

NEW GENERATION WARFARE FOR AIR FORCE
SPECIAL OPERATIONS COMMAND

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

DANIEL R. JUCHCINSKI, MAJOR, USAF
MAS, Embry-Riddle Aeronautical University, Worldwide Campus, FL, 2011
BS, University of Illinois, Champaign-Urbana, IL, 2005

Fort Leavenworth, Kansas

2019

Approved for public release; distribution is unlimited. Fair use determination or copyright permission has been obtained for the inclusion of pictures, maps, graphics, and any other works incorporated into this manuscript. A work of the United States Government is not subject to copyright, however further publication or sale of copyrighted images is not permissible.

REPORT DOCUMENTATION PAGE				<i>Form Approved</i> <i>OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 14-06-2019		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From - To) AUG 2018 – JUN 2019	
4. TITLE AND SUBTITLE New Generation Warfare for Air Force Special Operations Command				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Daniel Robert Juchcinski				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)				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 The U.S. can learn a great deal from our competitions' accomplishments. Russian new generation warfare elevated information operations outside of the realm of national military power and into all types of national power. Superpowers evaluate this type of warfare for new tactics, techniques, and procedures (TTPs). Air Force Special Operations Command (AFSOC) is ideally placed to adapt new generation warfare TTPs given current capabilities, and the commands ability to change to an evolving operational environment. A literature review identified the pre-cursors to new generation warfare, new generation warfare development, new generation warfare characteristics, and possible AFSOC contributions to new generation warfare. A comparative case study of three recent conflicts provides a list of new generation warfare tactics. This thesis evaluated these tactics against AFSOC capabilities and the U.S. joint operations principles of restraint and legitimacy using a prescriptive research method. The evaluation provided AFSOC capabilities in support of new generation warfare tactics employment. The U.S. military is limited in its authorities compared to Russia, but new generation warfare tactics might be just the topic to challenge those old norms allowing the U.S. to adapt and overcome future adversaries.					
15. SUBJECT TERMS AFSOC, Russia, Ukraine, Estonia, Georgia, New Generation Warfare, Hybrid Warfare, MISO, Information Operations.					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT (U)	b. ABSTRACT (U)	c. THIS PAGE (U)			19b. PHONE NUMBER (include area code)
			(U)	77	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Daniel R. Juchcinski

Thesis Title: New Generation Warfare for Air Force Special Operations Command

Approved by:

_____, Thesis Committee Chair
Lieutenant Colonel Steven C. Hanson, M.S.

_____, Member
Richard E. Berkebile, Ph.D.

_____, Member
Lieutenant Colonel Christopher L. Schilling, MMAS

Accepted this 14th day of June 2019 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

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

ABSTRACT

NEW GENERATION WARFARE FOR AIR FORCE SPECIAL OPERATIONS
COMMAND, by Daniel R. Juchcinski, 77 pages.

The U.S. can learn a great deal from our competitors' accomplishments. Russian new generation warfare elevated information operations outside of the realm of national military power into all types of national power. Superpowers evaluate this type of warfare for new tactics, techniques, and procedures (TTPs). AFSOC is ideally placed to adapt new generation warfare TTPs given current capabilities, and the commands ability to change to an evolving operational environment.

A literature review identified the pre-cursors to new generation warfare, new generation warfare development, new generation warfare characteristics, and possible AFSOC contributions to new generation warfare. A comparative case study of three recent conflicts provides a list of new generation warfare tactics. This thesis evaluated these tactics against AFSOC capabilities and the U.S. joint operations principles of restraint and legitimacy using a prescriptive research method. The evaluation provided AFSOC capabilities in support of new generation warfare tactics employment. The U.S. military is limited in its authorities compared to Russia, but new generation warfare tactics might be just the topic to challenge those old norms allowing the U.S. to adapt and overcome future adversaries.

ACKNOWLEDGMENTS

I owe a huge debt of gratitude to my MMAS thesis committee members, in particular, my committee chair, Lt Col Steven Hanson. He provided excellent advice and guidance. Furthermore, he gave me the academic freedom to explore the topic and allowed me to take my research where it needed to go. Thanks to LTC Chris Schilling for reminding me of common pitfalls and issues this type of study. I appreciate his knowledge and experience. I also want to thank Dr. Lester Grau at the Foreign Military Studies Office. Although not part of my committee, he shared his wealth of knowledge about the Soviet Union and Russian history during the early stages of my research. Finally, Dr. Richard Berkebile for his quick and thoughtful edits to the dozens of rough drafts through the year. His exceptional dedication greatly motivated me to keep thinking and writing on this topic.

I must also thank my always supportive spouse, Ben, who has sacrificed so much for us to be together. The Saturday morning coffee shop reading and writing sessions for this thesis with him by my side were invaluable to my success. Without his support, I would not have completed this thesis, and I share this accomplishment with him.

TABLE OF CONTENTS

	Page
MASTER OF MILITARY ART AND SCIENCE THESIS APPROVAL PAGE	iii
ABSTRACT.....	iv
ACKNOWLEDGMENTS	v
TABLE OF CONTENTS.....	vi
ACRONYMS.....	viii
TABLES	ix
CHAPTER 1 INTRODUCTION	1
Background.....	1
Problem Statement.....	3
Primary and Secondary Research Questions	4
Key Definitions.....	4
New Generation Warfare	4
Hybrid Warfare	6
IW	7
IO and IE.....	8
Military Information Support Operations (MISO)	9
Methodology.....	10
Assumptions.....	11
Thesis Structure	11
CHAPTER 2 LITERATURE REVIEW	13
Pre-Cursor to New Generation Warfare	13
New Generation Warfare Development	14
New Generation Warfare Characteristics	17
AFSOC Contribution to New Generation Warfare.....	24
CHAPTER 3 RESEARCH METHODOLOGY	27
Research Limitations and Delimitations.....	27
Comparative Case Study Method	28
Prescriptive Research Method	29
CHAPTER 4 CASE STUDY	33

Russia-Estonia Conflict	33
Russia-Georgia Conflict	36
Russia-Ukraine Conflict	39
New Generation Warfare Tactics Evaluation	45
CHAPTER 5 WHY AFSOC?	47
Introduction.....	47
New Generation Warfare Applied to AFSOC	49
AFSOC Direct Support to New Generation Warfare	51
AFSOC Indirect Support to New Generation Warfare	52
Emerging Technology.....	53
CHAPTER 6 CONCLUSION.....	57
Implications	58
Future Research	60
Summary	62
BIBLIOGRAPHY.....	63

ACRONYMS

A2/AD	Anti-Access, Area Denial
AFSOC	Air Force Special Operations Command
AO	Area of Operation
DOD	Department of Defense
EU	European Union
GRU	English version of Russian acronym <i>ГРУ</i> , which means Main Intelligence Directorate
IE	Information Environment
IO	Information Operations
ISR	Intelligence, Surveillance, and Reconnaissance
IW	Irregular Warfare
MISO	Military Information Support Operations
NATO	North Atlantic Treaty Organization
NDS	National Defense Strategy
NSAv	Non-Standard Aviation
OE	Operational Environment
ROMO	Range of Military Operations
SOCOM	Special Operations Command
SOF	Special Operations Forces
U.S.	United States
VPK	<i>Voyenno-Promyshlennyy Kurier</i>

TABLES

	Page
Table 1. Estonia Conflict New Generation Warfare Tactics Summary.....	35
Table 2. Georgia Conflict New Generation Warfare Tactics Summary.....	38
Table 3. Ukraine Conflict New Generation Warfare Tactics Summary.....	44
Table 4. New Generation Warfare Tactics Summary.....	46
Table 5. AFSOC New Generation Warfare Tactics Bins	50

CHAPTER 1

INTRODUCTION

Print is the sharpest and strongest weapon of our party.

—Joseph Stalin, quoted in HQDA, FM 3-0, *Operations*

Background

Joseph Stalin, Soviet leader from 1922 to 1953, describes propaganda as the strongest weapon of the communist party during the reign of the Soviet Union.¹ The United States (U.S.) Army Field Manual 3-0, published in December 2017, uses Joseph Stalin's quote to start the information environment (IE) section of the publication.² Although the historic reference might seem unimportant to an average reader, the quote speaks volumes to anyone knowledgeable of Russian international policy. The 2018 National Defense Strategy (NDS) highlights Russian aggression towards their *near abroad* as challenging sovereign nations, projecting economic and diplomatic power, and impacting the security decisions of its neighbors.³ FM 3-0 highlights this as “a hybrid threat.”⁴

¹ Peter Kenez, *The Birth of the Propaganda State: Soviet Methods of Mass Mobilization, 1917-1929* (London, UK: Cambridge University Press, 1975), 31.

² Headquarters, Department of the Army (HQDA), Field Manual (FM) 3-0, *Operations* (Washington, DC: Government Printing Office, October 2017), 1-6.

³ Secretary of Defense (SecDef), *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge* (NDS) (Washington, DC: Department of Defense, January 2018), 2.

⁴ HQDA, FM 3-0, 1-6.

Although the Soviet Union collapsed in 1991, Russia re-emerged as an aggressive power led by President Vladimir Putin. In his first year as the Russian president in 1999, Putin focused his attention on a Chechen rebel incursion in the Russian Republic of Dagestan. President Putin gained high national approval for this initial effort and laid the foundation of a new generation of warfare.⁵ Stalinist propaganda provided Putin a starting point on which to build. Putin built on Soviet propaganda techniques using current technological capabilities and the internet. Russia's news media, multi-media, and information operations (IO) are a proven force multiplier for its political aspirations. Russia demonstrated great success in Estonia (2007), Georgia (2008), and Ukraine (2014 - present) using new generation warfare to influence the operational environment (OE) before conducting traditional warfare.

While Russia re-established itself, Air Force Special Operations Command (AFSOC), as the air component of Special Operations Command (SOCOM), established a growing counter-insurgency capability around the world. AFSOC and SOCOM focused on the irregular warfare (IW) counter-insurgency mission in a permissible threat environment for almost two decades after the 11 September 2001 attacks. The NDS and other current strategic Department of Defense (DOD) guidance, however, describe a future of large-scale combat operations against a near-peer adversary employing an anti-access/area denial (A2/AD) strategy to prevent U.S. from obtaining air superiority in the

⁵ Adi Ignatius, "A Tsar is Born: Person of the Year 2007," *Time Magazine*, 19 December 2007, para 3, accessed 30 March 2019. http://content.time.com/time/specials/2007/personoftheyear/article/0,28804,1690753_1690757_1690766,00.html.

area of operation (AO).⁶ This A2/AD strategy challenges AFSOC's current posture and capabilities geared toward counter-insurgency operations. AFSOC can confront future adversaries with new generation warfare's asymmetric tactics and capabilities.

Problem Statement

The DOD estimates that the OE of the future will include A2/AD areas integrating traditional warfare, IW, and hybrid warfare.⁷ An adversary employing A2/AD capabilities will also effectively manage a complex IE providing a sophisticated IO capability. IE integrates wireless communication systems, social media, and other information technology through the internet. This networked environment allows adversaries to exploit, disrupt, and disable military systems, critical infrastructure systems, and civilian systems through IO. IO disseminates misinformation, propaganda, foster mistrust, and discredit national legitimacy while promoting the adversary's creditability.⁸ Russian new generation warfare effectively manages this complex IE capability. Russia provides an excellent example to learn from by studying their actions towards multiple nations over the last decade.

Russia's new generation warfare has gone unchallenged by the U.S. military. This new type of warfare does not align with any U.S. military capability. The responsibility

⁶ SecDef, NDS, 2; Chairman, Joint Chiefs of Staff (CJCS), Joint Publication (JP) 3-0, *Operations* (Washington, DC: JCS, 17 January 2017), VI-1.

⁷ Frank G. Hoffman, "Hybrid Warfare and Challenges" *Joint Forces Quarterly* 52 (1st Quarter 2009): 34; Secretary of Defense (SecDef), *Department of Defense: Strategy for Operations in the Information Environment* (Washington, DC: Department of Defense, June 2016), 2.

⁸ SecDef, *Strategy for Operations in the Information Environment*, 2.

to combat this type of warfare, let alone adopt and evolve, is underdeveloped. Russia's new generation warfare would best align with IW. SOCOM is tasked to conduct IW. SOCOM is also responsible for counter-insurgency and consequently has few resources or efforts devoted to new generation warfare. In the future IE, SOCOM, and subsequently AFSOC, will need to master new generation warfare tactics efficiently. How?

Primary and Secondary Research Questions

The primary research question: "What Russian new generation warfare tactics could AFSOC adopt in future conflicts?" This question leads to other secondary research questions to explore the capabilities and limitations of new generation warfare analysis:

1. What are Russia's new generation warfare tactics?
2. How did Russia employ new generation warfare before and during the Estonian conflict in 2007, Georgian conflict in 2008, and Ukrainian conflict in 2014?
3. How can AFSOC employ new generation warfare tactics in an A2/AD environment?
4. What capabilities can AFSOC develop to enable new generation warfare?

