2022-12

TEXTS, TWEETS, AND TACTICAL STRIKES: RUSSIAN INFORMATION WARFARE METHODS AND IMPLICATIONS FOR THE UNITED STATES AND NATO

Chesley, Brendan J.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

TEXTS, TWEETS, AND TACTICAL STRIKES: RUSSIAN INFORMATION WARFARE METHODS AND IMPLICATIONS FOR THE UNITED STATES AND NATO

by

Brendan J. Chesley

December 2022

Thesis Advisor: Scott E. Jasper
Second Reader: Ryan Maness

THIS PAGE INTENTIONALLY LEFT BLANK

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

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the 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 Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
TEXTS, TWEETS, AND TACTICAL STRIKES: RUSSIAN INFORMATION WARFARE METHODS AND IMPLICATIONS FOR THE UNITED STATES AND NATO

5. FUNDING NUMBERS

6. AUTHOR(S) Brendan J. Chesley

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

The character of warfare is constantly evolving, beset by friction, and clouded with relentless ambiguity. This study explores the rapidly changing operational environment through a focused analysis of the Kremlin's military adventurism in Georgia, Syria, and Ukraine. This recently escalated conflict, encompassing the largest front on the European Continent unseen since the Second World War, provides valuable insights into the complexity of warfare's changing character. Specifically, the Kremlin's evolving approach to Information Warfare reveals a proliferation of new technologies and means that seek to contest the information domain, maximize uncertainty, and paralyze the decision-making ability of their adversaries. This thesis addresses the following questions: 1) What new technological capabilities has the Kremlin employed to create psychological effects and disrupt decision-making at tactical and operational levels? 2) How effective are these methods, and how do they fit within a broader concept of Information Warfare? In addressing these questions, this research will trace the Kremlin's post-2008 reforms and determine what enduring aspects of Russian Information Warfare (namely cyber, unmanned systems, and EMSO) tell us about the current operational environment. Finally, this research demonstrates how these observed methods may shape the future battlespace, and what wider tactical and operational implications these threats pose to the U.S. and her strategic partners.

14. SUBJECT TERMS
Russia, cyber, cyber strategy, information warfare, IW, information dominance, information operations, IO, operations in the information environment, OIE, information superiority, information domain, psychological operations, PSYOP, contested information environment, electronic warfare, EW, military deception, MILDEC, C4I

15. NUMBER OF PAGES
99

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

TEXTS, TWEETS, AND TACTICAL STRIKES: RUSSIAN INFORMATION WARFARE METHODS AND IMPLICATIONS FOR THE UNITED STATES AND NATO

Brendan J. Chesley
Major, United States Marine Corps
BA, Western Michigan University, 2010

Submitted in partial fulfillment of the
requirements for the degrees of

**MASTER OF ARTS IN SECURITY STUDIES
(EUROPE AND EURASIA)**

and

MASTER OF SCIENCE IN INFORMATION STRATEGY AND POLITICAL WARFARE

from the

**NAVAL POSTGRADUATE SCHOOL
December 2022**

Approved by: Scott E. Jasper
Advisor

Ryan Maness
Second Reader

Carter Malkasian
Chair, Department of Defense Analysis

Afshon P. Ostovar
Associate Chair for Research
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The character of warfare is constantly evolving, beset by friction, and clouded with relentless ambiguity. This study explores the rapidly changing operational environment through a focused analysis of the Kremlin's military adventurism in Georgia, Syria, and Ukraine. This recently escalated conflict, encompassing the largest front on the European Continent unseen since the Second World War, provides valuable insights into the complexity of warfare's changing character. Specifically, the Kremlin's evolving approach to Information Warfare reveals a proliferation of new technologies and means that seek to contest the information domain, maximize uncertainty, and paralyze the decision-making ability of their adversaries. This thesis addresses the following questions: 1) What new technological capabilities has the Kremlin employed to create psychological effects and disrupt decision-making at tactical and operational levels? 2) How effective are these methods, and how do they fit within a broader concept of Information Warfare? In addressing these questions, this research will trace the Kremlin's post-2008 reforms and determine what enduring aspects of Russian Information Warfare (namely cyber, unmanned systems, and EMSO) tell us about the current operational environment. Finally, this research demonstrates how these observed methods may shape the future battlespace, and what wider tactical and operational implications these threats pose to the U.S. and her strategic partners.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

A2/AD	Anti-Access / Area Denial
AWACS	Airborne Early Warning and Control System
BTG	Battalion Tactical Group
C2	Command and Control
C4	Command, Control, Communications, and Computers
DOD	U.S. Department of Defense
EABO	Expeditionary Advance Base Operations
ELINT	Electronics Intelligence
EMCON	Emissions Control
EMSO	Electromagnetic Spectrum Operations
EW	Electronic Warfare
GPS	Global Positioning System
GSM	Ground Station Mobile
HALE	High Altitude Long Endurance
HF	High Frequency
IE	Information Environment
IO	Information Operations
ISR	Command, Control, Communications, and Computers
IW	Information Warfare
JADC2	Joint, All-Domain, Command and Control
JSTAR	Joint Surveillance Target Attack Radar System
LEO	Low Earth Orbit
LOS	Line of Sight
MALE	Medium-Altitude Long Endurance
MILDEC	Military Deception
MoD	Russian Ministry of Defense
NATO	North Atlantic Treaty Organization

OIE	Operations in the Information Environment
OPSEC	Operational Security
PSYOPS	Psychological Operations
RF	Radio Frequency
RMA	Revolution in Military Affairs
SEAD	Suppression of Enemy Air Defenses
SIGINT	Signals Intelligence
SMS	Short Message Service
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Combat Aerial System
USSR	Union of Soviet Socialist Republics

EXECUTIVE SUMMARY

This thesis seeks to address the following questions: 1) what enduring methods and technological capabilities have the Russian military developed to disrupt decision-making at the tactical and operational levels? and 2) How effective are these methods, and how do they fit within a broader framework of Russian Information Warfare methodology?

This study explores the rapidly changing operational environment through a focused analysis on the Kremlin's military adventurism in Georgia, Syria, and now Ukraine. This recently escalated conflict, encompassing the largest front on the European Continent unseen since the Second World War, provides valuable insights into the complexity of warfare's changing character. Specifically, their evolving approach to maneuver reveals a proliferation of new technologies and methods that seek to contest the information domain, maximize uncertainty, and paralyze the decision-making ability of their adversaries.

Peer/near peer adversaries (i.e., Russia) who cannot compete symmetrically will use various, disruptive means to gain a relative advantage vis-à-vis the U.S./NATO. These methods can be encapsulated as follows: battlefield sensors, electronic warfare, and malign influence via cyberspace.

Recent wargames and training scenarios indicate not only the West's over-dependence on advanced C4ISR (command, control, communications, and computers intelligence, surveillance, and reconnaissance), navigation aids, and information networked capabilities but also dangerous assumptions regarding information dominance and technological overmatch. The low-intensity, counterinsurgency wars of the previous two decades have not adequately prepared the West for these pursuits against a peer adversary. We can no longer assume the next fight will occur in the permissive environments to which we have grown accustomed. Accordingly, the more we understand these threats now, the better the U.S., her allies, and strategic partners will cope in this environment in a potential future engagement.

This study proposes the following recommendations:

1. Senior leaders must continue to reexamine, revise, and modify our doctrine, equipment, training, and perhaps even notions of command culture if we are to maintain our technological and competitive edge in the information environment.

2. Commanders must continue to reinforce training that emphasizes sustained combat operations and maneuver in highly contested, command and control (C2) degraded operational environments.

3. Commanders must also assume future operational environments will be saturated with sensor platforms and unmanned systems, rendering not only maneuver, but tactical cover and concealment extremely difficult.

4. Commanders must continue to reinforce training down to the small unit level that emphasizes personal data protection and resiliency to enemy disinformation. The West must prepare for an adversary that will leverage cyberspace for malign influence campaigns directly targeting our servicemembers, their families, and military cohesion itself.

5. Scholarly research of the topics presented herein indisputably warrant further exploration and study as this war will likely rage into spring 2023. The Russo-Ukrainian War offers ample opportunity to not only examine the effects of Russian IW methodology at the tactical and operational levels, but also their implications to the larger phenomenon of war itself.

ACKNOWLEDGMENTS

I am extremely grateful for the countless hours of support I have received from fellow officers, faculty, and NPS staff in not only the development of this thesis, but the pursuit of my academic endeavors at this institution. First and foremost, I wish to thank my advisor Dr. Scott Jasper, along with faculty Dr. Anne Clunan, and Dr. Kalev Sepp—a trio of "OG Cold Warriors," scholars, and great Americans that offered both guidance and inspiration for this work. To my co-advisor Dr. Ryan Maness and Ms. Rebecca Lorentz, for not only your support within the Defense Analysis Department, but the adventures we shared abroad: "We'll always have Tbilisi." To my writing coach Dr. Cheryldee Huddleston, thank you for your steadfast encouragement throughout this process. LTC William D. Swenson—a quality of mentor and human being that one rarely encounters in a career, your friendship and guidance during COVID purgatory was invaluable. I am especially indebted to my former bosses, LtCol Rob Featherstone and Colonel Marc Walker, for your continued mentorship and keeping me honest throughout the years, without which I probably wouldn't even be here. And finally, to my loving wife—this may not be a dissertation, but I now possess a semblance of understanding what you endured as a doctoral student. You continue to inspire me to be better, and without your love and support this would not have been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Since antiquity, the nature of warfare is characteristic of an extremely chaotic, fast paced, and rapidly changing environment, beset by friction and clouded with relentless ambiguity and uncertainty. Clausewitz's famously attributed theory of the "fog of war" endures among the most pervasive concepts in discussions on warfare in the modern era, constantly evolving and affecting a commander's decision cycle transcending the strategic to tactical levels of conflict.[1] The Kremlin's highly innovative information warfare methods witnessed during the Russo-Georgian War in 2008, followed by the annexation of Crimea in 2014, and leading up to the invasion of Ukraine in February 2022 indicate the proliferation of new technologies and methods that seek to contest the information domain, maximize uncertainty, and paralyze their adversaries' decision-making ability.[2]

This thesis seeks to address the following questions: 1.) What methods and new technological capabilities has the Russian military developed and employed to create psychological effects and disrupt decision-making at tactical and operational levels? 2.) How effective are these methods, and how do they fit within a Russian doctrine or concept of Information Warfare? In addressing these questions, this thesis will trace the Russian military's post-2008 reforms, and determine what enduring aspects of Russian information warfare, observed in the aforementioned conflicts tell us about the current contested information domain. Finally, this research seeks to uncover how these observed methods may shape the future battlespace.

A. SIGNIFICANCE OF THE RESEARCH QUESTION

Russian attempts to manipulate the information domain to deceive adversaries is certainly not a new concept, having mastered the techniques of *maskirovka* against the German Wehrmacht during the Great Patriotic War of the 20th Century, and further

[1] Carl von Clausewitz, *On War*, Michael E. Howard and Peter Paret, eds. (Princeton, NJ: Princeton University Press, 1976), 120.

[2] Mason Clark, "Russian Hybrid Warfare," *Institute for the Study of War* (September 2020), 18–19; Keir Giles, *Handbook of Russian Information Warfare*, (Rome: NATO Defense College, 2016), 22.

developed by the KGB and Soviet military intelligence apparatus during the Cold War.[3] In recent decades, from the invasion of Georgia in 2008, to disruptions in Estonia and other western NATO allies, and the most recent "Special Military Operation" into Ukraine, the Kremlin has sought to employ more methodical and adept approaches to information warfare. These aggressive acts demonstrate how information warfare, via multiple forms can successfully obfuscate enemy intent, exploit fault lines in adversaries' populations, and leverage technology (via cyber, unmanned systems, and electronic warfare) to achieve effects at the strategic, operational, and tactical levels of conflict.

