, the U.S. government began a "naming and shaming" information campaign in concert with the threat of economic sanctions.[31] Consequently, the U.S. and China signed a bilateral agreement to cease state-sponsored cyber-attacks. One key CYBERCOM imperative is to "create information advantages to support operational outcomes and achieve strategic impact."[32] In response to adversarial disinformation campaigns during the 2018 midterm elections, CYBERCOM and the National Security Agency (NSA) reduced disinformation by shutting down adversarial cyber access on election day.[33] By pairing information operations with defensive cyber operations to expose Chinese intentions, the joint force can decrease the legitimacy of China's cyber actions and promote greater security for partners and allies.

---

[29] Friend and Hicks, 8
[30] Nicole Perlroth, "Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies," The New York Times (The New York Times, February 18, 2019), https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html.
[31] Friend and Hicks, 8.
[32] Paul M. Nakasone. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command.* Fort Meade, Maryland, 2018, 9.
[33] Hicks and Dalton, 21.

LOE 4 – Expose and Counter Chinese Malign Space Operations

The space domain has evolved into a susceptible environment for gray zone operations. Due to the vastness of space and the reliance on space technologies in both civilian and military sectors, China has been able to gain traction in space to exploit U.S. weaknesses incrementally.[34] Chinese malign actions in space are often difficult to attribute directly to China and are selectively activated, complicating U.S. response options.[35] Chinese systems, such as spoofers, jammers, and dazzlers, can deny U.S. communication, early warning, and navigation systems yet subsist by not tripping redlines that provoke an escalation response.[36] Over time and without a response, China's continued space disruptions will establish a new status quo that will diminish U.S. space-enabled capabilities.

As with malign Chinese cyber actions, information operations can contribute to exposing and countering Chinese malign space operations. The U.S. Space Force, in concert with U.S. Space Command, has been working on three priorities based on the 2020 *Defense Space Strategy* to "maintain space superiority; provide space support to national, joint, and combined operations; and ensure space stability."[37] As the DoD bolsters its space defense capabilities and gains better awareness within the space domain, information operations can delegitimize China's actions and impose the risk of escalation on Chinese leadership. If China decides to continue its actions, the U.S. retains an ability to intensify its information campaign to encourage partners and allies to decrease or cease their interactions with the Chinese National Space Administration (CNSA), thus imposing higher costs on continued malicious activity.

---

[34] Hicks and Dalton, 19.
[35] Hicks and Dalton, 19.
[36] Hicks and Dalton, 19.
[37] U.S. Department of Defense. *Defense Space Strategy Summary.* Washington, D.C., 2020, 2.

To organize the joint force's robust employment of information operations to identify, expose, and counter Chinese gray zone actions, the joint force must first establish objectives and LOEs for information operations to address Chinese gray zone operational trends. Matched against Chinese trends, the four LOEs are: *1) Identify and Counter Provocation by State-Controlled Forces, 2) Identify and Expose Chinese Economic Coercion, 3) Expose and Counter Chinese Malign Cyber Operations, and 4) Expose and Counter Chinese Malign Space Operations*. Each of these LOEs, and their associated military objectives, provide desired outcomes to apply the information and influence relational framework.

Information and Influence Relational Framework

The information and influence relational framework provides an initial structure for the joint force to conceptualize the information environment and identify the target audience to apply information operations. The Joint Publication 3-13 *Information Operations* describes the information and influence relational framework and provides a foundation for the joint force to apply information operations.[38] By applying the framework to the established lines of effort and objectives addressing Chinese gray zone actions, the joint force can further refine how information operations can impact Chinese gray zone actions.

