The Wicked Game: Planning for Nonlinear Warfare

A Monograph

by
MAJ Christopher S. Sweitzer
US Army

School of Advanced Military Studies
US Army Command and General Staff College
Fort Leavenworth, KS

2019

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 23-05-2019	**2. REPORT TYPE** Masters Thesis	**3. DATES COVERED** *(From - To)* JUN 2018 – MAY 2019

4. TITLE AND SUBTITLE The Wicked Game: Planning for Nonlinear Warfare	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) MAJ Christopher S. Sweitzer, US Army	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	**8. PERFORMING ORG REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Advanced Military Studies Program	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

As the United States realigns its military ways and means to deter and defeat the nation's near-peer adversaries in large-scale combat operations, the United States must not overlook its adversary's capability to employ nonlinear warfare to achieve political objectives. Both China and Russia are attempting to expand their regional and global influence while countering US global influence. This occurs primarily through the information and cyber domains. The employment of cyber and information technologies provides Russia and China with an asymmetric advantage over the West. Both nations acknowledge the value of the cyber and information domains, which is reflected in emerging Chinese and Russian nonlinear warfare doctrine. The Russian incursion into Ukraine and Chinese activities within the South China Sea provide recent examples of their nonlinear doctrine in action. To assist in meeting these challenges, the US military should consider adapting its operational art framework to assist planners in developing campaign plans that are distinctively suited for defeating nonlinear threats. A planning framework for countering nonlinear threats requires an operational art framework for comprehending these ill-structured problems. Designing campaigns to counter nonlinear warfare – specifically within the cyber and information domains – requires planners to use a "grammar" unique to this type of conflict.

15. SUBJECT TERMS
Operational Art, Nonlinear Warfare, Hybrid Warfare, Russia, China, Ukraine, South China Sea, Cyber Domain, Information Domain, Gerasimov Doctrine, Three Warfares,

16. SECURITY CLASSIFICATION OF: Unclassified			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** MAJ Christopher S. Sweitzer
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	42	918-758-3300

Monograph Approval Page

Name of Candidate: MAJ Christopher S. Sweitzer

Monograph Title: The Wicked Game: Planning for Nonlinear Warfare

Approved by:

__________________________________, Monograph Director
Dan Cox, PhD

__________________________________, Seminar Leader
Larry V. Geddings, COL

___________________________________, Director, School of Advanced Military Studies
Kirk C. Dorr, COL

Accepted this 23rd day of May 2019 by:

___________________________________, Director, Graduate Degree Programs
Robert F. Baumann, PhD

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the US Army Command and General Staff College or any other government agency. (References to this study should include the foregoing statement.)

Abstract

The Wicked Game: Planning for Nonlinear Warfare, by MAJ Christopher S. Sweitzer, US Army, 42 pages.

As the United States realigns its military ways and means to deter and defeat the nation's near-peer adversaries in large-scale combat operations, the United States must not overlook its adversary's capability to employ nonlinear warfare to achieve political objectives. Both China and Russia are attempting to expand their regional and global influence while countering US global influence. This occurs primarily through the information and cyber domains. The employment of cyber and information technologies provides Russia and China with an asymmetric advantage over the West. Both nations acknowledge the value of the cyber and information domains, which is reflected in emerging Chinese and Russian nonlinear warfare doctrine. The Russian incursion into Ukraine and Chinese activities within the South China Sea provide recent examples of their nonlinear doctrine in action. To assist in meeting these challenges, the US military should consider adapting its operational art framework to assist planners in developing campaign plans that are distinctively suited for defeating nonlinear threats. A planning framework for countering nonlinear threats requires an operational art framework for comprehending these ill-structured problems. Designing campaigns to counter nonlinear warfare – specifically within the cyber and information domains – requires planners to use a "grammar" unique to this type of conflict.

Table of Contents

Acronyms

ADP	Army Doctrine Publication
ARVN	Army of the Republic of Vietnam
CACD	Commander’s Appreciation and Campaign Design
CCP	Chinese Communist Party
CMC	Central Military Commission
DoD	Department of Defense
IP	Intellectual Property
JFC	Joint Force Commander
JOPP	Joint Operation Planning Process
LSCO	Large-Scale Combat Operations
NDAA	National Defense Authorization Act
NSS	National Security Strategy
OE	Operational Environment
PCA	Permanent Court of Arbitration
PLA	People’s Liberation Army
PLAN	People’s Liberation Navy
RT	Russia Today
SSF	Strategic Support Force
TRADOC	US Army Training and Doctrine Command

Illustrations

Introduction

Even as the US military shifts emphasis and resources from seventeen years of counterinsurgency operations to large-scale combat operations (LSCO), the nonlinear or unconventional threat confronted by the United States remains. US adversaries will continue to exploit perceived fissures and weaknesses within US capabilities through the use of nonlinear and asymmetric techniques. Furthermore, nonlinear warfare provides an assortment of challenges to military planners that reflect a complex problem-set that demands adaptive and innovative solutions.

As the United States realigns its military ways and means to deter and defeat the nation's near-peer adversaries in LSCO, the U.S. must not overlook its adversary's capability to employ nonlinear warfare to achieve political objectives. The 2017 US *National Security Strategy* asserts that China and Russia "challenge American power, influence, and interests" while attempting to "make economies less free and less fair, to grow their militaries, and to control information and data to repress their societies and expand their influence."[1] China and Russia are endeavoring to expand their regional and global influence while making attempts to counter the West's global power. This is occurring primarily through the information and cyber domains. For certain, both China and Russia are growing in military force structure while modernizing their military hardware. However, the United States must not ignore or fail to prepare for the nonlinear threat that each competitor continues to pose to the West.

Russia's 2014 incursion into Ukraine demonstrated its unique ability to combine conventional and unconventional warfare to achieve political objectives. The swift seizure of Crimea and portions of eastern Ukraine shocked the West as Russia applied mostly unconventional means to overwhelm Ukrainian resistance. Russia's use of hybrid warfare in

[1] The White House, *The National Security Strategy of the United States of America* (Washington DC, 2018), accessed October 12, 2018, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Ukraine reflects an evolution and growth of Russian nonlinear warfare since the beginning of the twenty-first century.[2] For example, Russia's 2007 cyberattack against Estonia and its use of nonlinear methods during the 2008 Russo-Georgian War provide evidence of Russia's growing penchant for using nonlinear warfare against nations with a proclivity towards the West.

Russia and China employ nonlinear techniques to counter the traditional military strength of the United States. For example, China's use of nonlinear warfare is guided by its unconventional doctrine of "Three Warfares." First introduced in 2003, China's nonlinear approach utilizes psychological, media, and legal warfare to gain both strategic and operational advantages over the West. As China's economic and geopolitical influence grows, China analysts look closely at both China's conventional and unconventional methods of influence within the Indo-Pacific region and beyond. The overarching objective of China's "Three Warfares" is the employment of information and cyber warfare to gain a strategic, operational, or tactical advantage over its adversaries.

Some experts compare the concepts and structures associated with China's "Three Warfares" to Russia's use of nonlinear warfare as it also incorporates cyber and information operations within gray zone conflict. As China and Russia continue to exert their regional power and place increasing pressure on neighboring countries within their respective spheres of influence, much can be gleaned from how both countries exert influence through the information and cyber domains.

Scholars continue to debate the significance of Russian and Chinese nonlinear warfare. However, most pundits agree, the use of nonlinear warfare remains a factor within the international arena. From gray zone conflict to unconventional warfare, variations of nonlinear warfare remain a fundamental characteristic of modern conflict. Many scholars warn the

[2] Timothy Thomas, "The Evolving Nature of Russia's Way of War," *Military Review* 97, no. 4 (July-August 2017): 34.

increased use of nonlinear warfare within the current operational environment provides important security challenges to the United States and its allies.

To assist in meeting these challenges, the US military should consider adapting its operational art framework to assist planners in developing campaign plans that are distinctively suited for defeating nonlinear threats. The framework associated with traditional operational art is best suited for conventional operations and lacks the appropriate grammar for countering these threats. The research and findings from this paper will assist in providing military planners with the framework required to design operational approaches to counter the threats associated with nonlinear warfare.

The monograph is organized into six sections: introduction, literature review, methodology, case study, conclusion, and recommendations. The literature review defines the threats within the current operational environment associated with nonlinear warfare, examines Joint and Army operational art and planning doctrine, and considers the current doctrine applied by planners to solve complex problems. Next, the methodology section provides a systems theory framework for examining Chinese and Russian nonlinear operations within the information and cyber domains. The conclusion will focus on the similarities and difference between Russian and Chinese nonlinear warfare. The recommendations section will identify certain facets of operational art that should be amended to assist the military practitioner operating within the ambiguous and complex environment linked to nonlinear warfare.

Literature Review

Today, military planners must navigate within complex operational environments that includes both conventional and unconventional threats. As planners endeavor to connect strategic goals with tactical actions on the ground, they are sometimes challenged by the lack of tools available to decipher the complex problems often associated with nonlinear and hybrid warfare. Hybrid warfare – the combination of conventional and unconventional warfare – has existed since man's early history and continues to influence conflict today.[3] In fact, America's most recent wars in Iraq and Afghanistan have shown the complex nature of current conflict as the United States continues to struggle in providing stability to these nations. Even as the US military revises its doctrine and invests in modernizing military hardware and technology to defeat its near-peer adversaries in LSCO, the nonlinear threat remains a reality.

An evaluation of the trends within global conflict reveal a significant decrease in interstate conflict over the last several decades with armed conflict between states considered a "rare event."[4] A recent Rand report finds "deadly political conflict has been gradually declining, and anticipated trends in the major drivers of war and peace suggest that such conflict is likely to continue to decline over the next couple of decades."[5] Several factors have contributed to this period of relative stability which include global economic growth, spread of democratic institutions, and the continued engagement by the United States in world affairs.[6] Yet, even with the decline in interstate conflict, volatile regions and belligerent actors pose real challenges to global security. However, current threats are mostly realized and experienced within nonlinear or gray zone conflict, somewhere in the space between war and peace.

Defining Nonlinear Warfare

Recent bellicose actions by Russia and China within their respective spheres of influence has reinvigorated the terms nonlinear and hybrid warfare within the warfighting lexicon. Frank Hoffman describes the spectrum of today's nonlinear conflict as consisting of gray zone,

[3] Williamson Murray and Peter R. Mansoor, eds., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (Cambridge: Cambridge University Press, 2012), 2.

[4] Thomas Szayna, *What Are the Trends in Armed Conflicts, and What Do They Mean for U.S. Defense Policy?* (Santa Monica, CA: RAND Arroyo Center, 2017), accessed October 16, 2018, https://www.rand.org/pubs/research_reports/RR1904.html.

[5] Ibid.