Irrespective of the level of target, Russian information warfare methods seek to disrupt the decision space of both military and political leadership. New forms of Russian psychological warfare coined "pinpoint propaganda" observed in eastern Ukraine since 2014 employ a close combination of unmanned aerial systems (UAS), kinetic fires, and electronic signature detection. This is demonstrated through such tactics as SMS text message barrages sent to front line troops, with intent to disrupt cohesion and undermine morale at the micro level, often implicating the loved ones and families of Ukrainian soldiers on the ground.[4] Significant changes have been made to the Russian military's task organization of field units, with both unmanned aerial systems and EW capabilities now an organic component of maneuver at the battalion and company levels. Their usage substantiate the former commander of USSOCOM's reference to Syrian battlegrounds as "the most aggressive EW environment on the planet," indicative of what NATO and the West may face in a future conflict.[5] Furthermore, Colonel Liam Collins, former director of the Modern War Institute at West Point had proffered a sobering assessment of Russian

[3] David Glantz, "The Red Mask: The Nature and Legacy of Soviet Military Deception in the Second World War," *Intelligence and National Security* 2, no. 3 (1987).

[4] Raphael Satter and Dmytro Vlasov. "Ukraine Soldiers Bombarded by 'Pinpoint Propaganda' Texts," *The Associated Press*, 11 May 2017, https://apnews.com/article/russia-kiev-ukraine-only-on-ap-archive; Duncan McCrory, "Russian Electronic Warfare, Cyber and Information Operations in Ukraine," *The RUSI Journal* 165, no. 7 (Winter 2021): 36.

[5] Colin Clark, "Russia Widens EW War, 'Disabling' AC-130s in Syria," *Breaking Defense*, 24 April 2018, https://breakingdefense.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/

electronic warfare (EW) capabilities in early 2020, questioning the West's ability to contend with a peer adversary in a similar, contested information space.[6]

Recent wargames and large scale training exercises indicate not only the U.S. military's over-dependence on advanced C4ISR and networked capabilities, but severe shortcomings in our own assumptions regarding pursuit of 'information dominance.'[7] A "corrosive over-response" approach to a politically fraught public opinion and social media, identified in a recent Congressional report as a "critical vulnerability" exposes the force to nefarious information operations conducted by foreign actors.[8] A recent article in *Proceedings* further illustrates this point in a fictitious (but likely) scenario in which a highly effective U.S. Naval commander is promptly removed from a combat operation due to a fabricated social media smear campaign exposing his email account.[9] Many experts and military leaders have suggested that Moscow is far ahead of the United States in terms of its information warfare capabilities, finding new and innovative ways to exploit not only cultural vulnerabilities but expose major weaknesses and paralyze command structures of their adversaries in a near-peer fight.

The low intensity, counterinsurgency wars of the previous two decades has not adequately prepared the U.S. for information dominance against a peer threat. We can no longer assume the next fight will occur in the permissive environments that we have grown accustomed. The better we understand these threats now, the more prepared the U.S., its allies, and strategic partners will be in a future engagement. Our leaders must reexamine, revise, and modify our doctrine, equipment, and training if we hope to maintain our competitive edge in the information domain.

---

[6] "A Conversation with COL Liam Collins," *Fletcher Security Review*, March 2020, https://www.fletchersecurity.org/post/a-conversation-with-col-liam-collins

[7] Tara Copp, "'It Failed Miserably': After Wargaming Loss, Joint Chiefs are Overhauling How the U.S. Military Will Fight," 26 July 2021, *Defense One*, https://www.defenseone.com/policy/2021/07/it-failed-miserably-after-wargaming-loss-joint-chiefs-are-overhauling-how-us-military-will-fight/184050/

[8] U.S Congress, "A Report on the Fighting Culture of the United States Navy Surface Fleet." Conducted at the Direction of Senator Tom Cotton, Congressmen Jim Banks, Dan Crenshaw, and Mike Gallagher. 12 July 2021.

[9] Don Gomez, "Canceled in Combat: Get Ready for Smear War," *Proceedings* 147, no. 6 (June 2021).

B. LITERATURE REVIEW

An entire body of scholarly research on the Kremlin's theoretical approach, methodology, and employment of information warfare emerged as early as 2007, in response to the wave of Russian cyberattacks on Estonia. Sensationalized and often exaggerated hyperbole has inundated the mainstream and media discussion, providing commentary from the 2008 Russo-Georgian War to the current Ukraine crisis and beyond. This is further complicated by the volumes of intense scholarly debate producing a myriad of definitions, analysis, and terminology seeking to compartmentalize and explain in isolation not only Russian IW methods, but Western interpretations of the post-Cold War Russian understanding of conflict in the new century.

Given the rapid development of new capabilities following the post-2008 reforms within the Russian Armed forces, underscored by their recent military adventurism in Syria and Ukraine, a scholarly analysis of hybrid, grey zone, and political warfare models emerged.[10] A major shift in intellectual discourse among Russian political and military elites has transpired in recent years, which led Western experts to attribute a model of Hybrid Warfare to a speech (and later article) penned by the Russian Chief of General Staff Valery Gerasimov in February 2013. In his article, titled "The Value of Science is in Foresight," General Gerasimov explains the gravity of recent Color Revolutions (such as the Arab Spring and others), and provides possible solutions to combat threats posed by "foreign propaganda and subversion."[11] Western theorists soon took hold and attributed his comments to what was later termed, (and eventually debunked) to a model of hybrid warfare known as "Gerasimov Doctrine."[12] Western theorists quickly seized upon Gerasimov's comments as what many claimed to be a "holy grail" explaining "anything and everything about Russia's mix and use of hard and soft power."[13] Despite these

[10] Philip Kapusta, "The Grey Zone," *Special Warfare* 28, no. 4, (October 2015).

[11] As quoted in: Roger McDermott, "Does Russia Have a Gerasimov Doctrine?" *Parameters* 4, no, 1 (Spring 2016), 98–9.

[12] Mark Geleotti, "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/

[13] McDermott, 99.

criticisms, the lethality and effectiveness in the application of the methods outlined in these analyses cannot be understated.

Oscar Jonsson seeks to navigate through the nebulous of interpretations and provide a conclusive answer to the question of whether a shift of strategic thinking and understanding of conflict within the Russian military has occurred, and *how*. Through a detailed examination of Russian primary source documentation and comparative analysis of both western and Russian scholarly writing, he concludes that the Kremlin's understanding of war has indeed changed significantly. This shift having been brought on through advances in communications technology and the emergence of populist movements (such as the Arab Spring and later Color Revolutions) since the mid-2000s. His findings indicate the Kremlin's conclusion is that the most effective way to wage contemporary war is through political and information warfare vis-a-vis the strategic level.[14]

What Jonsson also ascertains in fact is the Kremlin's explicit acknowledgement of the increased role of information and information technology in achieving decisive effects in both peace and war. As Jonsson highlights, "information" is mentioned countless times throughout official Russian military doctrines and publications released since 2000. The Kremlin seeks to bridge the gap in its lack of comparative advantage in conventional military capabilities with asymmetrical advantages in IW, viewing it as not strictly a military concept, but a constant ongoing activity "blurring the lines between war and peace."[15] As such, information warfare, and the existential threat posed by political revolutions abroad is reflected (and arguably, guiding) their geo-political grand strategy since 2007. The effectiveness and lethality of their methods was shown to the world during the seizure and annexation of Crimea in 2014.

Cyber warfare, cyberstrategy, and its variants thereof have been part of the U.S. military operational lexicon since the 2008 Russo-Georgian War. Yet, the vast majority of

[14] Oscar Jonsson, *The Russian Understanding of War: Blurring the Lines Between War and Peace*, (Washington: Georgetown University Press, 2019), 4.

[15] Jonsson, 7.

contemporary scholarly research is focused on Russian information warfare the strategic level. As such, Western scholars widely agree that cyber strategies function as political warfare, complementing more traditional forms of statecraft and national power as but one facet or tool within an overarching grand strategy. Foremost among experts on Russian security issues, Mark Galeotti frames Russian information operations in their sphere of influence (namely Georgia, Estonia and now Ukraine) as not hybrid warfare, but a form of political warfare he calls "guerrilla geopolitics" which seeks to leverage their opponent's weaknesses against their relative asymmetries in the information domain.[16]

Continuing this analysis of Russian information warfare through a geo-political strategic lens, Maness, Valeriano, and Jensen emphasize the Kremlin's cyber operations as a strategic level weapon used for political warfare and coercion, subordinate to more conventional forms of national power (diplomatic, economic, military, etc). Despite ranking sixth in global cyber capacity, Russia is labeled the second most dangerous and aggressive state actor in cyberspace.[17] Viewed within this context of grand strategy, the authors illustrate how the Kremlin employs these cyber methods to shape adversaries' decision-making at the strategic level, arguing that "the goal of Russian cyber operations appears to reside in sowing discontent and chaos in targeted populations in rival states as a means of pressuring decision makers and bolstering larger propaganda efforts."[18] Again, the authors place emphasis of Russian IW methods as effective in shaping decisions and creating effects in the *strategic* realm, and not necessarily immediate tactical or operational gains in the battlespace.

With regard to Russian cyber strategy, Maness, Valeriano and Jensen focus on the 2016 U.S. election hack and ancillary propaganda efforts in Ukraine, to frame and illustrate their argument that Russia's aggression in cyberspace are consistent with their overarching goal to undermine democracy and meddle in the internal affairs and political processes of

[16] Mark Gaelotti. "Hybrid, Ambiguous, and Non-Linear? How New is Russia's New Way of War?" *Small Wars and Insurgencies* 27, no. 2 (2016), 283.

[17] Brandon Valeriano, Benjamin Jensen and Ryan Maness, Cyber Strategy: The Evolving Character of Power and Coercion, (Cambridge: Oxford University Press, 2018), 110.

[18] Maness et al., 111.

neighboring states, (their "near abroad.") This is conducted through weaving methods of cyber disruption, espionage, and degradation into their diplomatic and propaganda efforts.[19] The authors describe these actions as akin to a modern form of coercive diplomacy, "operating more in the ambiguous world of spies and saboteurs than the open battlefield."[20]

In examining Russian Information Warfare at the lower level of conflict, Dr. Scott Jasper (senior lecturer at Naval Postgraduate School) provides context as how the Kremlin leverages cyber and information warfare to create effects that can bridge the strategic and operational levels. He examines the 2007 cyber-attacks in Estonia and the 2008 invasion of Georgia and how these effects can be achieved in the physical domain in combination with kinetic action. Although the Russian objectives for its military incursion into South Ossetia were geo-political in nature, Dr. Jasper illustrates how this conflict is unique within the scope of cyber and information warfare in that that the military invasion was accompanied by a large-scale IO campaign (via cyber disruption), with attacks against government and public facing websites conducted as ancillary measures to influence public opinion. These actions were also designed to not only cause confusion within the Georgian government and populace but promulgate the Russian version of events reported in the news media by regional and global outlets in an attempt to isolate the event from the West.[21] The effectiveness of their efforts have become subject of heavy scrutiny and debate over the last few years. However, this tactic has been employed via multiple means and channels in not just the media, but the physical and logical layers of cyber and telecommunications infrastructure since 2008.

Despite the voluminously high degree of scholarly research available, there is a concerning lack of meaningful, in-depth study on Russian IW methods and their effects at the operational and tactical levels. Nevertheless, a significant amount of data and research conducted on this topic is documented in official government and North Atlantic Treaty

[19] Maness et al., 110; 12–13.

[20] Maness et al., 7.

[21] Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. (Washington: Georgetown University Press, 2020), 36.

Organization (NATO) publications, RAND, and MITRE Corp think tank studies. Additionally, the excellent writings and observations of General Ben Hodges, Roger McDermott, the publications from the Army University Press and the Foreign Military Studies Office aboard Ft. Leavenworth, and the Modern War Institute at West Point proved extremely helpful in both inspiring this research and scoping this topic.

One study in particular, a piece by David Hollis, a senior policy analyst for the Undersecretary of Defense for Intelligence is noteworthy as it was among the early scholarly examinations conducted on Russian cyber warfare. It was widely circulated within the U.S. information warfare community and served as the author's early inspiration for this research.[22] Additionally, it signaled a renewed focus on a Revolution in Military Affairs (RMA) and near-peer threats during a time when the U.S. military was engaged in counterinsurgency fights in Iraq and Afghanistan. Although a great deal of insight on Russian cyber, electronic, and information warfare capabilities remains at the classified level and cannot be explored here in great detail, the author was able to glean an adequate amount of open-source data from European news outlets, peer reviewed scholarly studies, and unclassified reports to support the claims presented herein.