The Information Environment

This framework begins by first understanding and analyzing the critical aspects of the information environment (IE). The IE is "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."[39] Within the IE, there are three

[38] U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013, VI-3.
[39] U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013, I-1.

dimensions, the physical, informational, and cognitive dimensions.[40] The physical dimension comprises the leadership, the command and control (C2) systems, and the supporting hardware to enable information interaction, such as computers, books, and smartphones.[41] The informational dimension comprises "where and how information is collected, processed, stored, disseminated, and protected," such as the U.S. military's Non-Classified Internet Protocol Router Network (NIPRNet).[42] The cognitive dimension encompasses "the minds of those who transmit, receive, and respond to or act on information."[43] This dimension is the most important and accounts for how people interpret their information based on human factors such as beliefs, norms, emotions, education, and ideologies.[44]

Applied to the Chinese gray zone activities, analyzing the information environment is critical to understanding the lens that China and its people use to interpret the world. In the cognitive dimension, China has embraced a culture of Sino-centrism, with China as the cultural center of the world.[45] Coupled with the "century of humiliation" where the Chinese people saw their culture destroyed by multiple wars and outsider influence, China's leadership has turned to a new age of economic reform.[46] In the physical dimension, Chinese leadership highly values the preservation of the communist party and the continued economic rise of China. China's rapidly growing economy is the second-largest globally and is on track to surpass the U.S. by 2026.[47]

---

[40] U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013, I-2.
[41] U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013, I-2.
[42] U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013, I-3.
[43] U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013, I-3.
[44] U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013, I-3.
[45] Burnett et al, 35.
[46] Burnett et al, 35.
[47] Burnett et al, 36.

Lastly, in the information dimension, China employs a high degree of state censorship and control over outside information available to the Chinese population; thus, the ability to target the Chinese population with information operations may be difficult.

Selecting the Target Audience

After conceptualizing the IE, the next step is to identify the target audience (TA) and understand how that audience interprets their environment based on rules, norms, and beliefs.[48] Each of the three IE dimensions provides access points to influence the TA. Planners should select TAs based on how influencing that audience will ultimately affect the desired end state. As each potential TA might perceive their environment differently, it is essential to develop an understanding of each audience's rules, norms, and beliefs. The goal of information operations is to influence how the TA interacts with their respective rules, norms, and beliefs.[49] As beliefs are generally fundamental truths that influence behavior and exist across social systems, they are often difficult to change.[50] In analyzing China's gray zone actions, although some TAs will overlap across the joint force's LOEs, it is vital to analyze the TA within each gray zone LOE.[51]

LOE 1) Identify and Counter Provocation by State-Controlled Forces

Supporting the military objectives to safeguard the freedom of the seas and promote adherence to international laws and standards, the information objective for this LOE is to delegitimize Chinese expansion efforts in the SCS. The TAs for these information operations are the Chinese political leadership and the state-controlled forces. Ultimately, the goal of this LOE

---

[48] U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013, I-5.
[49] U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013, I-5.
[50] U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013, I-5.
[51] While this preliminary analysis is helpful to frame the gray zone problem, the joint force will need to accomplish a further analysis of the rules, norms, and beliefs of each TA during joint planning.

is to convince Chinese political leadership and state-controlled forces that state sovereignty will be respected, upheld, and enforced within the SCS. The intent is not to subjugate China's industry needs in the SCS but to promote an environment that benefits all users based on internationally recognized territorial boundaries and norms. By focusing on producing effects that modify how Chinese political leadership and state-controlled forces accept rules and norms, the joint force can use information operations to promote adherence to international laws and standards while safeguarding freedom of the sea.

LOE 2) Identify and Expose Chinese Economic Coercion

Supporting the interagency objective to counteract coercion and subversion, the joint force can identify Chinese dual-use infrastructure and use information operations to expose Chinese coercive practices and subversive intentions. The desired objective of the information operations for this LOE is to discourage China from continuing coercive economic activities while protecting U.S. partners and allies. The TAs for these information operations are China's political leadership and U.S. partners and allies within the region. As a portion of China's ambition also seeks legitimate growth opportunities within the BRI construct, the desired outcome of this LOE is focused only on predatory and malign activity. By influencing China's political leadership and messaging support to U.S. partners and allies, information operations can persuade China's leaders to embrace international standards and allow partners and allies ample warning of malign Chinese intentions.

LOE 3) Expose and Counter Chinese Malign Cyber Operations

The joint force's implementation of information operations is paramount to support CYBERCOM's imperative to create information advantages supporting operational outcomes. Integrating with joint cyber operations, the objective of information operations for this LOE is to

expose China's malign cyber operations and, if necessary, enhance the legitimacy of a U.S. response. The Chinese political leadership and cyber operators are the TAs for these information operations. By reinforcing international law and rapidly exposing malign activity, information operations integrated with cyber defenses can degrade China's political leadership and cyber operators' ability to continue operations without risk of escalation.