[6] Ibid.

irregular, hybrid, and limited conventional conflicts.[7] Figure 1 shows Hoffman's spectrum of conflict in unconventional warfare. While Hoffman does not discredit the threat associated with conventional warfare, his analysis of trends within the current environment reveals a proclivity towards nonlinear conflicts. In addition, Hoffman finds US near-peer competitors choose to engage in nonlinear warfare against the United States as a way to exploit the "gap in our intellectual preparations of the battlespace and a seam in how we think about conflict."[8] As adversaries exploit fissures within US capabilities and intellectual thought about current conflict, military planners are challenged to provide appropriate solutions to counter these threats.

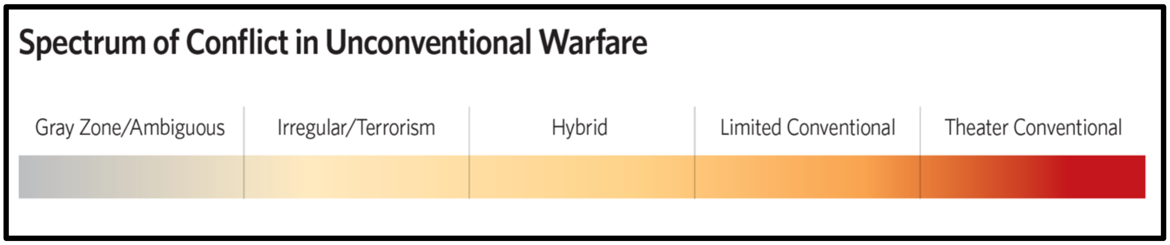


Figure 1. Frank Hoffman, *The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War* (Washington, DC: The Heritage Foundation, 2016), accessed October 3, 2018, https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_ ESSAYS _HOFFMAN.pdf.

As military pundits struggle to understand the complexity of twenty-first century conflict, many scholars are making attempts to define the current phenomena. How is nonlinear warfare characterized? What are the components of hybrid warfare? Through his analysis of Russian operations within Ukraine, Tad Schnaufer characterizes Russia's actions as nonlinear warfare. Although some scholars choose to describe Russia's incursion into Ukraine as hybrid warfare, Schnaufer chooses to describe it as nonlinear warfare. Schnaufer defines nonlinear warfare as "the application of collective subversive measures on a state(s) by another state actor, targeting its

[7] Frank Hoffman, *The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War* (Washington, DC: The Heritage Foundation, 2016), accessed October 3, 2018, https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_ ESSAYS _HOFFMAN.pdf.

[8] Ibid.

government, population, and vital social functions, in order to fulfill a grand strategy and to do the latter is will without a clear declaration of war."[9] Primarily through the use of nonmilitary methods, such as cyber and information operations, Russia attained its strategic objectives in Ukraine without a declaration of war or engaging in large-scale combat operations. Attacking its adversary's social systems – government institutions and civil society – appears to be the hallmark of Russian nonlinear warfare.

While some scholars are confident in defining Russia's behavior in Ukraine as hybrid or nonlinear warfare, others are hesitant to offer a distinctive label for Russia's actions. Michael Kofman and Matthew Rojansky find Russia lacks a specific hybrid warfare doctrine, but instead employs all instruments of national power to attain a strategic advantage.[10] As the U.S. employs diplomacy, information, economics for global influence and to sustain its standing throughout the world, Russia uses the same tools within its own spheres of influence. Kofman and Rojansky caution policymakers against using the concept of hybrid warfare to describe an evolution of twenty-first century Russian doctrine. Instead, the authors warn that policymakers should focus on "how to deal with a major power such as Russia when it chooses to employ its full range of national power."[11]

The Nonlinear Operational Environment

Through his analysis of the writings published by the Russian General Staff Chief Valery Gerasimov, Timothy Thomas provides insights into Russia's view of twenty-first century conflict. Thomas asserts Russia recognizes the significance of combining nonmilitary methods

[9] Tad Schnaufer, "Redefining Hybrid Warfare: Russia's Non-Linear War Against the West," *Journal of Strategic Security* 10, no. 1 (2016): 24.

[10] Michael Kofman and Matthew Rojansky, *A Closer Look at Russia's Hybrid War* (Washington, DC: The Wilson Center, 2015), accessed October 14, 2018 https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf.

[11] Ibid.

with military methods to achieve its strategic objectives. For example, Thomas finds Gerasimov acknowledges the "protest potential of the population, covert military measures, information operations, and special forces' activities, are being implemented by some nations to control conflict."[12] In addition, US adversaries choose to use nonmilitary means over military means within contemporary conflict to achieve their strategic objectives. The increasing use of nonmilitary means by China and Russia within the international arena intensifies the complexity of warfare as they choose to operate in the space between war and peace.

The cornerstone of Russian nonlinear warfare is the incorporation of information and cyber operations into its military doctrine to gain a strategic advantage over its adversaries. James Sherr finds "today's Russian state has inherited a culture of influence deriving from the Soviet and Tsarist past . . . it bears the imprint of doctrines, disciplines and habits acquired over a considerable period of time in relations with subjects, clients and independent states."[13] Russia displayed its culture of influence through the use of information and cyber operations during the Russo-Georgian War in 2008 and the Russo-Ukrainian War in 2014. In addition, Russia demonstrated its proclivity for influence operations, applied through the information and cyber domains, during the 2016 US presidential elections.

Through his analysis of General Gerasimov's writings, Charles Bartles finds the "Russian military is seeing war as being something much more than military conflict."[14] There is a growing appreciation within the Russian defense establishment for nonmilitary means to counter the West's strengths. In fact, through his analysis of the current operational environment, Gerasimov acknowledges a four to one ratio of nonmilitary and military means. Bartles examination of

[12] Thomas, "The Evolving Nature of Russia's Way of War," 36.

[13] James Sherr, *Hard Diplomacy and Soft Coercion: Russia's Influence Abroad* (London: Chatham House, 2013), 24.

[14] Charles Bartles, "Getting Gerasimov Right," *Military Review* 96, no. 1 (2016): 34.

Russian and Western views on nonmilitary measures within contemporary conflict concludes that the "West considers these nonmilitary measures as ways of avoiding war, Russia considers these measures as war."[15] Furthermore, Russia's influence within the cyber and information domains are connected to Gerasimov's view on the utility of the information domain. Figure 2 illustrates Russia's view of contemporary warfare that incorporates nonmilitary means during conflict. Gerasimov finds that "the information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy."[16]

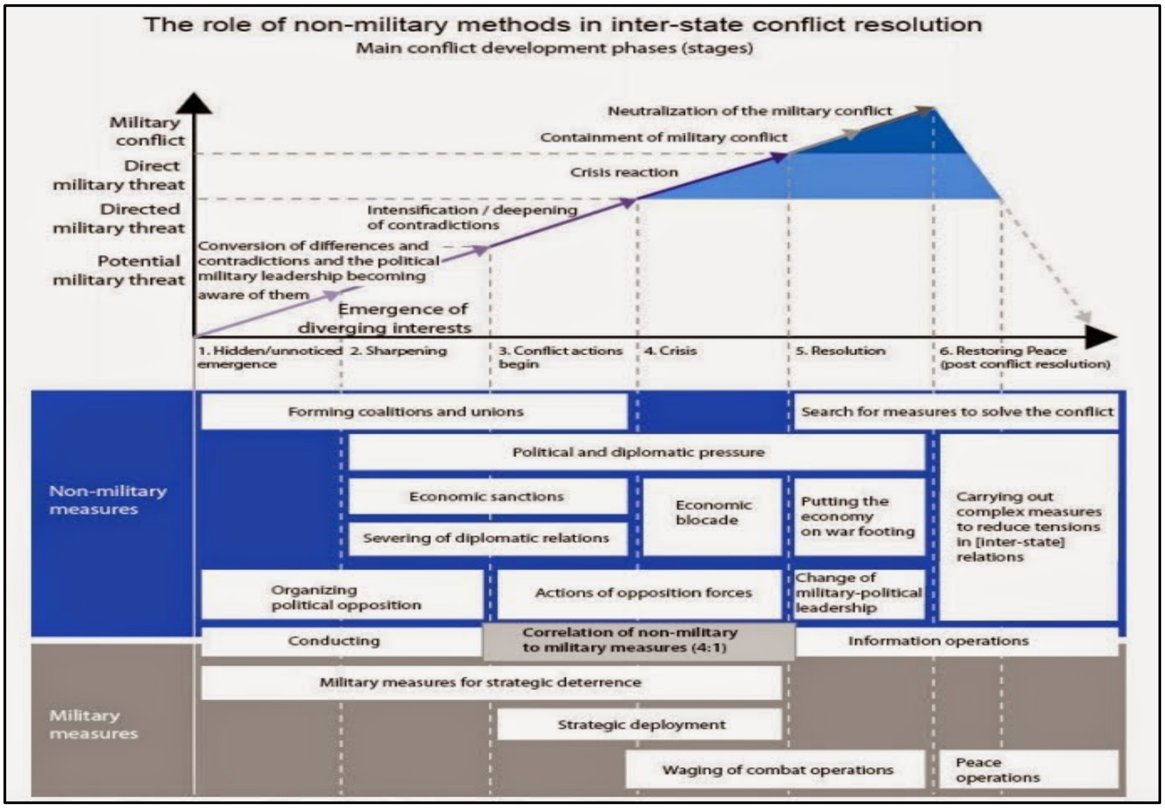

The role of non-military methods in inter-state conflict resolution
Main conflict development phases (stages)
Military conflict
Direct military threat
Directed military threat
Potential military threat
Neutralization of the military conflict
Containment of military conflict
Crisis reaction
Intensification / deepening of contradictions
Conversion of differences and contradictions and the political military leadership becoming aware of them
Emergence of diverging interests
1. Hidden/unnoticed emergence
2. Sharpening
3. Conflict actions begin
4. Crisis
5. Resolution
6. Restoring Peace (post conflict resolution)
Non-military measures
Forming coalitions and unions
Search for measures to solve the conflict
Political and diplomatic pressure
Economic sanctions
Severing of diplomatic relations
Economic blocade
Putting the economy on war footing
Carrying out complex measures to reduce tensions in [inter-state] relations
Organizing political opposition
Actions of opposition forces
Change of military-political leadership
Conducting
Correlation of non-military to military measures (4:1)
Information operations
Military measures
Military measures for strategic deterrence
Strategic deployment
Waging of combat operations
Peace operations

Figure 2. Charles Bartles, "Getting Gerasimov Right," *Military Review* 96, no. 1 (2016): 34.

Similar to Russia's application of nonlinear warfare, China's "Three Warfares" – psychological, media, and legal warfare – seek to exploit flaws within the traditional view of conflict held by the United States. Stephan Halper finds that China's use of "Three Warfares" is

[15] Bartles, "Getting Gerasimov Right," 34.

[16] Ibid., 31.

