REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
15-05-2021	Master of Military Studies (MMS) thesis	AY 2020-2021

4. TITLE AND SUBTITLE
The Bear Influenced the Mountain

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
DeMarco, Scott C. (Lieutenant Commander)

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The twenty-first-century information environment compels the United States to rethink how it employs information as an element of national power. The United States needs to update its information operations strategy to compete and win in the future operating environment. Similarly, an appropriate first step toward developing a unified American information strategy is to develop an understanding of Russia's.The Russian incursion in Ukraine and its annexation of Crimea present a unique case study in a mostly successful information warfare campaign effectively coordinated from strategic to tactical.

15. SUBJECT TERMS
Information Warfare, Information Operations, Operations in the Information Environment; Russia; Crimea.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU		19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:

THE BEAR INFLUENCED THE MOUNTAIN

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF MILITARY STUDIES

AUTHOR:

LIEUTENANT COMMANDER SCOTT DEMARCO

AY 2020-21

MMS Mentor Team and Oral Defense Committee Member:
LTC Jeremy T. Glauber
Approved: _____
Date: 20 May 2021.

MMS Mentor Team and Oral Defense Committee Member:
Jill Goldenziel
Approved: Jill Goldenziel
Date: 20 May 2021

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:

THE BEAR INFLUENCED THE MOUNTAIN

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF MILITARY STUDIES

AUTHOR:

LIEUTENANT COMMANDER SCOTT DEMARCO

AY 2020-21

MMS Mentor Team and Oral Defense Committee Member:

_____
Approved: _____
Date: _____

MMS Mentor Team and Oral Defense Committee Member:

_____
Approved: _____
Date: _____

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Executive Summary

Title: The Bear Influenced the Mountain.

Author: Lieutenant Commander Scott DeMarco, United States Navy

Thesis: The United States needs to update its information operations strategy to compete and win in the future operating environment. Consequently, the United States should re-establish an agency to lead its information domain of national power like that of the Information Agency, which it demobilized in 1999 and folded within the State Department.

Discussion: The twenty-first-century information environment compels the United States to rethink how it employs information as an element of national power. The Russian incursion in Ukraine and its annexation of Crimea present a unique case study in a mostly successful information warfare campaign effectively coordinated from strategic to tactical. Indeed, Russia has refined its information warfare approach to offset its diminishing hard power and military capabilities vis-a-vis the world's strongest military, the United States.[1] In light of accelerating technological advancements in how information is produced and transmitted, information will likely continue to grow in importance as a source of national power and security.[2] Similarly, an appropriate first step toward developing a unified American information strategy is to develop an understanding of Russia's.

Conclusion: As communication and media technology advance, information will increasingly be a critical factor in how the United States government and military engage with adversaries, allies, and partners.[3] Clear and consistent strategic communication promulgated from a United States Government agency—an agency charged with information and information alone—will help reassure the United States' allies and partners and counter adversaries. The United States needs to create a new agency to leverage the tools of the modern information age and effectively wield information as a source of national power.[4]

Table of Contents

Page

Introduction

The twenty-first-century information environment compels the United States to rethink how it employs information as an element of national power. The Russian incursion in Ukraine and its annexation of Crimea present a unique case study in a mostly successful information warfare campaign effectively coordinated from the strategic to the tactical levels. Indeed, Russia has refined its information warfare approach to offset its diminishing hard power and military capabilities vis-a-vis the world's strongest military, the United States.[5] In light of accelerating technological advancements in how information is produced and transmitted, information will likely continue to grow in importance as a source of national power and security.[6] Accordingly, an appropriate first step toward developing a unified American information strategy is to develop an understanding of Russia's.

Russia sought to reclaim its influence over Ukraine in 2014 after pro-Western forces ousted Ukrainian President Viktor Yanukovych.[7] Events unfolded quickly after the interim pro-Western government assumed power. While the Ukrainian elite was preoccupied with political infighting, demonstrations, and protests, Russia executed a covert operation using special forces (SPETSNAZ), naval infantry, and proxy organizations.[8] Russia capitalized on its preparation of the information environment while its military forces employed speed, surprise, and small-unit precision to quickly seize control of the Crimean Peninsula. Within three weeks of its forces seizing the peninsula, a hastily organized referendum formally acceded Crimea to the Russian Federation.

Russia's military operation in Crimea represented a coordinated and decisive use of state power to achieve a desired political objective. Along the way, Russia proved adept at using multiple state power levers to achieve its goals in pursuit of both its military and political

objectives.[9] However, one lever proved critical—information. Russia's autocratic control of all its national media organs combined with equally tight control of all its levers of power ensured that its informational activities were coordinated from the strategic to tactical levels. Indeed, well-planned and effectively coordinated Russian information warfare activities preceded, accompanied, and followed Russian military operations in Crimea. These activities included deception, psychological operations, social media, propaganda, and an older Soviet-era technique, reflexive control. Since the collapse of the Soviet Union, Russia has adopted lessons learned from various American operations and adapted its methods to meet modern conflict realities.[10] Critically, it has made information a primary effort in achieving its objectives, with military efforts in a supporting role. In Crimea, any direct military actions supported disinformation and special operations forces.[11] Indeed, Russia's Information Warfare campaign played a central role in seizing another state's territory with no direct casualties, little fighting, and even less Western intervention.[12]

Russia and other United States adversaries actively plan, develop, refine, and employ methods to combine their various information warfare parts into a unified whole. The United States needs to refine its information strategy to achieve the same. Information is such a powerful force that the United States recognizes it as an instrument of national power. For decades, "Information" has earned its rightful place alongside Diplomacy, Military, and Economics as one of the four sources of U.S. national power, commonly referred to as "DIME." Nevertheless, the U.S. Government does not have an organization charged with leading the informational function. The Department of State leads the diplomatic function, the Department of Defense, the military, and the Department of Treasury, the economic.[13] The United States needs an updated information operations strategy to compete and win in the future operating

environment. Consequently, the United States should re-establish an agency to lead the information domain of national power similar to that of the **United States** Information Agency, which it disbanded in 1999 and folded within the State Department.

The twenty-first-century information environment compels the United States to rethink how it employs information as an element of national power. The Russian incursion in Ukraine and its annexation of Crimea present a unique case study in a mostly successful information warfare campaign effectively coordinated from strategic to tactical. Indeed, Russia has refined its information warfare approach to offset its diminishing hard power and military capabilities vis-a-vis the world's strongest military, the United States.[14] In light of accelerating technological advancements in how information is produced and transmitted, information will likely continue to grow in importance as a source of national power and security.[15] Similarly, an appropriate first step toward developing an integrated American information strategy is to develop an understanding of Russia's.