4) Expose and Counter Chinese Malign Space Operations.

In support of SPACECOM's objectives to maintain space superiority and ensure space stability, the objective of information operations for this LOE is to expose China's malign space activities and, if necessary, assist in isolating China's space program should they choose to continue adversarial actions. The TA for this LOE is China's political leadership, the CNSA, and U.S. partners and allies in space. By strengthening support for a free and open space commons, information operations can isolate China's continued development in space with devastating effects on their economy and future if they continue provocative actions.

Within each LOE, the desired target of information operations may also differ from the specified target audience. Ultimately, the objective of information operations in addressing Chinese gray zone actions is to change the behavior of Chinese political leadership. Thus, the joint staff must always consider how influencing the actions of secondary target audiences will also shape the intended target of the Chinese political leadership.

Selecting Information Related Capabilities

After conceptualizing the information environment and identifying the target audience, the final step is to organize information-related capabilities (IRCs) against the target audience. If the joint force is the means of influencing TAs within the IE, then IRCs are the ways by which

that means creates effects.[52] IRCs are "Tools, techniques, or activities using data, information, or knowledge to create effects and operationally desirable conditions within the information environment's physical, informational, and cognitive dimensions."[53] As specified in JP-3-13, the ownership of the IRCs is not as important as their integrated application to achieve the JFC's end state.[54] With a combined understanding of the LOEs, the IE, and the TAs to address Chinese gray zone actions, the four IRCs of *military information support operations; civil-military operations; presence, profile, and posture; and public affairs* are most appropriate for the joint force to address China's activities in the gray zone.

Military Information Support Operations

Military information support operations (MISO) communicate selected information to foreign audiences to ultimately influence the behavior of foreign governments, organizations, and groups.[55] An essential function of MISO is military information (MILINFO) which combines psychological actions and persuasive messages to influence the TA.[56] Applied against all gray zone LOEs, MISO is the appropriate IRC to influence the opinion of the Chinese government, state-sponsored forces, the CNSA, and Chinese cyber operators. Although each TA's intended behavior differs, MISO provides a centrally controlled messaging source to synchronize effects against Chinese gray zone actions.

---

[52] U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013, I-5.
[53] U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013, I-4.
[54] U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013, I-5.
[55] Department of the Army. *The Conduct of Information Operations, Army Techniques Publication (ATP) 3-13.1*. 4 October 2018, 3-5.
[56] Department of the Army. *The Conduct of Information Operations, Army Techniques Publication (ATP) 3-13.1*. 4 October 2018, 3-5.

Civil-Military Operations

Civil affairs or other military forces perform civil-military operations (CMOs) to influence relationships between military forces and indigenous populations.[57] CMOs focus on maintaining stability within a region to achieve joint force objectives. To meet the challenges of LOE 1, CMOs could enable advising and assistance to local coast guards to uphold the rule of law against malign Chinese activity in the SCS. For LOE 2, CMOs could help indigenous governments to develop financing practices that avoid susceptibility to malign debt-trap practices that lead to expanded dual-use infrastructure. CMOs simultaneously strengthen and reassure partners and allies of U.S. commitment while countering Chinese gray zone activities.

Presence, Profile, and Posture

Presence, Profile, and Posture (PPP) is the deliberate, steady-state activities of military forces within the region that bring credibility to all aspects of information operations and apply to all gray zone LOEs.[58] If carefully planned with information operations, PPP can strengthen the effectiveness of other IRCs in the gray zone by providing credible deterrence. By synchronizing freedom of navigation (FON) operations, air demonstrations, and military exercises with messaging from other IRCs, the joint force can counter gray zone actions by forcing risk dilemmas on Chinese leadership. In this environment, the posture of the joint force is paramount to ensure actions remain legitimate in competition.

---

[57] Department of the Army. *The Conduct of Information Operations, Army Techniques Publication (ATP) 3-13.1*. 4 October 2018, 3-3.
[58] Department of the Army. *The Conduct of Information Operations, Army Techniques Publication (ATP) 3-13.1*. 4 October 2018, 3-7.