Key Definitions

New Generation Warfare

Russia's new generation warfare is often incorrectly interchanged with the term hybrid warfare. Distinguishing the two types of warfare is essential. Hybrid warfare, defined in the next section, is contained inside a state's national military power and consists of both traditional warfare and IW employed in a complementary manner

focused on achieving a military objective towards a particular enemy.⁹ Russian new generation of warfare uses political, economic, diplomatic, and other non-military measures in combination with the use of military force.¹⁰ New generation warfare focuses first in the information domain and employs psychological warfare to manipulate, control, and demoralize the enemy population and military forces.¹¹ The guiding principle of new generation warfare is to defeat the enemy or severely weaken the enemy to avoid or limit traditional warfare. An aggressor utilizing new generation warfare involves all public institutions in the target states and surrounding states. Denial and obfuscation in the target state soften the enemy making them more pliable to the adversary's influence.¹² New generation warfare involves news media, religious organizations, non-governmental organizations, and social media to influence and persuade the population to directly or indirectly support adversary's objectives.¹³ The target state's population essentially becomes a proponent of the aggressor; an asymmetric action to the target state's ability to conduct war. Chapter 2 further explains new generation warfare's origin.

⁹ Hoffman, "Hybrid Warfare and Challenges," 34.

¹⁰ Charles K. Bartles, "Getting Gerasimov Right," *Military Review* (January-February 2016): 30-38, accessed 30 March 2019, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf.

¹¹ Sergei G. Chekinov and Sergei A. Bogdanov, "The Nature and Content of a New-Generation War," *Military Thought*, no. 4 (2013): 17.

¹² Richard E. Berkebile, "New Generation Warfare and the Just War Tradition," *InterAgency Journal* 9, no. 3 (2018): 18.

¹³ Chekinov and Bogdanov, "The Nature and Content of a New-Generation War," 17.

Hybrid Warfare

Over the last decade, theorists have inappropriately equated the western concept of hybrid warfare to Russia's new generation warfare. Anyone can search "Russian hybrid warfare" on an internet search engine and instantly find over four million results further promoting this idea that Russia is developing a new type of warfare – hybrid warfare.¹⁴ Lieutenant Colonel Frank G. Hoffman, U.S. Marine Corps (Retired) authored several publications discussing hybrid warfare over the last two decades and is often referenced by others when trying to capture the meaning of the term.¹⁵ Hoffman defines hybrid warfare as a combination of traditional warfare, IW, and criminal activity. "Hybrid war incorporates a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder."¹⁶ DoD Joint Publications describe traditional warfare, IW, terrorism, and criminal activities across the range of military operations (ROMO).¹⁷ Future enemies, using advancement in technology and hybrid warfare, could engage the U.S. at multiple levels of the ROMO, simultaneously. Hoffman provides several examples in history including Napoleon's battles in Spain between the

¹⁴ Google, "Results from A Google Search of 'Russian Hybrid Warfare'," 3 October 2018, accessed 3 October 2018, <https://www.google.com/search?q=russian+hybrid+warfare&oq=Russian+Hybrid+Warfare&aqs=chrome.0.0j69i60l3j69i59j0.5096j1j7&sourceid=chrome&ie=UTF-8>.

¹⁵ Hoffman, "Hybrid Warfare and Challenges," 34.

¹⁶ Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Warfare* (Arlington, VA: Potomac Institute for Policy Studies, December 2007), 14.

¹⁷ CJCS, JP 3-0, V-4.

traditional British Army and irregular Spanish guerrillas leading to devastating attrition of French forces and eventual fall of Napoleon's Spanish army.¹⁸ Hybrid warfare is a challenging and effective way to conduct operations, but a U.S. Marine coined the term, not the Russian military.

IW

JP 1-0 describes warfare as either being traditional or irregular.¹⁹ IW is a type of warfare consisting of a violent struggle between state and non-state actors for legitimacy and influence over the targeted audience.²⁰ Special operations forces (SOF) are specially assessed, trained, and equipped to conduct all forms of IW.²¹ IW is a persuasive form of warfare to gain control and influence over a population. SOF uses IW to provide an indirect or asymmetric approach along the full ROMO to erode the enemies power, influence, and will.²² SOF should employ IW in conjunction with diplomatic, informational, and economic forms of national power using Unified Action, as defined in JP 1-0.²³ IW will not only include U.S. SOF but also recognize the local militias, resistance fighters, and insurgents in opposition to the enemy's conventional military

¹⁸ Hoffman, "Hybrid Warfare and Challenges," 36.

¹⁹ Chairman, Joint Chiefs of Staff (CJCS), Joint Publication (JP) 1-0, *Doctrine for the Armed Forces of the United States* (Washington, DC: JCS, July 2017), I-5.

²⁰ Ibid., I-5.

²¹ Chairman, Joint Chief of Staff (CJCS), Joint Publication (JP) 3-05, *Special Operations* (Washington, DC: JCS, July 2014), II-1.

²² CJCS, JP 1-0, I-5.

²³ CJCS, JP 1-0, I-5, xiii.

forces.²⁴ Readers should not confuse IW with unconventional warfare. Unconventional warfare is a subset of IW with a narrower focus. SOF conduct unconventional warfare through or with a guerrilla force in a denied area to overthrow coerce, disrupt, or overthrow an opposition's government.²⁵

IO and IE

Joint Publication 3-13 defines IO as “integrated employment . . . of information-related capabilities . . . to influence, disrupt, corrupt, or usurp the decision making of adversaries while protecting our own.”²⁶ IO includes any interaction in the IE. In practice, IO is a key component in new generation warfare. IO allows the nation to consolidate gains and promote the legitimacy of actions to multiple audiences.²⁷ A new generation warfare strategy will include IO to control the narrative of intent and subverts opposition efforts to provide a counter-argument.²⁸ The IE is “the collection of individuals, organizations, and systems that collect, process, disseminate, or act on information.”²⁹ The IE allows a broad spectrum of capabilities available to any state and

²⁴ CJCS, JP 1-0, I-6.

²⁵ CJCS, JP 3-05, 8.

²⁶ Chairman, Joint Chief of Staff (CJCS), Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: JCS, 20 November 2014), ix.

²⁷ Vice Chairman, Joint Chiefs of Staff (VCJCS), *Joint Concept for Integrated Campaigning* (Washington, DC: JCS, 16 March 2018), 17.

²⁸ *Ibid.*, 21.

²⁹ CJCS, JP 3-13, I-1.

non-state actor determined to influence and persuade a target audience. The IE and IO provide a new venue and actions where new generation warfare shapes conflict.

Military Information Support Operations (MISO)

The U.S. President's Unified Command Plan designates SOCOM responsible for integrating and coordinating MISO in the IO domain.³⁰ MISO communicates information to an audience to “influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.”³¹ The joint warfighter manages MISO within the IO cell of joint operations center to synergize effects between public affairs, civil-military operations, and joint interagency coordination groups.³²

MISO variables include the type of audience, size of the audience, duration of effect, and desired outcome for a given military operation. MISO targets include adversaries, friendly forces, or neutral populations. MISO influences different audience sizes from a single person to an entire state's population. Furthermore, MISO achieves a range of desired effects over a given amount of time from only a few minutes to a lifetime of influence. MISO application contributes to all military operations spanning the ROMO.³³ MISO variables are managed by SOCOM through the IO cell to provide the desired effect for a joint force commander or geographic combatant commander.

³⁰ CJCS, JP 3-13, III-2.

³¹ Ibid., II-9.

³² Ibid., II-10.

³³ Ibid.

Methodology

The researcher adopted a mixed research method. The mixed research method follows the construct of a sequential explanatory approach. The subsequent explanatory strategy begins with a research approach followed by a different research approach to evaluate the collected tactics.³⁴ The first research method was a comparative case study of Russian new generation warfare methods in Estonia, Georgia, and Ukraine. The case study delimits the conflicts by time for Estonia (27 April – 10 May 2007), Georgia (7 – 15 August 2008), and Ukraine (27 February – 24 September 2014). The case study focused on Russian new generation warfare tactics activities.³⁵ Although the duration and scope of Russian new generation warfare vary between these three events, the case study focused on finding the similarities employed consistently through different events. After completing the case study, the researcher identified a clear list of common tactics associated with Russian new generation warfare.

The new generation warfare list is the starting point for the next method. The prescriptive research method provides a filter of possible tactics AFSOC could employ based on a threshold of evaluation criteria. The prescriptive research evaluation criteria are legitimacy, restraint, and AFSOC applicability. Restraint applied to joint operations prevents excessive use of force.³⁶ Restraint applied from the perspective of a reasonable citizen from an objective point of view. Legitimacy describes operations that maintain

³⁴ John W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 2nd ed. (Thousand Oaks, CA: Sage Publication, 2003), 215.

³⁵ Ibid., 15.

³⁶ CJCS, JP 3-0, A-3.

legal and moral authority.³⁷ The other joint operations principles published in JP 3-0 were considered but not applied based on their relevance to the IO domain. Finally, the AFSOC applicability was added as a criterion to ensure the thesis could answer the primary research question.

Assumptions

Some key assumptions to scope this research are:

1. Cyberspace operation attribution is often difficult or impossible to directly link. Offensive Cyberspace operations originating from Russian geographic borders are assumed to be linked to the Russian government directly or indirectly.
2. Although different from new generation warfare, this research includes hybrid warfare in the literature review to broaden readers perspective. The new perspective provides expanding detail on the interconnection between these different types of warfare. Based on the definition used, some new generation warfare tactics explained in this thesis could be considered hybrid warfare.

Thesis Structure

This thesis uses a six chapter format to answer the primary research question systematically. Chapter 2 distills the new generation warfare relevant literature to explain better where this type of warfare came from, how it has matured over the last few decades, and how some AFSOC capabilities could efficiently employ these tactics.

³⁷ CJCS, JP 3-0, A-4.

Chapter 3 explains the research method. The author describes the evaluation criteria to identify a list of tactics AFSOC can employ in future conflicts. Chapter 4 reviews recent conflicts in Estonia, Georgia, and Ukraine using a comparative case study. A new generation warfare tactics table summarizes and evaluates the comparative case study. Chapter 5 provides an AFSOC-tailored solution given the best tactics that pertain to the command's specific capabilities. Chapter 6 summarizes the intent of the thesis, the key implications, and provides possible future technology and capabilities that AFSOC could invest in better support new generation warfare operations in an A2/AD environment.

CHAPTER 2

LITERATURE REVIEW

The relevant literature on this topic is relatively broad spanning the last century. To better understand new generation warfare, the researcher includes hybrid warfare literature to encapsulate multiple perspectives even when the nomenclature is not perfectly aligned. The four components of this chapter are pre-cursor to new generation warfare, new generation warfare development, new generation characteristics, and AFSOC contribution to new generation warfare. The development section describes the history and evolution of this type of warfare. The characteristics section explains some fundamental themes, ideas, and principles repeated through past operations. Finally, the AFSOC contribution section explores strategic documents that support the purpose of supporting or executing new generation warfare tactics.

Pre-Cursor to New Generation Warfare

According to Russian theorists, the concept of new generation warfare dates back to the Falkland War in 1982 and the Gulf War in 1991. General-Major Vladimir Slipchenko, a Russian military author and theorist, and Makhmut Gareev assert there are six generations of warfare: edged-weapons, gunpowder, rifled, automatic and mechanized, nuclear, and precision-strike weapons.³⁸ In a 1991 speech to US Army War College, Slipchenko explains the end of the Cold War coupled with the success of the

³⁸ Makhmut Gareev and Vladimir Slipchenko, *Future War* (Fort Leavenworth, KS: Foreign Military Studies Office, February 2007), vii.

Falkland and Gulf War shows a transformation from industrial to information societies..³⁹ In the Falkland and Gulf War, The U.K. and U.S., respectively, employed cruise missiles and demonstrated a proof of concept that “non-contact war” could be a viable strategy..⁴⁰ The non-contact war required advanced systems and weaponeering, an entry requirement most regular armies around the world did not have available to them in the 1990s and early 2000s. After the collapse of the Soviet Union, Russia lacked the financial resources to develop cruise missiles and other precision strike weapons. Instead, Russia pursued information warfare and asymmetric warfare to counter precision-strike weapons..⁴¹

New Generation Warfare Development

New generation warfare is described by the Russian Chief of General Staff, General Valery Gerasimov, in a speech given on 27 February 2013 and reprinted in “The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Carrying out Combat Operations” published in *Voyenno-Promyshlennyy Kurier* (VPK) (Military-Industrial Courier)..⁴² In 2014, Mark Galeotti’s *Moscow’s Shadow* blog obtained an English translated version of the VPK article and presented the “Gerasimov Doctrine” as to how the Russians were constructing a new non-linear warfare approach..⁴³

³⁹ Gareev and Slipchenko, *Future War*, vii.

⁴⁰ Ibid.

⁴¹ Ibid., viii.

⁴² Bartles, “Getting Gerasimov Right,” 30.

⁴³ Mark Galeotti, “The ‘Gerasimov Doctrine’ and Russian Non-Linear War,” *Moscow’s Shadow* (blog), 6 July 2014, accessed 30 March 2019,

For several years, the Gerasimov Doctrine received attention from U.S scholars, pundits, and policy-makers; consequently, they called on the DOD to counter this new Russian strategy. However, in 2018, Galeotti published an article in *Foreign Policy* titled “I’m Sorry for Creating the ‘Gerasimov Doctrine’.” Galeotti explained that he mischaracterized Gen. Gerasimov’s speech and went on to explain the Russian General was speaking to a Russian audience about how he perceived the U.S. strategy against the Russian people.⁴⁴

Russia’s new generation warfare consists of common characteristics, objectives, and tools. These traits highlight how Russia is using multiple instruments of power and influence to propagate their national interests. These traits provide a framework to use when reviewing case studies.