Nothing New

Since Russia annexed Crimea in 2014, information warfare has found renewed interest for the United States military and security professionals.[16] Moreover, the interest was elevated to near obsession as Western news reported Russian interference in the 2016 United States presidential election. The renewed focus led many to believe that Russia had employed a distinctive approach with fundamentally new concepts. In the process, this created a perception of novelty. Indeed, the United States military coined several terms to reinforce the perception: hybrid warfare, asymmetric warfare, non-linear warfare, Russian new-generation warfare (RGNW), and Gerasimov doctrine. The widespread adoption of many of these terms indicated

an attempt to brand, characterize, and understand a suggestively new and unique Russian approach. However, Russia's information warfare approach, employed both in Crimea and the 2016 U.S. elections, is not a new phenomenon. Instead, Russia took old Soviet-era concepts and adapted them to the modern information environment. Further, Russia adopted lessons from different Western operations and applied and adapted what it had learned within its particular circumstances.[17]

Russia's modern information warfare approach results in part from its observation of different Western operations.[18] After observing the United States and European operations in the 1991 Gulf War, Operation Iraqi Freedom, and the intervention in Libya, General Valery Gerasimov, former chief of the general staff of the Russian Federation, noted that modern information technology had reduced the "spatial, temporal, and information gap between army and government."[19] Gerasimov contended that in modern conflict, information superiority is increasingly becoming more important relative to military power.[20] Gerasimov's observations led him to publish a report widely referred to in the United States as the "Gerasimov doctrine." Many Western readers understood the report to describe a new uniquely Russian approach to information warfare. However, the report indeed described the opposite: a *Russian* view of *Western* approaches.[21]

The idea of a uniquely Russian approach exemplifies a common pitfall within the United States military: buzzwords replacing critical thinking. Indeed, Keir Giles identified this problem in his paper, *Russia's 'New' Tools for Confronting the West.* In the report, Giles referenced a 2015 speech from General Joe Votel, commander of U.S. Special Operations Command at the time. Votel stated that the United States increasingly sees "adversaries purposefully selecting such strategies to stay within the gray zone. If anything, they have broadcasted their intentions as

we see in China's Three Warfares and Russia's Gerasimov Doctrine."[22] However, a prominent NATO study made clear that Gerasimov's research described "not Russia's own approaches, but the approaches which… are adopted by foreign powers seeking to harm Russia."[23] Although many Western observers credit Gerasimov's ideas as the bedrock through which Russia demonstrated information dominance in Crimea, Gerasimov's own words indicate that his ideas are not homemade Russian theory, but indeed an adoption of what Russia considers American practice.[24] In this sense, Gerasimov contributed to what can be understood as a merger of Russian perceptions of United States battlefield tactics with established Russian informational warfare doctrine. Recent studies of modern Russian operations, including their actions in Crimea, make this point clear.[25]

Deciphering Doctrine, Definitions, and Deliberation: Russia and the United States

Russia

Understanding Russian information warfare requires an understanding of Russian doctrine and thinking. Russia's emphasis on information warfare is reflected in its most recent official doctrine, the *Military Doctrine of the Russian Federation*, released on 26 December 2014.[26] The report describes information warfare as employing "modern technical means and information technology… at the global and regional level" for "military and political purposes."[27] The report reinforces that the goal of information warfare is "to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favorable response from the world community to the utilization of military force."[28] Additional insight into Russian thinking is also emphasized in an earlier document, *Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space*, approved in 2011.

According to *Conceptual Views*, Russia employs information warfare to stimulate "mass psychological work on the population to destabilize the society and state."[29] Again, it is important to note that these documents describe concepts mainly in defensive terms resisting what Russia considers threats against itself.[30]

Nonetheless, these documents suggest three things. First, that information warfare will increasingly continue to be a component of Russian conflict. Second, Russia's conception of information warfare has a significant political dimension. Last, Russian information warfare is not information warfare as the United States understands it.[31] Indeed, the Russian approach is far broader.

The United States should not measure its concept of information operations against the Russian concept of information warfare.[32] A search for the term *information warfare* within the glossary published by the Military Academy of the General Staff "makes a clear distinction between the Russian definition—all-encompassing, and not limited to wartime—and the Western one—limited, tactical information operations carried out during hostilities."[33] Similarly, Russian military officers have emphasized that hostilities need not be declared before employing hostile information activity.[34] For example, former Deputy Chief of the General Staff, LtGen Aleksandr Burutin, stated in 2008 that Russia employs information warfare "in an efficient manner in peacetime as well as during war."[35] This thinking is in lockstep with Russia's peacetime investments in mass media exploitation tools such as trolls (Internet personas run by humans), bots (personas run by automated processes), and strategic communication, in addition to the more traditional tools of espionage, reconnaissance, and cyber.[36] Indeed, the autocratic nature of Russia's government affords it an advantage in employing these tools regardless of its peace-war status. In contrast, the United States is making progress in expanding its use of information as a

lever or national power. However, the liberal democratic nature of the United States government does not permit most similar activity until the fighting starts.

United States

The current onrush of interest notwithstanding, defining information warfare has proven a challenge within the United States. Indeed, the United States government does not currently maintain an official definition of the term, a likely result of intending to limit the perception of a governmental "weaponization" of the Internet.[37] Furthermore, a common feature of the Department of Defense information doctrine is the mishmash of different terms and definitions. However, the Department of Defense (DoD) has included information warfare—or equivalent terms of similar meaning— as part of its vocabulary for almost thirty years. DoD first enshrined the term "information warfare" within its joint doctrine in 1992 following the Persian Gulf War.[38] However, in the intervening period, the concepts, activities, and terminology have rapidly evolved. In 2006, DoD officially removed the term "information warfare" from its vocabulary and replaced it with "information operations."[39] The current doctrinal definition of information operations is as follows:

> *The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.*[40]

In July 2017, the Chairman of the Joints Chiefs of Staff assigned information as the seventh warfighting function, joining the six prevailing functions—command and control, intelligence, fires, maneuver, logistics, and force protection. However, there is an ongoing debate about the continued use of the term *information operations* at the time of this writing.[41] DoD released Joint Concept for Operating in the Information Environment (JICOE) in July 2018 and with it a broader term, operations in the information environment (OIE).[42] Although DoD released the JICOE to "institutionalize and operationalize the Joint Force's approach to information," DoD does not currently define OIE even though it is likely to replace the term information operations.[43] Many terms, concepts, and definitions have shaped the use of information as a warfighting function. However, whichever term and definition one uses, three things are clear: (1) the use of information is strictly relegated to military activities during hostilities; (2) the role of information is not well understood across the force; (3) the first step in developing practical information doctrine should be to define terms in ways that Joint Force members can understand.

DoD information-related doctrine mainly focuses on command-and-control systems and technology. The term's thrust and intent center almost exclusively on command and control: the quality and flow of friendly and adversary information in state-on-state conflicts. The doctrine mainly instructs people on how to take advantage of technology to arm the commander with information dominance and enable tactical and operational combat objectives.[44] Studies have concluded that for the United States, "IW is almost by definition counter-command and control warfare."[45] Indeed, the approach is rarely broader than "technical responses to technical threats" and largely disregards the connection with information warfare in the broader Russian sense of the term.[46]

However, one can draw several implications from the United States' doctrine on information war. First, the United States views information as a critical warfighting domain in which to improve. The Marine Corps created a Deputy Commandant for Information and established information groups within the Marine Expeditionary Forces, indicating that manpower, funds, and attention are shifting into the developing field. Finally, DoD still presents information warfare primarily as a whole-of-government affair that requires cooperation and input from "United States Government (USG) departments and agencies as well as the commercial industry."[47]

Origins of Modern Information Warfare

Despite the attention that it has received in the United States, many of the concepts and techniques of modern Russian information warfare trace their roots back to the Soviet Union. Indeed, modern Russian information warfare is very similar to that which the Soviets employed against the West in the Cold War. Russia combines older Soviet psychological influence techniques known as reflexive control with modern information technology facilitated by the Internet and social media. However, what is new is that Russia's strategy has evolved as a deliberate response to its assessment of Western actions in the twenty-first century.[48] Russia intends its information warfare strategy to work within the limits of the modern international "environment and Russia's budget constraints."[49] Russian efforts' success depends on maintaining its activities below the international, namely Western accepted threshold for war. Although it considers the international standard antiquated, Russia has tailored its information warfare approach to parry and thrust this threshold without crossing it.[50] Similarly, the

continuity of Russian information warfare **thinkers** was enabled by continuity of thought in Russian leadership.