C. POTENTIAL EXPLANATIONS AND HYPOTHESIS

I hypothesize that Russian IW methods observed in Georgia, Syria, and Ukraine are indicative of a revolutionary change in how war will be conducted in the coming years. The Kremlin's exploitation of social media and use of new technological means to disseminate and distort information is changing the character of warfare down to the tactical level. There is no question that the U.S. had enjoyed unparalleled information dominance in the conventional battlespace since the end of the Cold War. However, the annexation of Crimea in 2014, and the ongoing Ukraine crisis indicate that the Russian military possess a competitive edge in this realm, with effective asymmetric capabilities in IW achieving deadly effects in the battlespace. Unless we fully understand, learn from, and adapt to these methods, the U.S. may not be ready to confront this threat in a future fight.

[22] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, (January 2011).

Knowing full well the disparity it possessed in its own conventional means, the Russian military sought to bridge the gap and compensate through investing in IW and battlespace networked capabilities after 2008. Although their approach to the information domain is not necessarily a new or revolutionary strategy, and despite their early failures in the 2022 invasion, the Russian military skillfully adopted and integrated new IW technologies in their approach to tactical maneuver. Observations indicate they are highly adept, efficient, and ruthless in meeting challenges in the digital terrain of the new century. Experts agree these methods were decisive and pivotal to their 2014 successes in Ukraine, in which they employed a diverse array of simplistic but also sophisticated methods to achieve cognitive and psychological effects. It is clear that the Russian military achieves these battlespace effects via leveraging three methods: informational, cyber, and electronic warfare. Furthermore, their ability to create effects by converging methods of kinetic and IW into a comprehensive "fires package" indicates a new delivery method of IW and psychological effects at the tactical level, of which U.S. and its allies may not be adequately prepared to counter.

I hypothesize that future great power competition will undoubtedly involve a high degree of information warfare, with conflicts perhaps even *decided* in the information domain. My research has indicated that the West may be dangerously behind peer adversaries in current IW technology and capabilities, and may have difficulty coping in a multi-domain fight in the future battlespace. A detailed and careful analysis of Russian IW methodology in these aforementioned conflicts offers a glimpse into what the future operating environment may look like, providing some lessons learned for how the U.S. and NATO can prepare for success in the contested information environment of the 21st Century.

D. RESEARCH DESIGN

I have used comparative case studies to illustrate the effect of Russian IW methods in Georgia, Syria, and the ongoing Ukraine crisis. I have selected these conflicts due to the depth, relevant nature, and amount of scholarly research available (having been conducted within the previous 5–10 years). In order to provide an appropriate context of Russian IW

methodology it is necessary for the author to consider the current U.S. and NATO doctrinal definitions of IW, and contrast with its Russian counterparts. I will then explore the major components of Russian IW (informational, cyber, and electromagnetic spectrum) and how they converge in the newly interconnected battlespace to create effects and disrupt the decision-making processes of their adversaries. Furthermore, I will closely examine the post-2008 "New Look" Reforms, and its impact on the Russian military's subsequent performance in these case studies (having largely occurred in the past 14 years) to include Syria, and post-2014 Ukraine, respectively. These analyses will therefore not be made in isolation, as these factors have a similar impact on trends and observations of current capabilities. While due consideration of China is necessary as a premier threat in the information domain, some concepts regarding PLA capabilities are addressed, however my research is primarily focused on Russian military capabilities.

Additionally, the scope of this thesis will not extend outside of the aforementioned conflicts. At the time of this writing, the three-pronged Russian military offensive that began in earnest on 23 February 2022 has largely failed to achieve its primary objectives; to include capturing the Ukrainian capital of Kyiv, removal of President Volodymyr Zelenskyy, and installation of a pro-Kremlin regime.[23] Early reports of their abysmal battlefield performance merely weeks into this campaign came as shocking surprise to many. Expecting a showcase of its newly acquired, widely flaunted battlefield tech, experts were dismayed not only at the underutilization of these resources at the outset of the invasion, but the systematic failures and ineptitude of the Kremlin's supposed, newly re-armed and revitalized "military powerhouse." Exact casualty numbers at the time of this writing remain unclear, but conservative estimates of Russian military combat losses are upwards of 50,000 killed in action.[24] It is evident that the Kremlin severely underestimated the resolve, vigor, and tenacity of the Ukrainian resistance –as did the West.

[23] Amos C. Fox, "Reflections on Russia's 2022 Invasion of Ukraine: Combined Arms Warfare, the Battalion Tactical Group, and Wars in a Fishbowl," *Association of the United States Army Institute of Land Warfare*, Land Warfare Paper No. 149, (September 2022), 1.

[24] "Total Combat Losses of the Enemy from 24.02 to 01.10," Ministry of Defense of Ukraine, Official website, accessed 1 October 2022, https://www.mil.gov.ua/en/news/2022/10/01/the-total-combat-losses-of-the-enemy-from-24-02-to-01-10/

Nearly a full year into the campaign, the Russian military continues to sustain heavy losses. This includes ceding their digital "information war" to the Ukrainians, leaving experts reeling from their post-Crimea "Little Green Men" appraisals on Russian capabilities that have since proved wildly inaccurate, which has astounded analysts, government policymakers and military experts alike.[25] My research into Russian military capabilities began prior to February 2022, and the exact reasons for the Kremlin's initial failures and disastrous miscalculations may remain unclear for some time. Although the Russian military may not have proved to be the "ten foot tall" beast that experts warned, we are remiss to over-correct these assessments and dismiss their performance and capabilities at this stage.[26] A conflict of this magnitude has not been seen since the end of the Second World War. Accordingly, we must not make premature conclusions and fall victim to "mirror imaging" in our assessments of the Russian military in a nearly eight-year conflict with seemingly no end in sight.[27] The Russians have not fought the war we expected them to, nor did they even follow their own military doctrine. As such, a full exploration into their failures within the scope of the 2022 invasion is not the purpose of this study. As the current phase of the Russo-Ukrainian War rages into its eleventh month, a full assessment at the time of this research is not possible, and therefore a complete picture will likely remain unclear until the cessation of hostilities is complete, and operational security measures of both sides are relaxed.[28] Lastly, while further escalation into a full spectrum, kinetic conflict between NATO and Russia remains highly unlikely, this thesis will focus on the more likely and wider-ranging potential scenarios short of full-scale conflict.

[25] Rob Johnson, "Dysfunctional Warfare: The Russian Invasion of Ukraine," *Parameters* 52, no. 2 (Summer 2022): 5–20.

[26] Jack Watling, "Just How Tall are Russian Soldiers?" *The RUSI Journal* 24, (March 2022).

[27] Zachary Shore, "Mirror Imaging: Thinking the Other Side Thinks Like Us," in *Blunder: Why Smart People Make Bad Decisions*. (New York, NY: Bloomsbury, 2008), 161.

[28] Roger N. McDermott, *Russia's Path to the High-Tech Battlespace*, (Washington, DC: The Jamestown Foundation, 2022), xiii.

THIS PAGE INTENTIONALLY LEFT BLANK

II. RUSSIAN MILITARY MODERNIZATION AND THE NEWLY INTERCONNECTED BATTLESPACE

The proliferation of unmanned systems, sensor platforms, and an increasingly contested information environment (IE) are dramatically reshaping the battlegrounds of the 21st Century. The military employment of Unmanned Aerial Systems (UAS) technology has not simply proliferated; it is now an integral aspect of conflict across the globe. The previous five years alone witnessed sweeping technological progress in drone technology by U.S. adversaries. Specifically, the Kremlin has invested significantly in development of UAS technology since 2009, boasting a fleet of over 1,800 of these systems since 2012.[29] These weapons are employed with tactical ingenuity, operational art, and increased lethality across a wide spectrum of applications, and the Kremlin's shrewd research, development, and fielding of these systems is but one aspect of this wider dilemma of information warfare in the battlespace that the West must confront.

The U.S. military's employment of UAS technology proved a revolutionary, asymmetric tool used throughout the two decades of counterinsurgency wars in Iraq and Afghanistan. The military advantages to employing UAS boasts a wide spectrum of capabilities in the delivery of standoff munitions, not to mention a highly cost effective and efficient way to strike targets and saturate the battlespace with sensors. However, in Syria, and now the current Ukraine conflict, drones are proving to be ever more capable, ubiquitous, and conventional force multipliers for belligerents on both sides of conflict. It can be further argued that in Ukraine, these systems have made the most impact on any conflict in recent years; as one need not look further than daily news reports. From a TB-2 Bayraktar's role in sinking the Russian flagship Moskva in the Black Sea, to their prominence in Ukrainian information operations campaigns, and even a patriotic song commemorating the Turkish drone's battlefield utility, the war in Ukraine provides us a glimpse into how battlefield sensor platforms and information networked capabilities are

[29] McDermott, *Russia's Path to the High-Tech Battlespace*, 385.

reshaping conflict.[30] Since 2014, their widespread use has showcased this capability, and provided ample opportunity to study the strengths and limitations of these systems in a kinetic environment. And perhaps this conflict will show that whether the side who possesses the tactical edge with these systems, will prove the victor.

Although not traditionally defined within the lexicon of Information Warfare, Unmanned Aerial Systems (or "drones") are, by nature "information dependent weapons." Therefore, for the purposes of this study it is fitting to explore the Kremlin's employment of these systems not only within the context of their Information Warfare methodology, but how they are expanding the information environment itself.[31] Zachary Kellenborn, a researcher and author of several publications on lethal autonomous weapon systems, further argues that UAS systems and their employment *must* be considered within an overarching framework and holistic understanding of information warfare. As such, a widely agreed definition of information warfare is "strategy for the use and management of information to pursue a competitive advantage."[32] As evident throughout the Syria and Ukraine conflicts, the Russian military has converged multiple aspects of IW with the employment these weapons, namely electronic warfare, cyber, and psychological warfare to produce lethal effects and achieve tactical advantage in both fires and maneuver.

This chapter seeks to explore the Russian military's employment of UAS systems within the context of Information Warfare. In the following pages I will first briefly discuss how and why the Russian military reforms following the 2008 Russo-Georgian War brought about major procurements, developments and investments in unmanned systems and information networked capabilities. I will then explore how Russia employs combinations of these weapons to achieve asymmetric advantages with both kinetic and psychological effects on their adversaries at the tactical level. Additionally, I will

[30] David Hambling, "Ukraine's Bayraktar Drone Helped Sink Russian Flagship," *Forbes*, 14 April 2022. https://www.forbes.com/sites/davidhambling/2022/04/14/ukraines-bayraktar-drones-helped-destroy-russian-flagship/?sh=580993c03a7a

[31] Zachary Kallenborn, "InfoSwarms: Drone Swarms and Information Warfare," *Parameters* 2, no. 52 (Summer 2022): 87–8.

[32] Catherine A. Theohary, *Defense Primer: Information Operations*, Report No. IF10771 (Washington, DC: Congressional Research Service, December 2020); as referenced in Kallenborn, "InfoSwarms," 89.

demonstrate how the Russian military had effectively employed combinations of UAS systems with cyber, Electronic Warfare (EW), and Information Operations (IO) into a comprehensive "fires package" in Syria and Ukraine. I will then trace their development of networked capabilities over the past two decades, providing a glimpse as to what the future battlespace may look like, with unmanned systems in both the kinetic and information domain. Finally, I will examine how these developments highlight some critical vulnerabilities that, if exploited, can potentially prove a significant asymmetric advantage over U.S. and NATO in a potential near-peer conflict.

A. BACKGROUND: AN ARMY IN TRANSITION

The Russian Armed Forces quickly applied tactical lessons learned following their combat losses during the 2008 Russo-Georgian War, initiating the most sweeping modernization of its military in decades. These reforms focused on several key areas, but greatest consideration was given to far-reaching structural changes and technological developments, noting their relative disadvantages in Command, Control, Communications, Computers, (C4) and Intelligence Surveillance, and Reconnaissance (ISR) capabilities.[33] These reforms resulted in major investments to modernize its equipment and battlefield tech, with the overarching goal of increasing its military effectiveness, ability to share information amongst systems, and project power within its near periphery and beyond.[34]

In the wake of the 2008 Russo-Georgian War, the Kremlin conducted a sobering self-assessment to fully understand its relative materiel and technological weakness compared to U.S. and NATO.[35] Instead of attempting to "catch up" with the West, Moscow invested in specific "key enablers" that seek to asymmetrically challenge a technologically superior foe, such as electronic warfare and unmanned systems.[36] These developments on

[33] Timothy L. Thomas, "The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia." *Journal of Slavic Military Studies* 22, no. 1 (2009): 33.