Russian new generation warfare tactics build on the operational art originated by Aleksandr Svechin; who focused on a strategy of attrition. M.N. Tukhachevsky further expanded operational art by developing deep operations theory, which focused on the annihilation of the enemy through the depth of his defenses.⁴⁵ Tukhachevsky also proposed factors of depth, continuity, synergism, and wholeness eventually creating an

<https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>.

⁴⁴ Mark Galeotti, “I’m Sorry for Creating the ‘Gerasimov Doctrine’,” *Foreign Policy*, 5 March 2018, <https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/>.

⁴⁵ Ronald Sprang, “Russian Operational Art, New Type Warfare, and Reflexive Control,” *Small Wars Journal* (3 November 2018), para 3, accessed 3 November 2018, <http://smallwarsjournal.com/jrnl/art/russian-operational-art-new-type-warfare-and-reflexive-control>.

operational approach that achieves simultaneous paralysis of the entire depth of the enemy.⁴⁶ Originating in the early 1920s, the deep battle concept has been modernized by current Russian leaders with new generation warfare. General-Lieutenant Andrey Kartapolov, Deputy Minister of Defense and Chief of the Main Military-Political Directorate of the Russian Federation Armed Forces, described “new-type warfare” (a synonym to new generation warfare) in 2015 as consisting of “80-90 percent propaganda and 10-20 percent violence.”⁴⁷ General Kartapolov stated that traditional warfare should also employ diplomatic pressure, economic pressure, and target multiple audiences with propaganda by large scale IO to create dissatisfaction.⁴⁸

The deep battle concept and thus new generation warfare leads to a second modernization theory employed in conjunction: reflexive control. New generation warfare expands on the deep battle concept using technology to reach further and influence the enemy leadership and population through targeted messaging called reflexive control. Reflexive control focuses on “decision making and organizational decision-making systems and processes.”⁴⁹ Reflexive control focused on an enemy’s ability to adjust the tempo by targeting key technological nodes used by the enemy to

⁴⁶ Sprang, “Russian Operational Art,” para 5.

⁴⁷ Timothy Thomas, “The Evolving Nature of Russia’s Way of War,” *Military Review* (July-August 2017): 40, accessed 30 March 2019, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20170831_THOMAS_Russias_Way_of_War.pdf.

⁴⁸ Ibid., 39-40.

⁴⁹ Sprang, “Russian Operational Art,” para 7.

evaluate changes in the OE. Russia specifically focuses on reconnaissance assets, satellites, weapons guidance systems, and associated technology and systems to shape the opponent.⁵⁰ Reflexive control's conditioning requires an understanding of links in the opponent's decision-making process. An adversary uses those exploitable links to gain access and influence. This influence is a key strength of this approach. Reflexive control provides temporary paralysis of the opponent's operational tempo and decision-making process.⁵¹ The temporary paralysis provided by reflexive control acts as a force multiplier to new generation warfare tactics thwarting an enemies defense and shaping the OE for any future ROMO.

New Generation Warfare Characteristics

The key characteristics of Russian new generation warfare are economy of force, persistence, and population-centricity. Russian conventional forces and nuclear assets are positioned to project military power in their southern *near-abroad*. Russia employs an economy of force with new generation warfare tactics increasing their influence covertly.⁵² Furthermore, Russia employs different new generation warfare tactics simultaneously across the ROMO. This persistent approach produces an insidious effect on the target demonstrated in Estonia, Georgia, and Ukraine. Finally, Russia recognized

⁵⁰ Sprang, "Russian Operational Art," para 8.

⁵¹ Ibid., para 7.

⁵² Christopher S. Chivvis, *Understanding Russian 'Hybrid Warfare': And What Can Be Done About It?* Testimony presented before the House Armed Services Committee Testimony, 22 March 2017 (Santa Monica, CA: RAND Corporation, 2017), 2.

that western states' cultures change with the advent of the internet over the last quarter century. New generation warfare tactics coupled with the internet create an opportunity to target different groups of people to promote Russian objectives within existing political and social frameworks.⁵³ The Russian new generation warfare characteristics of the economy of force, persistence, and population-centric focus provide a means to an end.

The means of Russian new generation warfare generally support three common objectives including capturing land without conventional forces, providing context to justify the use of force, or influencing the politics and policies of other sovereignties. Russia's successful annex of Crimea in 2014 highlighted the strength of this first approach. Russia seized territory without conventional forces. The "little green men" that first marched into Crimea were later discovered to be Russian special forces of the newly created Russian special operations command.⁵⁴ These Russian SOF units were successful in their bloodless takeover because of the synchronized efforts of a supporting information operation and loyal Russian proxies delaying the Ukrainian defensive response. In discussing the Crimean operations, General Gerasimov highlighted that non-military means are used four times more than conventional operations in modern conflict.⁵⁵ Crimea provides an excellent example of this "non-contact war" previously discussed by Slipchenko.

⁵³ Chivvis, *Understanding Russian "Hybrid Warfare,"* 2.

⁵⁴ Ibid., 2.

⁵⁵ Bartles, "Getting Gerasimov Right," figure 1.

Another Russian new generation warfare objective influences the OE and provides a justified reason to deploy convention forces in support of military operations. The Baltic States fear Russia could create a false narrative using multi-media resulting in a conflict between a Lithuania's minority Russian population and a false-repressive state. In a hypothetical example, Lithuanian persecution of the ethnic Russian population leads to charges from Russian sponsored media outlets. These false charges would propagate through social media and fake news stories inside and outside of Russia. Russian secret agents and proxies could stage and coordinate violent rallies and demonstrations in Lithuania. These riots could be picked up by local and world news media networks to reinforce a false narrative further. Russia would mobilize units into Lithuania to stop "human rights atrocities" under pretenses. Russia would further complicate Lithuania, and North Atlantic Treaty Organization (NATO) organized responses by conducting cyberspace operations to degrade or deny coordination efforts.⁵⁶ This hypothetical example provides context for how new generation warfare can create a pretext for conventional military operations.

The last objective of Russia's new generation warfare is a covert, constant influence of foreign politics and policies of other countries. The 2016 U.S. presidential election serves as a prime example of when Russian new generation warfare influenced the U.S. electoral and political process by inserting false news stories into circulation on social media websites and applications.⁵⁷ The most vulnerable countries to this new

⁵⁶ Chivvis, *Understanding Russian "Hybrid Warfare,"* 3.

⁵⁷ Karen Yourish and Troy Griggs, "8 U.S. Intelligence Groups Blame Russia for Meddling, but Trump Keeps Clouding the Picture," *New York Times*, 2 August 2018,

generation warfare objective are those with weak legal and anti-corruption measures with similar domestic groups that share Russian interests, i.e., former Soviet Union countries and those states in Russia's *near-abroad* region.⁵⁸ The danger of this type of new generation warfare tactic is that it can serve as a starting point for the other objectives to escalate into armed conflict.

The final characteristic of new generation warfare are the different tools employed by Russia to carry out this type of warfare. New generation warfare tools include information operation, cyberspace operations, proxies, economic and political influence, and clandestine measures. The Russian military combined with intelligence agencies can employ these tools creating a synergistic effect often hard to recognize or defend against quickly. The new generation warfare tools provide a broad sampling that may not always apply given the desired goal.

New generation warfare IO venture far from the JP definition described in chapter 1. Russia uses IO as a strategic shaping tool to generate favorable narratives. *Russia Today* and *Sputnik News* provide outlets able to create and propagate pro-Russian strategies and ideas. Russia also supports television programming, European think tanks, and an increasing number of internet trolls, bots, and fake news farms.⁵⁹ The distinct features to this new generation tool versus Cold War propaganda are the rapid,

para 3, accessed 10 November 2018, <https://www.nytimes.com/interactive/2018/07/16/us/elections/russian-interference-statements-comments.html>.

⁵⁸ Chivvis, *Understanding Russian "Hybrid Warfare,"* 3.

⁵⁹ Ibid.

continuous, and repetitive high-volume of the contemporary multichannel model.⁶⁰

Furthermore, this tool does not require objective reality or consistency demonstrated with a simple example.⁶¹ For example, a pro-Russian article published in *Russia Today*. From that article, computer bots post the article between several fake accounts on social media adding additional false details or “arguing” about the topic. Consequently, the narrative of the original article changes and real users on social media begin to re-post the article with additional commentary unknowingly elevating the subject to more and more people like a digital game of “telephone.” The first news article might be benign, but by the time it has gone through a few thousand re-posts between bots and actual users challenges the truth. Although these tools might not convince people the stories are entirely factual, IO introduce doubt of factually accurate alternatives and shape perception. The entire focus of this approach is to benefit the Kremlin.

Cyberspace operations are a more sophisticated and technical new generation warfare tool that further shapes the Russian influence of a targeted audience. Russian cyber operators are believed to have influenced the 2016 U.S. presidential election using this new generation warfare tool. Furthermore, more advanced cyber tools can directly manipulate or affect other countries or private sector internet or intranet information systems relied on by those entities for daily operations and crucial infrastructure software

⁶⁰ Christopher Paul and Miriam Matthews, *The Russian “Firehose of Falsehood: Propaganda Model: Why It Might Work and Options to Counter It* (Santa Monica, CA: RAND Corporation, 11 July 2016), 2, accessed 11 November 2018, <https://www.rand.org/pubs/perspectives/PE198.html>.

⁶¹ Ibid.

components.⁶² Cyberspace operations continue to evolve, and capabilities become more accessible and cheaper as computing power increases and proliferates through the world.

A third new generation warfare tool, proxies, allow Russia to influence targeted audiences through other means. Led by friends of President Putin, the Night Wolves are an example. They are an anti-American, ultranationalist biker gang.⁶³ The Night Wolves have been known to intimidate populations and enable shaping operations. In 2016, proxies provided financial backing to anti-European Union (EU) groups to challenge a trade referendum between Ukraine and Netherlands. In another example, a Kremlin-linked local Bulgarian group protested Bulgarian government efforts to reduce energy dependence on Russia.⁶⁴ With the help of a global economy and the internet, it is increasingly difficult to determine what non-profit organizations and cause-driven groups are secretly proxies for nation states.

Economic and political influence are new generation warfare tools that align with non-military national instruments of power and are often primary levers used to gain their national interest. New generation warfare tools of economic and political influence linked to other new generation tools as supporting a more significant strategic aim of Russia in a more subversive or indirect approach. Russia uses large scale investment in the Soviet-built gas pipelines providing energy to many European countries. The Russian state-

⁶² Chivvis, *Understanding Russian "Hybrid Warfare,"* 3.

⁶³ Ibid., 4.

⁶⁴ Kerin Hope, "Bulgarians See Russian Hand in Anti-Shale Protests," *Financial Times*, 30 November 2014, para 8, accessed 11 November 2018, <https://www.ft.com/content/e011d3f6-6507-11e4-ab2d-00144feabdc0>.

owned gas company, Gazprom, has negotiated many back-room deals with other states further strengthening Russian national interests without being directly linked to the government.⁶⁵ Economic and political influence inside Russia also allows current leaders to derail or discredit opposition political leaders. Again, this tactic is not uncommon. However, when used in conjunction with other new generation warfare tools, they act as a great force multiplier with regards to their effectiveness.

The final new generation warfare tool is clandestine measures. Clandestine measures include espionage, bribing, extortion, and SOF capabilities.⁶⁶ Russian military intelligence and special forces conducting IW provide a gateway and different channels of influence completely detached and un-attributable to their government. Clandestine measures can also serve as force multipliers similar to political and economic influences. In 2016, Russian military intelligence instigated a plot to overthrow the pro-NATO government of Montenegro.⁶⁷ Similarly, Russian special forces were crucial to seizing Crimea and adding legitimacy to Donbass separatists.⁶⁸ Clandestine measures are closely related to IW described in chapter 1. Similar to economic and political influences, clandestine measures are not a new concept but when combined with other new

⁶⁵ Chivvis, *Understanding Russian "Hybrid Warfare,"* 4.

⁶⁶ Ibid.

⁶⁷ Andrew Higgins, "Finger Pointed at Russians in Alleged Coup Plot in Montenegro," *New York Times*, 26 November 2016, para 5, accessed 12 November 2018, <https://www.nytimes.com/2016/11/26/world/europe/finger-pointed-at-russians-in-alleged-coup-plot-in-montenegro.html>.

⁶⁸ Chivvis, *Understanding Russian "Hybrid Warfare,"* 4.

generation warfare tools create an entirely new line of effort on which to wage asymmetric warfare.

The characteristics of new generation warfare consist of three possible objectives and five tools that can be used in conjunction to provide multiple approaches to influence another country into supporting Russia's national interests. These approaches utilize a spectrum of tools from the benign re-posting of articles to the illegal, violent acts of gangs. No one tool or objective is uniquely special to new generation warfare. However, the strength of the new generation warfare is the dovetailing of these seemingly different tactics to create a result much more influential than the sum of the individual parts. Chapter 4 expands on these tools and objectives.