Officials at the highest levels of the Russian government understand information as a source of great power.[51] Most major influential governmental figures indeed have backgrounds in intelligence. Similarly, many of President Vladimir Putin's closest associates share earlier experiences in the KGB. They have long placed great value on the primacy of information and asymmetric methods to manipulate their enemies and accomplish Russian objectives.[52] President Putin himself affirmed that Russia "must take into account the plans and directions of development of the armed forces of other countries… Our responses must be based on intellectual superiority, they will be asymmetric, and less expensive."[53] Notably, many influential Russian figures have emphasized that Russia need not declare hostilities for combative information activity to begin.[54]

The writing and analysis of prominent Russian military thinkers note the emergence of the grey zone and its blurred threshold between war and peace. In one example, the findings from a Russian Special Forces study note that "a new type of war has emerged, in which armed warfare has given up its decisive place in the achievement of the military and political objectives of war to another kind of warfare—information warfare."[55] Russia has identified its actions within the information space as making conflict possible without overstepping the formally declared war threshold.[56] In general, Russia weaponized this threshold to gain flexibility and advantage against materially stronger Western powers. This thinking and similar developments that influenced the Russian information warfare approach employed in Crimea had advocates at the top of the Russian government. However, two noted academics and one military officer decisively shaped Russia's modern information warfare approach: Igor Panarin, Aleksandr

Dugin, and Valery Gerasimov. These three men helped craft Russian information warfare doctrine and have first-hand experience carrying it out.

Professor Igor Panarin has advanced degrees in psychology and political science and is a professor at the Russian state-sponsored Diplomatic Academy of the Ministry of Foreign Affairs.[57] He was a KGB member under the Soviet Union and is a close Putin associate.[58] Panarin advocates for a tightly "controlled information warfare campaign" backed by rigorous intelligence analysis and uses propaganda, media manipulation, and precise SPETZNAS operations to influence politicians and the population.[59] His advocacy for aggressive state-controlled information operations results from his observations and analysis of recent U.S. operations he deemed successful. In his book, *Information Warfare and Communications*, he states, "the national information warfare system which both secretly and openly controls communication processes must be adequate to the modern global reality. Based on the best Soviet experiences, it must be enriched by the US and Chinese experiences."[60] He went on to affirm that the "success of all geopolitical projects" are "inextricably linked to advantage in information warfare."[61] His operational approach distinguishes five cyclical stages: (1) forecasting and planning; (2) organization and stimulation; (3) feedback; (4) operation adjustment; (5) performance control.[62] Panarin branded Russia's information warfare campaign in Crimea as a combined, planned, and coordinated—media, diplomatic, financial-economic, and military—effort.

Aleksandr Dugin is also a political science professor but holds a background in philosophy and religious history. He uses the term "net-centric warfare" to define the phenomena whereby the U.S. military created new information infrastructures "involving interactive elements and fast communication."[63] In response, he advocates for a "Eurasian

netwar model" to "offer a symmetric response to the" challenges from the U.S, or "Atlantic Network" (i.e., U.S.-led Western coalitions and NATO).[64] However, initially derived and applied as a tactical and operational method to control distant military forces, Dugin modified the U.S. model into a Russian geopolitical idea. He intended to link distant joint military forces with the entire culture and information apparatus in a political and social contest.[65] He adapted to modern times the classical 1920s notion of Eurasianism where "individualistic and egoistic Europe" was the cause of increasing Western evil influence.[66] According to Dugin, Ukraine was the "battlefield of titans" where good (Russia) and evil (the United States) struggled for influence. Dugin is a leading Russian propagandist and similarly propagates messaging emphasizing unifying Eastern Slavs, with and Ukrainians and Russians uniting as one nation under the "Russian World." [67]

While the views of Panarin and Dugin underlie Russian doctrine, Russia's strategy in Crimea represented the application of ideas developed by General Valery Gerasimov, the Chief of Russia's General Staff.[68] Gerasimov's main contribution is his recognition that "modern conflict differs significantly from World War II" or even Cold War-era conflicts.[69] Instead, Gerasimov argues that in modern war, Russia must focus on intelligence and "domination of the information space."[70] Recognizing Russia's material weakness relative to Western powers, Gerasimov advocated for more unconventional capabilities to fight and win against adversaries with more significant economic and technological resources. His calls for greater investment in asymmetric capabilities also helped influence a "subtle but important shift in Russian foreign policy."[71] In a paper he wrote in 2016, he stressed the importance of the "global internet network to exert a massive, dedicated impact on the consciousness of the citizens of states that are the targets of the aggression. Information resources have become one of the most effective

types of weapons" and "enable the opposing side to be deprived of its actual sovereignty without the state's territory being seized."[72] Gerasimov's model contains six stages of conflict development: covert origins, escalations, the start of the conflict, crisis, resolution, and post-conflict settlement.[73] Gerasimov wrote that "In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template."[74]

Combined, these three men shaped the doctrine and strategy underpinning Russian methods in Crimea. Certain principles and ideas entwined all three men's writing and analysis and were evident in Russian actions on the ground in Crimea. They advocate for the primacy of non-military efforts, with military efforts in a supporting role. These non-military efforts include penetrating and saturating the target area with propaganda, deception, disinformation, and misinformation. Further, "when required, Russian information warfare must include military" action.[75] However, they recommend persistent (even plausible) denial of military operations through employing special forces and creating the appearance of spontaneous actions of local populations, troops, and militias. Gerasimov, in particular, believed that through carefully planned information operations using deception, one could mask the commencement of open hostilities and gain an advantage by confusing adversaries about its goals. Russia's initial actions in Crimea demonstrate this point well.

Crimea: A Case Study in Reflexive Control

For decades during the latter half of the twentieth century, the Soviet Union employed reflexive control. The term is close in meaning to psychological influence. However, its specific goal is to influence perceptions of a situation, causing an adversary to voluntarily choose actions

most advantageous to Russian objectives.[76] During the Cold War, the Soviet Union used reflexive control to make targeted societies more amenable to the Communist agenda. Reflexive control "is achieved by means of providing" an adversary "with the grounds by which he is able logically to derive his own decision, but one that is predetermined by the other side," according to a case study of Russia's efforts preceding the conflict with Georgia in 2008.[77] This can be achieved by threat of force, manipulating an adversary's understanding of the initial situation, shaping the adversary's objectives, or by influencing the adversary to choose to make a decision at a time favorable to its opponent.

In Crimea, Russia used a modern platform-enabled version of reflexive control and adapted it to the geopolitical circumstances to similarly influence perceptions favorable to Russia.[78] Russia's reflexive control strategy was not limited to influencing a single decision or a single audience.[79] Indeed, Russia had three intended target audiences: domestic Russians, Ukrainians (including those in Crimea), and the international community. Russia tailored its messages and themes to each audience using many forms of media—official government statements, newspapers, television, radio, social media, and front organizations.[80] The themes were protecting ethnic Russians, economic prosperity, and defense against corrupt Western values. Their messaging ranged from simple to confusing to even contradictory. However, what remained largely consistent was their broad narrative: you can trust Russia more than NATO.[81] Russia's autocratic control over all its national media organs ensured that that narrative permeated all its messaging.