"a new way of thinking about conflict that has the advantage of both obtaining the sought-after objective and engaging the United States in an asymmetrical manner."[17] Through the application of nonmilitary ways and means to achieve its political and economic objectives, China is able to side-step traditional sources of US power, both globally and within the Pacific region. Visible through the construction of artificial islands in the South China Sea and theft of US intellectual property (IP), China seeks to bypass US instruments of national power through the employment of its own variant of asymmetric doctrine.

The principal theme flowing throughout each component of the "Three Warfares" is China's manipulation of the information environment to influence both domestic and international audiences. For example, Elsa Kania finds "in peacetime and wartime alike, the application of the "Three Warfares" is intended to control the prevailing discourse and influence perceptions in a way that advances China's interests, while compromising the capability of opponents to respond."[18] China's unique combination of media warfare, psychological warfare, and legal warfare provides the Middle Kingdom with an asymmetric platform to challenge the United States for regional influence without resorting to a strategy of direct confrontation.

Although there is a substantial body of research examining China's "Three Warfares" and Russia's nonlinear warfare, scholarly research that solely compares Chinese and Russian information and cyber operations is limited. Peter Mattis finds the difference between Chinese and Russian approaches to information operations "is that the Chinese are human or relationship-centric while the Russians are operation or effects-centric."[19] In his article, Mattis fails to

[17] Stephan Halper, *China: The Three Warfare* (Washington, DC: Office of the Secretary of Defense, 2013), 19.

[18] Elsa Kania, "The PLA'a Latest Strategic Thinking on the Three Warfares," *Jamestown Foundation: China Brief* 16, no.12 (August 2016): 15.

[19] Peter Mattis, "Contrasting China's and Russia's Influence Operations," *War on the Rocks*, January 16, 2018, accessed October 3, 2018, https://warontherocks.com/2018/01/contrasting-chinas-russias-influence-operations.

acknowledge the "Three Warfares" and role that it plays in China's approach to information operations. However, Mattis does believe China's information operations are evolving to incorporate Russian techniques of influence.

Most comparisons of Chinese and Russian nonlinear warfare examine their gray zone strategies, which encompass the information and cyber domains. Michael Mazarr finds "both China and Russia have explicitly chosen gray zone-style strategies to peruse their measured revisionist goals."[20] Marzarr's analysis of Chinese and Russian strategies applies a linear approach categorizing gray zone operations on a continuum that ranges from low-intensity warfare to high-intensity warfare. The major distinction drawn between Chinese and Russian nonlinear warfare is China's propensity to employ a low-intensity strategy with Russia operating on the other end of the continuum. Examining the application of Chinese and Russian nonlinear warfare provides insight into the increasing complexity of today's operational environment.

Even with the challenge of precisely labeling Russian and Chinese actions in Ukraine and the South China Sea, national security experts do seem to agree that their methods are unconventional. Frank Hoffman contends, regardless of the label assigned to recent Russian and Chinese actions, the US national security establishment remains primarily focused on traditional military threats.[21] Failure by the United States to prepare for the growing tendency of its near-peer competitors to engage in unconventional or nonlinear methods is dangerous. Hoffman calls on the US government to increase its effort to quell the nonlinear threat through a likely whole-of-government approach. In an attempt to focus US national security efforts and resources on nonlinear threats, Hoffman asks, "where should the loci of US capability and doctrinal

[20] Michael J. Mazarr, "Mastering the Gray Zone: Understanding a Campaign Era of Conflict," Strategic Studies Institute (December 2015): 96.

[21] Frank Hoffman, "On the Not-So-New Warfare: Political Warfare VS Hybrid Threats," *War on the Rocks*, July 28, 2014, assessed October 16, 2018, https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats.

development exist: Defense, State, Intelligence, or something uniquely joint/interagency?"[22] Undoubtedly, protecting the United States and its interests from nonlinear threats requires a concerted effort from most of the interagency partners from within the US national security establishment. Other important questions that must be asked is which US agency is best suited to lead this effort? Who is best prepared to connect the ways and means to national policy? What is the end state within nonlinear warfare?

Military Planning for Nonlinear Warfare

Military planners use the conceptual framework associated with operational art and design to plan campaigns and operations. Joint Publication 3-0 defines operational art as a cognitive approach used by commanders and their staffs "to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, and means."[23] Furthermore, operational art is a process used to "mitigate the ambiguity and uncertainty of a complex operating environment."[24] Operational art serves as the connective tissue between strategy and tactics as military planners endeavor to apply the appropriate resources and operational approach to achieve a desired end state. To assist in this effort, military planners sometimes incorporate operational design into the planning process to better understand the operational environment and problem.

The majority of the problems that military planners attempt to solve through the planning process are complex problems, often requiring creative or nonlinear thinking to generate an effective solution. To assist planners in developing solutions to complex problems, Joint Doctrine provides planners with an operational design framework. Joint Publication 5-0 defines operational

[22] Hoffman, "On the Not-So-New Warfare: Political Warfare VS Hybrid Threats," 20.

[23] US Department of Defense, Joint Staff, *Joint Publication (JP) 3-0, Joint Operations* (Washington, DC: Government Printing Office, 2018), II-3.

[24] US Joint Staff, *JP 3-0, Joint Operations* 2018, II-3.

design as "one of several tools available to help the Joint Force Commander (JFC) and staff understand the broad solutions for mission accomplishment and to understand the uncertainty in a complex operational environment (OE)."[25] As a nonlinear problem-solving model, operational design provides planners with an established framework to use to increase their comprehension of the operational environment. This framework assists planners in accurately defining the problem prior to initiating detailed planning.

By recognizing most operational problems as complex and difficult to solve, the US Army developed supplementary planning doctrine to assist commanders and their operational planners. The Commander's Appreciation and Campaign Design (CACD) seeks to "create a systemic and shared understanding of a complex operational problem and to design a broad approach for its resolution."[26] The CACD acknowledges twenty-first century warfare is complex. In fact, the CACD finds that contemporary operational problems offered to military planners are mostly "structurally and interactively complex."[27] These ill-structured problems require planners to spend more time in the design phase of the planning process as they attempt to provide structure to complex problems.

John Schmitt supports the need for planners to spend more time in design prior to engaging in detailed planning. Schmitt finds "planning addresses a problem within the boundaries of an existing paradigm, while design is about questioning assumptions and creating new a paradigm for addressing a problem on its own terms."[28] This is especially true for operational problems that are associated with nonlinear warfare. The existing planning construct for

[25] US Department of Defense, Joint Staff, *Joint Publication (JP) 5-0, Joint Planning* (Washington, DC: Government Printing Office, 2017), IV-6.

[26] US Department of the Army, *TRADOC Pamphlet 525-5-500, Commander's Appreciation and Campaign Design* (Washington, DC: Government Printing Office, 2008), 4.

[27] US Army, *TRADOC Pamphlet 525-5-500* (2008), 7.

[28] John F. Schmitt, "A Systemic Concept for Operational Design," accessed October 21, 2018, http://www.au.af.mil/au/awc/awcgate/usmc/mcwl_schmitt_op_design.pdf.

conventional warfare is inadequate in dealing with the ill-structured problems that accompany nonlinear warfare. In dealing with complex problems, Schmitt recommends that planners use systems thinking to adequately construct the problem or system that is attempting to be deciphered. The incorporation of systems thinking into design will "establish the terminology, symbology, and constructs that will constitute the language and grammar of all planning and execution."[29]

Antulio Echevarria makes the claim that warfare has having "two grammars." Borrowing the concept "grammar of war" from Carl von Clausewitz, Echevarria defines grammar as "its unique ability to capture the collective concepts, principles, and procedures germane to the conduct of war."[30] According to Echevarria, conventional and nonlinear warfare each possess its own distinctive characteristics and methods for attaining strategic or political objectives. Echevarria argues American operational artists are proficient in defeating its adversaries within conventional conflict using war's "first grammar." However, the application of traditional operational art to defeat US adversaries engaging in nonlinear or irregular warfare – war's "second grammar" – is lacking. Military planners are hindered when applying concepts and processes intended for conventional warfare to nonlinear or complex problems. Lessons from the last seventeen years in Iraq and Afghanistan have demonstrated the challenges faced by military planners in applying conventional thought to unconventional problems.

Acknowledging the array of complex problems that nonlinear warfare presents to military planners is an important first step toward developing an appropriate solution. In dealing with these threats, Frank Hoffman calls on the military to modify its operational art and adapt its

[29] Schmitt, "A Systemic Concept for Operational Design," 31.

[30] Antulio J. Echevarria, "American Operational Art, 1917-2008," in *The Evolution of Operational Art: From Napoleon to the Present*, ed. John Andreas Olsen and Martin van Creveld, (New York: Oxford University Press, 2011), 137.

campaign planning to defeat hybrid threats.[31] Hoffman recognizes that innovative thinking is required by planners to overcome twenty-first century threats that often appear through nonlinear warfare. In addition, using lessons learned in Ukraine and the South China Sea, the US national security establishment understands its near-peer adversaries will not restrict their activities to merely traditional state-based conventional warfare.[32] After experiencing success using nonlinear techniques within their respective spheres of influence, Russia and China will continue to improve and employ nonlinear tactics against the West.

Operational Art and Design for Complex Problems

T.C. Greenwood finds that modern conflict is best defined as “interactively complex” with the Department of Defense (DoD) struggling to adapt its Joint Operation Planning Process (JOPP) to defeat “wicked” or ill-structured problems.[33] Greenwood evaluates current Joint and Army planning doctrine and its limitations in guiding planners toward solutions for complex problems. He finds the current definition of operational art used by the DoD as being inadequate and too narrow, unable to “integrate political, economic, diplomatic, informational, and cultural power into a national or even international campaign.”[34] The assimilation of all instruments of national power into the planning process is needed. A whole-of-government approach is necessary to defeat threats often using both military and nonmilitary means to achieve its objectives. Greenwood is accurate in calling on the DoD to adapt its operational art and planning process for nonlinear warfare.

[31] Frank G. Hoffman, “Hybrid Warfare and Challenges,” *Joint Force Quarterly*, no. 52 (Fall 2009): 38.

[32] Ibid., 39.

[33] T.C. Greenwood, “War Planning for Wicked Problems,” *Armed Forces Journal* (December 2009), accessed September 28, 2018, http://armedforcesjournal.com/war-planning-for-wicked-problems.

[34] Ibid.

Brigadier General (Ret.) Huba Wass de Czege acknowledges the complexity of twenty-first century conflict and advocates for the adoption of an operational design to assist commanders and military planners in meeting difficult challenges. Wass de Czege finds "because today's missions present novelty and complexity combined, designing components of operational art requires systematizing collective critical and creative thinking within a headquarters."[35] The process of enabling critical and creative thinking within operational planning teams is facilitated through the development of doctrine that assist planners with this endeavor. Wass de Czege's systemic operation design "relies on mental models to structure thinking, learning, and shifts thinking about a reality that is fundamentally unstructured, ephemeral, and intractable."[36] Providing conceptual structure to Chinese and Russian nonlinear warfare is the first step in assisting operational planners in developing methods for countering its threat.