AFSOC Contribution to New Generation Warfare

AFSOC's strategic messaging provides guidance to seek out new ways to maintain relevancy. New generation warfare tactics offer a way for present and future relevancy. AFSOC Vision: "Air Commandos . . . Ready Today, Relevant Tomorrow, Resilient Always."⁶⁹ Furthermore, the AFSOC mission and priorities support this idea of being relevant tomorrow. The AFSOC Mission: "Provide our Nation's specialized airpower, capable across the spectrum of conflict . . . Any Place, Any Time, Anywhere."⁷⁰ From these, two of the three AFSOC priorities contribute directly to present and future relevancy, "ensure readiness to execute global special operations

⁶⁹ Air Force Special Operations Command (AFSOC), "About Us," U.S. Air Force, accessed 4 November 2018, <https://www.afsoc.af.mil/About-Us/>.

⁷⁰ Ibid.

today . . . transform our force and fleet to maintain relevance tomorrow”⁷¹ AFSOC has the responsibility to explore IW using new generation warfare tactics in future A2/AD environments.

Current AFSOC capabilities include precision strike, intelligence, surveillance, and reconnaissance (ISR), special mobility, electronic warfare, MISO, and austere field control. The two most relevant AFSOC capabilities conducive to new generation warfare tactics are MISO and shaping operations, through special mobility, for access into an A2/AD OE. New generation warfare tactics have an asymmetric and indirect approach to influencing the target population, and thus overt AFSOC capabilities should not be considered when employing new generation warfare tactics. The subsequent paragraphs of this chapter explain relevant AFSOC capabilities. Chapter 5 links AFSOC capabilities to viable new generation warfare tactics.

AFSOC contributes to MISO through unique asset employment, mission sets, and enabling operations. The EC-130J Commando Solo provides MISO and civil affairs broadcasts in FM radio, television, and military communication bands.⁷² The Commando Solo provides an airborne radio station to keep a target audience informed about the enemy and friendly activities and intentions. Also, MC-130 variants and non-standard aviation (NSAv) aircraft mission set of leaflet drops and resupply provide another MISO capability. Leaflet drops provide a scalable method to inform either a very small group of

⁷¹ AFSOC, “About Us.”

⁷² U.S. Air Force, “EC-130J Commando Solo,” 14 January 2016, accessed 16 January 2019, <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104535/ec-130j-commando-solo/>.

people or a broad audience of U.S. intentions and support to gain favor. This capability informs the public of both allied and enemy intentions to gain favor through information. Finally, special mobility airdrops can enable other new generation warfare operations through resupply of equipment or people. AFSOC provides several MISO abilities to communicate with a target audience through various means and provide them resupply to influence their perception and subsequent support.

AFSOC can also significantly add to U.S. capabilities of special mobility to shape an OE against a near-peer adversary. New generation warfare tactics against a near-peer adversary require increased flexibility and reaction time to influence the IO and cyberspace domains. First, AFSOC as the air component of SOCOM works on a tight timeline from request for support to employment. In an A2/AD environment, MC-130 or NSAv with special tactics airmen can conduct austere airfield operations to support other SOF or guerrilla forces operations. Shaping operations are supported around the world to create and enhance IW operations. Also, AFSOC assets operate with a small footprint providing a covert and clandestine infiltration and exfiltration option for personnel and equipment. Finally, AFSOC has a habitual working relationship with other SOF components, intergovernmental agencies, and foreign military units. Over the last two decades of counter-insurgency, AFSOC expanded around the world to support these end-users. The speed and reach of AFSOC are two fundamental characteristics that contribute to new generation warfare with regards to special mobility to shape and create access in an A2/AD environment.

CHAPTER 3

RESEARCH METHODOLOGY

This chapter explains research methods used to answer the research questions presented in chapter 1. The three main parts of this chapter are limitations and delimitations, comparative case study methodology, and prescriptive research methodology. The researcher used these mixed research methods to answer: How can AFSOC adopt new generation warfare tactics in future conflicts?

New generation warfare tactics are not listed in a library available to tacticians to pick and choose from like a menu. The very opposite is true. Russia deliberately distorts and hides its new generation warfare tactics through misinformation and false legitimacy. New generation warfare tactics seek to influence a target audience and are most impactful when their efforts are covert and clandestine. To clarify, a target audience is most influenced when that audience is unaware of their adversary's actions or intent. This thesis employs a systematic and deliberate mixed research methodology to overcome misinformation and false legitimacy.

Research Limitations and Delimitations

Russia's new generation warfare tactics are the limits of this research. The U.S., China, and Iran contribute to the concept of new generation warfare. However, these countries tactics will not be explored to limit the scope of the investigation.

The researcher delimits chapter 4 by three recent conflicts. The Russia-Estonia conflict occurred in April 2007. New generation warfare tactics of influence without military action provide an excellent starting point. Next, the Russia-Georgia conflict in

August 2008 demonstrates the full capability of new generation warfare integrated with conventional military operations. Finally, the Russia-Ukraine conflict in February 2014 illustrates how Russia further improved new generation warfare tactics from the lessons learned from both Russia-Estonia and Russia-Georgia Conflict.

This thesis remains at the operational and tactical levels. The operational and tactical level approach better implements AFSOC capabilities using new generation warfare. The Russian new generation warfare tactics span the range of tactical and strategic level employment and implementation. This research references explicitly some strategic leaders in the case study and throughout the thesis to provide additional details regarding the state's perceived ends. The implication section of chapter 6 mentions future research at a strategic level and possible benefits.

Comparative Case Study Method

The researcher used a comparative case study research method to obtain possible new generation warfare tactics for evaluation. Given a large amount of relevant literature on new generation warfare, the comparative case study focused on tactics specifically employed towards Estonia, Georgia, and Ukraine. A timeframe was the initial delimitation factor; however, some events are outside the time windows described in chapter 1 to provide more relevant information and context.

The Russia-Georgia conflict and the Russia-Ukraine conflict include a conventional warfare element. The case study focused on Russian new generation warfare tactics activities primarily in the cyberspace and information operation domain. However, some conventional operations are included to highlight synchronization required for new generation warfare tactics and conventional warfare operations.

Although the duration and scope of Russian new generation warfare vary among these three events, the case study will focus on finding the repeated similarities employed through different events. This approach of finding common practices and themes between the three case studies describes comparative case studies research.⁷³ After completing the case study, the researcher summarizes the findings with a list of tactics associated with Russian new generation warfare through four tables. The first three tables provide a summation of the individual conflicts, and the last table offers a compiled list with the prescriptive research method evaluation criteria listed beside each tactic.

Prescriptive Research Method

The researcher employed the prescriptive research method as a forecasting approach to select new generation warfare tactics enabled by AFSOC. Prescriptive research benefits this thesis over other forecasting research methods: normative decision research and descriptive research. The normative decision research provides a method for how a person should conform.⁷⁴ Descriptive research focuses instead on how people may conform.⁷⁵ However, the prescriptive research method provides a middle ground between those two extremes and provides options on how a person could conform “with desired normative principles.”⁷⁶ This prescriptive research method presents an evaluation table

⁷³ Creswell, *Research Design*, 15.

⁷⁴ L. Robin Keller, *Annals of Operations Research* (Amsterdam, The Netherlands: Baltzer Scientific Publishing, October 1987), 485.

⁷⁵ Ibid.

⁷⁶ Ibid.

conforming with normative principles.⁷⁷ The AFSOC new generation warfare criteria table provides a framework and structure using the prescriptive research method providing clear results.

The prospective evaluation criteria are restraint, legitimacy, and applicability to AFSOC capabilities. The principle of joint operations definitions describes restraint and legitimacy criteria. Restraint prevents the unnecessary use of force and balances the need for security with military operations and national objectives.⁷⁸ Restraint is a qualitative measure that weighs the negative effect on the target audience or neutral bystanders versus the positive effect on a state conducting the operation. Restraint balances preservation versus action through how much a state is willing to jeopardize, people or resources, to achieve their objectives. Restraint is linked and possibly enhances another criterium, legitimacy. Legitimacy preserves actual and perceived legal and moral authority of interested audiences.⁷⁹ The perception of legitimacy is a challenging qualifier because it must be linked to an audience. Whose perception of legitimacy is being considered? In this evaluation, legitimacy measured from an outside third party, the international community, will be the audience. New generation warfare tactics are most effective when the target audience cannot directly contribute the outside influence or who is trying to influence them. The exception to this principle is if the target audience perceives the tactic is legitimate or in their own best interest. This principle is an essential

⁷⁷ Keller, *Annals of Operations Research*, 486.

⁷⁸ CJCS, JP 3-0, A-4.

⁷⁹ Ibid., A-5.

distinction for U.S. operations where honesty and truthfulness are valued characteristics to operations. These criteria evaluate new generation warfare tactics and are crucial to successful employment.

The last criterion is applicability to AFSOC capabilities. The AFSOC capabilities of MISO and special mobility are selected based on their covert and clandestine nature as described in chapter 2. The evaluation components to filter tactics against AFSOC capabilities is how quickly and obviously can the actions of the forces conducting the tactics be attributed back to the state employing the tactic. The last component of the AFSOC evaluation based on the researcher's experience, how quickly and seamlessly could an AFSOC Air Commando implement or employ the tactic. This implementation considers the minimum training and hindrance of primary missions of the equipment or personnel.

A scale using numbers to represent desirability provides a method to evaluate each new generation warfare tactic against the three previously mentioned criteria. In table 4, each new generation warfare tactic will be given either a one through five to describe the given quality of the tactic: 1 – Very Unacceptable, 2 – Unacceptable, 3 – Neutral, 4 – Acceptable, and 5 – Very Acceptable. A very acceptable evaluation, a five, means that the new generation warfare tactic addresses or supports that specific criteria concern the most. The very unacceptable evaluation, a one, means that the new generation warfare tactics disagrees or does not support the specific criteria concerns. The total summation of a given tactic can range from three, the least desirable tactic for AFSOC employment, to fifteen, the most desirable tactic for AFSOC employment. This evaluation captured in the fourth table of this thesis provides a new generation warfare

tactics summary and evaluation in chapter 4. An average will be used to create a cut line, and the most desirable tactics will be further examined in chapter 5.

CHAPTER 4

CASE STUDY

Russia-Estonia Conflict

Russian first demonstrated new generation warfare capabilities in an attack on the Estonian government, bank, and internet service providers. On Friday, 27 April 2007, Russian speaking internet forums posted instructions on how to disable Estonia's government websites by overwhelming servers with traffic.⁸⁰ This was the first of many virtual volleys of Russian cyber fires conducted on Estonia for two weeks. This is widely believed to be in response to Estonia moving a Soviet-era memorial.⁸¹ Estonian presidential, prime minister, parliamentary, and government ministries websites were defaced and shut down in a matter of hours based on virtual vandalism and excessive traffic. By 30 April, Estonia isolated internet traffic from Russia and the cyber-attacks became more sophisticated. Estonian websites started receiving attacks from robot networks (botnets) from over one million computers in the U.S., China, Vietnam, Egypt, and Peru. Botnets are business and home computers remotely commanded to participate in a cyber-attack.⁸² Botnet attacks forced Estonian newspapers, government, universities,

⁸⁰ Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *Washington Post*, 19 May 2007, para 2, accessed 17 November 2018, <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html>.

⁸¹ Jamie Palagi, "Wrestling the Bear: The Rise of Russian Hybrid Warfare," (Thesis, Joint Forces Staff College Joint Advanced Warfighting School, Norfolk, VA, 13 April 2015), 15.

⁸² Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," para 2.

and nongovernmental organizations to isolate their websites to only in-country traffic. Finally, on 10 May 2007, Estonia experienced the most sophisticated attack, a bombardment of bank websites. Estonian bank website traffic that day far exceeded previous levels prompting Linnar Viik, a government information technology consultant, to say “the nature of the latest attack is very different...things you can’t buy from the black market.”⁸³ NATO, the EU, and the U.S. deployed information technology experts to support Estonia. Estonia was able to eventually bring their systems back online and develop a more robust and redundant network to discourage future attacks.

U.S. joint doctrine describes the types of attacks on Estonia as offensive cyberspace operations.⁸⁴ The new generation warfare aspect of these cyberspace attacks demonstrates an important distinction to take away from this case study. The cyberspace operations originated from both state, Russian infrastructure, and non-state, contracted hackers, assets to engage the desired target.⁸⁵ Furthermore, to add legitimacy for these attacks, Russia highlighted the movement of the Soviet monument and ethnic Russian protests in Estonia as justification even though Russia would not claim responsibility for the attacks.

The attack on Estonia’s strategic significance is that Russia is willing and able to influence the physical domain of another sovereign state through the cyberspace domain. New generation warfare used eleven different tactics targeting specific, diverse

⁸³ Finn, “Cyber Assaults on Estonia Typify a New Battle Tactic,” para 28.

⁸⁴ Chairman, Joint Chief of Staff (CJCS), Joint Publication (JP), *DOD Dictionary of Military and Associated Terms*, (Washington, DC: JCS, 1 September 2018), 170.