Russia first directed its messaging to its domestic population. A central goal of authoritarian leaders is to retain power, and President Putin is no exception. Focusing on external threats was a helpful distraction from Russia's domestic threats, including its

increasingly authoritarian government. Russia tailored its messaging at home to foster support for Russian actions in Crimea. Putin shaped its messaging to depict NATO, led by the United States, encroaching along Russia's periphery. Russian state-backed media even went so far as to propose that the West, again led by the United States, planned to occupy Crimea to claim Sevastopol as a NATO naval base.[82] Central to its theme directed on its domestic population was that the Russian people's history and military, religious, and cultural greatness were artificially divided by Western powers following the collapse of the Soviet Union.

Similarly, concerning their actions in Crimea, Russian media heralded that the United States was behind the villainous scheme to deny Russians from maintaining peace, security, and unity.[83] This disciplined theme and consistent messaging were evident at the highest level of the Russian government. In a speech following the annexation of Crimea, President Putin affirmed that the West constantly tried to sweep Russia "into a corner because we have an independent position, because we maintain it and because we call things like they are and do not engage in hypocrisy… our western partners have crossed the line, playing the bear and acting irresponsibly and unprofessionally."[84] Russia had a primary strategic objective in the reflexive control techniques directed toward Ukrainian and international audiences to pursue its goals in Crimea: to keep Western powers out.[85]

In pursuit of this objective, the key elements of Russia's information campaign in Crimea were a manifestation of reflexive control and well-aligned with its actions on the ground.[86] Russia used deception and denial to conceal or obfuscate Russian forces' presence on the ground, including deploying "little green men." The little green men were Russian SPETSNAZ donning unmarked uniforms and operating covertly to provide the Russian government with plausible—if not improbable— deniability. By repeatedly denying Russian military involvement

in the conflict, like-minded and sympathetic members of the international community recognized Russia as an interested party instead of a participant.[87] At a certain point, Russia adjusted its influence campaign, shaping its messages to paint the environment as conducive—even favorable— to Russian intervention.[88] When Russia finally declared that it had deployed military forces, it did so under the veneer of crisis management, peacekeeping, and humanitarian assistance. Despite overwhelming evidence to the contrary, continuous Russian denials combined with messaging tailored to each phase of its operations divided Western allies' response to Russia's actions.

At the strategic level, Russia consistently denied the presence of its forces to obfuscate the monitoring of its actions by outside parties and complicate adversary decision cycles.[89] Similarly, Russian information warfare enabled Russia to achieve surprise at the tactical level by gaining the advantage against any potential resistance by Ukrainian forces. Russian tactical and strategic informational efforts indeed mutually supported one another.

Just before deploying boots on the ground in Crimea, Russia executed distributed denial of service (DDoS) attacks on Ukrainian government websites to disrupt the Ukrainian forces' communications systems based in Crimea.[90] Further, the day after Russian SPETSNAZ arrived at the Simferopol airport, they seized key government buildings and infrastructure, including print and television offices and internet service providers. Notably, a Ukrainian telecommunication company *Ukrtelecom*, announced that armed men in unidentified uniforms seized its facilities resulting in a total communication outage.[91] Subsequently, *Ukretelecom* released a report stating that the soldiers damaged and tampered with its fiber optic and conductor units. The unmarked gunmen even "equipped the remaining active cables with intercept devices" to monitor all ensuing communications.[92]

In taking control of all print and broadcast media, telecommunications, and the Simferopol Internet Exchange Point, Russia essentially isolated Crimea from the outside world. Russia's methods to achieve this isolation were denial of service attacks quickly followed by gaining "physical control of Internet" and telecommunication infrastructure and "selectively denying cable connections to the mainland."[93] Russia's isolation efforts were mostly successful in cutting off Crimea informationally from the rest of Ukraine and the world, and the result was twofold. First, the Crimean and global public's perception of Crimea's events was actively being shaped and directed by Russia.[94] Second, on March 2nd, Russian troops entered Crimea mostly unopposed.[95]

Although Russian information warfare in Ukraine began well before the conflict, deception operations accompanied Russia's first military actions.[96] Masked soldiers in uniforms devoid of insignia provided Russia with an immediate tactical advantage.[97] Operating covertly in unmarked uniforms, these forces provided the Russian government plausible deniability and obfuscated Ukrainian decision-making, obviating a timely and coordinated Ukrainian response. The unidentified personnel clandestinely seized critical buildings and facilities, only to disappear when marked forces arrived to hold their gains.[98] Moving quickly through the region, they preempted adversary action and limited adversary options by occupying airports, media outlets, internet service providers, and other critical infrastructure. Although the Western Press called these forces "Little Green Men," the Russian media and many Crimean called them "nice" or "polite men," referencing their manners and orderly withdrawal once an area was secured.[99] These "polite men" were Russian SPETSNAZ operating covertly to provide the Russian government with plausible—if not improbable— deniability.[100] As the SPETSNAZ secured

critical infrastructure, Russian forces also donned indigenous uniforms, pretended to be Ukrainian military and police, and worked with local "self-defense" units.[101]

In line with the strategy of reflexive control, a key element of Russia's information campaign was its preparation of the environment before hostilities. The objective was to target segments of Crimea's population for manipulation or cooption. Subsequently, when Russia activated military action, it did so by, with, and through portions of the local population.[102] These local "self-defense" proxy forces had embedded Russian officers in their structure and were provided essential equipment by Russian "advise, assist, and accompany" teams.[103] The proxy forces produced three effects that contributed to Russian success: confusion, deniability, and manpower. The proxy forces, with Russian officers disguised and embedded within them, frustrated Ukrainian decision-making. Very few, if any, Ukrainian officials suspected that a Russian invasion was taking place. Instead, the news portrayed to the Ukrainian mainland "local-defense" forces seizing the Parliament building and controlling the Belbek airbase.[104] The proxy forces provided a veneer of credibility to the hostilities globally and strengthened Russia's narrative of spontaneous local—not Russian—action. As with the "polite men," the use of Russian-co-opted local elements fostered confusion and provided Russia further deniability.[105]

Russia maintained ambiguity in the conflict by employing unmarked SPETSNAZ, operators disguised and interspersed among locals, and proxy forces, together with deception and disinformation. The various Russian forces had a tremendous effect on the ground by establishing numerous checkpoints, showcasing new equipment, and seizing critical infrastructure. In addition to the deception accompanying the fast, well-planned operation, an information campaign that preceded it helped shape positive local support.[106] Indeed, the information campaign that Russia employed before the conflict played an essential role in its

success. The success was the culmination of a carefully planned and long-standing information campaign designed to influence the people of Crimea that belonging to Russia was in the territory's best interest.[107] Russia sought to influence the Crimean people, "not to destroy the enemy's morale or psyche, but to form such a perception of reality that would be in line with our military goals, in our interests."[108] Similarly, through public opinion warfare, Russia sought to influence international opinion to boost support for hostilities in Crimea and obfuscate Western decision-making. Russia's methods to influence several target populations in this scenario were reminiscent of those widely used by the Soviet Union during the Cold War.