[34] Andrew S. Bowen, *Russian Armed Forces: Military Modernization and Reforms*, CRS Report No. IF11603 (Washington, DC: Congressional Research Service, 2020), 1.

[35] Roger N. McDermott, *Russia's Path to the High-Tech Battlespace*, (Washington, DC: The Jamestown Foundation, 2022), xiv.

[36] Samuel Bendett, et. al., "Advanced Military Technology in Russia: Capabilities and Implications," Research Paper, Chatham House, (September 2021): 8.

full display in Syria and Ukraine, illustrate the lethality of future battlefields, featuring technological advances in sensor-shooter loops and denial actions in the electromagnetic spectrum that are fundamentally changing the battlespace dynamic, transcending multiple domains of warfare.[37]

1. Early Reforms and Soviet Relics

To fully understand Russia's development of unmanned systems we must first examine the incentive behind the sweeping reforms to come. The Russian military that annexed the Crimean Peninsula in 2014, intervened in Syria the following year, and subsequently crossed into sovereign Ukrainian territory in 2022 was nearly unrecognizable from the Cold War relic inherited by Vladimir Putin in December 1999.[38] Following the collapse of the former Soviet Union, and further exacerbated by the tumultuous Yeltsin era, the Russian military remained in a sad state of disrepair.[39] Continuing into the mid-2000s, the formerly proud Red Army had languished to a state of willful neglect resembling a hollowed-out shadow of its former self. A series of failed reforms, beginning in 1997, highlighted many systemic problems that existed for decades, to include rampant corruption, command structural issues, conscription woes, and scores of outdated weapons and equipment desperately requiring refit and modernization. Between 1988 and 1994 alone, its personnel had been reduced by four million, and endured a decimated budget that shrank to its lowest point in history, sinking from $246B in 1988 to $14B in 1994.[40] Accordingly, the Russian military of the 1990s through mid-2000s was merely deployed primarily within its own borders, such as in the Chechen Wars, or used for quelling small ethnic conflicts in its near periphery. But when the nuclear submarine *Kursk* sank to the

[37] Also known as "Kill Webs," a detailed concept prominent throughout Christian Brose's monograph, *The Kill Chain: Defending America in the Future of High-Tech Warfare,* (New York: The Hachette Group, 2020).

[38] Kier Giles, "Assessing Russia's Reorganized and Rearmed Military," Task Force White Paper, The Carnegie Endowment for International Peace, 3 May 2017.

[39] Bettina Renz, *Russia's Military Revival*. (Cambridge, UK: Polity Press, 2018), 52–3.

[40] Dmitri Trenin, "The Revival of the Russian Military: How Moscow Reloaded." *Foreign Affairs* 95, no. 3, (Spring 2016): 23.

bottom of the Barents Sea in August of 2000, the time had come for desperately needed change.[41]

The high-tech weapons performance on full display during Operation Desert Storm, followed by NATO's intervention in Serbia almost a decade later caused the Russian military leadership to conduct a series of internal reviews of its doctrine and equipment, marking what Alexei Arbatov called a "watershed in Russia's assessment of its own military requirements and defense priorities."[42] If the recently installed Prime Minister Vladimir Putin and his regime had any designs for the return of his country's former prestige as a great power competitor, a stronger and more capable military was paramount amongst priorities. However, it would not be until the lackluster (some say disastrous) performance of the Russian military in the 2008 Russo-Georgian War, that ultimately served as a catalyst for the most ambitious reform planning in decades.[43]

B. SERDYUKOV, SLIPCHENKO, AND 2009's "NEW LOOK"

Despite achieving a decisive victory in the five-day conflict in 2008, and even having underwent a series of previous reforms prior to that (1997 and 2003, respectively) the Russian military still remained in rough shape. The Russo-Georgian War was renowned as the first "high tech" conflict, as it featured the employment of cyberattacks in conjunction with a ground campaign.[44] But a closer examination reveals a vastly different story, found in damning assessments by their own state media, and concluding that their military was "uncontrollable and inadequate for conducting even local wars like the one in Georgia."[45] The campaign in South Ossetia was marred by incidents of fratricide, consistent failures in command-and-control structures that slowed its advance, a lack of

[41] Paul K. Baev, "The Trajectory of the Russian Military: Downsizing, Degeneration, and Defeat," in *The Russian Military: Power and Policy*, ed. Steven E. Miller and Dmitri Trenin (Cambridge: The MIT Press, 2004), 44.

[42] Renz, 60.

[43] Gregory P. Lannon, "Russia's New Look Army Reforms and Russian Foreign Policy," *The Journal of Slavic Military Studies* 24, no. 1 (Winter 2011): 34.

[44] John Arquilla, *Bitskrieg: The New Challenge of Cyberwarfare*, (Cambridge: Polity Press, 2021) 5, 6–7.

[45] Lannon, 35.

modern, precision guided munitions, poor air support, no UAVs, and dismal communications systems that often resulted in field commanders having to resort to use of personal cell phones.[46] This led to many in government and media clamoring for Defense Minister Anatoly Serdyukov's resignation. However, he stayed on until 2012, undertaking his military's most sweeping and ambitious transformations to date, having announced his plan in late fall 2008 under the auspices of newly elected President Medvedev.[47]

The publicly stated goals of the 2009 "New Look" reforms were multifaceted, focusing on several key areas. It sought to instill higher levels of universal combat readiness, facilitated through a dramatic drawdown and reshuffling of personnel. This aimed to completely restructure the Soviet era stove-piped four-tiered command structure into multiple consolidated, combined brigade combat teams (BCTs). The move was intended to create lighter, highly mobile, networked, and autonomous expeditionary combat teams better postured for the new century, as opposed to the bloated, military district driven, mass mobilization unit model considered a relic of the Cold War.[48] Moreover, Medvedev and Serdyukov sought to reduce its bloated officer corps, improve the quality of life standards for their troops, and transition away from a conscript army beset by corruption and terrible hazing practices to an all-volunteer force.[49] Currently, Serdyukov's vision of ending conscription awaits full realization, with conscripts filling a high percentage of the ranks deployed in the invasion of Ukraine that began late February 2022.[50]

Although not publicly acknowledged, New Look's highest urgency (and underlying driver for change) was predicated upon the desperately needed modernization of

[46] McDermott et al., *The Russian Armed Forces in Transition,* 9–10.

[47] Kathryn Stoner, *Russia Resurrected: Its Power and Purpose in a New Global Order*, (New York: Oxford University Press, 2021): 184–5.

[48] Stoner, *Russia Resurrected*, 184.

[49] Gil Bardollar, "The Best of Both Worlds? Russia's Mixed Military Manpower System," Center for Strategic & International Studies, 23 September 2020. https://www.csis.org/blogs/post-soviet-post/best-or-worst-both-worlds

[50] Suzanne B. Freeman and Katherine Kjellstrom Elgin, "What the Use of Russian Conscripts Tells Us About the War in Ukraine," *Politico Europe,* 17 March 2022. https://www.politico.eu/article/what-the-use-of-russia-conscripts-tells-us-about-the-war-in-ukraine/

Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) systems, underscoring their relative disadvantages in the Russo-Georgian War. Development of 'network centric' warfare capabilities was the driving force behind Serdyukov's reforms, says Russian military expert Roger McDermott.[51] Paramount amongst these goals was replacing the endless stores of outdated weapons and legacy equipment that former defense minister Pavel Grachev once described as "ruins and debris,"[52] The proceeding sections will discuss key areas in which the Russian military rapidly developed since 2009; their unmanned systems and C4ISR capabilities.

C. MERGING OLD WITH THE NEW: THE RECONNAISSANCE FIRES COMPLEX

Due to the rather dismal performance of their command-and-control apparatus during the Five-Day War, the Russian Ministry of Defense (MoD) initiated specific reforms to overhaul their C4ISR capabilities as early as 2009.[53] Accompanying these reforms was the introduction, employment, and fielding of several variants of unmanned aerial systems (UASs). Early UAS prototypes were first developed in the Soviet military in the 1950s, but this technology was never fully integrated into the forces until several years after the Russo-Georgian War.[54] These systems were eventually fielded with the purpose of coupling ISR with ground-based fires, demonstrating this lethal combination at the outset of the war in Eastern Ukraine beginning February 2014. During the early years of this conflict, the Russian military began effectively weaving UAV employment with kinetic fires and rocket artillery in a highly efficient, mutually supporting manner. A close study of this particular theatre reveals a well-documented, comprehensive illustration of Russian UAS capability development over the course of an extended, eight-year period, and its deadly effects in terms of sensor-shooter loops and target acquisition. Furthermore, the concurrent Syrian operation was essentially a testing ground for their new tech, and by

[51] Roger McDermott, "Russia's Perspectives on Network Centric Warfare: The Key Aim of Serdyukov's Reform," (Ft. Leavenworth, KS: Foreign Military Studies Office, 2011) 3–4.

[52] Stoner, 183; Giles, "Assessing Russia's Reorganized and Rearmed Military," 2–3.

[53] Bettina Renz, *Russia's Military Revival*. (Cambridge, UK: Polity Press, 2018), 81.

[54] Grau and Bartles, *The Russian Way of War*, 152.

2015, the Russian military was running 24-hour UAV operations continuously in Syria, becoming acutely aware of the necessity for integration of this capability into daily operations.[55]

It is a well-known adage of industrial age warfare regarding artillery's rightfully claimed status as the "King of Battle." This prominence in their doctrine is due to its destructive, kinetic power on enemy formations, and also the profound psychological impact for those unfortunate to find themselves on the receiving end of massed, indirect fires.[56] The employment of artillery during the First World War not only permanently scarred the European landscape, but forever altered the way modern wars were fought. History saw these concepts of fire and maneuver evolved into the combined arms tactics perfected on the Eastern Front between Soviet Russia and Nazi Germany. Accordingly, a Soviet era emphasis on massed fires, its preeminence and high regard of artillery (within Russian military tradition going back to the Tsarist era) ultimately achieved premier status as its own maneuver element, establishing its place throughout virtually every echelon of the Russian Ground Forces today.[57] In Ukraine and Syria, the Russian Ground forces perfected their aerial surveillance and target acquisition techniques, and have fully integrated their UAVs capabilities with ground-based artillery and electronic warfare.

1. UAS Development And Fires Integration

Among the most remarkable (and unique) features of the early stages of the Ukraine war was not simply Russia's extensive use of UAS themselves, but their versatility in integrating these ISR assets with indirect artillery, providing devastatingly lethal effects on their Ukrainian adversaries.[58] The Russian approach to UAVs in Ukraine is a significant

[55] Bendett et al., "Advanced Military Technology in Russia," 52.

[56] Liam Collins and Harrison Morgan, "King of Battle: Russia Breaks Out the Big Guns," *Army,* (February 2019): 45–6.

[57] Lester Grau and Bartles, *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces* (Ft. Leavenworth, KS: Foreign Military Studies Office, 2016), 260; Isabelle Facon, "Proliferated Drones: A Perspective on Russia," *The Center for A New American Security,* Accessed 1 April 2022. <http://drones.cnas.org/reports/a-perspective-on-russia/>

[58] Lester Grau and Chuck Bartles, "Integration of Unmanned Aerial Systems Within Russian Artillery," *Fires Bulletin: A Joint Publication for U.S. Artillery Professionals*, (July-August 2016): 31–8.

departure from the employment methods of their Western counterparts, as U.S./NATO UAS doctrine is centered around much larger, far more advanced standoff armed platforms, possessing long range reconnaissance or strike missions flown at high altitudes.[59] At the time of this writing, the Kremlin is still in the process of developing and procuring these more advanced capabilities.