Methodology

This monograph will examine nonlinear threats within the information and cyber domains that offer challenges to military planners when applying only linear planning tools. Through the examination of Chinese and Russian nonlinear warfare, the monograph will first establish evidence of the persistent nonlinear threat presented to the United States and the West by both actors. Next, a comparative analysis of Russian and Chinese nonlinear warfare will utilize a systems theory framework to identify the structural similarities and differences between Russian and Chinese operational approaches to nonlinear warfare.

John Schmitt defines systems thinking as "a mental process that seeks to understand and represent subjects as interactively complex wholes functioning within a broader environment."[37]

[35] Huba Wass de Czege, "Systemic Operational Design: Learning and Adapting in Complex Missions," *Military Review*, no.1 (January-February 2009): 7.

[36] Ibid., 2.

[37] Schmitt, "A Systemic Concept for Operational Design," 23.

According to systems theory, systems are composed of structures and processes functioning together for a particular purpose. In addition, complex systems interact with its environment, which also contain other systems; figure 3 illustrates the systems thinking framework. Applying this framework to Chinese and Russian nonlinear warfare will assist in identifying the structures, processes and purposes of their activities within the information and cyber domains. Consequently, this comparison and analysis will assist in identifying the shortfalls linked to the current operational art framework which is challenged to provide military practitioners with the necessary tools for countering nonlinear threats.

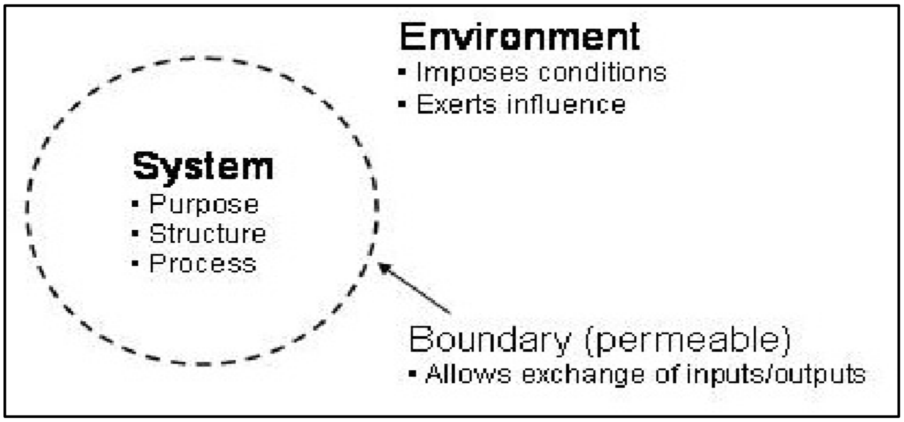


Figure 3. John F. Schmitt, “A Systemic Concept for Operational Design,” accessed October 21, 2018. http://www.au.af.mil/au/awc/awcgate/usmc/mcwl_schmitt_op_design.pdf.

Case Studies: The Strategic Environment

An analysis of the strategic environment provides insights into Russian and Chinese inclinations toward the use of nonlinear warfare. The *2017 National Security Strategy* (NSS) describes Russia and China as revisionist powers that compete with the United States for power and influence across multiple domains.[38] In addition, the NSS finds that both countries “use technology and information to accelerate these contests in order to shift regional balances of

[38] The White House, *The National Security Strategy of the United States of America* (Washington, DC, December 2017), 25.

power in their favor."[39] The use of cyber and information technologies allow Russia and China to gain an asymmetric advantage over the West. Both militaries acknowledge the value of the cyber and information domains reflected in emerging Chinese and Russian nonlinear doctrine. Although these countries continue to invest in conventional military capabilities, both prefer asymmetric approaches to conflict as a means to bypass US military strength.[40]

Russia: Strategic Environment

A resurgent Russia seeks to maintain its influence over its former Soviet republics and satellite states such as Belarus, Georgia, and Ukraine in an attempt to buffer the Russian homeland from the West. Stephen Kotkin finds that "Russia's pursuit of a Eurasian sphere of influence is a matter of national identity not readily susceptible to material cost-benefit calculations."[41] Russia's national identity reaches far back into Eurasian history. It contains bitter reminders of efforts by European powers to subjugate the Russian people and exploit their lands. From Napoleon in 1812 to Hitler in 1941, European hegemons have long targeted Russia for its resources and supposed threat to European powers. These relatively recent historical episodes of attempts at conquest are not forgotten by Vladimir Putin and the Russian populace.

Russia continues to thwart US and NATO efforts to encroach on traditional Russian spheres of influence. Cyberattacks against Estonia in 2008 and Russia's seizure of the Crimean Peninsula in 2014 serve as grim reminders to former Soviet republics and satellite states that drift

[39] The White House, *The National Security Strategy of the United States of America,* 25.

[40] In a competitive world, both Russia and China look for opportunities to counter US power through a variety of nonlinear techniques. The 2018 National Defense Authorization Act (NDAA) warns that "Russia's ongoing malign influence activities—misinformation, disinformation, propaganda, cyberattacks, election interference, active measures, and hybrid warfare operations—pose not only a threat to the security interests of the United States and those of our allies and partners in Europe but also to the integrity of Western democracies and the institutions and alliances they support." US Congress, Senate, Conference Report Highlights: National Defense Authorization Act for Fiscal Year 2018, 115th Cong, 1st sess., 2017.

[41] Stephen Kotkin, "Russia's Perpetual Geopolitics: Putin Returns to the Historical Pattern," *Foreign Affairs*, May/June 2016, 8.

too close to the West and democratic institutions. Russia's recent bellicose behaviour in opposition to the spread of the European Union and NATO along its periphery is cause for concern for the West.[42] Successfully deterring Russian aggression within the region requires a fundamental understanding of Russia's employment of both military and non-military means achieve its objectives.

China: Strategic Environment

Powered by a burgeoning economy, China endeavors to unseat the United States as the hegemonic power within the Indo-Pacific region. The economic rise of China is well-documented by Chinese experts with the Middle Kingdom's unparalleled economic growth since the 1980s. The economic reforms established by Deng Xiaoping in 1978 continue to reverberate within China's social stratum as millions of Chinese are now able to enjoy the fruits of middle-class living. Economist estimate China's economy is on track to surpass US economic output in terms of Gross Domestic Product (GDP) by 2029.[43] Graham Allison posits that "China primarily conducts foreign policy through economics" which is shown through the regional and world trade imbalance that heavily favor Chinese markets.[44] China's use of economic muscle as a means to tilt the balance of power within the region in its favor is characterized as "geoeconomics."[45] The immensity of China's economy allows it to use economic pressure as a coercive instrument to sway its neighbors within the region.

[42] In 2016, NATO SACEUR General Curtis Sacporotti stated "a resurgent Russia is striving to project itself as a world power and to address these challenges, we must continue to maintain and enhance our levels of readiness and our agility in the spirit of being able to fight tonight if deterrence fails." Bettina Renz, "Why Russia is Reviving its Conventional Military Power," *Parameters* 46, no. 2 (2016):1.

[43] Malcolm Scott, "Here's How Fast China's Economy is Catching Up to the U.S.," *Bloomberg*, May 24, 2018, accessed November 22, 2018, https://www.bloomberg.com/graphics/2016-us-vs-china-economy.

[44] Graham Allison, *Destined for War: Can America and China Escape Thucydides' Trap?* (New York: Harcourt Press, 2017), 21.

[45] Mark Beeson, "China Rises, America Falters, and Geoeconomics Rears its Head," *War on the Rocks*, August 23, 2018, accessed November 20, 2018. https://warontherocks.com/2018/08/china.

As Chinese economic power and influence expand within the region, it endeavors to establish geopolitical conditions favorable for realizing its goal of becoming the regional hegemon. The growing friction between China and the United States over China's belligerent activities within the South and East China Seas reveal China's increasingly brazen challenges to US regional authority. Andrew Krepinevich finds China is a "revisionist power seeking to dominate the western Pacific" as it lays claim to the "1.7 million square miles that make up the East China and South China Seas where six other countries maintain various territorial and maritime claims."[46] As China's economic and military power increase, it is emboldened to contest the traditional Indo-Pacific balance of power. Moreover, China seeks to weaken US regional alliances. China's militarization of numerous islands within the South China Sea provides it with man-made platforms to project power into an economic zone that sees nearly $5.3 trillion in trade pass through each year.[47] China's island-building strategy, coupled with its investments in anti-access and area denial capabilities, could eventually impede US access to an economic zone with immense geostrategic value.

Nonlinear Warfare Doctrine: Russian and China

While there is no definitive nonlinear warfare doctrine available to decrypt Russian actions in Ukraine, recent Russian military writings and speeches by prominent Russian military leaders provide clues into their view on the use of nonlinear methods in modern conflict. To understand Russian military thought and bearing in the twenty-first century, Russian analysts often turn to the writings of Russian General Chief Valery Gerasimov. Gerasimov's reflections on twenty-first century warfare provide the West with valuable insight into how the Russian military views modern conflict. In *The Value of Science is in the Foresight: New Challenges Demand*

[46] Andrew Krepinevich, "How to Deter China: The Case for the Archipelagic Defense," *Foreign Affairs*, March/April 2015, 79.

[47] Allison, *Destined for War*, 128.

Rethinking the Forms and Methods of Carrying Out Combat Operations, Gerasimov writes the "very rules of war have changed" as "the role of nonmilitary means of achieving political and strategic goals has grown, in many cases, they have exceeded the power of force of weapons in their effectiveness."[48] In this statement, Gerasimov is referring to lessons from the Arab Spring. In addition, his declaration about modern conflict is linked to Russian observations of the multiple color revolutions that have occurred in certain former Soviet republics over the last two decades such as the Rose Revolution in Georgia and the Orange Revolution in Ukraine.

As Russia pursues an asymmetric advantage over the West, lessons learned from the Arab Spring and the Color Revolutions provide Russia with a potential template for nonlinear warfare. Timothy Thomas highlights Gerasimov's findings that "a combination of nonmilitary methods, including the protest potential of the population, covert military measures, information operations, and special forces activities, are being implemented by some nations to control conflict."[49] It is reasonable to argue Russia applied this nonlinear template during the 2014 Russian incursion into Ukraine. Russia's manipulation of eastern Ukraine's Russian ethnic population through targeted cyber and information operations, coupled with its limited employment of special operations forces, resulted in the swift annexation of the Crimean Peninsula. It is evident that Russia successfully employed nonmilitary means to achieve its political and strategic goals in Ukraine.