Neither Russian nor Ukrainian officials ever announced the war in Crimea. Russian forces commenced military action during official peacetime by quickly occupying and blockading most military bases in Crimea. Preceded and accompanied by deception operations, Russian forces compelled the Ukrainian forces to either switch sides or leave their posts. Gerasimov's strategy indicates a state is most likely to achieve its objectives when the lines between war and peace are blurred. The center of gravity is transformed from the physical terrain to the hearts and minds of the population. In this scenario, non-military efforts should precede military efforts. Indeed, intelligence, economic, and political efforts may likely bypass military efforts. However, a state must have a firm grip on the catalysts and crises accompanying a conflict rather than simply react to events as a passive observer. By seizing the media outlets, these "polite men" helped Russia control the pace of many of the headline events within Crimea and their flow outside of it.[109]

Russian techniques succeeded in accomplishing their objectives in Crimea, but the broader strategic campaign continues. In general, the purveyors of Russian information direct the thrust of their messaging on the Russian diaspora living within various post-Soviet era states.[110]

These purveyors shape the information environment through penetration, saturation, obfuscation, and confusion. Their methods include continuous activity, emotional appeals, platform control, and manipulation of the Russian diaspora.[111] Russia's tactical information efforts serve to prepare the operational environment and gain support from sympathetic and neutral local nationals while discrediting Western European and NATO powers. Their strategic information efforts aim to gain legitimacy throughout the world, predominately through campaigns to discredit NATO.[112]

Information Operations in the 21st century

Russia's understanding of information warfare as a tool in achieving its objectives is in lockstep with its exploitation of the global information space. This was manifest in its global effort to shape the narrative about the Crimea conflict using social and formal media. The case of Crimea may likely indicate Russia's plans in the decades to come. Russia's autocratic control of all national media organs combined with equally tight control of all its levers government power ensures that Russian information efforts are uniquely coordinated from strategic to tactical.[113] They employ a style of mission command with their information campaigns nested under key messages and themes.

Russia's information operations are a vital component of its broader military and security strategy. Russia's primary concerns throughout their planning and operations revolved around potential counteractions from the United States and Western European powers. From the outset, Russia took multiple actions within the information realm to seize the initiative within Ukraine and, at the same time, reduce the likelihood of confrontation with the West. Through "coordinated manipulation of the entire information domain," Russia created doubt across all

components of the conflict zone, swayed and confused audiences worldwide, and delayed and disrupted adversarial leaders' decision cycles (Ukrainian, NATO, and the U.S.).[114] Indeed, information operations were a key component of Russia's success in seizing the operational initiative, blunting Western confrontation, and ultimately annexing a piece of territory that had been a part of Ukraine for decades.

Modern Russian efforts are akin to a refined version of reflexive control and other measures that the Soviet Union employed for decades to foment and facilitate revolutions and undermine U.S. and NATO efforts. Similarly, today, environments within the Grey Zone are most prone to Russian information campaigns.[115] According to Senate testimony by Dr. Olga Oliker, a senior United States Government adviser on Russia, the "grey zone refers to operations… that are more difficult to define as either peace or war, and indeed… those undertaken intentionally to obfuscate and blur the lines between the two."[116] Russia's success depends on maintaining its activities below the accepted threshold for open conflict.[117]

Russia's employment of information warfare in public opinion and media warfare relies on the West's free press. Thus, Russia "seems to believe that by constantly repeating its message in the Western press and other forms of contact, it will be accepted. In the United States and other Western countries, the free press remains the primary counter to Russia's controlled messages. Many reporters are careful enough or cynical enough not to accept every message they are given; they check facts. However, traditional media filters have been eroded by social media."[118]

Recommendations for the United States Government

Countering Russian Information Operations

Strategic communications integrated within a united information campaign played a central role in the United States' strategy to combat the Soviet Union during the Cold War. The United States' strategic communications strategy to counter Soviet propaganda centered on two principles. First, let the truth inherent to a free society speak for itself. Second, identify and expose those that promulgate lies without worrying about every individual lie.[119] However, the force of this campaign was lost when the Cold War receded, and Congress passed the Foreign Affairs Reform and Restructuring Act of 1998.[120] The act disbanded the organization charged with leading the campaign, the United States Information Agency, and incorporated it into the State Department under a newly established Under Secretary of State for Public Diplomacy and Public Affairs.[121]

A United States strategic communications strategy integrated within a unified information campaign is likely even more necessary today due to the hyperconnected modern information environment. As communication and media technology advance, information will increasingly play a critical role in how the United States government and military interact with adversaries, partners, and allies.[122] Clear and consistent strategic communication promulgated from a United States Government agency—an agency charged with information and information alone—will help reassure the United States' allies and partners, counter Russian disinformation, and bring awareness to apparent lies.

To manufacture a lie is easy, and it is relatively inexpensive and simple to ensure it is widely disseminated.[123] In contrast, refuting that lie is difficult, expensive, and takes significant time and resources.[124] Further, the Internet's inherently open and unrestricted nature helps the lie prevail and begets other lies. As a result, a direct and energetic United States response to every

Russian lie is inadvisable, unwise, and nearly impossible. "It will never, in fact, be possible for the West to respond exactly in kind to a hybrid mix of tactics such as that employed by Moscow" in Crimea, a detailed report noted in 2015.[125] Although the United States "special forces and intelligence agencies can do clever things, Western governments cannot effectively restrict information flows, for example by narrowing Internet freedoms" like the Russian government.[126] In the United States, significant falsehoods or attempts at disinformation or deception will eventually get revealed, making them unfavorable and counterproductive. Instead, awareness should be the preferred tool for countering Russian lies and information operations. The awareness needs to be directed by a United States Government agency and manifested in the mainstream media, national leaders, and most importantly, the population that Russian purveyors target in their lies and operations.

An area with a steady stream of information containing far fewer filters and entry roadblocks is social media. The United States adversaries now seek to exploit social media to support their policies and actions, discredit United States actions, harm its interests, and create domestic strife.[127] Consequently, instead of attacking military targets via social media, United States adversaries can influence public opinion throughout all stages of a potential conflict, including before it even starts. For example, Facebook and Twitter use algorithms to evaluate hashtags, words, and phrases to rank topics by popularity. One study revealed that a trending topic "will capture the attention of a large audience for a short time," which then "contributes to agenda-setting mechanisms."[128] Even if the information is misleading or false, a social networking service can promulgate the narrative as fact with enough shares.

While social media likely currently serves as a net benefit for our adversaries, it can also help the U.S. achieve its objectives, including within the information domain. Russian missteps

in tactical digital messaging and security violations have resulted in strategic-level implications. For example, during the Crimean conflict's initial phase, the Atlantic Council used social media posts from Russian forces to prove Russian involvement, overturning Russia's narrative.[129] Fortunately for the United States and other liberal democracies, the truth can still be relevant.

Establish a United States Information Agency and integrated information strategy

Modern information technology and the ensuing global circulation of information have changed the character of 21st-century conflict. Future conflict will likely require deploying information as much as it does tanks and strike aircraft to defend the United States' interests and values.[130] While the information challenges posed by Russia and other adversaries are indeed an all-of-government and whole-of-society challenge, it is nonetheless a strategic challenge above all else. Consequently, the United States needs to create a new agency to leverage the tools of the modern information age and effectively wield information as a source of national power.[131]

Indeed, the defining factor of the modern information environment is accelerating information technology, which "incorporates information systems and resources (hardware and software) used by military and civilian decisionmakers to send, receive, control, and manipulate information necessary to enable 21st-century decision making."[132] This information agency must employ these advances as an asset to the United States and its allies and render them a potential vulnerability for our adversaries. As was lacking in Crimea, a renewed and energetic United States response to informational threats will affect adversaries' risk calculus and ensuing actions. The twenty-first-century information environment compels the United States Government to rethink how it employs information, starting at the strategic level.