By 2018 however, the number of UAS possessed by the Russian military was estimated between 500 and 1000.[60] During both Syrian and Ukraine conflicts, the MoD widely emphasized the use of smaller tactical platforms, mainly for the purpose of spotting and target acquisition for their artillery batteries. Although the Russian military still lags behind the West in terms of its UAS capabilities, they are quickly catching up. As of the ZAPAD exercise in Fall 2021, sources indicated a far larger fleet of Russian UAS systems and continued to test and develop combat strike capability from these newly developed and procured platforms.[61]

Despite their shortcomings in technology regarding long range, heavier UAV platforms, the Russian Ground Forces displayed great ingenuity in developing a Soviet era doctrine formerly known as the Reconnaissance Strike-Fire Complex (RUK/ROK). This concept was designed to link fires targeting, intelligence data, and the ground fires' battery Fire Direction Center (FDC), to coordinate and enable engagement of kinetic targets in the battlespace.[62] Among the earliest references of RUK/ROK was in a 1987 publication by Russian Lieutenant General V.G Reznichenko, noting that such a system should have the ability to "engage targets in near real time, and have four components, among them: an automated guidance system, a mobile ground control center, high precision weapons; and

[59] Joint Chiefs of Staff, *Joint Air Operations*, JP 3-30 (Washington, DC: Joint Chiefs of Staff, 2021), Ch III, 30–34.

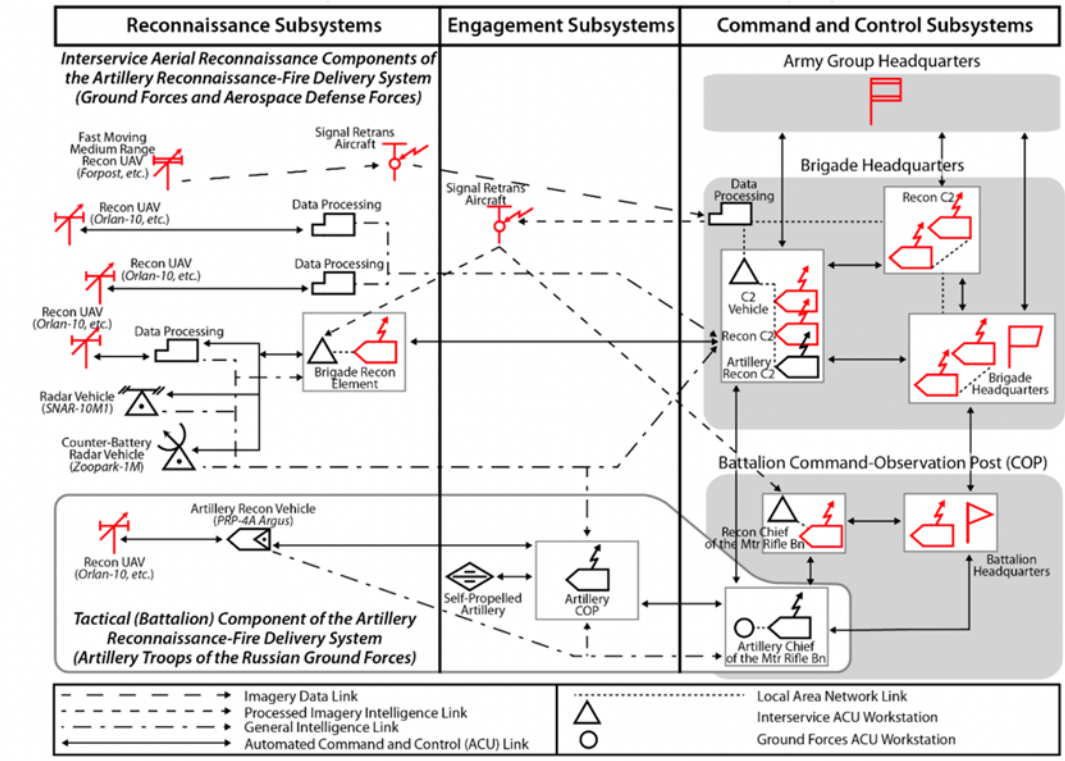
[60] Facon, "Proliferated Drones."

[61] Roger McDermott, "Russia's Armed Forces Enhance UAV Strike Capability," *The Eurasia Daily Monitor* 18, no. 148 (Fall 2021); Mark Episkopos, "Zapad: Russia Wants to be Ready for a War with NATO," *The National Interest*, 21 September 2021, <https://nationalinterest.org/blog/buzz/zapad-russia-wants-be-ready-war-nato-193859>

[62] Lester Grau and Charles Bartles, "The Russian Reconnaissance Fire Complex Comes of Age," *Oxford University Changing Character of War Centre*, (May 2018).

a system for the precise determination of the location of system components."[63] This concept can be compared to similar concepts in U.S./NATO lexicon as "Network Centric Warfare."

Figure 1. Russian Artillery Reconnaissance Fire Delivery System [64]



The RUK/ROK eventually evolved into *Razvedyvatelno-Ognevaya Sistema*, or the Reconnaissance Fire System (ROS) depicted in Figure 1 above. This concept was developed and tested throughout the Syrian conflict and is now fully integrated into their fires doctrine.[65] Russian capabilities in their Reconnaissance-Strike Concept in conjunction

[63] As translated from Russian language sources in Timothy Thomas, "Russian Electronic, Information, Navigation, and Reconnaissance-Strike and Fire Methods: Definitions and Use," A Report for the MITRE Corporation and the U.S. Army Futures and Concepts Center, (Nov 2020), 12–13.

[64] Source: Grau and Bartles, *The Russian Reconnaissance Fire Complex Comes of Age*, 13.

[65] Dmitry Adamsky, "Russian Lessons From the Syrian Operation and The Culture of Military Innovation," *George C. Marshall European Center for Security Studies, Security Insights* 47, (February 2020).

with UAVs was on full display during the early stages of the Ukraine crisis. One particular instance serves as a cold example of its lethality. Although Ukrainian forces has been spotting Russian UAVs since early that Spring, on 11 July 2014 at Zelenophillya, a combination of tube and rocket artillery unleashed upon a Ukrainian position killed over thirty troops and eliminated two of their battalions' combat capability within a matter of minutes.[66] Countless examples of these massed fires facilitated by "aerial spotter drones" characterized the fight in Donbas as "The Artillery War."[67] At the time of this writing, the campaign confined to Donbas had claimed the lives of over 14,000 people.[68] As the war escalated into full-fledged invasion in February 2022, it is estimated that Russian rocket and howitzer cannon fires is attributed to approximately 85% of the total Ukrainian casualties, eerily resembling siege warfare of the First World War.[69]

D. RUSSIAN UAS PLATFORMS: SYRIA AND UKRAINE

NATO classifies UAV systems into separate categories based on size and other attributes particular to its mission set or means of employment (altitude, range, etc.) These include the strategic level, High-Altitude Long Endurance (HALE) variants (Class I); the operational level, Medium Altitude Long Endurance (MALE) variants (Class II); and smaller, tactical variants (Class III).[70] Operational and tactical level UASs were most prevalent in Ukraine and Syria, and for the purposes of this study I primarily discuss the employment of systems in the two latter categories (Class II and III). The most prominent UAS in the Russian inventory (and most prevalent in Ukraine and Syria) is the Orlan-10,

[66] Amos C. Fox and Andrew J. Rossow, "Making Sense of Russian Hybrid Warfare: A Brief Assessment of the Russo-Ukrainian War," *Association of the United States Army Institute of Land Warfare*, Land Warfare Paper No. 112, (March 2017), 10.

[67] Grau and Bartles, 2016, 38.

[68] "Conflict in Ukraine's Donbas: A Visual Explainer," *The International Crisis Group,* Accessed 3 March 2022, https://www.crisisgroup.org/content/conflict-ukraines-donbas-visual-explainer

[69] Phillip A. Karber, "Lessons Learned from the Russo-Ukrainian War: Personal Observations," draft, Johns Hopkins Applied Physics Laboratory and U.S. Army Capabilities Center, (July 2015).

[70] "NATO UAS Classification Table," in *A Comprehensive Guide to Countering Unmanned Aircraft Systems*, (Kalkar, Germany: NATO Joint Air Power Competence Center, 2020), 510–11.

employed primarily for ISR and target acquisition in conjunction with indirect ground-based fires.[71]

The introduction of UAVs in Syria and the early Ukraine conflict (confined to in Donbas) has been a game changer for Russian ground forces, by carrying a multitude of payloads and combining effects of Information Operations (IO) with kinetic targeting. The Russians have weaved Electronic Warfare into their targeting methods since the early days of the conflicts, far increasing the lethality and effectiveness of their artillery strikes. One particular configuration observed in Ukraine (and later Syria) is the Russian "Leer-3" system, which employs a combination of ground-based EW sensor platforms and up to three UAVs to detect, jam, or suppress electronic signals (namely cell phones), exploiting geo-locational data from these signals to coordinate artillery or rocket fire. This "comprehensive fires package" has proven to have deadly effects in the kinetic and psychological realm.[72] This capability will be further explored in the proceeding chapter.

Experts widely agree that among the most notable aspects of the Ukraine conflict is the "ubiquitous presence of unmanned aerial vehicles," which increase the range and lethality of indirect and massed artillery fires.[73] The most remarkable aspect to note here, is not simply MoD's widespread introduction of UAVs into the battlespace, but this new and innovative approach of employing UAVs in conjunction with their relative strength in ground-based artillery; a tactic that was not widely observed prior to 2014.

Relative advantages in capability notwithstanding, one can conclude that the Russian Ground Forces have found in the UAV a solution that is a cheap, reliable alternative to manned aircraft. Employed thus far mainly for reconnaissance purposes, these systems enable rapid target acquisition (under 15 minutes), as well as provide them a highly effective capability for post-strike, immediate Battle Damage Assessments (BDA)

[71] Grau and Bartles, *The Russian Way of War*, 371.

[72] Duncan McCrory, "Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States," *The RUSI Journal* 165, no. 7, (Nov 2020): 88.

[73] Zoltán Őze, "Special Features of the Russian-Ukrainian Armed Conflict," *Hadmérnök* 15, no. 1, (May 2020), 214.

for fires adjustment.[74] Additionally, the use of long-range artillery in the Donbas region from 2014–15 is consistent with the hybrid nature of tactics pursued by the Russian military. Since their artillery systems can remain in their own territory, aggressive acts (such as indirect fires) remain ambiguous and possess a non-attributive nature and in keeping with their own version of the narrative as portrayed in Russian media outlets.[75]

Samuel Bendett, a subject matter expert on Russian military systems at the Center for Naval Analysis, argues that the Russian military's combat lessons and experiences in Syria "has been the single most defining experience for the MoD over the past 20 years… [with] the testing and use of [UAVs] beginning to redefine how the Russian military fights today and tomorrow."[76] The Russian experience in Syria led directly to major developments within their UAV fleet inventory, as well as structural changes within the MoD in shaping their future force. This includes the addition of UAV platoons at even lower echelons within their ground forces (UAV companies in direct support of artillery battalion formations) and expanding their present fleet from 40 total companies across their ground forces and navy.[77] Pre-2022 Russian training exercises, such as ZAPAD 2021 had emphasized the continued, omnipresent use and integration of UAVs throughout the ground forces for ISR, EW and fires correction.[78]

Since early 2017, the Russian MoD launched several joint initiatives with academia and civilian industry to expand and further develop its unmanned systems, to include loitering munitions, swarming, robotics, and artificial intelligence.[79] In April 2021 the

---

[74] Aaron F. Brantly, Nerea M. Cal, and Devil P. Winkelstein, "Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW," *The Army Cyber Institute at West Point*, (2017), 33.

[75] Frank Christian Sprengel, "Drones in Hybrid Warfare: Lessons From Current Battlefields," Hybrid CoE Working Paper, *The European Centre of Excellence for Countering Hybrid Threats,* (June 2021): 14.

[76] Samuel Bendett, "Russian Unmanned Vehicle Developments: Syria and Beyond," in *Improvisation and Adaptability in the Russian Military*, a report for the Center for Strategic and International Studies, (April 2020), 44.

[77] Bendett, "Russian Unmanned Vehicle Developments," 44–5.

[78] Bendett, 44; Mason Clark and George Barros, "Russia's Zapad-2021 Exercise," *Institute for the Study of War*, 17 September 2021, https://www.understandingwar.org/backgrounder/russia%E2%80%99s-zapad-2021-exercise

[79] Samuel Bendett, "Strength in Numbers: Russia and the Future of Drone Swarms," 20 April 2021, *Modern War Institute at West Point*, <https://mwi.usma.edu/strength-in-numbers-russia-and-the-future-of-drone-swarms/>

Russian MoD released footage of their new loitering munition UAV, the "Lancet-3" conducting strikes against stationary and moving targets in Syria.[80] These "kamikaze drones" are similar in size and capability to the Israeli systems used by Azeri forces against Armenian targets during the Nagorno Karabakh War in late 2020. In 2019, the SU-70 Okhotnik (Hunter-B) long range strike platform took its maiden flight.[81] And as of late 2021 the Kronshtadt Group has finally begun mass production of their MALE class "Orion" combat strike platform, which can provide long range, long duration capability with a variety of payloads and configurations such as EW, ISR, and guided munitions.[82] These late developments indicate the Kremlin's determination to quickly catch up to the West in unmanned systems capability.