⁸⁵ Palagi, “Wrestling the Bear: The Rise of Russian Hybrid Warfare,” 15.

populations that were significant to the success of the operations, see table 1. The historic attack resulted in NATO establishing the Cooperative Cyber Defence Centre of Excellence bringing together cyber experts to defend against future attacks.⁸⁶

Table 1. Estonia Conflict New Generation Warfare Tactics Summary

<u>Tactic</u>	<u>Descriptions</u>
Cyber Attack: Government agencies	Offensive cyberspace operations designed to degrade, disrupt, or deny state's government services
Cyber Attack: News Agencies	Offensive cyberspace operations designed to degrade, disrupt, or deny news agencies services
Cyber Attack: Non-government agencies	Offensive cyberspace operations designed to degrade, disrupt, or deny nongovernment agencies services
Cyber Attack: financial market	Offensive cyberspace operations designed to degrade, disrupt, or deny infrastructure or financial system services
Info Ops: news	News article promotion to target audience (specific country population; international population; focused group)
Info Ops: Key Leader Saturation	Mass media towards specific key leader accounts; spam; saturation on multiple forums/modes
Info Ops: Hacking	Malicious activity to deny, disrupt, or degrade target computer system connectivity
Info Ops: Botnet	Online service saturation spam of bank, news outlet, & government bodies
Info Ops: Mass Media	Broad spectrum information passed to largest audience; propagation of information across forums/modes
Electronic Warfare	Disrupting tactical radios by sector-wide EW. Furthermore, It was used to identify fires, command posts, and shutdown data and voice communication
Guerilla Support	Resource minority element in target country to promote ethnic minorities disturbances

Source: Created by author.

⁸⁶ Emily Tamkin, "Better Prepared for Cyber Threats?" *Foreign Policy*, 27 April 2017, accessed 17 November 2018, <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/>.

Russia-Georgia Conflict

On 7 August 2008, Russian and Georgian conventional forces clashed in South Ossetia and Abkhazia.⁸⁷ By 15 August, the two countries declared a ceasefire with Russia occupying both South Ossetia and Abkhazia. A majority of the international community recognize South Ossetia and Abkhazia as a part of the Republic of Georgia. Russia considers both regions to be states of the Russian Federation joining ethnic Russians with neighboring Russian communities.⁸⁸ Putin justified Russian operations to protect ethnic Russian regardless of state boundaries. The ground invasion of Russian conventional forces marked the first time Russia had invaded another state since Afghanistan in 1979.⁸⁹ The more important factors of this conflict are the unorthodox shaping operations leading up to the conflict.

Days before the conventional attack, Russia employed both distributed denial of services and information technology infrastructure sabotage.⁹⁰ The infrastructure attacks disabled landline communication, cellular networks, and local internet access.⁹¹ These

⁸⁷ Palagi, "Wrestling the Bear," 17.

⁸⁸ Human Rights Watch, "Up in Flames: Humanitarian Law Violations and Civilian Victims in the Conflict over South Ossetia," 1 January 2009, 5, accessed 17 November 2018, https://www.hrw.org/sites/default/files/reports/georgia0109_brochure_web.pdf.

⁸⁹ Rupert Cornwell, "Charlie Wilson: Obituaries," *The Independent*, 13 February 2010, accessed 17 November 2018, <https://www.independent.co.uk/news/obituaries/charlie-wilson-congressman-whose-support-for-the-mujahideen-helped-force-the-soviet-union-out-of-1898180.html>.

⁹⁰ Palagi, "Wrestling the Bear," 17.

⁹¹ Ibid.

efforts ensured that the Georgian government and military command and control would be degraded or wholly denied during conventional operations. Also, civilian Russian hackers attacked Georgia governmental and private sector websites and uploaded Russian propaganda and messaging.⁹² These combined efforts achieved the desired effect of confusion and instability targeting the Georgian people, their government, and their military. In the end, the week-long conflict resulted in 64 Russian servicemen, 228 Georgian civilians, and 169 Georgian servicemen killed.⁹³ The Georgia-Russia Conflict provides another data point in this case study of combining new generation warfare tactics as shaping operations for conventional operation, a first, see table 2.

⁹² Palagi, “Wrestling the Bear,” 18.

⁹³ Simon Shuster, “Russia lost 64 troops in Georgia War, 283 wounded,” *Reuters*, 21 February 2009, 3, accessed 17 November 2018, <https://uk.reuters.com/article/us-russia-georgia-deaths/russia-lost-64-troops-in-georgia-war-283-wounded-idUKTRE51K1B820090221>

Table 2. Georgia Conflict New Generation Warfare Tactics Summary

<u>Tactic</u>	<u>Descriptions</u>
Criminal activity	Destabilization of state through drug, arms, and other criminal activities
Cyber Attack: Government agencies	Offensive cyberspace operations designed to degrade, disrupt, or deny state's government services
Cyber Attack: News Agencies	Offensive cyberspace operations designed to degrade, disrupt, or deny news agencies services
Cyber Attack: Non-government agencies	Offensive cyberspace operations designed to degrade, disrupt, or deny nongovernment agencies services
Cyber Attack: financial market	Offensive cyberspace operations designed to degrade, disrupt, or deny infrastructure or financial system services
Info Ops: news	News article promotion to target audience (specific country population; international population; focused group)
Info Ops: Key Leader Saturation	Mass media to specific member accounts; spam; saturation on multiple forums/modes
Info Ops: Hacking	Malicious activity to deny, disrupt, or degrade target computer system connectivity
Info Ops: Botnet	Online service saturation spam of bank, news outlet, & government bodies
Info Ops: Mass Media	Broad spectrum information passed to largest audience; propagation of information across forums/modes
Electronic Warfare	Disrupting tactical radios by sector-wide EW. Furthermore, It was used to identify fires, command posts, and shutdown data and voice communication
Policing Action	Create artificial/fabricated incident that warrants policing action

Source: Created by author.

Russia-Ukraine Conflict

The Russia-Ukraine conflict in 2014 demonstrated the operational realization of the new generation warfare successfully integrating non-military and military operations seamlessly.⁹⁴ Russia's goal was to annex the Crimea region of Ukraine, a strategic seaport to the Black Sea with a large ethnic Russian population.⁹⁵ Russian covert operations began as early as 2010 with the election of a pro-Russian President Yanukovych.⁹⁶ Within his first year as president, Yanukovych shifted Ukraine's Parliament away from pursuing NATO membership, something the previous president had been pursuing for several years.⁹⁷ Putin dissuaded Ukraine from signing a free trade agreement with the EU in November 2013.⁹⁸ Instead, on 16 December 2013 Ukraine signed a \$15 billion loan with Russia and secured a discount on imported natural gas.⁹⁹

⁹⁴ Janis Berzins, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy" (policy paper, National Defence Academy of Latvia, Center for Security and Research, Riga, Latvia, April 2014), 4.

⁹⁵ Robert A. Culp II, "Exploiting Vulnerabilities in the Russian Approach to Hybrid Warfare," (strategic research project, U.S. Army War College, Carlisle, PA, 1 April 2016), 40, accessed 29 November 2018, <http://publications.armywarcollege.edu/pubs/786.pdf>

⁹⁶ Robert R. Leonhard and Stephen P. Phillips, "'Little Green Men': A Primer On Modern Russian Unconventional Warfare, Ukraine 2013–2014" (research project, Assessing Revolutionary and Insurgent Strategies, Fort Bragg, NC, 2015), 51, accessed 21 September 2018, http://www.jhuapl.edu/ourwork/nsa/papers/ARIS_LittleGreenMen.pdf.

⁹⁷ Culp, "Exploiting Vulnerabilities in the Russian Approach to Hybrid Warfare," 40.

⁹⁸ Leonhard and Phillips, "Little Green Men," 51.

⁹⁹ Ibid.

The natural gas deal insured Ukraine reliance on Russia. These overt and covert operations focused towards diplomatic and economic influence on Ukraine and set the stage for additional layers of new generation warfare operations.

On 20 February 2014, a violent protest in Kiev, Ukraine killed sixty people after a month-long Russian campaign to create conflict. Several hundred members of Spetsnaz GRU, Russian foreign military intelligence agency's special forces, employed unconventional warfare tactics to create "popular uprising" and GRU agents bribed ethnic Russians to win support for Russia's annex of the Crimea region.¹⁰⁰ These IW operations are not unique to the Ukraine conflict. The deliberate and synchronized IO including cyberspace operations provide another case study in new generation warfare operations. As previously mentioned in chapter 2, Kartapolov essentially expressed this direct and indirect coupled approach when describing new type warfare in 2015.¹⁰¹ Crimea's landline, internet, and mobile services were severely disrupted during subsequent militia and unconventional warfare operations for the next several months.¹⁰² All these operations focused on Russian legitimacy to support ethnic Russians in Ukraine. The Russian goal to persuade Ukrainians and Non-Ukrainians globally used deception, deflection of responsibility, lies, and propagation of an alternative reality.¹⁰³

¹⁰⁰ Leonhard and Phillips, "Little Green Men," 51.

¹⁰¹ Thomas, "The Evolving Nature of Russia's Way of War," 40.

¹⁰² Leonhard and Phillips, "Little Green Men," 52.

¹⁰³ Timothy Thomas, "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations," *Defense Strategic Communications Journal* 1, no. 1 (Winter 2015): 11.

Russia promoted the idea the Ukrainian government was fascist or even Nazi.¹⁰⁴ This theme of legitimacy was targeted not only to the Ukrainian population but to the EU, NATO, and the U.S. to discourage intervention and ensure non-contact military operations continued in the region.¹⁰⁵

The Ukraine conflict highlighted a different aspect of new generation warfare: reflexive control. Reflexive control focused on denying and deflecting attribution or forensic evidence to conceal the presence of Russian force in Ukraine.¹⁰⁶ Between 27 February to 15 March 2014, The famous “little green men” interviewed on local news deceived reporters of where they came from and what they were doing in Crimea.¹⁰⁷ The Russian soldiers dressed entirely in green without insignia, hence the descriptive term. A Ukrainian journalist reached out to other local reporters and citizens to get them to stop using the affectionate term to describe an invading force.¹⁰⁸ The real power of reflexive control is hiding attribution. The state can also conceal their motives or intentions. In Ukraine, Moscow de-legitimized the Ukrainian government obscured operational goals and unnerved some countries. The Russian foreign minister Sergey Lavrov refused to

¹⁰⁴ Leonhard and Phillips, “Little Green Men,” 53.

¹⁰⁵ Ibid.

¹⁰⁶ Maria Snegovaya, “‘Reflexive Control’: Putin’s hybrid warfare in Ukraine is straight out of the Soviet Playbook,” *Business Insider*, 22 September 2015, para 10, accessed 3 November 2018. <https://www.businessinsider.com/reflexive-control-putins-hybrid-warfare-in-ukraine-is-straight-out-of-the-soviet-playbook-2015-9>.

¹⁰⁷ Vitaly Shevchenko, “‘Little Green Men’ or ‘Russian Invaders’,” *BBC News*, 11 March 2014, para. 7, accessed 14 November 2018, <https://www.bbc.com/news/world-europe-26532154>.

¹⁰⁸ Shevchenko, “‘Little Green Men’ or ‘Russian Invaders’,” para 9.

meet with Ukrainian foreign minister, Andriy Deshchytsia because the Ukrainian government was an illegal government.¹⁰⁹ Russia's hidden motives convinced other countries that since the operations were limited in scope with no intentions given, they were acceptable.¹¹⁰ Most countries, including Ukraine, understood that the "little green men" were Russian soldiers. However, Russia still retained superficially plausible legality by consistently denying any involvement in Crimea. Russia further deflected involvement by comparing Western actions in Kosovo in the 1990s and Iraq in 2003.¹¹¹

On 19 March 2014, Crimean "self-defense" troops, likely led by GRU, took control of the Ukrainian Navy seaport in Crimea.¹¹² Twenty-five thousand Ukrainian troops retreated to Eastern Ukraine without firing a single shot.¹¹³ Russian IO kept up the strategic messaging campaign regarding legitimacy that "97 percent of the Crimean population supported a Russian annex."¹¹⁴ The West, led by the U.S., threatened sanctions and called for Russia to "pull back its troops" from entering into East Ukraine. Russia annexed Crimea in approximately three weeks without armed conflict, a testament to the influence and power of new generation warfare.

¹⁰⁹ Leonhard and Phillips, "Little Green Men," 51.

¹¹⁰ Snegovaya, "Reflexive Control," para 12.

¹¹¹ *Ibid.*, para 13.

¹¹² Leonhard and Phillips, "Little Green Men," 51.

¹¹³ *Ibid.*, 52.