A recent Defense Science Board report recognized modern strategic communications as a "dynamic process with responsibility held by those at the highest levels of government—the President and senior government leaders."[133] Although senior government leaders have made some progress, effective strategic communications "requires a commitment not yet seen."[134] This lack of commitment is likely due to no one United States Government agency serving as a focal point for strategic information activities. Without a dedicated agency, leadership is preoccupied with other responsibilities, resulting in untimely, disjointed, and less potent strategic communications. In contrast, a new agency with focused leadership could define a strategic communications concept, develop an information strategy, and synchronize information-related activities across government departments.

The Under Secretary of State for Public Diplomacy and Public Affairs office within the State Department is not performing these functions or performing them poorly. The mission of the Under Secretary of State for Public Diplomacy and Public Affairs office includes to "enhance national security by informing and influencing foreign publics and by expanding and strengthening the relationship between the" American people and "citizens of the rest of the world."[135] Further, their mission includes "messaging to counter-terrorism… violent extremism" and other malign ideologies, influences, and threats to national security and international institutions.[136] Likely, the office's efforts are insufficient because Congress authorized its functions before the ubiquitous nature of modern Internet and communications technology brought about today's near-unrestricted cross-border flow of information.

Critics may recommend an interagency committee, led by the National Security Staff, to lead this effort. However, a committee made up of individuals from different agencies will likely have other competing responsibilities and priorities and will not be fully dedicated to

efforts within the information domain. The competing responsibilities and ensuing lack of focus of those running the committee will likely result in unsynchronized plans and slow, ponderous action. The United States cannot afford to continue along a slow, disjointed, and ad hoc path.

A new United States agency with a sole information focus would benefit the United States during peacetime. The agency could engage in persistent strategic messaging to reassure allies and counter and deter potential adversaries. During peacetime, the thrust of the agencies' work would promote human rights, international law, and the benefits of the rules-based international order. A critical United States strength lies in its ability to assemble broad coalitions of allies, nations, and partners who value freedom and human rights. Consistent messaging promoting a citizen-centric, free and open order would help to reassure like-minded nations of a shared commitment to similar interests and values.[137] The agency could use similar messaging against adversaries that test those interests and values. Information preceding, accompanying, and following any conflict could build allied support, isolate the adversary informationally, and undermine any potential military response. Likewise, the agency's messaging should seek to undermine the adversary's state functions and, at a minimum, disseminate the truth, if not a pro-United States narrative of any ensuing conflict.

From a military standpoint, the agency would work in lockstep with the Department of Defense to develop a strategy that drives information operations, integrating the actions from the individuals who implement policy down to the individual combat soldier.[138] Integration helps ensure that the military's tactical actions are aligned with the strategic communication efforts of the United States Government. Similarly, understanding the information landscape relative to potential adversaries is vital to determine potential actions across the range of military operations, including information operations. With no informational focal point, the United

States Government rarely thinks of information as an end in itself, even though the information environment affects everyone daily. Engaged leadership could articulate the effects of information operations that often contribute to slow, ponderous, and inconsistent action. Indeed, the lack of focused leadership that understands how military action influences the information space contributes to the military's narrow employment of information-related activities.

The military's current conception of information-related activity is primarily limited to tactical information operations carried out during hostilities. However, new information technology offers potential for the military to achieve broader objectives using a more efficient and less-lethal method during peacetime or hostilities—information-based deterrence. Information-based deterrence means manipulating the risk-calculus of a potential adversary to prevent him from attacking in the first place. Deterrence in this regard intends to sow doubt in the adversary's mind about the likely outcome of his aggression. Doubt is accomplished by turning international opinion against the potential adversary or altering his perception of the relative strength of military forces.

A critical United States strength is its ability to assemble broad coalitions against potential adversaries, severing them from external material and moral support. Building and maintaining these coalitions requires that international opinion perceives an adversary as an aggressor acting inconsistently with international law or human rights. The military could help foster international opinion by establishing a rapid-reaction information force to capture adversary preparations or attacks on video. The video or imagery could reveal aggressive intent, counter suggested adversarial pretexts for aggression, and catalyze international opinion to support a United States-led coalition to confront the adversary. This rapid-reaction information force could respond to short-warning attacks, providing hard physical evidence to foster

international opinion and opposition against the aggressor. In the modern, hyper-connected information environment, international opinion—and even the possibility of negative international opinion—has proven a deciding factor motivating the actions or inaction of national leaders. In Crimea, the United States could have taken a more proactive approach using these methods.

Undeniable evidence—video or imagery—captured early in the conflict documenting Russian forces on the ground in Crimea could have blocked or countered Russian efforts to obfuscate or conceal its operations in Crimea. Further, another good defense against false information is accounts from those with experience fighting or with first-hand knowledge of the realities of the situation on the ground. Undeniable visual proof, including recorded accounts from people with first-hand knowledge, quickly promulgated by the United States Government, could have swayed international opinion and increased Russia's cost-benefit analysis regarding its continued actions in Crimea.

However, it is implausible for the military to wield international norms and standards against adversaries through information-based deterrence without a United States Government information strategy. Military planners would find it difficult to articulate why its forces should take a specific action, when it should occur, and what problem it solves if the action is not nested underneath an overall strategic (informational) concept. Likewise, it is implausible for the United States Government to develop an effective information strategy without a dedicated information agency.

Conclusion

In modern conflict, virtually all activities depend on information technology. In the more obvious way, orders are no longer sent by a horse and rider, they are sent through satellite broadcasts and fiberoptic cables. Navigation and positioning are no longer accomplished through maps and a compass but via terrestrial satellites. Moreover, winning or losing a conflict is no longer accomplished solely through overwhelming firepower or the correct application of fire and maneuver. It is accomplished through persuasion via information targeting each opponents' populations' will. The realities of the modern information environment should compel the United States Government to broaden how it employs information as an element of national power. Consequently, as a good first step, the United States should re-establish an agency to lead the information domain.

Russia and other state and non-state actors increasingly exploit the modern information environment, undermining United States national and global security interests. This activity poses sufficient concern to merit a coordinated government response. However, the United States response will require careful navigation that draws upon the principles underlying the concept of freedom of information and transcends the difficulties presented by any imposition of transborder information flow restrictions. Consequently, careful navigation of these principles and pitfalls demands an agency wholly dedicated to the information domain.

As noted in the 2018 National Defense Strategy, "we cannot expect success fighting tomorrow's conflicts with yesterday's weapons or equipment."[139] The United States military must adopt different approaches and seek innovative solutions to effectively leverage modern information technology and the hyper-connected reality of the twenty-first century to deter potential adversaries and win future conflicts. Similarly, the United States Government must modernize its information strategy and concepts. As was lacking in Crimea, an excellent first

step is a unified, integrated, and renewed United States response to informational threats to deter adversaries and reassure allies and partners.