Public Affairs

Public affairs (PA) are internal and external communications that support the JFC's responsibility to keep the joint force and the public informed.[59] Applicable to all gray zone LOEs, PA helps to maintain domestic public support and inspires confidence in partners and allies. Over the last decade, social media has been a vital delivery mechanism for PA messaging. Social media provides a valuable tool to counter malicious disinformation and virtually broadcast military presence and intentions in the gray zone. If leveraged appropriately, PA social media operations can further delegitimize Chinese gray zone actions and impose costs of continuing malign activity.

The joint force requires a robust framework to conduct information operations against Chinese gray zone actions. Through conceptualizing the information environment, identifying the target audiences based on Chinese gray zone trends, and selecting information-related capabilities to target selected audiences, the joint force gains a robust information operations framework to identify, expose, and counter Chinese gray zone actions. During planning and execution, the joint force will need to continuously assess the information environment and develop and assess measures of effectiveness to validate the success of information operations.

[59] Department of the Army. *The Conduct of Information Operations, Army Techniques Publication (ATP) 3-13.1*. 4 October 2018, 3-7.

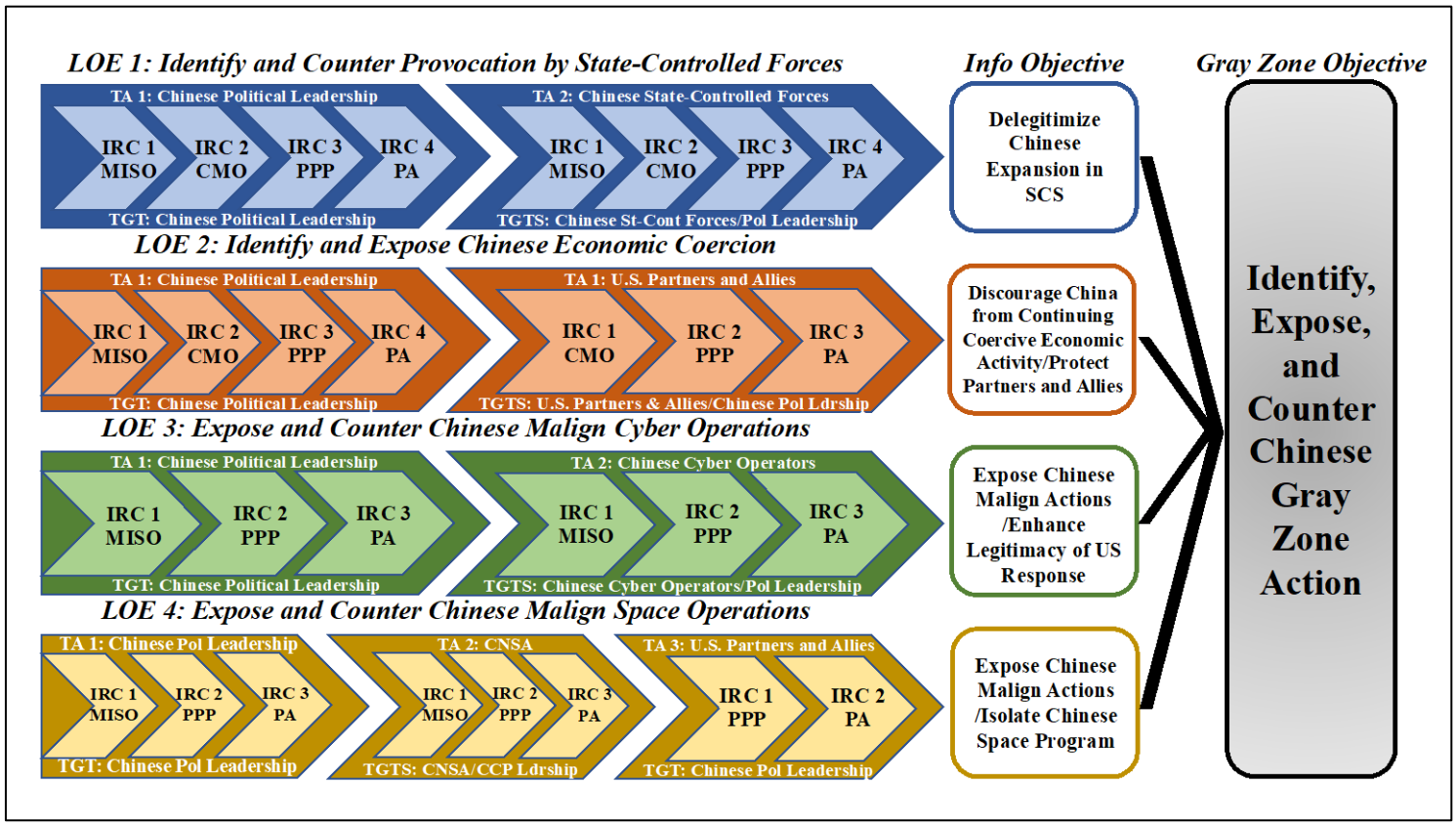

Figure 1: Gray Zone Information Operations Framework

Limitations of the Information Operations

There is an argument that information operations are insufficient to meet the challenges and complexity of countering Chinese gray zone actions. Instead, the joint force should develop credible deterrence capabilities to hold Chinese political leaders at risk should they cross established boundaries. Furthermore, to instill better confidence in American strength for allies and partners, the joint force should focus on strengthening hard power mechanisms to enforce deterrence by denial.[60] By convincing the Chinese leadership that if they continue malign actions, they will eventually face military failure, deterrence by denial is the most effective military gray zone strategy. Through making a piece of territory harder to take, harder to keep, or

[60] Green et al, 37.

more robust industrially, deterrence by denial offers the best strategy to force competitive dilemmas on Chinese leadership.[61]

Furthermore, information strategies that seek to expose and denounce adversarial action rarely are effective.[62] Developing attribution, particularly in the space and cyber domains, takes weeks to months to reach the required 95% confidence level to authorize a U.S. response.[63] Where direct observation of malign actions can speed up attribution, this rarely occurs against gray zone activity.[64] With such a delayed response, information operations may only increase China's belief that it can continue to thrive in the gray zone.