¹¹⁴ *Ibid.*

Russian new generation warfare's reflexive control in Ukraine showed an emerging use of cyber reconnaissance. Cyber reconnaissance capabilities allowed Russia to understand Ukraine's plan before deploying forces. Knowing the Ukrainian military response, Russia adjusted their maneuver and fire positions to maximize outcomes with minimum effort.¹¹⁵ Russia essentially eavesdropped on Ukraine using cyber means. Russia demonstrated the strength of new generation warfare to combine reflexive control and cyber reconnaissance to defeat Ukraine's military response. Liam Fox, the former United Kingdom Secretary of Defense, described these operations as Russia asserting its national powers to protect ethnic Russians regardless of other states laws, government, or constitutions or international law.¹¹⁶

Russia enhances reflexive control by distracting the world with threats to the West through the overflight of NATO airspace, threatened use of nuclear weapons, and inflated claims of Russia's military capabilities and strength.¹¹⁷ Russia also demonstrated the power of new generation warfare tactics, see table 3, combined with conventional operations efforts to thwart Ukraine's military response. Although Russia's military

¹¹⁵ Ronald Sprang, "Russia in Ukraine 2013-2016: The Application of New Type Warfare Maximizing the Exploitation of Cyber, IO, and Media," *Small Wars Journal*, 11 September 2018, para 8, accessed 18 September 2018. <http://smallwarsjournal.com/jrnl/art/russia-ukraine-2013-2016-application-new-type-warfare-maximizing-exploitation-cyber-io-and>

¹¹⁶ Liam Fox, "Hybrid War-Hybrid Response," *NATO Review Magazine*, 25 November 2014, accessed 17 November 2018, <https://www.dvidshub.net/video/377850/nato-review-hybrid-war-hybrid-response>.

¹¹⁷ Snegovaya, "Reflexive Control," para 10.

threats remain empty towards NATO and Western states, new generation warfare allows Russia to retain Crimea without further NATO military actions or Western intervention.

Table 3. Ukraine Conflict New Generation Warfare Tactics Summary

<u>Tactic</u>	<u>Descriptions</u>
Criminal activity	Destabilization of state through drug, arms, and other criminal activities
Cyber Attack: Government agencies	Offensive cyberspace operations designed to degrade, disrupt, or deny state's government services
Cyber Attack: News Agencies	Offensive cyberspace operations designed to degrade, disrupt, or deny news agencies services
Cyber Attack: Non-government agencies	Offensive cyberspace operations designed to degrade, disrupt, or deny nongovernment agencies services
Cyber Attack: financial market	Offensive cyberspace operations designed to degrade, disrupt, or deny infrastructure or financial system services
Info Ops: news	News article promotion to target audience (specific country population; international population; focused group)
Info Ops: Key Leader Saturation	Mass media to specific member accounts; spam; saturation on multiple forums/modes
Info Ops: Hacking	Malicious activity to deny, disrupt, or degrade target computer system connectivity
Info Ops: Botnet	Online service saturation spam of bank, news outlet, & government bodies
Info Ops: Mass Media	Broad spectrum information passed to largest audience; propagation of information across forums/modes
Electronic Warfare	Disrupting tactical radios by sector-wide EW. Furthermore, It was used to identify fires, command posts, and shutdown data and voice communication
Policing Action	Create artificial/fabricated incident that warrants policing action
Guerrilla Support	Resource minority element in target country to promote ethnic minorities disturbances

Source: Created by author.

New Generation Warfare Tactics Evaluation

Table 4 provides a summary of all new generation warfare tactics employed in the three conflicts. Furthermore, the table contains the evaluation of each tactic using the prescriptive research method explained in chapter 3. The new generation warfare tactics have been listed in order from most applicable to least applicable. The comparative case study produces thirteen specific new generation warfare tactics for evaluation with a mean total score of 8.8. The top eight tactics are all viable options that AFSOC can employ using either MISO or access to shaping operations to provide new generation warfare capabilities to future operations. Chapter 5 groups the following eight tactics and demonstrates how AFSOC can use these tactics in an A2/AD environment. Finally, the chapter highlights some on-the-horizon capabilities AFSOC could employ to further contribute to new generation warfare.

Table 4. New Generation Warfare Tactics Summary

<u>Tactic</u>	<u>Descriptions</u>	<u>Example</u>	<u>Restraint</u>	<u>Legitimacy</u>	<u>AFSOC Capes</u>	<u>Total</u>
Guerrilla Support	Resource element in target state, promote ethnic minority mistreatment	E,U	5	4	5	14
Electronic Warfare	Disrupting data and voice comms. Used to ID fires & command nodes	E, G, U	4	5	4	13
Info Ops: Key Leader Saturation	Mass media to ind. accounts; spam; saturate multiple forums/modes	E, G, U	5	4	3	12
Policing Action	Create fabricated incident, warrants policing action	G, U	3	3	5	11
Info Ops: Botnet	Online service saturation banks/news outlet/gov	E, G, U	4	3	4	11
Info Ops: news	News article promotion to target audience (specific country population; international population; focused group)	E, G, U	3	4	4	11
Info Ops: Hacking	Malicious activity to deny, disrupt, or degrade target computer system connectivity	E, G, U	4	3	3	10
Cyber Attack: Gov. agencies	Offensive cyberspace operations designed to degrade, disrupt, or deny state's government services	E, G, U	4	3	3	10
Criminal activity	Destabilization through drug, arms, and other criminal activities	G, U	2	1	3	6
Info Ops: Mass Media	Information passed to large audience; propagation across forums/modes	E, G, U	1	2	1	4
Cyber Attack: News	Ops designed to degrade, disrupt, or deny news agencies services	E, G, U	2	2	2	4
Cyber Attack: Non-government agencies	Offensive cyberspace operations designed to degrade, disrupt, or deny nongovernment agencies services	E, G, U	1	2	1	4
Cyber Attack: financial market	Offensive cyberspace operations designed to degrade, disrupt, or deny infrastructure or financial system services	E, G, U	1	2	1	4

Source: Created by author.

NOTE: 1 – Very Unacceptable, 2 – Unacceptable, 3 – Neutral, 4 – Acceptable, and 5 – Very Acceptable; E – Estonia, G – Georgia, U – Ukraine.

CHAPTER 5

WHY AFSOC?

Introduction

Some theorists characterize the western concept of hybrid warfare as something interchangeable with Russia's new generation warfare. Although they are distinctly different, hybrid warfare and new generation warfare employed together by the U.S. may be the next step towards a revolution in military affairs. Regardless of a potential future revolution of military affairs, AFSOC tacticians can benefit from blending these concepts and capturing effective tactics employed in future conflicts.

AFSOC cultivated counter-insurgency TTPs over the last seventeen years. The AFSOC community, approximately 19,000 strong, provides geographic combatant commanders special aviation capabilities "any time, any place." These air commandos, combat-proven proficient and knowledgeable, support joint warfighters in the current fight. Future operations are not guaranteed to be more of the same. The NDS calls the military to prepare for the A2/AD environment against near-peer adversaries. AFSOC has a great opportunity with this inflection point to develop capabilities and capacity supporting joint warfare in this new OE.

SOCOM can more easily refocus land-based SOF operators compared to aviation SOF by promoting unconventional warfare and foreign internal defense in the land domain.¹¹⁸ AFSOC could follow suit and revert to more traditional special operations

¹¹⁸ Jonathan Schroden, "How Special Ops Can Step It Up," *War on The Rocks*, 19 December 2018, para 1, accessed 19 December 2018, <https://warontherocks.com/2018/12/how-special-ops-can-step-it-up/>.

aviation missions supporting these operations. However, AFSOC can take from both hybrid warfare, both irregular and conventional warfare, and new generation warfare tactics and provide a new force multiplier capability for the entire joint force. The proven tactics of Russian new generation warfare provide AFSOC a starting point to increase U.S. influence in multiple domains during all phases of developing a new AO. Specifically, AFSOC can quickly provide IO access through direct and indirect support. The “gray-zone” competition between future adversaries could be the new OE.¹¹⁹

“Gray-zone” operations require politically sensitivity, minimum signature, and plausible deniability access.¹²⁰ AFSOC has a scalable capability providing access through MC-130 and NSAv. Furthermore, AFSOC aircraft can quickly respond to rapidly changing OE through training operations to desensitize the local populous. In an A2/AD environment, AFSOC aircraft may employ using innocent circumstances in support of humanitarian efforts. AFSOC aircraft fly possible routes desensitizing the local populous and enemy early warning capabilities to allow access. Furthermore, AFSOC operations could be used for military deception disguising or misrepresenting friendly forces movement.

Russian new generation warfare is notably different in their approach compared to the U.S. joint phase-based operations. The U.S. military constructs joint operations in six phases from Phase 0: Shape, Phase 1: Deter, Phase 2: Seize Initiative, Phase 3: Dominate,

¹¹⁹ Schroden, “How Special Ops Can Step It Up,” para 4.

¹²⁰ Ibid.

Phase 4: Stabilize, Phase 5: Enable Civil Authorities and eventual return to phase 0.¹²¹

Although JP 3-0 initially presented these six phases as an example, the U.S. military has turned these examples into a best practice of sequential and mechanical phases for joint operations.¹²² In contrast, Russia's new generation warfare sees the different capabilities used in these phases instead as bins. Russian forces are prepared to utilize these capabilities in different bins.¹²³ Russian leaders use these bins when circumstances and opportunities present themselves regardless of phase. AFSOC provides an air component that could quickly adapt to such changes in the OE and facilitate both directly and indirectly to new generation warfare tactics through a bin construct. AFSOC should pursue and develop the ability to conduct ROMO in an episodic and continual battle of "cyber intrusion, influence actions, and ambiguous force without sustained conflict."¹²⁴

New Generation Warfare Applied to AFSOC

AFSOC provides a powerful asymmetric advantage employing new generation warfare tactics against near-peer adversaries in an A2/AD environment. Previous chapters discussed case studies and prescriptive evaluation results in a compiled list of tactics available to the joint warfighter. Table 5 combines Russian's bins approach and U.S. MISO joint doctrine categories of exploit/deceive, disrupt, and deny to new

¹²¹ CJCS, JP 3-0, V-13.

¹²² Joint Chiefs of Staff (JCS), "Joint Concept for Integrated Campaigning: Executive Overview" (PowerPoint presentation, Joint Chiefs of Staff, Washington, DC, December 2017), slide 25.

¹²³ Ibid., slide 24.

¹²⁴ Ibid., slide 25.

generation warfare tactics.¹²⁵ These tactics are compared against AFSOC capabilities to either contribute through MISO operation or instead contribute by providing access to shaping operations. AFSOC transitions from direct MISO to providing indirect access to shaping operations conducted by cyberspace and information operation authorities responsible for these U.S. capabilities. The viability of this approach acknowledges that U.S. authorities compared to Russian authorities are more restricted. Many decisions are made at the highest levels of the U.S. government. Although special mobility has been a tenant of AFSOC since its inception, special mobility synchronized with information operation allows the U.S. to use new generation warfare tactics against a near-peer adversary in an A2/AD environment.

Table 5. AFSOC New Generation Warfare Tactics Bins

<u>Exploit/Deceive</u>	<u>Disrupt</u>	<u>Deny</u>
• Key leader saturation • Policing Actions • Guerrilla Support • EW	• Botnet • Hacking • Cyber Attack • EW • Guerilla	• Botnet • Hacking • Cyber Attack
MISO ←———— AFSOC Contribution —————→ Access to Shape		

Source: Created by author.

The A2/AD environment of future conflicts will look to deny freedom of movement to the U.S. However, the global economy and current technology can allow

¹²⁵ Chairman, Joint Chief of Staff (CJCS), Joint Publication (JP) 13-2, *Military Information Support Operations* (Washington, DC: JCS, 21 November 2014), II-6.

access through irregular means exploited and capitalized on by AFSOC. A near-peer adversary will likely continue to contribute to the global economy for energy and resources which inherently allows access to them. Furthermore, no area surveillance or airspace monitoring provides a 100 percent assurance of detection. The three-dimensional nature of sovereign airspace using radar or visual observers have exploitable weaknesses. Even an extremely advanced adversary lacks reaction speed and intelligent surveillance to deny access completely. AFSOC can exploit these vulnerabilities to provide access where there otherwise does not exist. New generation warfare can further expand on this IW tool.

AFSOC Direct Support to New Generation Warfare

AFSOC MISO capabilities could employ new generation warfare tactics. AFSOC capabilities synchronized with botnet operations and IO targeting news agencies could spoil the enemy's IO, influence target audiences, and create new access to otherwise denied areas. MISO capabilities allow AFSOC to influence key leaders and deliver secure and hard to trace messages directly to single individuals in a clandestine matter. AFSOC MISO operations are technical, and classified approaches are outside the scope of this thesis. Finally, MISO can target a specific audience to contest enemy IO that lie or mislead about friendly actions or intentions. New generation warfare takes IO to a new level of employing all means necessary to influence friendly, neutral, and enemy forces. MISO contributes to that influence and can be easily adapted and synchronized with other domains and capabilities.

AFSOC can further use covert and/or clandestine special mobility operations to create access for new generation warfare tactics to further shape the OE. Referencing

case studies in chapter 4, a target audience will defend itself through denying access and isolating audiences when confronted with new generation warfare tactics. AFSOC's scalable-signature mobility platforms coupled with the SOF land component capabilities provide another layer to overcome access limitations and audience isolation. AFSOC new generation warfare tactics provide access for guerrilla support and policing action coordination. Also, these tactics provide IO targeting key leader saturation and hacking, and finally offensive cyber operations, cyber-attacks, towards government agencies.