[1] U.S. Joint Chiefs of Staff, Joint Concept for Operating in the Information Environment (JCOIE), Washington, D.C., 23.
[2] Ventre, Daniel. *Information Warfare*. 2nd ed. London, England, 2016, 8.
[3] William R. Gery and Se Young Lee. *Information Warfare in an information Age*. JFQ 85, 2nd Quarter 2017, 29.
[4] Ibid, 28.
[5] U.S. Joint Chiefs of Staff, Joint Concept for Operating in the Information Environment (JCOIE), Washington, D.C., 23.
[6] Ventre, Daniel. *Information Warfare*. 2nd ed. London, England, 2016, 8.
[7] Carpenter, Michael, and Olga Oliker. *Russian Influence and Unconventional Warfare Operations in the "Gray Zone": Lessons from Ukraine* (2017). http://www.fdsys.gov/ , 2.
[8] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." ARIS. Fort Bragg, NC: United States Army Special Operations Command, 2015, 51.
[9] Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1498.html. Also available in print form, 33.
[10] *"Analysis of Russia's Information Campaign against Ukraine."* NATO Strategic Communications Center of Excellence. Riga, Lithuania, 2015, 6.
[11] Keir Giles, '*The Next Phase in Russian Information Warfare'*, NATO Strategic Communications Centre of Excellence, November 2015, 2.
[12] Kofman, Michael, *Lessons from Russia's Operations in Crimea and Eastern Ukraine,* RAND Corporation, 11.
[13] William R. Gery and Se Young Lee. *Information Warfare in an information Age*, 23.
[14] U.S. Joint Chiefs of Staff, Joint Concept for Operating in the Information Environment (JCOIE), 23.
[15] Ventre, Daniel. *Information Warfare*, 8.
[16] Keir Giles, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, Chatham House, March 2016, https://www.chathamhouse.org/publication/russias-new-tools-confronting-west , 6.
[17] *"Analysis of Russia's Information Campaign against Ukraine."* NATO Strategic Communications Center of Excellence*,* 5.
[18] Kofman, Michael, *Lessons from Russia's Operations in Crimea and Eastern Ukraine,* 33.
[19] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 17-18.
[20] *"Analysis of Russia's Information Campaign against Ukraine."* NATO Strategic Communications Center of Excellence, 4.
[21] Carpenter, Michael, and Olga Oliker. *Russian Influence and Unconventional Warfare Operations in the "Gray Zone": Lessons from Ukraine* (2017). http://www.fdsys.gov/ , 9.
[22] General Joe Votel, Commander US SOCOM, 'SOF Operations In The Gray Zone', presentation at NATO Special Operations Headquarters, 10 September 2015.
[23] Kofman, Michael, *Lessons from Russia's Operations in Crimea and Eastern Ukraine,* RAND Corporation, 2.
[24] Keir Giles, '*The Next Phase in Russian Information Warfare'*, NATO Strategic Communications Centre of Excellence, November 2015, 4.
[25] Kofman, Michael, *Lessons from Russia's Operations in Crimea and Eastern Ukraine,* RAND Corporation, 32.
[26] Military Doctrine of the Russian Federation', approved 26 December 2014, https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf
[27] Ibid.
[28] Ibid.
[29] Unwala, Azhar and Ghori, Shaheen (2015) "Brandishing the Cybered Bear: Information War and the Russia Ukraine Conflict," Military Cyber Affairs: Vol. 1: Iss. 1, Article 7, 2. Available at: https://scholarcommons.usf.edu/mca/vol1/iss1/7
[30] Keir Giles, '*The Next Phase in Russian Information Warfare'*, NATO Strategic Communications Centre of Excellence Warfare, 24.
[31] Maria Snegoyava, *'Russia Report 1: Putin's Information Warfare in Ukraine'*, Institute for the Study of War, Washington, DC, 9. Available at www.understandingwar.org8
[32] Keir Giles, '*The Next Phase in Russian Information Warfare'*, NATO Strategic Communications Centre of Excellence, 3.
[33] Keir Giles, *Handbook of Russian Information Warfare*. Rome, Italy: NATO Defense College "NDC Fellowship Monograph Series", 2016, 4. Available at https://bdex.eb.mil.br/jspui/bitstream/123456789/4262/1/2016_Handbook,%20Russian%20Information%20Warfare.pdf
[34] Keir Giles, *Handbook of Russian Information Warfare*. NATO Defense College, 10.
[35] Ibid
[36] *"Analysis of Russia's Information Campaign against Ukraine."* NATO Strategic Communications Center of Excellence, 4.
[37] Carpenter, Michael, and Olga Oliker. *Russian Influence and Unconventional Warfare Operations in the "Gray Zone": Lessons from Ukraine, 8.*
[38] Warner, M. "A Century of Convergence: Technology, Ideology, and U.S. National Security." *Journal of Information Warfare*, vol. 15, no. 2, 2016, 2. *JSTOR*, www.jstor.org/stable/26487533
[39] Ventre, Daniel. *Information Warfare*. 2nd ed. London, England, 2016, 2.
[40] U.S. Joint Chiefs of Staff, DoD Dictionary of Military and Associated Terms, Washington, D.C., last updated January 2021, p. 104.

[41] Schwille, Michael, Anthony Atler, Jonathan Welch, Christopher Paul, and Richard C. Baffa, *Intelligence Support for Operations in the Information Environment: Dividing Roles and Responsibilities Between Intelligence and Information Professionals*. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR3161.html Also available in print form.
[42] U.S. Joint Chiefs of Staff, Joint Concept for Operating in the Information Environment (JCOIE), 35.
[43] U.S. Joint Chiefs of Staff, DoD Dictionary of Military and Associated Terms, Washington, D.C., last updated January 2021, p. 104; Schwille, Michael, Anthony Atler, Jonathan Welch, Christopher Paul, and Richard C. Baffa, *Intelligence Support for Operations in the Information Environment: Dividing Roles and Responsibilities Between Intelligence and Information Professionals*. Santa Monica, CA: RAND Corporation, 2020.
[44] Hammes, Thomas. "Technology Convergence Is Changing Warfare," Journal of Asymmetric Warfare 3, 3, no. 1 (May 2018), 6.
[45] Keir Giles, *Handbook of Russian Information Warfare*. NATO Defense College, 17.
[46] Ibid, 13.
[47] U.S. Joint Chiefs of Staff, Joint Publication 3-13.1: Information Operations. Washington, D.C., I-4.
[48] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 15.
[49] Maria Snegoyava, *'Russia Report 1: Putin's Information Warfare in Ukraine'*, Institute for the Study of War, 7.
[50] JAW, 43
[51] Margarita Levin Jaitner. Russian Information Warfare: Lessons from Ukraine, 88.
[52] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 34.
[53] V. Putin, "Солдат есть звание высокое и почетное" ('Soldier' is an honorable and respected rank), excerpts from annual Address to the Federal Assembly of the Russian Federation, Krasnaya zvezda, May 11, 2006, http://old.redstar.ru/2006/05/11_05/1_01.html.
[54] Keir Giles, *Handbook of Russian Information Warfare*. NATO Defense College, 10.
[55] V. Kvachkov, Спецназ России (Russia's Special Purpose Forces), Voyennaya Literatura, 2004, http://militera.lib.ru/science/kvachkov_vv/index.html Vladimir Kvachkov is a former GRU officer, whose "theory of special operations," including information operations, has reportedly been adopted as the basis for Russian military instructional and training materials.
[56] Keir Giles, '*The Next Phase in Russian Information Warfare'*, NATO Strategic Communications Centre of Excellence, 4.
[57] Darczewska, Jolanta, *The Anatomy of Russian Information Warfare: the Crimean Operation, a Case Study.* OSW Point of View Number 42, May 2014, 14.
[58] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 16.
[59] Ibid.
[60] Darczewska, Jolanta, *The Anatomy of Russian Information Warfare: the Crimean Operation, a Case Study*, 16.
[61] Panarin, *Information Warfare and Communications, 25*
[62] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 16.
[63] Darczewska, Jolanta, *The Anatomy of Russian Information Warfare: the Crimean Operation, a Case Study*, 16.
[64] Ibid.
[65] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 16.
[66] Darczewska, Jolanta, *The Anatomy of Russian Information Warfare: the Crimean Operation, a Case Study,* 70.
[67] *"Analysis of Russia's Information Campaign against Ukraine."* NATO Strategic Communications Center of Excellence, 18.
[68] Ibid, 26.
[69] Ibid, 27.
[70] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 17.
[71] Michael Carpenter, Russian Influence and UW testimony, 2
[72] V. Gerasimov, "По опыту Сирии" (Based on the experience of Syria), Voyenno-promyshlennyy kur'er, 9 March 2016, http://vpk-news.ru/sites/default/files/pdf/VPK_09_624.pdf (accessed 22 June 2016).
[73] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 18.
[74] Mark Galeotti, "The 'Gerasimov Doctrine' And Russian Non-Linear War," July 6, 2014, Https://Inmoscowsshadows.Wordpress.Com/2014/07/06/The-Gerasimov-Doctrine-And-Russian-Non-Linear-War/
[75] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 22.
[76] Maria Snegoyava, *'Russia Report 1: Putin's Information Warfare in Ukraine'*, Institute for the Study of War, 7.
[77] C. Blandy, Provocation, Deception, Entrapment: The Russo-Georgian Five Day War, Defense Academy of the United Kingdom, March 2009, http://conflictstudies.org.uk/files/04.pdf (accessed 23 June 2016).