A Case for Integrated Information Operations

While it is true that a deterrence by denial strategy can be effective against gray zone operations and attribution information strategies often fail, these arguments fail to address the power of information operations when integrated with other military activities, including deterrence. A deterrence by denial strategy, which focuses on vertical escalation, is generally more effective when facing an adversary whose military is weaker. The weaker adversary chooses to deescalate in the face of military defeat; however, this premise is not necessarily true with China. Over the last decade, China has rapidly increased its military capabilities and, in certain areas, surpassed the capabilities of the U.S. A deterrence by punishment strategy, which focuses on horizontal escalation, risks embroiling the U.S. military in a tit-for-tat feedback loop while failing to resolve the problem. As information operations are objective and outcome-focused, integrating information operations with military plans in the gray zone can target

[61] A. Wess Mitchell, "The Case for Deterrence by Denial." American Interest. 12 August 2015, 5.
[62] Hicks and Dalton, 61.
[63] Hicks and Dalton, 62.
[64] Hicks and Dalton, 61.

China's political leadership's will rather than solely relying on exquisite technological development.

Integrating information operations into other military operations enhances the credibility and likelihood of success of that military action. For deterrence by denial, rather than risk continued vertical escalation and major theater war, information operations can decrease the value of the political object for the adversary, thus increasing the likelihood of de-escalation. Furthermore, against malign cyber or space activity where attribution is difficult, information operations are more effective when integrated with defensive cyber or space operations. Where defensive capability effectively blunts the cyber or space malign action, information operations remain helpful in exposing the malign actor and highlighting U.S. capability when attribution becomes possible. The result of decreasing the value of the object for the adversary is the same.

Conclusion

China's gray zone actions threaten the international rule of law and are outpacing U.S. reactions. Without a deliberate and integrated response, China can continue to hold U.S. global interests at risk through provocation by state-controlled forces in the South China Sea, coercive economic strategies, and disruptive cyberspace and space actions. As the DoD crafts doctrine and strategy to address military actions in the gray zone, a framework to integrate information operations with military responses is paramount for joint force commanders and staff to begin framing credible response options to delegitimize and deter China's coercive activities.