The Kremlin announced in early 2021 that they would possess swarm capabilities for UAV performing missions in conjunction with manned aircraft by the end of that year.[83] However, despite state news reports about Russian swarming capability during the ZAPAD exercise in late 2021, this has yet to be seen in Ukraine. Although it is clear they still lag behind the U.S., China, Turkey, and Israel in UAV technology, their developments may indicate that Russia is soon catching up with the world's leading producers of unmanned technology. Nevertheless, of even greater concern is further proliferation of these technologies, and their ubiquity in contemporary conflict.[84]

1. Ukraine Developments: 2022 Campaign And Beyond

As Russia's recently intensified and expanded war in Ukraine reaches its tenth month, the long-held assumptions of Russian capabilities are now challenged as they

[80] Roger McDermott, "Russian UAV Technology and Loitering Munitions," *The Eurasia Daily Monitor* 18, no. 72, (May 2021)

[81] General John R. Allen, Gen. Ben Hodges, and Julian Lindley-French, *Future War and the Defense of Europe*, Oxford, UK: Oxford University Press, 2021, 119–20.

[82] Thomas Newdick, "Russia Provides a Glimpse of Its Orion Drone Executing Combat Trials in Syria," 22 February 2021, *The Drive*, https://www.thedrive.com/the-war-zone/39381/russia-provides-a-glimpse-of-its-orion-drone-executing-combat-trials-in-syria

[83] Bendett, "Strength in Numbers."

[84] Andrew Eversden, "A Warning to DOD: Russia Advances Quicker than Expected on AI, Battlefield Tech," 24 May 2021, *C4ISRNET*, <https://www.c4isrnet.com/artificial-intelligence/2021/05/24/a-warning-to-dod-russia-advances-quicker-than-expected-on-ai-battlefield-tech/

sustain heavy casualties in what many are predicating will be a long, ugly fight. The lack of the prominent employment of electronic warfare and unmanned systems at the outset of Russia's invasion puzzled experts, and warrants further study as this conflict develops.[85] At this point in the campaign it appears the state-media touted superiority of Russian UAS has not matched up with reality, as combat losses of the Orlan-10 system were estimated between 60–80 since February 2022.[86] However, as the Russian drone fleet began suffering major losses (coupled with a dwindling supply chain and heavily sanctioned defense industry), reports surfaced of the Kremlin's quick moves to procure Iranian systems in early summer 2022. These systems, first seen in Ukraine in early September 2022, include the Iranian Shahed 136 loitering munition (renamed the Geran-2), and Shahed 191 and 129 variants.[87] Unlike the majority of their Russian counterparts, Iranian systems possess strike capability, and are designed for standoff munitions payloads in pursuit of high value targets.[88] Although Iran has supplied these systems to other countries as well as proxy and insurgent groups in the past, this may demonstrate a concerning new trend signaling Iranian commitment and support to Russia's military aims in the region.

The previous 14 years of conflict in the aforementioned battlegrounds suggest that the U.S. and NATO will no longer have the luxury in assuming technological dominance in the increasingly contested information and sensor saturated battlespace of the 21st Century. Prior to February 2022, senior military experts had even predicted Moscow was outpacing the United States and her allies in terms of their information warfare capabilities, finding new and innovative ways to exploit not only asymmetrical vulnerabilities but expose major weaknesses and paralyze the command structures of their adversaries. It is clear that from these case studies that information networked capabilities and sensor

[85] Andrew Eversden and Jaspreet Gil, "Why Hasn't Russia used its Full Scope of Electronic Warfare?" 28 March 2022, *Breaking Defense*, <https://breakingdefense.com/2022/03/why-hasnt-russia-used-its-full-scope-of-electronic-warfare>

[86] Sine Ozkarasahin, "Can Iranian Drones Respond to Putin's Call for Help?" *Eurasia Daily Monitor* 19, no. 112 (July 2022).

[87] Laura Seligman, "Huge Problem: Iranian Drones Pose New Threat to Ukraine," *Politico*, 26 Sept 2022.

[88] Farzin Nadimi, "Iranian Drones to Russia: Capabilities and Limitations," *The Washington Institute for Near East Policy*, 1 August 2022. https://www.washingtoninstitute.org/policy-analysis/iranian-drones-russia-capabilities-and-limitations

platforms via UAS systems are key enablers of Russian information warfare. The following chapter will explore Russian capabilities in electronic warfare.

III. RUSSIAN ELECTROMAGNETIC SPECTRUM OPERATIONS

"We have lost the electromagnetic spectrum," relented Alan Shaffer, former Pentagon senior engineering and research chief in 2014.[89] This sentiment was again echoed three years later by LTG John Morrison, commander of the U.S. Army Cyber Center of Excellence, warning: "When it comes to electronic warfare, we are outgunned—we are plain outgunned by peer and near-peer competitors."[90] Statements like these have been repeated numerous times by senior defense leaders since 2014, when the Russian military began deployment of an impressive array of new systems in Syria and Eastern Ukraine, a direct result of the Kremlin's calculated efforts to expand and modernize its EW inventory as part of the 2009 New Look reforms. This was further evident as a major shift in their command organization structures and doctrine of their ground forces began to unfold, accompanied by the integration of organic EW elements down to the brigade level. This aspect of New Look was undertaken deliberately to counter what they observed as U.S./NATO's critical vulnerability: an overreliance and dependence on space-based, high bandwidth, continuous uninterrupted communications links, and unabated Western assumptions regarding pursuit of "information dominance."[91]

As noted in Chapter II, Russian EW is another area that some claim was grossly overestimated, even hyped by defense experts prior to February 2022.[92] General Ben Hodges, former commander of U.S. Army Europe, has since acknowledged their battlefield prowess has not matched up with earlier predictions, along with the EW capabilities once described as

[89] Sydney J. Freedberg Jr., "US Has Lost 'Dominance in Electromagnetic Spectrum': Shaffer," *Breaking Defense*, 3 September 2014, https://breakingdefense.com/2014/09/us-has-lost-dominance-in-electromagnetic-spectrum-shaffer/

[90] Mark Pomerleau, "US is 'outgunned' in electronic warfare, says cyber commander," *C4ISRNET*, 10 August 2017, https://www.c4isrnet.com/show-reporter/technet-augusta/2017/08/10/us-is-outgunned-in-electronic-warfare-says-cyber-commander/

[91] Timothy Thomas, *Russia's Electronic Warfare Force: Blending Concepts with Capabilities*, Report Number 19–2714 (McLean, VA: MITRE Center for Technology and National Security, 2020) 2.

[92] Yuri Lapaiev, "EW Hype? The Reasons Behind the Limited Effectiveness of Russia's Electronic Warfare in Ukraine," *Eurasia Daily Monitor* 19, no. 51 (April 2022); Andrew Eversden and Jaspreet Gill, "Why Hasn't Russia used its "Full Scope' of Electronic Warfare?" *Breaking Defense*, 28 March 2022, https://breakingdefense.com/2022/03/why-hasnt-russia-used-its-full-scope-of-electronic-warfare/

"eye watering" in 2015. Gen Hodges now predicts defeat of the Russian military is all but inevitable.[93] Nevertheless—while it is indeed tempting to disregard their tech developments as over-hyped, considering their wider failures at the time of this writing, it would be imprudent to prematurely dismiss the threat of malign Electromagnetic Spectrum Operations (EMSO) leveraged by a near peer adversary in a future conflict. Simply stated, assumptions regarding our technological overmatch are now challenged—with the proliferation of such tech ending up in enemy hands. We can no longer assume unchallenged and unfettered control of the EM spectrum in a future fight, and therefore, we must closely examine these capabilities so that we can learn, adapt and successfully operate in a contested C2 environment.

Recent reports of their battlefield performance notwithstanding, Russia has been a global leader in not only EMSO, but the development of complementary military doctrinal and theoretical application of this technology, going back over a century. Their military interventions since 2014 have boasted impressive and evolved capabilities, and a close observation of these systems provide us ample opportunity to study how EW can be exploited in the interconnected, "informationized," networked battlespace.[94] Accordingly, if we are to succeed in a future fight, we must understand how these wars will be fought. This means we must also have a solid understanding of how "invisible" wars are fought in the information domain— namely, the electromagnetic spectrum.

This chapter will show how EMSO, and Russian military concepts of Information Warfare are inexplicably linked. I will explore the Russian military's employment of EW technology, and the ways in which they use this to achieve asymmetric advantages over adversaries, whilst simultaneously challenging the West's pursuit of "information dominance." I will briefly discuss the history of Russian EW, tracing the development of their doctrine during the Cold War era, into the New Look reforms of 2009, explaining how these

[93] Sohrab Ahmari, "Weekend Interview with Frederick B. Hodges: The View from NATO's Russian Front." *Wall Street Journal*, 7 Feb 2015; See also Gen Hodges'comments on the status of Russian forces in the 2022 invasion: "All Roads Lead to Crimea: The War in Ukraine with General Ben Hodges," 11 October 2022, *The Renew Democracy Initiative*, video, 11:41, https://www.youtube.com/watch?v=g5WztvkeMLc

[94] A term used frequently in military writings to describe the integration of networked command and control systems which rely on the dissemination of large amounts of data amongst other "information dependent weapons" in contemporary military operations. Often used interchangeably with "network-centric," or 'multi-domain operations." See McDermott, *Russia's Path to the High-Tech Battlespace*, 290–5.

concepts are manifested in their present-day understanding of Information Warfare. Finally, I will present a survey of their current equipment inventory and observed capabilities since 2014, emphasizing how and why this technology poses a major threat to the U.S. and NATO in a potential future conflict.

A. ROLE OF ELECTRONIC WARFARE IN THE RUSSIAN MILITARY: DEFINITIONS, HISTORY, AND DOCTRINE

Electronic Warfare is frequently misunderstood as simply "jamming" of an enemy's electronic systems, but a more accurate picture of EW (in U.S./NATO vernacular) presents it as "military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum to attack the enemy."[95] There are three subcategories of EW: electronic attack, electronic protection, and electronic warfare support (summarized in Figure 2). The most traditional methods have been employed in Area Access, Area Denial (A2/AD) applications and against anti-air assets (known as SEAD, or Suppression of Enemy Air Defenses) in the shaping phase of major conflicts, as noted prominently by Russian military theorists in their close observations of the U.S. military's performance during the opening stages of Operation Desert Storm.[96]

From a U.S./NATO perspective, Electronic Warfare is considered separate and distinct from attacks in the cyber domain, a clear departure from how Russian theorists view Information Warfare. Instead of the Western norm of compartmentalizing these capabilities into neatly organized sub-categories (e.g., offensive cyber operations, EW, PsyOps, Information Operations, etc.), Russian military theorists distinguish them simply between Information-Technical and Information-Psychological.[97] Russian concepts of EW are no exception, as Timothy Thomas and Keir Giles note how Electronic Warfare is just one aspect of an overarching strategy Russian theorists have termed "Information Confrontation" (informatsionnoe protivoborstvo, or IPb) frequently cited as a component of their strategic

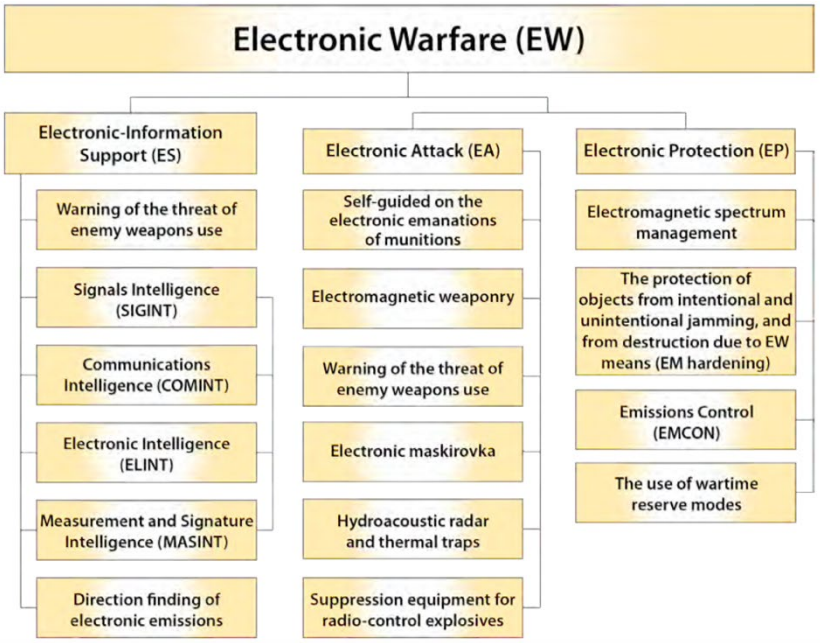
[95] Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Operations* JP 3-85 (Washington, DC: Joint Chiefs of Staff, 2020).