AFSOC MISO and special mobility capabilities provide a currently developed and practiced tactic employed in a new generation warfare way. These tactics include broadcasting over-the-air communication, leaflet drops, resupply, and personnel movement to austere and A2/AD environments. These tactics, when employed in conjunction with other IO and cyberspace operations, provide a powerful capability that counters an adversary's offensive operations and stops their initiative. AFSOC aircraft can provide a small logistics footprint. Some AFSOC aircraft can even operate from dirt fields and roads. This rapid, special mobility allows policing and guerrilla forces to quickly move to counter adversary activities creating civil unrest or influence minority populations.

AFSOC Indirect Support to New Generation Warfare

AFSOC contributes indirectly to new generation warfare tactics of computer hacking, employing botnets, influencing news agencies, or cyber-attacks against different government agencies and senior leadership. The U.S. military has several agencies that conduct cyberspace operations and news agencies coordinate efforts that are outside the scope of this thesis. These government agencies can hinder access in a near-peer

adversary employing new generation warfare tactics and denied OE. AFSOC special mobility and MISO can deliver current and future capabilities to this A2/AD environment working with interagency partners and other SOF components specializing in psychological warfare and IO. Furthermore, when special mobility and MISO capabilities synchronized with IO towards a specific targeted audience, the U.S. can provide a capability to defend against adversary's IO and further influence the OE for the U.S. benefit.

Emerging Technology

AFSOC influences the OE through the delivery of other capabilities. AFSOC benefits from being comprised of a small fleet of aircraft. With a relatively small fleet, AFSOC modifies and fields capabilities much faster than most other U.S. Air Force operational units. AFSOC operators frequently handle ambiguous and ill-defined problems, and the fielding of emerging technology easily aligns with this mentality.

AFSOC can also rapidly deliver commercial and experimental cutting-edge technology to influence target audiences. AFSOC can deliver temporary communication infrastructure to thwart enemies A2/AD operations with regards to cellular and network connectivity. For example, an MC-130 airdrops Loon balloon-deployable temporary cellular network antenna in an A2/AD environment to support U.S., coalition, and local population integration.¹²⁶ This tactic requires validation, but conceptually an MC-130 could circumnavigate or threat penetrate an A2/AD environment and deliver Loon balloons. The Loon system then provides rapid connectivity to support coordination with

¹²⁶ Loon, "About the Technology," accessed 19 December 2018, <https://loon.co/>.

a target audience in a remote or isolated OE. IO are a crucial component of near-peer adversary domain supremacy that must be constantly challenged and further reinforced to pursue the initiative.

For example, AFSOC assets could deliver Lattice automated technology designed to provide remote and early warning capabilities around underdeveloped OEs. Lattice can integrate into a multitude of portable devices from stationary towers, unmanned aircraft, or vehicles.¹²⁷ Lattice fuses multiple detection capabilities to intelligently decide and verify a given parameter is present, i.e., a particular person or piece of equipment is moving through the systems field of view and even track the given parameter.¹²⁸ Lattice essentially creates an advanced early warning network with minimum resources or limited human passive detection capabilities. Applications of Lattice technology are numerous in new generation warfare tactics listed in table 5. Lattice early warning could help to manage guerilla operations in a certain area or activate policing actions to hinder an adversary attempt to create civil unrest. Finally, Lattice autonomous software using multiple third-party sensors establish a pattern of life on key leadership, government agencies, or infrastructure support for follow-on cyberspace operations. The pattern of life knowledge helps to refine targeting a specific audience through IO.

Access to the target audience will always challenge new generation warfare tactics due to its subversive and indirect nature. AFSOC could deliver another cutting-edge technology in the form of airborne-delivered swarms to support new generation

¹²⁷ Anduril, “Lattice,” Accessed 10 December 2018, <https://www.anduril.com/lattice-ai/>.

¹²⁸ Ibid.

warfare tactics. A swarm, similar to a locust swarm, contains a collection of drones working together autonomously to accomplish complex missions in an A2/AD environment.¹²⁹ This tactic would combine several proven and previously demonstrated methods of drone employment. A thousand Intel® “Shooting Star” drones demonstrated multiple times the ability of swarms to communicate and integrate during the Olympics Closing Ceremony and Consumer Electronics Show in 2018.¹³⁰ Furthermore, the DOD, Strategic Capabilities Office in conjunction with the Naval Air System Command launched 103 Perdix quad-copter drones from three F/A-18s Super Hornets. The demonstrations provide proof of the concept that a swarm could execute using collective decision-making, adaptive formative flying, and resilient re-tasking.¹³¹ A drone swarm employing artificial intelligence and delivered through AFSOC aircraft provide access to new generation warfare tactics. A drone swarm conceptually could carry ISR sensors to map out infrastructure vulnerabilities or collecting emissions in the electromagnetic environment and transmit back locations and activities for analysis. A drone swarm could even deliver other payloads including smaller drones capable of delivering new

¹²⁹ Clayton Schuety and Lucas Wills, “An Air Force ‘Way of Swarm’: Using Wargaming and Artificial Intelligence to Train Drones,” *War on The Rocks*, 21 September 2018, accessed 26 January 2019, <https://warontherocks.com/2018/09/an-air-force-way-of-swarm-using-wargaming-and-artificial-intelligence-to-train-drones/>.

¹³⁰ Mallory Locklear, “Intel put on an Olympic light show with 1,218 drones,” *Engadget*, 09 February 2018, accessed 25 January 2019, <https://www.engadget.com/2018/02/09/intel-olympic-light-show-1-218-drones/>.

¹³¹ U.S. Department of Defense, “Department of Defense Announces Successful Micro-Drone Demonstration,” News Release No: NR-008-17, 9 January 2017, accessed 25 January 2019, <https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1044811/departments-of-defense-announces-successful-micro-drone-demonstration/>.

generation warfare cyber-attacks to target computer systems. From a more kinetic approach, a drone swarm could carry small explosives providing a hunter-killer tactic towards enemy integrated air defense or other A2/AD systems preventing further access into the AO. The hunter-killer tactic divides the swarm using ISR sensors to collect data, verify valid targets, and task explosive-filled killer drones to attack valid targets. The swarm could gather and report battle damage assessment to higher headquarters. AFSOC special mobility employing airborne delivered or launched swarms to deliver new generation warfare tactics against a near-peer adversary indirectly.

AFSOC can contribute access and shaping operations using new generation warfare tactics against A2/AD OE. AFSOC IW experience provide an excellent reason why air commandos should employ new generation warfare tactics. AFSOC primary capabilities of MISO and special mobility deliver both direct and indirect new generation warfare tactics to an A2/AD environment. New generation warfare tactics provide a growth market for AFSOC as emerging technologies including Loon, Lattice, and swarm tactics capabilities mature. New generation warfare tactics linked with AFSOC current capabilities provide an asymmetric advantage for future operations.

CHAPTER 6

CONCLUSION

Joseph Stalin was a cruel dictator of the former Soviet Union. Although his ends were sinister, his means and ways of propaganda demonstrated the strength of a state to influence a targeted audience. Over a century later, a globally connected world created a new information domain. Many state and non-state actors pursue influence in the information domain to advance their interests. Russia in particular advances propaganda of the 21st century synchronizing multiple tactics including the information domain to create new generation warfare. Russian new generation warfare uses political, economic, diplomatic, and other non-military measures in combination with the use of military force.¹³² New generation warfare starts in the information domain employing psychological operations to manipulate, control, and demoralize a target audience.¹³³ These tactics focus on reducing the need for conventional military power and convincing the adversary's civil population to support the desire of the influencer.¹³⁴

The U.S. builds upon Russian new generation warfare with the help of the IW air component, AFSOC. AFSOC missions of MISO and special mobility are perfectly suited to contribute directly and indirectly to new generation warfare. This thesis answers the

¹³² Bartles, "Getting Gerasimov Right," 36.

¹³³ Chekinov and Bogdanov, "The Nature and Content of a New-Generation War," 17.

¹³⁴ Shahzada Rahim, "New-Generation Warfare and the Future of State Security," *The Jerusalem Post*, 3 September 2018, para 6, accessed 9 February 2019, <https://www.jpost.com/Opinion/New-generation-warfare-and-the-future-of-state-security-566421>.

question of how AFSOC can adopt new generation warfare tactics to provide an asymmetric capability against a near-peer adversary. AFSOC adopts these tactics by employing MISO or providing access to shaping operations including a range of effects from key leader saturation to cyber attacks (see table 5). This chapter provides further insight into possible implications of new generation warfare tactics and additional research to further develop these emerging tactics.

Implications

Russia progressively developed new generation warfare tactics from its initial operations in Estonia in 2007. This section forecasts the future of new generation warfare. Each iteration of new generation warfare tactics provides a better organized and more sophisticated collaboration with conventional warfare and IW tactics to expanding Russian influence. The Russia-Ukraine conflict is ongoing today, and Russia seeks to consolidate physical gains and influence in their near-abroad. Although this thesis focuses on Russian new generation warfare tactics, these common implications are not state-specific.

New generation warfare tactics will continue to be characterized by a high level of capability, continually evolving, and likely morphing into a different form of its previous self. States will re-adjust their approach to be more asymmetric, covert, and clandestine in future employment. The nature of these tactics is technical, synchronized, and robust to influence the target audience. An advanced military, integrated with intergovernmental agencies, deploys traditional and non-military tactics against the target

audience..¹³⁵ The communication equipment and the deliberate nature of layering effects require professional experience. For all these reasons, a few developed states likely reserve new generation warfare tactics to themselves due to budgetary requirements.

Furthermore, how a population consumes information from their government and outside entities dictates the changing nature of new generation warfare. This changing nature directly links to the principle of “the main battle space is in the [adversaries] mind.”¹³⁶ New generation warfare tactics influence the adversary’s mind by any means necessary. For example, the social media preferences of a target audience provide a changing platform for new generation warfare to monitor and target audiences continually. Brian Steed in his discussion of “narrative warfare” address social media as a tool to deliver a message..¹³⁷ New generation warfare builds on this narrative concept to use multiple tools to deliver a message to a target audience. An adversary’s future means of transmitting a message creates a constantly changing tool of how to target and influence an audience.

New generation warfare’s last future characteristic is the rapid development and employment of advanced technology. Artificial Intelligence development coupled with cyberspace operations will dramatically alter how new generation warfare will employ in

¹³⁵ Rahim, “New-Generation Warfare and the Future of State Security,” para 4.

¹³⁶ Ibid., para 5.

¹³⁷ Brian Steed, “Maneuvering within Islam’s Narrative Space,” *Strategic Review Indonesia*, para 18, accessed 9 February 2019, <http://sr-indonesia.com/read/maneuvering-within-islam-s-narrative-space>.

the future.¹³⁸ Artificial intelligence allows computers to monitor millions of target audiences simultaneously and react to changing moods and behaviors to concentrate influence efforts based on when an audience is most impressionable.¹³⁹ Prototype warfare, described as unproven technology or combining commercial-off-the-shelf technology in new ways, will further expand new generation warfare tactics.¹⁴⁰

A state interested in new generation warfare must invest in technology and integration of military and non-military agencies to eventually reach the bare minimums required for effective employment. Furthermore, a state must continually adapt their tactics of new generation warfare to remain covert and clandestine in its approach. A state or non-state actor interested in employing new generation warfare tactics requires a large investment in time and resources to achieve their desired end-state.

Future Research

There are several more related topics worthy of future research to understand new generation warfare tactics. Future research at the classified level, strategic level, or with evolving technology should provide additional tactics to advance new generation warfare.

¹³⁸ Rahim, “New-Generation Warfare and the Future of State Security,” para 7.

¹³⁹ David Fastabend and Jeffery Baker, *The Operational Environment and the Changing Character of Future Warfare*, (research paper, United States Army Training and Doctrine Command G-2 Operational Environment, 2017), 8, accessed 30 March 2019, <https://madsciblog.tradoc.army.mil/tag/the-operational-environment-and-the-changing-character-of-future-warfare/>.

¹⁴⁰ Ian Sullivan, “Lessons Learned in Assessing the Operational Environment,” *United States Army Training and Doctrine Command Mad Science Laboratory* (blog), 1 February 2018, para 8, accessed 9 February 2019, <https://madsciblog.tradoc.army.mil/tag/new-generation-warfare/>.

Although this research acknowledged several components, this section suggests a collection of future research on new generation warfare tactics.

This thesis uses open-source reporting and unclassified documents and publications to describe new generation warfare tactics. However, a classified review of literature should provide future researchers with more detailed and technical information regarding the study and development of tactics. Also, The U.S. and AFSOC classified capabilities should further enhance new generation warfare tactics in an A2/AD environment. These classified capabilities might include both direct and indirect approaches providing access to a covert or clandestine nature.

This thesis remained at the operational and tactical level to better implement AFSOC capabilities using new generation warfare. However, Russia executes new generation warfare on a spectrum between the tactical and strategic levels. Future research should compare and contrast new generation warfare with U.S. unified action with regards to legal authorities at a strategic level. Unified Action is “the synchronization, coordination, and /or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort.”¹⁴¹ New generation warfare gives the Russian General Staff the authority to execute these tactics using all available assets of the state. Inversely, The U.S. Unified Action makes the joint task force commander work in conjunction with other government agencies to gain access to all capabilities. Russian new generation warfare authorities rest with individuals. Unified action divides authorities between multiple agencies responsible for

¹⁴¹ CJCS, *DOD Dictionary of Military and Associated Terms*, 244.

their specialties. At the strategic level, new generation warfare could provide the U.S. with a strategic framework to better synchronize efforts under one commander providing unity of effort and the added benefit of unity of command.