As China's economic and regional influence continues to grow, Chinese analysts look closely at both China's conventional and unconventional methods of influence within the Indo-Pacific region. The People's Liberation Army (PLA) provides a conceptual foundation for

[48] Valery Gerasimov, "The Value of Science in Foresight: New Challenges Demands Rethinking the Forms and Methods of Carrying Out Combat Operations," trans. Robert Coalson, *Military Review* 96, no. 1(January-February 2016): 46.

[49] Timothy Thomas, "The Evolving Nature of Russia's Way of War," *Military Review* 97, no. 4 (July-August 2017): 40.

Chinese nonlinear warfare with the release of *Unrestricted Warfare* in 1999. Composed by two PLA Colonels – Qiao Liand and Wang Xiangsui – in response to Western military power, the document determines "warfare in the modern world will no longer be primarily a struggle defined by military means or even the military at all."[50] According to the document, the use of nonmilitary means to achieve political or strategic objectives is enhanced with the arrival of twenty-first century technological innovations within the information and cyber domains. While reflecting on the influence of information technology on modern warfare, *Unrestricted Warfare* finds "all the boundaries lying between the two worlds of war and non-war, of military and non-military, will be totally destroyed, and it also means that many of the current principles of combat will be modified, and even that the rules of war may need to be rewritten."[51] China's search for asymmetric mechanisms to counter US military power is established with the creative employment of nonlinear means through the information and cyber domains.

When examining China's nonlinear methods for exerting its influence, many scholars focus on the concepts outlined in the "Three Warfares" to assist in explaining China's actions within the region. The Chinese Communist Party (CCP) Central Committee and the Central Military Commission (CMC) incorporated "Three Warfares" into Chinese strategic doctrine in 2003.[52] The primary components of China's "Three Warfares" include psychological warfare, media warfare, and legal warfare. Under the oversight of the CMC, China's Political Work Department is responsible for planning and administering China's policies and operations associated with the strategic and operational employment of "Three Warfares." Timothy Thomas

[50] David Barno and Nora Bensahel, "A New Generation of Unrestricted Warfare," *War on the Rocks*, April 19, 2016, accessed November 16, 2018. https://warontherocks.com/2016/04/a-new-generation-of-unrestricted-warfare.

[51] "Unrestricted Warfare," 12.

[52] Timothy Walton, *China's Three Warfares* (Herndon, VA: Delex Consulting, Studies and Analysis, 2012), accessed December 12, 2018, http://indianstrategicknowledgeonline.com/web/Three%20Warfares.pdf.

finds that “information warfare has assumed a central role in Chinese military writings over the past decade.”[53] With the theoretical framework provided by the “Three Warfares” doctrine, China is more capable of shaping the strategic and operational environment through the information and cyber domains.

Russia and China in the Information and Cyber Domains

The Chinese and Russian people share common histories of existing under authoritarian regimes where the central government monopolizes the dissemination of information, both domestically and internationally. This is important to note as China and Russia leverage information and cyber operations as an asymmetric instrument to counter the strength of the U.S. Senior Russian military leaders acknowledge the potential of the information space to provide Russia with an asymmetric advantage over the West and NATO.[54] Similarly, China grasps the opportunities within the information domain to counterbalance US power in the Indo-Pacific region. Timothy Thomas finds the rise of information technology has “flattened” the levels of war as new technologies have “reduced the distance” between adversaries.[55] Recent Russian and Chinese gray zone and nonlinear campaigns against the West provide useful examples of their mounting activity within the information and cyber domains to further their interests while eroding US influence. Russia’s 2014 incursion into Ukraine and China’s ongoing dispute and operations within the South China Sea provide such examples.

Russia: Information Domain

Russian activity within the information and cyber domains is advanced and well-practiced. Dating back to its Bolshevik roots, Russian manipulation of the information domain to

[53] Walton, *China’s Three Warfares*, 12.

[54] Charles Bartles, “Getting Gerasimov Right,” *Military Review* 96, no. 1 (2016): 36.

[55] Timothy Thomas, “The Evolving Nature of Russia’s Way of War,” *Military Review* 97, no. 4 (July-August 2017): 40.

influence both domestic and international populations is timeless. Using active measures and reflexive control to advance its interests and curb the expansion of Western influence during the Cold War, Russia gained valuable experience in the art of strategic and operational influence operations. For example, since the rise of the communist party during the 1920s, Russia has used active measures "to influence political attitudes and public opinion in non-communist countries through deceptive and covert means."[56] In addition, Russia's progression in the art of reflexive control provides it with honed tools within the information domain to shape and influence its adversary's decision-making through state coordinated and targeted propaganda.[57]

Russia's combined use of active measures and reflexive control provides it with effective tools of deception – *Maskirovka* – that endure within the information and cyber domains. When examining the Russo-Ukrainian War, Julian Lindley-French finds Russia's use of *Maskirovka* demonstrated "a purposeful strategy of deception that combines use of force with disinformation and destabilization to create ambiguity in the minds of [NATO] alliance leaders about how best to respond."[58] Russia's influence operations against the West continues today as evidenced by its strategic disinformation campaigns targeting Western democracies and its strategic and operational use of information operations during its 2014 incursion into Ukraine.

The chaos within Ukraine stemming from political and social discord during the 2014 Euromaidan Revolution provided Russia with a strategic opportunity. As Ukrainian citizens filled Independence Square in the capitol city of Kiev to protest their government's renunciation of Western institutions, Vladimir Putin and his disinformation apparatus exploited Ukraine's

[56] Dennis Kux, "Soviet Active Measures and Disinformation: Overview and Assessment," *Parameters, Journal of the US Army War College* 15, no. 4 (Winter 1985): 19.

[57] Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies,* 17 (2004): 237.

[58] Julian Lindley-French, *NATO: Countering Strategic Maskirova* (Calgary: Canadian Defense and Foreign Affairs Institute, 2015), accessed December 12, 2018, https://d3n8a8pro7vhmx.cloudfront.net /cdfai/pages /543/ attachments /original/ 1432247421/NATO_Countering_Strategic_ Maskirovka.pdf.

growing social disharmony to advance Russian interests in the region. This historic episode culminated with Ukrainian President Yanukovych fleeing Kiev for the safe enclaves of Russia and was quickly followed by Russia's incursion into eastern Ukraine and the Crimean Peninsula.

During the initial days and weeks of unrest, Russian manipulation of the information domain generated a cloud of propaganda and disinformation that fueled Ukrainian social and ethnic tensions while impeding a diplomatic or military response by the West. Russian influence operations themes and messages "proactively targeted pro-Russian rebels, the domestic population, and the international community to alienate Ukraine from its allies and sympathizers."[59] Moreover, the pro-Russian narrative found its most welcoming audience in eastern Ukraine.

The ethnic Russian population residing within eastern Ukraine and Crimea provided Russian information operations with its target audience. As Russia's "little green men" infiltrated government buildings on the Crimean Peninsula, Russia's disinformation campaign stoked historical and ethnic tensions within Ukraine. For example, Russian political leaders and state media labeled the Euromaidan Revolution as a fascist movement in an attempt to "awaken memories of the Soviet fight against Nazi Germany."[60] In drawing upon Ukraine's collective memory of the atrocities committed by the Nazi's during World War II, Russia endeavored to associate the West-leaning Euromaidan protests with one of the darkest periods of Ukrainian history. Driving a social and political wedge between Ukraine's Russian ethnic population and the Western leaning government in Kiev proved to be Russia's primary means for fulfilling its strategic objectives.

[59] Emilio Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," *Parameters* 47, no. 2 (2017): 57.

[60] Heidi Reisinger and Alexzander Golts, *Russia's Hybrid Warfare: Waging War Below the Radar of Traditional Collective Defense* (Rome: NATO Defense College, 2014), accessed January 19, 2019, http://www.ndc.nato.int/news/news.php?icode=732.

Another facet of Russian information operations revealed during the Ukraine conflict was Russia's use of social media to manipulate eastern Ukraine's social and political fabric. Since the onset of the conflict and the subsequent 2016 US presidential elections, investigative journalists and academic literature has extensively documented the existence of Russian social media "troll" factories.[61] The notorious troll factory located at 55 Savushkina Street in St. Petersburg is responsible for Russia's methodical effort to manipulate the information environment through social media platforms such as Facebook and Twitter.[62] The pro-Russian content produced in the St. Petersburg facility continues to target the aggrieved ethnic Russian populations living within Crimea and the Donbas region. Russia's influence operations targeting the Russian ethnic populations living within the Donbas demonstrates "the business of war does not occur as some independent and isolated event, but unfolds within a broad field of unique natural, social, and political conditions."[63] Russia is particularly skillful at manipulating social and political variables to promote its interests, both operationally and strategically.

Since the Ukrainian conflict, the target of Russian information operations has expanded to include strategic objectives. Julian Lindley-French finds that "Moscow has established a new level of ambition – strategic *Maskirovka* – by which disinformation is applied against all levels of NATO's command chain and wider public opinion to keep the West politically and militarily off-balance."[64] This is mainly achieved through Russia's use of state media outlets to promote a pro-Russian narrative and sow disharmony within socially and politically delicate environments.

[61] Evan Osnos, Joshua Yaffa, and David Remnick, "Trump, Putin, and the New Cold War," *The New Yorker*, March 6, 2017, accessed January 11, 2019, https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war.

[62] David Patrikarakos, *War in a 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century* (New York: Basic Books, 2017), 141.

[63] Roger Ames, ed., *Sun Tzu: The Art of War* (New York: Ballantine Books, 1993), 76.

[64] Julian Lindley-French, "NATO: Countering Strategic Maskirova" (Calgary: Canadian Defense and Foreign Affairs Institute, 2015), accessed December 12, 2018, https://d3n8a8pro7vhmx.cloudfront.net /cdfai/pages /543/ attachments /original/ 1432247421/NATO_Countering_Strategic_ Maskirovka.pdf.

Russian state sponsored news organizations such as Russia Today (RT) and Sputnik provide Russian domestic and international media markets an alternative voice that promotes pro-Russian news stories while attacking democratic ideologies and institutions. Some estimate the Russian government spends around $1 billion dollars per year on international media broadcasting targeting foreign audiences.[65]

An example of Russia's war of public opinion occurred in Germany in 2016 as Russia's media incensed portions of the German population through a distorted media report. Russian media outlets mislead the German public about a 13-year-old Russian-German girl allegedly sexually assaulted by a group of Arab migrants.[66] A police investigation later revealed that the girl had misled authorities after she admitted to running away from home and fabricating her story to avoid punishment from her parents. However, Russian media outlets used the initial police report of the girl's supposed attack by migrants to stir divisions among the German population that exacerbated hostilities toward German Chancellor Angela Merkel's pro-immigrant policies. Russia's manipulation of social media and traditional news feeds to sow discontent within targeted audiences has proven a threat to democratic societies and institutions.