[96] Mary C. Fitzgerald, "The Soviet Military and the New 'Technological Operation' in the Gulf," *Naval War College Review* 44, no. 4 (Autumn 1991): 16–43.

[97] Robert Seely, "Defining Contemporary Russian Warfare," *The RUSI Journal* 162, no. 1 (Spring 2017): 53.

thinking in Russian military academic writings.[98] Accordingly, a close examination of these writings show that their use of EMSO to disrupt their adversaries' command and control (known as C2D, or C2 Disruption) is a foundational concept of not only this IW methodology but as Roger McDermott argues, an integral feature of contemporary Russian military thought.[99]

Figure 2. Russian Concept of Electronic Warfare[100]



The Russian military's interest in electronic warfare is consistent with its overarching focus on asymmetric methods to create disorder and disrupt the enemy's decision cycle and his ability to command and control forces. As such, the employment of EW is just one tool in its arsenal to create this effect. LTG Stephen Fogarty, currently the Commanding General of

[98] Timothy Thomas, *Advanced Weaponry and Russian Military Art of War*, Report Number 20–1890 (McLean, VA: MITRE Center for Technology and National Security, 2020): 2–3.

[99] Roger McDermott, "Electronic Warfare in Contemporary Russian Military Thought," in *Russia's Path to the High-Tech Battlespace*, (Washington, DC: The Jamestown Foundation, 2022), 366; For further discussions on Russian IPb, see Michelle Grisé, et. al., *Rivalry in the Information Sphere: Russian Concepts of Information Confrontation*, RRA-198-8 (Santa Monica, CA: RAND, 2022).

[100] Source: Grau and Bartles, *The Russian Way of War,* 291.

U.S. Army Cyber Command (ARCYBER) spoke on this concept in 2015: "Russian activities in Ukraine... really are a case study in the potential for cyber-electromagnetic activities… It's not just cyber, it's not just electronic warfare, it's not just intelligence, but it's a really effective integration of all these capabilities with kinetic measures to actually create the effect that their commanders [want] to achieve."[101]

Moscow boasts a distinguished history in exploiting the EMS to gain asymmetric advantages over their adversaries, with EW considered among "the key pillars of Soviet military might."[102] Even celebrating 15 April as a public holiday commemorating "Day of the Electronic Warfare Specialist," the Ground Forces tout an array of achievements traced back to the earliest applications of radio technology in military operations.[103] During the Russo-Japanese War (1904-5), Russian troops successfully jammed radio transmissions of Japanese ships and prevented them from adjusting their guns during both the blockade of Port Arthur, and the subsequent Battle of Tsushima Strait.[104] Their interest in developing this capability was evident again during the First World War, when they employed SIGINT to disrupt enemy communications, among the few (if only) overmatch capabilities the Imperial Russian Army had possessed during that conflict.[105] Their EW expertise was proven again during the Great Patriotic War (1941-5), in which the Red Army fielded the first specialized EW units in history, conducting successful deception operations against German ground forces on the Eastern Front.[106] Additionally, the Russians coupled this skill with their strict EMCON and radio discipline to expertly evade German radio reconnaissance attempts in geo-location of

[101] Keir Giles, *The Next Phase of Russian Information Warfare*. (Riga: NATO Strategic Communications Center of Excellence, 2016), 13.

[102] Sergey Sukhankin, "Blind, Confuse, Demoralize: Russian Electronic Warfare Operations in Donbas," *The Jamestown Foundation*, 27 August 2021, https://jamestown.org/program/blind-confuse-and-demoralize-russian-electronic-warfare-operations-in-donbas/

[103] Duncan McCrory, "Russian Electronic Warfare, Cyber and Information Operations in Ukraine," *The RUSI Journal* 165, no. 7 (Winter 2021): 35.

[104] Andreas Turunen, "The Broader Challenge of Russian Electronic Warfare Capabilities," in *Improvisation and Adaptability in the Russian Military,* ed. Jeffrey Mankoff (Washington, D.C: Center for Strategic and International Studies, 2020), 14.

[105] Sukhankin, "Blind, Confuse, Demoralize."

[106] James T. Westwood, "Soviet Electronic Warfare: Theory and Practice," *Jane's Soviet Intelligence Review* 1, no. 9 (September 1989): 388; Sukhankin, "Blind, Confuse, Demoralize."

their positions; employing radio camouflage techniques cited as "the best in Europe."[107] The Soviets applied these lessons learned to further develop their EW theory into a formalized Radio Electronic Combat (REB) doctrine during the Cold War, and fielded entire EW battalions that continued to emphasize the importance of geo-locating, disorganizing, and disrupting an enemy's command and control networks.[108]

Development of their doctrine, and procurements of new technologies continued throughout the Cold War era but stalled during the 1990s following the fall of the former Soviet Union, and the ensuing chaos of the Yeltsin era. EW was used by Russian forces during the Chechen Wars but mainly against civilian infrastructure, limited to direction finding of cellular signals and SIGINT purposes during urban operations in Grozny.[109] It was again employed sporadically during the 2008 Georgian invasion, but subsequent studies and after-action reports indicate it was not used effectively.[110] Despite the Russian Air Force achieving local air superiority during their invasion, their lack of effective EW support in neutralizing Georgian air defenses during this campaign resulted in the loss of several of their aircraft.[111] After 2008 however, the Russian military began making significant strides and investments in EW procurement, fielding these systems in Eastern Donbas region, and later Syria in 2015, leading to the aforementioned observations by military experts such as General Ben Hodges and others during this timeframe.[112]

---

[107] David Kahn, *Hitler's Spies: German Military Intelligence in World War II*, (New York: Macmillan, 1978), 451.

[108] Jonas Kjellen, *Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces*, Report Number FOI-R-4625-SE (Stockholm: Swedish Defense Research Agency, 2018), 19–21.

[109] Olga Oliker, *Russia's Chechen Wars 1994–2000: Lessons from Urban Combat*, MR-1289 (Santa Monica, CA: RAND, 2001), 52.

[110] Lionel Beehner et al., "Analyzing the Russian Way of War: Evidence from the 2008 Conflict with Georgia," Modern War Institute at West Point (March 2008), 50.

[111] Timothy Thomas, "The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia." *Journal of Slavic Military Studies* 22, no. 1 (2009):" 41–5.

[112] Observations of Russian EW performance in Syria and Ukraine during 2014–15 made several headlines and led to robust discussions within military academic circles, as well as policy actions to assess and begin investments to re-develop the U.S. military's neglected EW inventory. See Paul McLeary, "Report: Russia's Winning the Electronic War," *Foreign Policy*, 21 October 2015, https://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/

B. RUSSIAN DEVELOPMENTS POST-2009 REFORMS

Accordingly, the Russian General Staff recognized the necessity for major improvements in EW capabilities as part of the 2009 New Look reforms and sought to professionalize and fully modernize its EW community after 2008. On 9 January 2012, then-President Medvedev issued a classified executive policy order titled: "The Fundamentals of the Policy of the Russian Federation in Development of an Electronic Warfare System in the Period up to 2020 and Beyond."[113] This decree authorized the development and procurement of new EW capabilities and systems through 2020, as well as the creation of specialized interagency relationships for integrating EW with other national security assets.[114] As a result, Russian investments in EW systems more than doubled from ₽20 billion to ₽45 billion rubles from 2012–2016, with the addition of 9,000 to 12,000 military personnel to specialized EW units, which illustrates the newly increased significance Moscow leveraged on this capability.[115] This was further evident through the continued overhaul of doctrine and classification of EW as a specific combat support function, to include fielding fully manned and equipped EW companies as organic components of their BTGs.[116] Additional reports since 2018 include even plans for the formation of dedicated EW battalions.[117] Figures 3 and 4 illustrate the full integration of EW companies within the maneuver group structure.

[113] Roger McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*. (Tallin: International Center for Defense and Security, Republic of Estonia Ministry of Defense, 2017), 14.

[114] Pavel Luzin, "Electronic Warfare: Russia's Approach," *The Foreign Policy Research Institute*, February 2022, <https://www.fpri.org/article/2022/02/electronic-warfare-russias-approach/>

[115] Luzin, 8, 16.

[116] Jonas Kjellen, 29.

[117] Charles K. Bartles, "Russian Combined Arms Armies Plan Electronic Warfare Battalions," Foreign Military Studies Office, *OE Watch* 8, no. 11 (November 2018), 3–4.

Figure 3. Russian Ground Forces Motorized Rifle Brigade Structure[118]

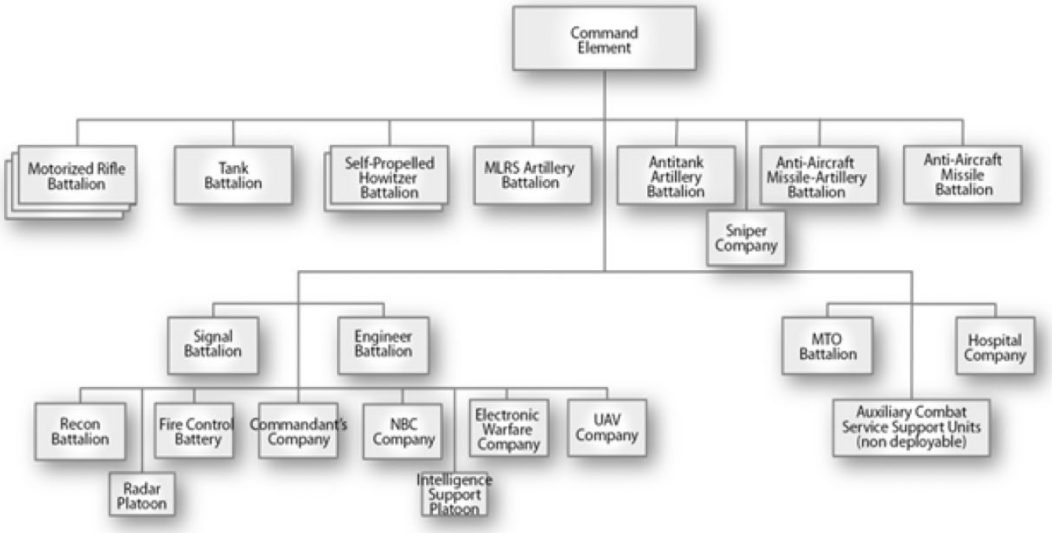
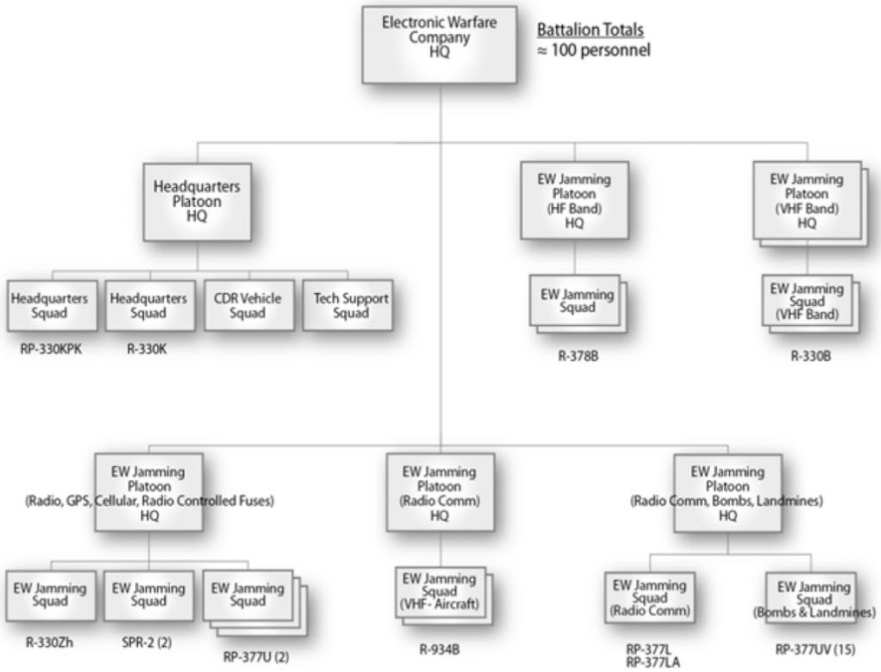


Figure 4. Electronic Warfare Company within Brigade Structure[119]



[118] Source: McDermott, *Russia's Path to the High-Tech Battlespace*, 334.