New generation warfare tactics will continue to evolve as new technologies become more accessible. Future researchers should explore artificial intelligence, machine learning, and quantum computing as tools to advance new generation warfare. Furthermore, new space and airborne systems could provide other ways to access an A2/AD environment and overcome adversaries defenses against current new generation warfare tactics. A future researcher will also need to update these tactics as Swarm, Loon, and Lattice employment continues to advance with other military operations.

Future researchers can advance new generation warfare tactics through additional research at a classified level, comparing Unified Action authorities at the strategic level, and the employment of new technology. New generation warfare is a complex system of conducting the ROMO with and without armed conflict that allows a state to influence others. It is paramount U.S. military professionals continue to explore and research this topic for better understanding and implementation.

Summary

Current capabilities could limit AFSOC assets operating in an A2/AD environment due to a lack of air superiority in the AO. AFSOC must find a different way to employ engrained in the command's IW heritage. Russian new generation warfare provides asymmetric tactics through the innovation of current AFSOC capabilities in future A2/AD environments.

BIBLIOGRAPHY

Air Force Special Operations Command. "About Us." U.S. Air Force, 4 November 2018. Accessed 4 November 2018. <https://www.afsoc.af.mil/About-Us/>.

Anduril. "Lattice." Accessed 10 December 2018. <https://www.anduril.com/lattice-ai/>.

Bartles, Charles K. "Getting Gerasimov Right." *Military Review* (January-February 2016): 30-38. Accessed 30 March 2019. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf.

Berkebile, Richard E. "New Generation Warfare and the Just War Tradition." *Inter-Agency Journal* 9, no. 3 (2018): 17-33.

Berzins, Janis. "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy." Policy Paper, National Defence Academy of Latvia, Center for Security and Strategic Research, Riga, Latvia, April 2014.

Chairman, Joint Chiefs of Staff. Joint Publication 1-0, *Doctrine for the Armed Forces of the United States*. Washington, DC: Joint Chiefs of Staff, July 2017.

———. Joint Publication 3-0, *Operations*. Washington, DC: Joint Chiefs of Staff, 17 January 2017.

———. Joint Publication 3-05, *Special Operations*. Washington, DC: Joint Chiefs of Staff, July 2014.

———. Joint Publication 3-13, *Information Operations*. Washington, DC: Joint Chiefs of Staff, 20 November 2014.

———. Joint Publication 13-2, *Military Information Support Operations*. Washington, DC: Joint Chiefs of Staff, 21 November 2014.

———. Joint Publication, *DOD Dictionary of Military and Associated Terms*. Washington, DC: Joint Chiefs of Staff, 1 September 2018.

Chekinov, Sergei G., and Sergei A. Bogdanov. "The Nature and Content of a New-Generation War." *Military Thought*, no. 4 (2013): 12-23.

Chivvis, Christopher S. *Understanding Russian 'Hybrid Warfare': And What Can Be Done About It?* Testimony presented before the House Armed Services Committee Testimony, 22 March 2017. Santa Monica, CA: RAND Corporation, 2017.

- Cornwell, Rupert. "Charlie Wilson: Obituaries." *The Independent*, 13 February 2010. Accessed 17 November 2018. <https://www.independent.co.uk/news/obituaries/charlie-wilson-congressman-whose-support-for-the-mujahideen-helped-force-the-soviet-union-out-of-1898180.html>.
- Creswell, John W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 2nd ed. Thousand Oaks, CA: Sage Publication, 2003.
- Culp II, Robert A. "Exploiting Vulnerabilities in the Russian Approach to Hybrid Warfare." Strategy Research Project, U.S. Army War College, Carlisle, PA, 1 April 2016. Accessed 29 November 2018. <http://publications.armywarcollege.edu/pubs/786.pdf>.
- Fastabend, David, and Jeffery Baker. "The Operational Environment and the Changing Character of Future Warfare." Research paper, United States Army Training and Doctrine Command G-2 Operational Environment, 2017. Accessed 9 February 2019. <https://madsicblog.tradoc.army.mil/tag/the-operational-environment-and-the-changing-character-of-future-warfare/>.
- Finn, Peter. "Cyber Assaults on Estonia Typify a New Battle Tactic." *Washington Post*, 19 May 2007. Accessed 17 November 2018. <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html>.
- Fox, Liam. "Hybrid War-Hybrid Response." *NATO Review Magazine*, 25 November 2014. Accessed 17 November 2018. <https://www.dvidshub.net/video/377850/nato-review-hybrid-war-hybrid-response>.
- Galeotti, Mark. "I'm Sorry for Creating the 'Gerasimov Doctrine'." *Foreign Policy*, 5 March 2018. Accessed 30 March 2019. <https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/>.
- . "The 'Gerasimov Doctrine' and Russian Non-Linear War." *Moscow's Shadow* (blog), 6 July 2014. Accessed 30 March 2019. <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>.
- Gareev, Makhmut, and Vladimir Slipchenko. *Future War*. Fort Leavenworth, KS: Foreign Military Studies Office, February 2007.
- Google. "Results from A Google Search of 'Russian Hybrid Warfare'." 3 October 2018. Accessed 3 October 2018. <https://www.google.com/search?q=russian+hybrid+warfare&oq=Russian+Hybrid+Warfare&aqs=chrome.0.0j69i60l3j69i59j0.5096j1j7&sourceid=chrome&ie=UTF-8>.

- Headquarters, Department of the Army. Field Manual 3-0, *Operations*. Washington, DC. Government Publishing Directorate, October 2017.
- Higgins, Andrew. “Finger Pointed at Russians in Alleged Coup Plot in Montenegro.” *New York Times*, 26 November 2016. Accessed 12 November 2018.
<https://www.nytimes.com/2016/11/26/world/europe/finger-pointed-at-russians-in-alleged-coup-plot-in-montenegro.html>.
- Hoffman, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Warfare*. Arlington, VA: Potomac Institute for Policy Studies, December 2007.
- . “Hybrid Warfare and Challenges” *Joint Forces Quarterly*, no. 52 (1st Quarter 2009): 34-39.
- Hope, Kerin. “Bulgarians See Russian Hand in Anti-Shale Protests.” *Financial Times*, 30 November 2014. Accessed 11 November 2018.
<https://www.ft.com/content/e011d3f6-6507-11e4-ab2d-00144feabdc0>.
- Human Rights Watch. “Up in Flames: Humanitarian Law Violations and Civilian Victims in the Conflict over South Ossetia.” 1 January 2009. Accessed 17 November 2018.
https://www.hrw.org/sites/default/files/reports/georgia0109_brochure_web.pdf.
- Ignatius, Adi. “A Tsar is Born: Person of the Year 2007.” *Time Magazine*, 19 December 2007. Accessed 30 March 2019.
http://content.time.com/time/specials/2007/personoftheyear/article/0,28804,1690753_1690757_1690766,00.html.
- Joint Chiefs of Staff. “Joint Concept for Integrated Campaigning: Executive Overview.” PowerPoint Presentation, Joint Chiefs of Staff, Washington, DC, December 2017.
- Keller, L. Robin. *Annals of Operations Research*. Amsterdam, The Netherlands: Baltzer Scientific Publishing, October 1987.
- Kenez, Peter. *The Birth of the Propaganda State: Soviet Methods of Mass Mobilization. 1917-1929*. London, UK: Cambridge University Press, 1975.
- Leonhard, Robert R., and Stephen P. Phillips. “‘Little Green Men’: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014.” Strategic Research Project, The United States Army Special Operations Command: Assessing Revolutionary and Insurgent Strategies, Fort Bragg, NC, 2015. Accessed 21 September 2018.
http://www.jhuapl.edu/ourwork/nsa/papers/ARIS_LittleGreenMen.pdf.
- Locklear, Mallory. “Intel put on an Olympic light show with 1,218 drones.” *Engadget*, 09 February 2018. Accessed on 25 January 2019.
<https://www.engadget.com/2018/02/09/intel-olympic-light-show-1-218-drones/>.

- Loon. "About the Technology." Accessed 19 December 2018. <https://loon.co/>.
- Palagi, Jamie. "Wrestling the Bear: The Rise of Russian Hybrid Warfare." Thesis, Joint Forces Staff College, Joint Advanced Warfighting School, Norfolk, VA, 13 April 2015.
- Paul, Christopher, and Miriam Matthews. *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. Santa Monica, CA: RAND Corporation, 11 July 2016. Accessed 11 November 2018. <https://www.rand.org/pubs/perspectives/PE198.html>.
- Rahim, Shahzada. "New-Generation Warfare and the Future of State Security." *The Jerusalem Post*, 3 September 2018. Accessed 9 February 2019. <https://www.jpost.com/Opinion/New-generation-warfare-and-the-future-of-state-security-566421>.
- Schroden, Jonathan. "How Special Ops Can Step It Up." *War on The Rocks*, 19 December 2018. Accessed 19 December 2018. <https://warontherocks.com/2018/12/how-special-ops-can-step-it-up/>.
- Schuety, Clayton, and Lucas Wills. "An Air Force 'Way of Swarm': Using Wargaming and Artificial Intelligence to Train Drones." *War on The Rocks*, 21 September 2018. Accessed 26 January 2019. <https://warontherocks.com/2018/09/an-air-force-way-of-swarm-using-wargaming-and-artificial-intelligence-to-train-drones/>.
- Secretary of Defense. *Department of Defense: Strategy for Operations in the Information Environment*. Washington, DC: Department of Defense, June 2016.
- . *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge*. Washington, DC: Department of Defense, January 2018.
- Shevchenko, Vitaly. "'Little Green Men' or 'Russian Invaders.'" *BBC News*, 11 March 2014. Accessed 14 November 2018. <https://www.bbc.com/news/world-europe-26532154>.
- Shuster, Simon. "Russia lost 64 troops in Georgia War, 283 wounded." *Reuters*, 21 February 2009. Accessed 17 November 2018. <https://uk.reuters.com/article/us-russia-georgia-deaths/russia-lost-64-troops-in-georgia-war-283-wounded-idUKTRE51K1B820090221>.
- Snegovaya, Maria. "'Reflexive Control': Putin's hybrid warfare in Ukraine is straight out of the Soviet Playbook." *Business Insider*, 22 September 2015. Accessed 3 November 2018. <https://www.businessinsider.com/reflexive-control-putins-hybrid-warfare-in-ukraine-is-straight-out-of-the-soviet-playbook-2015-9>.

- Sprang, Ronald. "Russia in Ukraine 2013-2016: The Application of New Type Warfare Maximizing the Exploitation of Cyber, IO, and Media." *Small Wars Journal*, 11 September 2018. Accessed 18 September 2018.
<http://smallwarsjournal.com/jrnl/art/russia-ukraine-2013-2016-application-new-type-warfare-maximizing-exploitation-cyber-io-and>.
- . "Russian Operational Art, New Type Warfare, and Reflexive Control." *Small Wars Journal*, 3 November 2018. Accessed 3 November 2018.
<http://smallwarsjournal.com/jrnl/art/russian-operational-art-new-type-warfare-and-reflexive-control>.
- Stalin, Joseph. Quoted in Headquarters, Department of the Army. Field Manual 3-0, *Operations*. Washington, DC: Government Printing Office, October 2017.
- Steed, Brian. "Maneuvering within Islam's Narrative Space." *Strategic Review Indonesia*. Accessed 9 February 2019. <http://sr-indonesia.com/read/maneuvering-within-islam-s-narrative-space>.
- Sullivan, Ian. "Lessons Learned in Assessing the Operational Environment." *United States Army Training and Doctrine Command Mad Science Laboratory* (blog), 1 February 2018. <https://madsciblog.tradoc.army.mil/tag/new-generation-warfare/>.
- Tamkin, Emily. "Better Prepared for Cyber Threats?" *Foreign Policy*, 27 April 2017. Accessed 17 November 2018. <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/>.
- Thomas, Timothy. "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations." *Defense Strategic Communications Journal* 1, no. 1 (Winter 2015): 11-26.
- . "The Evolving Nature of Russia's Way of War." *Military Review* (July-August 2017): 34-42. Accessed 30 March 2019,
https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20170831_THOMAS_Russias_Way_of_War.pdf.
- U.S. Air Force. "EC-130J Commando Solo." 14 January 2016. Accessed 16 January 2019. <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104535/ec-130j-commando-solo/>.
- U.S. Department of Defense. "Department of Defense Announces Successful Micro-Drone Demonstration." News Release No: NR-008-17, 9 January 2017. Accessed 25 January 2019. <https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1044811/departments-of-defense-announces-successful-micro-drone-demonstration/>.

Vice Chairman, U.S. Joint Chiefs of Staff. *Joint Concept for Integrated Campaigning*. Washington, DC: Joint Chiefs of Staff, 16 March 2018.

Yourish, Karen, and Troy Griggs. “8 U.S. Intelligence Groups Blame Russia for Meddling, but Trump Keeps Clouding the Picture.” *New York Times*, 2 August 2018. Accessed 10 November 2018.
<https://www.nytimes.com/interactive/2018/07/16/us/elections/russian-interference-statements-comments.html>.