Russia: Cyber Domain

Russia has revealed a prowess for manipulating the cyber domain to support its geopolitical objectives. During the 2008 Russo-Georgian War, the Russian military, supported by the Ossetian militia, engaged the Georgian military over political and economic disputes. David Hollis claims that Russia's 2008 invasion of Georgia "appears to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions with the other

[65] Jill Dougherty, "How the Media Become one of Putin's Most Powerful Weapons," *The Atlantic*, April 2015, accessed January 13, 2019, https://www.theatlantic.com/international/archive/2015/04/how-the-media-became-putins-most-powerful-weapon/391062/.

[66] Andreas Rink and Paul Carrel, "German-Russian Ties Feel Cold War Style Chill Over Rape Case," *Reuters*, February 1, 2016, accessed January 3, 2019, https://www.reuters.com/article/us-germany-russia/german-russian-ties-feel-cold-war-style-chill-over-rape-case-idUSKCN0VA31O.

warfighting domains."[67] Similar to the Russian cyberattacks of the Estonian government in 2007, Russian hackers overwhelmed Georgian government and financial websites through a coordinated distributed denial of service attack. During the conflict, Russia successfully demonstrated its propensity for hybrid warfare against pro-Western nations as the Russian military combined information, cyber, and conventional warfare into its operations. In addition, Russia's use of hybrid warfare in Georgia – and Ukraine in 2014 – provide NATO's former Soviet bloc countries with much apprehension as they seek to avoid the same fate of Crimea. During the Russo-Ukrainian conflict, cyberattacks against Ukrainian governmental targets reveal Russia's polished skills to employ non-lethal effects through the cyber domain.

Following the exodus of President Yanukovych to Russia, Ukrainian officials quickly moved to provide the populace with a legitimate democratic government by holding a nation-wide presidential election. As conflict spread between pro-Russian separatists and Ukrainian forces in eastern Ukraine, the acting government in Kiev moved to steady Ukrainian society. Just days before the scheduled election, officials from the Ukrainian Central Election Commission discovered that a cyberattack on its computer networks disabled their ability to display real-time voting results.[68] In addition, a distributed denial of service attack on the election commission's networks attempted to overwhelm and crash the system as Ukrainian citizens began casting their ballots.

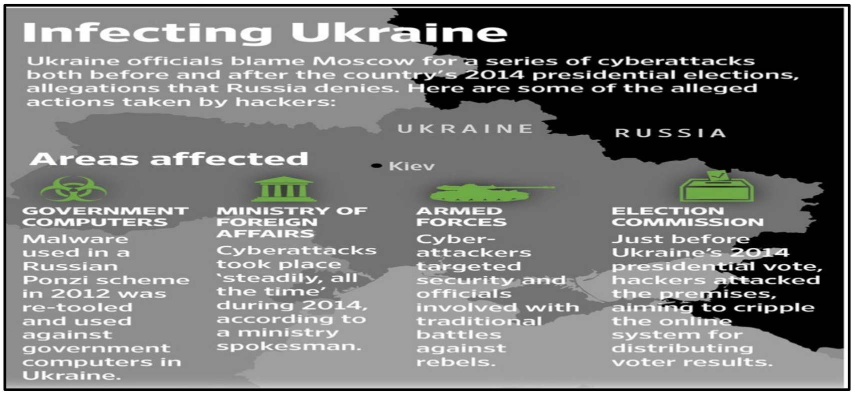
Ukraine computer and cyber experts struggled to maintain the integrity of their networks as perverse actors attempted to derail the election. These cyberattacks were later linked to a Russian hacking group named CyberBerkut after the group publicly claimed responsibility for the

[67] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small War Journal,* January 2011, accessed December 16, 2018, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

[68] Margaret Coker and Paul Sonne, "Ukraine: Cyberwar's Hottest Front," *The Wall Street Journal,* November 9, 2015, accessed December 2, 2018, https://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671.

attacks.[69] Although not directly linked to the Russian government, CyberBerkut and similar Russian hacking groups work to disrupt targeted networks through the cyber domain on behalf of the Russian government, proving Moscow with plausible deniability.

Russian cyberattacks against Ukraine were not limited to the Central Election Commission, but instead targeted multiple government institutions and their networks. For example, Russian cyberattacks also targeted the Ministry of Foreign Affairs and Ukrainian military units engaged in eastern Ukraine. Figure 4 illustrates the government entities targeted by Russian cyberattacks. The incorporation of the cyber domain into its strategic and operational approaches to the Ukrainian conflict provided the Kremlin with a non-lethal tool to stoke political chaos. James Wirtz finds Russia's cyber activities during the Ukrainian conflict "offer the best example of the employment of cyberattacks to shape the overall political course of a dispute."[70] When combined with Russian information operations, Russia's cyber operations proved especially effective at promoting Russian geopolitical interests while creating a *fait accompli* to fend off a Western response.



Infecting Ukraine

Ukraine officials blame Moscow for a series of cyberattacks both before and after the country's 2014 presidential elections, allegations that Russia denies. Here are some of the alleged actions taken by hackers:

GOVERNMENT COMPUTERS
Malware used in a Russian Ponzi scheme in 2012 was re-tooled and used against government computers in Ukraine.

MINISTRY OF FOREIGN AFFAIRS
Cyberattacks took place 'steadily, all the time' during 2014, according to a ministry spokesman.

ARMED FORCES
Cyber-attackers targeted security and officials involved with traditional battles against rebels.

ELECTION COMMISSION
Just before Ukraine's 2014 presidential vote, hackers attacked the premises, aiming to cripple the online system for distributing voter results.

Figure 4. Margaret Coker and Paul Sonne, "Ukraine: Cyberwar's Hottest Front," *The Wall Street Journal,* November 9, 2015, accessed December 2, 2018, https://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671.

[69] Coker, "Ukraine: Cyberwar's Hottest Front."

[70] James Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," in "Cyber War in Perspective: Russian Aggression Against Ukraine," ed. Kenneth Geers, special issue (NATO Cooperative Cyber Defense Center of Excellence, 2015), accessed January 22, 2019, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf.

China: Information Domain

A component to China's three-pronged information warfare strategy is psychological warfare. China's psychological warfare, or information warfare (*xinxi zhanzheng*), has its origins in classical Chinese strategy. The fundamental objective of Chinese psychological operations is to attack the adversary's morale, or *shiqi.*[71] As China's information warfare evolves, many China scholars point to a common theme that runs throughout Chinese information warfare writings: information dominance. Moreover, as China's Central Military Commission enacts recent military reforms, the Strategic Support Force (SSF) will "integrate and consolidate intelligence, communications, and technical reconnaissance with cyber warfare and electronic warfare to create an information dominance force."[72] According to cyber analyst Emilio Iasiello, China's "information dominance has two primary targets: the physical information infrastructure and the data that has passed through it, and perhaps more importantly, the human agents that interact with those data, especially those making decisions."[73] Operations within the information and cyber domains continue to offer China a low-intensity tool to conduct nonlinear warfare that aims to thwart its adversaries while protecting the CCP's domestic narrative of promoting the "Chinese Dream."

China's recent actions regarding the ongoing dispute over the South China Sea provides an opportunity to analyze its use of the "Three Warfares" to shape both domestic and international perceptions. In order to avoid a conventional conflict over its territorial claims, China is employing its nonlinear doctrine to keep regional challengers at a distance. China is

[71] Timothy Walton, *China's Three Warfares* (Herndon, VA: Delex Consulting, Studies and Analysis, 2012), accessed December 12, 2018, http://indianstrategicknowledgeonline.com/web/Three%20Warfares.pdf.

[72] John Costello, "China Finally Centralizes Its Space, Cyber, Information Forces," *The Diplomat*, January 20, 2016, accessed December 3, 2018. https://thediplomat.com/2016/01/china-finally-its-centralizes-space-cyber-information-forces/.

[73] Emilio Iasiello, "China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities," *Journal of Strategic Security* 9, no. 2 (2016): 55.

engaging in psychological and information warfare over the South China Sea as a means to promote its territorial claims while countering voices of protest. China's employment of psychological warfare prior to conflict is characterized by the posturing of its military forces or other instruments of national power with the "intention of intimidating adversaries and encouraging the acquiescence to PRC-desired outcome."[74] For example, China's intimidation of its neighbors within the South China Sea is partly achieved through the deployment of its maritime militia to strengthen its territorial claims.

China's maritime militia is composed of thousands of civilian vessels that fall under the informal control of the Chinese government. When deployed in service of the People's Liberation Army Navy (PLAN), experts posit these vessels have the potential to disrupt economic shipping lanes, attack offshore oil rigs, and interrupt US Naval operations in the region.[75] By subverting traditional rules of the sea, China's maritime militia has a negative effect on its adversary's ability to grasp China's true intentions when encountering the maritime militia. The employment of China's maritime militia "complicates the battlespace, degrades any opponent's decision-making process and exposes adversaries to political dilemmas."[76] By placing its adversaries in a psychological and political predicament, China is able to influence both the physical and information space by creating confusion within the decision-makers of those challenging China's claims to the South China Sea. In addition to using psychological warfare to influence the

[74] Doug Livermore, "China's Three Warfares in Theory and Practice in the South China Sea," Georgetown Security Studies Review, March 25, 2018, accessed December 15, 2018. http://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/.

[75] James Stavridis, "Maritime Hybrid Warfare is Coming," *Proceedings Magazine,* December 2016, accessed December 8 2018. https://www.usni.org/magazines/proceedings/2016-12-0.

[76] James Kraska, "China's Maritime Militia Upends Rules on Naval Warfare," *The Diplomat,* August 10, 2015, accessed January 11, 2019, https://thediplomat.com/2015/08/chinas-maritime-militia-upends-rules-on-naval-warfare/.

information domain, China is adept at incorporating media warfare to shape the narrative to its advantage.

China's use of media warfare is intended to influence both domestic and international audiences as a means to legitimize the CCP's policies and actions within China and throughout the region. Media warfare, sometimes referred to as public opinion warfare, "is aimed at influencing domestic and international public opinion to build public and international support for China's military actions and to dissuade an adversary from pursuing policies perceived to be averse to China's interests."[77] The medium used to transmit public opinion warfare can include television, newspapers, journals, and cyberspace. In addition, the cyber domain provides ample opportunity for China to shape public opinion through the Internet and social media. As China's influence continues to grow both economically and militarily, China acknowledges the need to increase its soft power within the region and abroad. Furthermore, China's need to propagate a pro-Chinese narrative through the effective use of the media is amplified as the Chinese endeavor to counter the dominance of Western media and culture throughout the world. A recent example of China's strategic use of public opinion warfare involves its citizens' use of social media to shape opinions and attitudes regarding maritime territorial disputes within the South China Sea.