[78] Christopher M. Andrew and Vasili Mitrokhin, The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB (New York: Basic Books, 1999), 9–17.
[79] Keir Giles, *Handbook of Russian Information Warfare*. NATO Defense College, 20.
[80] Keir Giles, '*The Next Phase in Russian Information Warfare'*, NATO Strategic Communications Centre of Excellence, 6.
[81] "*Russian New Warfare.*" Journal of Asymmetric Warfare, vol. 2, no. 1. Johns Hopkins Applied Physics Laboratory, Fort Mead, MD, 29.
[82] Ibid, 30. Also see Russian News Agency "Western Powers Regret Not Building NATO Naval Base in Crimea." November 28, 2018, https://tass.com/world/1033267
[83] Sergey Lavrov: Throwing Russia off balance is ultimate aim. September 10, 2014. https://tass.com/top-officials/748935
[84] The speech in English can be found at the following URL: http://eng.kremlin.ru/news/6889
[85] Maria Snegoyava, *'Russia Report 1: Putin's Information Warfare in Ukraine'*, Institute for the Study of War, 9.
[86] *"Analysis of Russia's Information Campaign against Ukraine."* NATO Strategic Communications Center of Excellence, 35.
[87] "*Russian New Warfare.*" Journal of Asymmetric Warfare, vol. 2, no. 1, 4-13.
[88] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 19.
[89] Maria Snegoyava, *'Russia Report 1: Putin's Information Warfare in Ukraine'*, Institute for the Study of War, 15.
[90] Keir Giles, '*The Next Phase in Russian Information Warfare'*, NATO Strategic Communications Centre of Excellence 12.
[91] *"Analysis of Russia's Information Campaign against Ukraine."* NATO Strategic Communications Center of Excellence 35.
[92] Unwala, Azhar and Ghori, Shaheen (2015) "Brandishing the Cybered Bear: Information War and the Russia Ukraine Conflict," Military Cyber Affairs, 6.
[93] Keir Giles, '*The Next Phase in Russian Information Warfare'*, NATO Strategic Communications Centre of Excellence 12.
[94] Ibid.
[95] Unwala, Azhar and Ghori, Shaheen (2015) "Brandishing the Cybered Bear: Information War and the Russia Ukraine Conflict," Military Cyber Affairs, 6.
[96] T.S. Allen and A.J. Moore. Victory without Casualties: Russia's Information Operations, 64
[97] Maria Snegoyava, *'Russia Report 1: Putin's Information Warfare in Ukraine'*, Institute for the Study of War, 7
[98] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 43.
[99] Olga Oliker. *Russian Influence and Unconventional Warfare Operations in the "Gray Zone": Lessons from Ukraine*, 4.
[100] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 7.
[101] Olga Oliker. *Russian Influence and Unconventional Warfare Operations in the "Gray Zone": Lessons from Ukraine*, 4
[102] "*Russian New Warfare.*" Journal of Asymmetric Warfare, vol. 2, no. 1, 4-13.
[103] Ibid.
[104] Carpenter, Michael, and Olga Oliker. *Russian Influence and Unconventional Warfare Operations in the "Gray Zone": Lessons from Ukraine*, 4.
[105] Ibid, 5.
[106] *"Analysis of Russia's Information Campaign against Ukraine."* NATO Strategic Communications Center of Excellence, 26.
[107] T.S. Allen and A.J. Moore. Victory without Casualties: Russia's Information Operations, 63
[108] A. V. Bedritsky, ["Realization of the Concepts of Information Warfare by the Military Political Leadership of the USA during the Modern Era"], RISI, 2007.
[109] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 50.
[110] Ibid, 15.
[111] T.S. Allen and A.J. Moore. *Victory without Casualties: Russia's Information Operations*, 65
[112] "*Russian New Warfare.*" Journal of Asymmetric Warfare, vol. 2, no. 1, 30.
[113] Ibid.
[114] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 74.
[115] Ibid, 47.
[116] Olga Oliker. *Russian Influence and Unconventional Warfare Operations in the "Gray Zone": Lessons from Ukraine* (2017). http://www.fdsys.gov/ , 2.
[117] *"'Little Green Men': A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*." United States Army Special Operations Command, 43.
[118] Wortzel, Larry. *The Chinese People's Liberation Army and Information Warfare*, 37
[119] Keir Giles. Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power, 58.
[120] https://www.scribd.com/document/112346692/Fact-Sheet-The-United-States-Information-Agency
[121] The United States Information Agency - A Commemoration, http://dosfan.lib.uic.edu/usia/abtusia/commins.pdf
[122] William R. Gery and Se Young Lee. *Information Warfare in an information Age.* JFQ 85, 2nd Quarter 2017, 29.
[123] Keir Giles, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, 94.
[124] Ibid.
[125] "Hybrid threats: perceptions and responses", International Institute for Strategic Studies, January 2015, 67.

[126] Ibid.
[127] Prier, Jared. *Commanding the Trend: Social Media as Information Warfare*, 51.
[128] Ibid, 52.
[129] "*Russian New Warfare.*" Journal of Asymmetric Warfare, vol. 2, no. 1, 47.

[130] Benjamin Jensen and Nathan Packard, *"The Next National Defense Strategy"*. War on the Rocks, November 30, 2020. https://warontherocks.com/2020/11/the-next-national-defense-strategy/
[131] William R. Gery and Se Young Lee. Information Warfare in an information Age. JFQ 85, 2nd Quarter 2017, 28.
[132] Richard M. Crowell, *War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare* (Newport, RI: U.S. Naval War College, 2010).
[133] *Report of the Defense Science Board Task Force on Strategic Communication* (Washington, DC: Department of Defense, January 2008), available at www.acq.osd.mil/dsb/reports/ADA476331.pdf
[134] Ibid.
[135] U.S. Department of State Under Secretary for Public Diplomacy and Public Affairs, *Our Mission* (accessed May 1st, 2021). Found at https://www.state.gov/about-us-under-secretary-for-public-diplomacy-and-public-affairs/
[136] Ibid.
[137] The White House. *United States Strategic Approach to the People's Republic of China*. Washington, DC, 2017, 1.
[138] William R. Gery and Se Young Lee. Information Warfare in an information Age. JFQ 85, 2nd Quarter 2017, 25.
[139] U.S. Department of Defense, 2018 National Defense Strategy of the United States of America, Washington, D.C., January 2021, P. 22.