In establishing LOEs and objectives for information operations to address Chinese gray zone activities, the joint force gains an initial vector to integrate information operations with military plans. Next, by utilizing the information and influence relational framework to analyze the information environment and identify target audiences for influence, the joint force can

further conceptualize the intended effects of information operations. Lastly, by selecting IRCs to target selected audiences within each LOE, the joint force gains a doctrinal approach and framework for information operations to address the wicked problem of the gray zone. While a more detailed refinement of the information environment and target audiences will be necessary during the planning and execution of military operations, this framework provides the foundation necessary for the joint force to begin shaping an integrated information operation. By eroding China's desire and ability to thrive in the gray zone, information operations will enable the joint force to compete and win.

Recommendations

1.) The U.S. military requires doctrine and strategy to address the joint force's role in addressing gray zone challenges by China, Russia, North Korea, and Iran.
2.) The U.S. government needs to designate a global integrator to lead the government's efforts against gray zone activities. Once identified, the U.S. military needs to implement a joint task force to synergize the government's approach.
3.) The U.S. military needs to define acceptable levels of risk in gray zone operations to avoid tripping potential red lines. This provides the balance between U.S. policy and military action.
4.) More research is needed to measure the effectiveness of information operations against gray zone operations when paired with a military deterrence strategy.
5.) More research is needed to refine the governing rules, norms, and beliefs of prospective target audiences of information operations in the gray zone.
6.) More research is required to integrate machine learning and data analytics with information operations to affect outcomes in the gray zone.

Bibliography

Burnett, Charles R., Nathan P. Freier, William J. Cain, Christopher D. Compton, Sean M. Hankard, Robert S. Hume, Gary R. Kramlich, et al. *Outplayed: Regaining Strategic Initiative in the Gray Zone*. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2016.

Department of the Army. *The Conduct of Information Operations, Army Techniques Publication (ATP) 3-13.1*. 4 October 2018.

Freier, Nathan P. "The Darker Shade of Gray: A New War Unlike Any Other." The Darker Shade of Gray: A New War Unlike Any Other | Center for Strategic and International Studies, September 12, 2014. https://www.csis.org/analysis/darker-shade-gray-new-war-unlike-any-other.

Friend, Alice Hunt, and Kathleen H. Hicks. *By Other Means: Part I, Campaigning in the Gray Zone*. Washington, D.C.: Center for Strategic & International Studies, 2019.

Green, Michael J., Kathleen H. Hicks, Zack Cooper, John Schaus, and Jake Douglass. *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence*. Washington, D.C.: Center for Strategic & International Studies, 2017.

Hicks, Kathleen H., and Melissa Dalton. *By Other Means: Part II, Adapting to Compete in the Gray Zone*. Washington, D.C: Center for Strategic and International Studies, 2019.

Hoffman, Frank G. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges." *PRISM: National Defense University* 7, no. 4 (January 1, 2018): 30–47.

Martin, Joshua K. Email interview with the author, February 2022.

Mattis, James. *Summary of the 2018 National Defense Strategy of the United States of America*. Washington D.C.: Secretary of Defense, 2018.

Mitchell, A. Wess. "The Case for Deterrence by Denial." American Interest. 12 August 2015.

Nakasone, Paul M. *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command.* Fort Meade, Maryland: CYBERCOM, 2018.

Pacatte, William C. "Be Afraid? Be Very Afraid? — Why the United States Needs a Counterstrategy to China's Belt and Road Initiative." *Defense360*, October 19, 2019.

Perlroth, Nicole. "Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies." The New York Times. The New York Times, February 18, 2019. https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html.

U.S. Department of Defense. *Defense Space Strategy Summary.* DoD, 2020.

U.S. Department of Defense. *The Asia-Pacific Maritime Security Strategy: Achieving U.S. National Security Objectives in a Changing Environment*. DoD, 2015.

U.S. Office of the Chairman of Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13. 27 November 2017, Change 1 20 November 2013.