In 2016, the Permanent Court of Arbitration (PCA) ruled in favor of the Philippines in its dispute with China over its "nine-dash line" claims within the South China Sea. Shortly after the PCA ruling, Chinese celebrities such as Zhang Jinlai, Zhao Wei and Fan Bingbing launched a social media barrage to denounce the PCA's findings and the Philippines actions while asserting China's rightful claims to the South China Sea.[78] All three celebrities have millions of followers

[77] Office of the Secretary of Defense. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2010*, accessed January 6, 2019, https://dod.defense.gov/Portals/1/Documents/pubs/2010_CMPR_Final.pdf.

[78] Tong, Linh. "The Social Media War Over the South China Sea." *The Diplomat*, July 16, 2016, accessed January 4, 2019, https://thediplomat.com/2016/07/the-social-media-war-over-the-south-china-sea/.

on Chinese Twitter – Weibo – and able to reach households throughout China with their social media messages. Though the anti-Philippines social media posts were spread only by Chinese celebrities and not directly by the Chinese government, it is clear Chinese internal propaganda is effective in promoting Chinese nationalistic views. Elsa Kania finds that "public opinion warfare involves using public opinion as a weapon through propagandizing through various forms of media in order to weaken the adversary's "will to fight" while ensuring the strength of will and unity among one's own side."[79] China continues to engage in the war of public opinion over maritime territorial disputes in the South China Sea. As China rebukes the authority of the South China Sea PCA findings, it shapes both international and domestic opinion through enhanced media strategies designed to promote a pro-Chinese narrative. Another strategic and operational tool used by China to promote its interests is the cyber domain.

China: Cyber Domain

China's determination to achieve information dominance within cyberspace is reflected through its use of the cyber domain to counter its geopolitical rivals. As a means to counter US dominance within the region, China engages in cyber operations "in an effort to extract information from diplomatic, economic, and defense industrial base sectors that support US national defense programs."[80] Furthermore, China's activities within cyberspace provide another example of its employment of the psychological component of "Three Warfares" to achieve its national security objectives. As previously discussed, a chief target of China's information dominance is the adversary's physical information infrastructure and the data that is transmitted within cyber nodes. For example, in 2010 Pentagon analysts discovered that China cyberattacks

[79] Elsa Kania, "The PLA'a Latest Strategic Thinking on the Three Warfares," *Jamestown Foundation: China Brief* 16, no.12 (August 2016), accessed December 14, 2018, https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/.

[80] Iasiello, "China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities," 46.

were responsible for "numerous computer systems around the globe, including US government systems, have been the target of Chinese offensive cyber operations" with the "exfiltration of massive amounts of data of strategic or military utility."[81] Moreover, the majority of Chinese cyberattacks against US networks are economically motivated as Chinese hackers target intellectual property, costing American companies hundreds of billions of dollars per year.[82] China's engagement in cyberespionage is not limited to economic targets, but instead extends into the US national security apparatus.

In addition to pursuing US intellectual property associated with domestic corporations and technology, Chinese hackers target the US military industrial base and defense contractors. For example, in 2018 Chinese hackers breached the secure computer systems of US Navy contractors, stealing a treasure trove of classified data related to an ongoing undersea warfare project.[83] China's cyber espionage targeting the US national defense establishment is motivated by their desire to gain US military technology that can be used to deliver Chinese military technologies and capabilities on par with the United States. In addition to attaining US Naval technology secrets, Chinese hackers have also attained data on US weapon systems such as the Joint Strike Fighter, the Patriot PAC-3 missile system, and the Littoral Combat Ship.[84] With the goal of achieving parity with US conventional military forces, China is forced to steal US conventional military technology through the cyber domain.

[81] George Manson, "Cyberwar: The United States and China Prepare for the Next Generation of Conflict," *Comparative Strategy* 20, no. 2, (April 2011): 123.

[82] Kate O'Keefe, "U.S. Adopts New Battle Plan to Fight China's Theft of Trade Secrets," *Wall Street Journal,* November 12, 2018, accessed December 20, 2018. https://www.wsj.com/articles/u-s-deploys-new-tactics-to-curb-chinas-intellectual-property-theft-1542027624.

[83] Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *The Washington Post,* June 8, 2018, accessed January 18, 2019, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-atrove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?utm_term=.dafac70f40b3.

[84] Ibid.

Conclusion: Comparing Russian and Chinese Nonlinear Warfare

Within an open system framework, the environment is composed of a multiplicity of actors vulnerable to influence. When discussing systems theory, Jamshid Gharajedaghi describes the concept of transactional environment where little is actually controlled, but influence can be exerted over the actors in an open system.[85] Through the information and cyber domains, Russia and China exert influence within their respective spheres of influence. Although unable to completely control their environments, both Russia and China are capable of influencing certain actors within the system to attain more favorable conditions. As China targets domestic and international actors to promote its South China Sea narrative, Russia stokes chaos in Western leaning nations along its periphery to keep the West off-balance. Social, economic, and political factors increase the complexity within each environment, providing Russia and China with ample targets for their information and cyber operations.

Information Domain

A clear distinction between Russia and China in their employment of information operations is Russia's more aggressive employment of information warfare. First, Russia has proven highly adept at combining unconventional and conventional warfare to achieve its political goals. Russian military operations in Georgia and Ukraine demonstrate an evolution of nonlinear warfare that culminated with Russia's successful annexation of Crimea in 2014. Next, it is evident that Russia is more aggressive than China in information warfare, especially when considering Russia's practice of using active measures to target its adversaries through propaganda and disinformation. Russian active measures influence the populations of sovereign nations on its periphery functions to propagate a Russian narrative while sowing discord as Russia seeks to promote its geopolitical interests. Russia's interference in the 2016 US presidential elections, characterized by Russia's support of social media trolls and other methods

[85] Jamshid Gharajedaghi, *Systems Thinking: Managing Chaos and Complexity: A Platform for Designing Business Architecture*, 3rd ed. (Amsterdam: Morgan Kaufmann, 2011), 32.

of disinformation to aggravate fissures within the US electorate, provides an example of Russia's aggressive use of information operations.

China has yet to demonstrate such brashness of technique in the South China Sea or elsewhere, choosing instead to rely mainly on nonmilitary methods to promote its interests as outlined in the "Three Warfares." Chinese information operations as described within the components of the "Three Warfares" remain indirect when compared to Russian information operations. When describing Chinese information operations, Marzarr finds that "China tends to favor patient, indirect approaches if at all possible, a preference grounded in classic Chinese strategic thought."[86] It is apparent that China will continue to use the information and cyber domains and as its primary tools for conducting nonlinear warfare. However, scholars are now looking for evidence that China might begin to incorporate information operations into gray zone activities similar to the Russian hybrid warfare in display in 2014. Continued territorial disputes within the South China Sea might provide China with an opportunity to use a gray zone strategy to incorporate these disputed territories within its orbit via *fait accompli*. If China moves toward a more aggressive position in the South China Sea, the deployment of "little blue men" to take control of disputed islands will indicate that China is using the Russian nonlinear techniques.

Cyber Domain

The recent technological evolution of the cyber domain provides China and Russia with tools to wield their influence within their respective regional systems. Chinese and Russian hackers have proven proficient in their ability to challenge Western influence through cyberattacks and cyberespionage. More importantly, both Russia and China are using cyberspace as a medium to distribute a narrative – through government sponsored news sites and social media – that promote their interests to regional and international audiences. While China and

[86] Michael Mazarr, "Mastering the Gray Zone: Understanding a Campaign Era of Conflict, Strategic Studies Institute (December 2015): 82.

Russia share some similarities within cyberspace in how each employ information operations, there are also clear distinctions between each modus operandi.

Russia's preference for cyberattacks versus the use of cyberespionage reflects its principal goal of spreading chaos within targeted systems. As previously mentioned, Russia's distributed denial-of-service-attacks against Georgia and Estonia contributed to degraded and interrupted public services. These disruptions aimed to influence the local populace and government. By targeting these actors, Russia intended to cultivate fissures between the local populace and their government. It is within these molested political and societal fractures that Russia excels at increasing chaos and discord within targeted systems. The same methods were employed against Ukraine in 2014 as Russia sought to drive a wedge between the government and its people. Janis Berzinis claims, "the Russian view of modern warfare is based on the idea that the main battlespace is the mind, and as a result, new-generation warfare wars are to be dominated by information and psychological warfare."[87] The cyber domain remains the primary conduit that allows Russia to "attack the minds" of its opponents through coordinated cyber and information operations.

While Russia's cyber operations are predominantly defined by cyberattacks, Chinese tendencies within the cyber domain persist in its propensity for cyberespionage. From the theft of US intellectual property to the theft of US military technology, Chinese behavior within the cyber domain is cause for concern. China's unlawful collection of intellectual property and military technology is tethered to its long-term economic and military goals. As China's economy and regional influence grows, it conducts cyberespionage against the United States and other nations in support of its national objectives.[88] For example, China's 13th Five-Year Plan highlights

[87] Janis Berzins, *Russia's New Generation Warfare in Ukraine: Implications for the Latvian Defense Policy* (National Defense Academy of Latvia Center for Security and Strategic Research), accessed February 10, 2019, https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf.

[88] Iasiello, "China's Three Warfares Strategy," 4.

China's desire to be more globally competitive in biopharmaceuticals and robotics.[89] China's desire to dominate certain economic markets drives its activities within the cyber domain to steal US intellectual property from within these economic sectors.

Recommendations

The case studies within this monograph demonstrate that Russian and Chinese nonlinear warfare is persistent. Both states exploit evolving technological advances within the cyber and information domains to their advantage. Conducting cyber and information operations against the West allows both Russia and China to distort the space between war and peace, which generates many dilemmas for military planners. Countering Russian and Chinese nonlinear warfare is a vast challenge for the United States, which requires a concerted effort among the national security establishment to counter. A recent publication from the US Army Training and Doctrine Command (TRADOC) finds that China and Russia "have blurred the distinctions between actions "below armed conflict" and "conflict," enabling the achievement of strategic objectives short of what the US traditionally considers war."[90] In order to design effective campaign plans to counter Russia and China in the space between war and peace, planners should consider adapting its operational art architecture for nonlinear warfare.

A planning framework for countering nonlinear threats requires an adapted operational art framework for comprehending these ill-structured problems. Military commanders and their planners must understand that twenty-first century competition and conflict between the United States and its near-peer adversaries is continuous. Cold War history offers a useful example. At

[89] US Congress, 2017 Report to Congress of the U.S. – China Economic and Security Review Commission, 115th Cong., 1st sess., 2017, accessed February 2, 2019, https://www.uscc.gov/sites/default/files/annual_reports/2017%20Executive%20Summary%20and%20Recommendations_1.pdf.

[90] US Department of the Army, *TRADOC Pamphlet 525-3-1, The US Army in Multi-Domain Operations 2028* (Washington, DC: Government Printing Office, 2018), 8.

the onset of the Cold War, George Kennan identified the Soviet Union's use of political warfare against the West as a serious challenge to US national security and its global interests. In his 1948 Policy Planning Staff Memorandum, Kennan defines political warfare as the "employment of all the means at a nation's command, short of war, to achieve its national objectives."[91] Kennan identifies both "white propaganda" and "black psychological warfare" as mechanisms used within political warfare to overtly and covertly achieve national objectives.[92] Applying Kennan's political warfare framework to the current strategic and operational environment is useful to military planners. Structures and processes used to counter these threats will be identified by military planners and then incorporated into campaign plans.

Designing campaigns to counter nonlinear warfare – specifically within the cyber and information domains – requires planners to use a "grammar" unique to this type of conflict. The elements of operational art provide planners with conceptual tools that assist with understanding the operational environment associated with LSCO.[93] Revision of these intellectual planning tools is needed for nonlinear warfare. For example, a modified list for nonlinear warfare would eliminate end state and conditions as an option. In an era of constant competition with near-peer adversaries, planners must conceptualize conflict within the cyber and information domains as never-ending. Operational planning tools must reflect this.

[91] George Kennan, "Memo on Political Warfare," Policy Planning Staff Memorandum, accessed March 3, 2019, https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=941dc9ee5c6e51333ea9ebbbc9104e8c.

[92] Ibid.

[93] US Department of the Army, *Field Manual (FM) 3-0, Operations* (Washington, DC: Government Printing Office, 2017), 1-20.

Bibliography

Allison, Graham. *Destined for War: Can America and China Escape Thucydides' Trap?* New York: Harcourt Press, 2017.

Ames, Roger, ed. *Sun Tzu: The Art of War,* New York: Ballantine Books, 1993.

Barno, David, and Nora Bensahel. "A New Generation of Unrestricted Warfare." *War on the Rocks*, April 19, 2016. Accessed November 16, 2018. https://warontherocks.com/2016/04/a-new-generation-of-unrestricted-warfare.

Bartles, Charles. "Getting Gerasimov Right." *Military Review* 96, no. 1 (2016): 30-38.

Beeson, Mark. "China Rises, America Falters, and Geoeconomics Rears its Head." *War on the Rocks*, August 23, 2018. Accessed November 20, 2018. https://warontherocks.com/2018/08/china-rises-america-falters-and-geoeconomics-rears-its-head.

Costello, John. "China Finally Centralizes Its Space, Cyber, Information Forces." *The Diplomat*. January 20, 2016. Accessed December 3, 2018. https://thediplomat.com/2016/01/china-finally-its-centralizes-space-cyber-information-forces/.

Dougherty, Jill. "How the Media Become one of Putin's Most Powerful Weapons." *The Atlantic,* April 2015. Accessed January 13, 2019. https://www.theatlantic.com/international/archive/2015/04/how-the-media-became-putins-most-powerful-weapon/391062/.

Echevarria, Antulio J. "American Operational Art, 1917-2008." In *The Evolution of Operational Art: From Napoleon to the Present*, edited by John Andreas Olsen and Martin van Creveld. New York: Oxford University Press, 2011.

Gerasimov, Valery. "The Value of Science in Foresight: New Challenges Demands Rethinking the Forms and Methods of Carrying Out Combat Operations." Translated by Robert Coalson. *Military Review* 96, no. 1 (January-February 2016): 23-29.

Gharajedaghi, Jamshid. *Systems Thinking: Managing Chaos and Complexity: A Platform for Designing Business Architecture*. 3rd ed. Amsterdam: Morgan Kaufmann, 2011.

Greenwood, T. C. "War Planning for Wicked Problems." *Armed Forces Journal* (December 2009). Accessed September 28, 2018. http://armedforcesjournal.com/war-planning-for-wicked-problems.

Halper, Stephan. *China: The Three Warfare*. Washington, DC: Office of the Secretary of Defense, 2013.

Hoffman, Frank G. *The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War*. Washington, DC: The Heritage Foundation, 2016. Accessed October 3, 2018. https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_ Essays _Hoffman.pdf.

———. “On the Not-So-New Warfare: Political Warfare VS Hybrid Threats.” *War on the Rocks*. July 28, 2014. Accessed October 16, 2018. https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats.

———. “Hybrid Warfare and Challenges.” *Joint Force Quarterly*, no. 52 (Fall 2009): 34-39.

Hollis, David. “Cyberwar Case Study: Georgia 2008.” *Small War Journal,* January 2011. Accessed December 16, 2018. http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

Iasiello, Emilio. “China’s Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities.” *Journal of Strategic Security* 9, no. 2 (2016): 45-69.

———."Russia's Improved Information Operations: From Georgia to Crimea." *Parameters* 47, no. 2 (2017): 51-63.

Kania, Elsa. “The PLA’a Latest Strategic Thinking on the Three Warfares.” *Jamestown Foundation: China Brief* 16, no. 12 (August 2016). Accessed December 13, 2018. https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares.

Kennan, George. “Memo on Political Warfare.” Policy Planning Staff Memorandum, May 4, 1948. Accessed March 3, 2019. https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=941dc9ee5c6e51333ea9ebbbc9104e8c.

Kofman, Michael, and Matthew Rojansky. *A Closer Look at Russia’s Hybrid War*. Washington, DC: The Wilson Center, 2015, accessed October 14, 2018 https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf.

Kotkin, Stephen. “Russia’s Perpetual Geopolitics: Putin Returns to the Historical Pattern.” *Foreign Affairs*, May/June 2016.

Kraska, James. “China’s Maritime Militia Upends Rules on Naval Warfare.” *The Diplomat.* August 10, 2015. Accessed January 11, 2019. https://thediplomat.com/2015/08/chinas-maritime-militia-upends-rules-on-naval-warfare/.

Krepinevich, Andrew. “How to Deter China: The Case for the Archipelagic Defense.” *Foreign Affairs*, March/April 2015.

Kux, Dennis. “Soviet Active Measures and Disinformation: Overview and Assessment.” *Parameters, Journal of the US Army War College* 15, no. 4 (Winter 1985): 19-28.

Lindley-French, Julian. “NATO: Countering Strategic Maskirova.” Calgary: Canadian Defense and Foreign Affairs Institute, 2015. Accessed December 12, 2018. https://d3n8a8pro7vhmx.cloudfront.net /cdfai/pages /543/ attachments /original/ 1432247421/NATO_Countering_Strategic_ Maskirovka.pdf.

Livermore, Doug. “China’s Three Warfares in Theory and Practice in the South China Sea.” *Georgetown Security Studies Review*. March 25, 2018. Accessed December 15, 2018. http://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/.

Manson, George. “Cyberwar: The United States and China Prepare for the Next Generation of Conflict.” *Comparative Strategy* 20, no. 2 (April 2011): 122-137.

Mattis, Peter. “Contrasting China’s and Russia’s Influence Operations.” *War on the Rocks*. January 16, 2018. Accessed October 3, 2018. https://warontherocks.com/2018/01/contrasting-chinas-russias-influence-operations.

Mazarr, Michael J. “Mastering the Gray Zone: Understanding a Campaign Era of Conflict.” Strategic Studies Institute, December 2015.

Murray, Williamson and Peter R. Mansoor, eds. *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge: Cambridge University Press, 2012.

Office of the Secretary of Defense. *Annual Report to Congress: 2010 Military and Security Developments Involving the People’s Republic of China*. https://dod.defense.gov/Portals/1/Documents/pubs/2010_CMPR_Final.pdf.

O’Keefe, Kate. “U.S. Adopts New Battle Plan to Fight China’s Theft of Trade Secrets.” *The Wall Street Journal.* November 12, 2018. Accessed December 20, 2018. https://www.wsj.com/articles/u-s-deploys-new-tactics-to-curb-chinas-intellectual-property-theft-1542027624.

Osnos, Evan, Joshua Yaffa, and David Remnick. "Trump, Putin, and the New Cold War.” *The New Yorker,* March 6, 2017. Accessed January 11, 2019. https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war.

Patrikarakos, David. *War in a 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century*. New York: Basic Books, 2017.

Schmitt, John F. “A Systemic Concept for Operational Design.” Accessed October 21, 2018. http://www.au.af.mil/au/awc/awcgate/usmc/mcwl_schmitt_op_design.pdf.

Schnaufer, Tad. “Redefining Hybrid Warfare: Russia’s Non-Linear War Against the West.” *Journal of Strategic Security* 10, no. 1 (2016): 17-31.

Scott, Malcolm. “Here’s How Fast China’s Economy is Catching Up to the U.S.” *Bloomberg*, May 24, 2018. Accessed November 22, 2018. https://www.bloomberg.com/graphics/2016-us-vs-china-economy.

Sherr, James. *Hard Diplomacy and Soft Coercion: Russia’s Influence Abroad.* London: Chatham House, 2013.

Stavridis, James. “Maritime Hybrid Warfare is Coming.” *Proceedings Magazine.* December 2016. Accessed December 8, 2018. https://www.usni.org/magazines/proceedings/2016-12-0.

Szayna, Thomas. *What Are the Trends in Armed Conflicts, and What Do They Mean for U.S. Defense Policy?* Santa Monica, CA: RAND Arroyo Center, 2017, Accessed October 16, 2018, https://www.rand.org/pubs/research_reports/RR1904.html.

The White House. *The National Security Strategy of the United States of America*. Washington, DC, December 2017.

Thomas, Timothy. "Russia's Reflexive Control Theory and the Military." *Journal of Slavic Military Studies,* 17 (2004): 230-239.

———. "The Evolving Nature of Russia's Way of War." *Military Review* 97, no. 4 (July-August 2017): 34-42.

Tong, Linh. "The Social Media War Over the South China Sea." *The Diplomat*, July 16, 2016. Accessed January 4, 2019. https://thediplomat.com/2016/07/the-social-media-war-over-the-south-china-sea/.

US Congress. Senate. Conference Report Highlights: National Defense Authorization Act for Fiscal Year 2018. 115th Cong, 1st sess., 2017.

Wass de Czege, Huba. "Systemic Operational Design: Learning and Adapting in Complex Missions." *Military Review*, no. 1 (January-February 2009): 2-12.

Wirtz, James. "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy." In *Cyber War in Perspective: Russian Aggression Against Ukraine*, edited by Kenneth Geers. Special issue, NATO Cooperative Cyber Defense Center of Excellence, 2015. Accessed January 22, 2019. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf.

US Department of Defense. Joint Staff. *Joint Publication (JP) 3-0, Joint Operations.* Washington, DC: Government Printing Office, 2018.

———. *Joint Publication (JP) 5-0, Joint Planning.* Washington, DC: Government Printing Office, 2017.

US Department of the Army. *Field Manual (FM) 3-0, Operations*. Washington, DC: Government Printing Office, 2017.

———. *TRADOC Pamphlet 525-5-500, Commander's Appreciation and Campaign Design*. Washington, DC: Government Printing Office, 2008.

———. *TRADOC Pamphlet 525-3-1, The US Army in Multi-Domain Operations 2028*. Washington, DC: Government Printing Office, 2018.