[119] Source: Grau and Bartles, *The Russian Way of War*, 290.

With the annexation of Crimea in 2014, the Kremlin began testing and fielding a diverse array of new platforms in the Donbas region and Syria, displaying an impressive edge in EW capability over their adversaries (to include affecting U.S. systems deployed in the region).[120] Sources indicated at least 30 separate and distinct EW platforms within the Ground Forces alone, designed to target UAS, GPS, military radio systems, and cellular networks.[121] Several instances of Russian use of this capability in Donbas are well documented since 2014, employed with chilling effect. In 2019, Ukrainian Colonel Ivan Pavlenko of the Joint Staff Armed Forces of Ukraine gave a sobering first-hand account at the Association of Old Crows (EW non-profit organization) of some of these effects witnessed first-hand.[122] These included the effective suppression of radio signals, the exploitation of UAS enabled direction-finding equipment to locate electronic signatures from troops on the ground, and the ability to exploit and steal information from troops' smartphones, and a virus used to exploit a radio repeater.[123] Additionally, reports indicate over one hundred Ukrainian UAS drones (many supplied by the U.S. and Turkey) have been lost (as of winter 2021) due to the Russians' effective employment of GPS spoofing.[124]

Employing EW, the Ground Forces have become particularly adept at a tactic coined "Pinpoint Propaganda" in which Ukrainian troops in Donbas were frequently harassed and bombarded with short message service (SMS) text messages, many implicating loved ones.[125] Christian Brose's monograph "The Kill Chain" recounts an incident that reflects a growing

[120] Michael Kofman, "Syria and the Russian Armed Forces: An Evaluation of Moscow's Military Strategy and Operational Performance," in *Russia's War in Syria: Assessing Russian Military Capabilities and Lessons Learned*, ed. Robert E. Hamilton, Chris Miller, and Aaron Stein, (Philadelphia, PA: Foreign Policy Research Institute, 2020), 61.

[121] Timothy Thomas, *Russia's Electronic Warfare Force: Blending Concepts with Capabilities*, 6.

[122] Dave Makichuk, "Lessons Learned from the Battle of Ukraine," *Asia Times*, 31 October 2019, <https://asiatimes.com/2019/11/lessons-learned-from-the-battle-of-ukraine/>

[123] Joseph Trevithick, "Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio Virus," 30 October 2019, *The Drive*, <https://www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics-including-radio-virus>

[124] Duncan McCrory, "Russian Electronic Warfare, Cyber and Information Operations in Ukraine," *The RUSI Journal* 165, no. 7 (Winter 2021): 36.

[125] Raphael Satter and Dmytro Vlasov. "Ukraine Soldiers Bombarded by 'Pinpoint Propaganda' Texts," *The Associated Press*, 11 May 2017; "Enemy Armies with Black Mirrors," *The Economist* 439, no. 9246 (22 May 2021): 30.

and disturbing trend in Russian EW units targeting the mobile devices and even family members of Ukrainian soldiers. In this particular instance, a mother of a renowned Ukrainian field commander had received a phone call from a Russian operative posing as a Ukrainian government official, and was informed her son was wounded in a field hospital. Despite his strict observance of OPSEC he returned his mother's phone call, enabling nearby Russian artillery batteries to quickly geo-locate and target his position.[126] Other messages such as: "your commanders have fled, you are alone and nobody will help you," or "they will find your body when the snow melts," are common, well documented, and have had varying degrees of effectiveness against cohesion and morale amongst the Ukrainian troops at the front since 2015.[127]

C. PLATFORMS AND SYSTEMS 2014-PRESENT

Moscow's rapid, intense modernization and procurement of its EW inventory was evident when an array of new equipment began to appear in Ukraine and Syria by 2014–15.[128] Both fronts provided what experts like Sam Bendett termed a "laboratory," and "testing ground," for the development of capabilities, experimentation, and testing of new systems.[129] Similar to their newly acquired UAV fleet, Russian EW systems were now far more prominent and effective in supporting ground operations than ever before. Between these two theatres however, their approach to EW differed slightly. Whereas Russian units in Syria appeared more focused on force protection of bases and delivery of effects against aerial systems and ISR, Russian EW in eastern Ukraine was employed extensively in support of ground operations, as well as testing combinations of EW with psyops and artillery fires.[130] As previously mentioned, the Ground Forces have fielded at least 30 separate platforms in

[126] Christian Brose, *The Kill Chain*, 23; and Valeriano et al., *Cyber Strategy*, 140

[127] Giles, *Handbook of Russian Information Warfare*, 106; Kenneth Rosen, "Kill Your Commanding Officer: On the Front Lines of Putin's Digital War With Ukraine," *Politico Magazine,* 15 Feb 2022.

[128] Note: In a 2014 interview, Russian EW commander Gen Yuri Lastochkin revealed that 18 new systems had completed testing during the period between 2010–2013. See Richard Scott, "Tuning In, Turning On: Russia Brings Radio Electronic Combat to the Fore," *Journal of Electromagnetic Dominance* 43, no. 11 (December 2020): 27.

[129] Turunen, "The Broader Challenge of Russian Electronic Warfare Capabilities," 16.

[130] McDermott, *Russia's Electronic Warfare Capabilities to 2025*, 21; Turunen, 16.

recent years. The following listing does not presume, nor intend to serve as an all-encompassing survey of the current Russian EW inventory. However, it nonetheless gives the reader both an understanding of their capabilities as well as an appreciation of some of the more prominent Russian EW ground systems observed in action as of late.

One system in particular, the Leer-3 (RB-341V) initially fielded in 2015, was first used in Syria, and illustrates the broad utility and approach Russian forces have employed EMSO to support ground operations.[131] This drone-based system consists of three specially configured Orlan-10 UAVs and a single C2 station mounted on a KamAZ 5350 truck. With the main components safely away from the battle area, the accompanying Orlan-10s suppress and "mimic" up to three nearby GSM cellular towers, essentially acting as forward, mobile base stations, thus forcing nearby subscriber devices (from a distance of up to 6 kilometers) to connect to it. Once the loop is complete, the system can send SMS messages, audio/video files, and even control the targeted subscriber devices, while simultaneously able to discern the devices of friendly forces.[132] Possessing a unique PsyOp function, multiple reports indicate the Leer-3 is used successfully for MILDEC applications, as well as confusing and demoralizing enemy troops and civilians alike.[133]

Another powerful, multifunctional land-based system is highly effective at suppressing (or "spoofing") enemy GPS and radar. The Krasukha family of systems, (Krasukha-2 and 4, respectively), employ broadband noise jamming techniques to neutralize enemy strike aviation radar systems, to include JSTAR Northrup Grunman E-8 and the Boeing E-3 Sentry.[134] It has been used extensively in Syria against enemy UAVs, and can simultaneously track up to 80 targets and process ELINT from 60 airborne systems

[131] Janes, "Leer-3 Electronic Warfare System," 2 May 2022, https://customer.janes.com/Janes/Display/JC4IA0399-JC4IA

[132] U.S. Army TRADOC, "Leer-3 Russian 6x6 Mobile-Drone Based EW System," ODIN, OE Data Integration Network, accessed 10 October 2022, https://odin.tradoc.army.mil/

[133] Bryan Clark, "The Fall and Rise of Russian Electronic Warfare," *IEEE Spectrum*, 30 July 2022, https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare; McDermott, *Russia's Electronic Warfare Capabilities to 2025,* 23.

[134] McDermott, *Russia's Path to the High-Tech Battlespace*, 336.

concurrently.[135] It is reported that a Krasukha unit was integral in the coordinated efforts to repel the swarming attack on the Khmeimim Airbase in January 2018.[136] Although disputed between Moscow and the U.S., the use of the newer Krasuka-4 is also linked to the purported "loss of 36 U.S. cruise missiles" in the Shayrat Airbase strike of 7 April 2017.[137] While the Krasuhka-2 has proved effective in neutralizing enemy UAVs and radar systems (namely, AWACS and radar guided missiles) at ranges of up to 250 km, the Krasukha-4 model is capable of a wide degree of missions in both electronic detection and attack, and reports indicate that it can emit RF beams powerful enough to physically damage electronic systems on specific targets. Furthermore, the new design is purportedly able to affect Low-Earth Orbit (LEO) satellite systems, as well as blind the onboard radar systems of 5th Generation aircraft.[138] Ukrainian forces reportedly captured an abandoned Krasukha-4 near Makariv, approximately 30 miles outside of Kyiv in early spring 2022.[139] A close, joint examination of this system would undoubtedly serve a major win for U.S./NATO's understanding of contemporary enemy EW capabilities.

One of the Ground Forces' newest systems, the Borisoglebsk-2 (RB-301B), is another powerful, multipurpose vehicular mounted system and is cited among the main platforms employed in the Army at the company level, and found within the maneuver brigades.[140] First spotted in Eastern Ukraine in 2015, it possesses four separate jamming systems within the

[135] Janes, "Krasukha Series Radar Jammers," 25 February 2022, https://customer.janes.com/Janes/Display/JC4IL0650-JC4IL

[136] Ridvan Bari Urcosta, "The Revolution in Drone Warfare: The Lessons from the Idlib De-Escalation Zone," *The Air Force Journal of European, Middle Eastern, and African Affairs* 2, no. 3. (August 2020)

[137] Roger McDermott, "Russia's Electronic Warfare Capabilities as a Threat to GPS," *Eurasia Daily Monitor* 18, no. 40 (March 2021).

[138] Janes, "Krasukha Series Radar Jammers," 25 February 2022, https://customer.janes.com/Janes/Display/JC4IL0650-JC4IL; McDermott, *Russia's Path to the High-Tech Battlespace*, 350.

[139] Kelsey D. Atherton, "What to Know About the Russian Device Reportedly Captured in Ukraine," *The Center for Public Integrity*, 30 March 2022, https://publicintegrity.org/national-security/ukraine-in-crisis/what-to-know-about-the-russian-device-reportedly-captured-in-ukraine/

[140] McDermott, 348.

entire complex, which is distributed across nine armored vehicles.[141] It possesses SIGINT, geo-location, direction finding, and can also suppress GPS and satellite communications.[142]

The Murmansk-BN is a long haul, strategic level asset and is reportedly among the most powerful EW systems in existence. Initially fielded in 2016, the Kremlin has reportedly deployed this system on the Crimean Peninsula with the purpose of monitoring NATO vessels operating in the Mediterranean Sea.[143] It is designed to jam and intercept communications operating on the HF spectrum (to include the U.S. High Frequency Global Communications System) as well as navigation and control systems of aircraft and naval ships (to include sub-surface vessels) at ranges up to 8000 km.[144]

D. CONCLUSIONS

The Kremlin's increased expenditure and development in EW emphasize a modernization driven by tactical lessons learned since 2008. The Kremlin prioritized and invested in EW capabilities where the U.S. did not, as two decades of counterinsurgency fights in Iraq and Afghanistan resulted in the atrophy of skills and divesture in EW equipment in the U.S. arsenal. As rapidly developing technology is vastly increasing the lethality and range of new weapons systems, the sensor saturated battlespace enables those weapon systems to detect signals in the electromagnetic spectrum, thus effectively linking weapons systems with targets (sensor-shooter loop, or "kill chain.")

Dr. Jan Kallberg of the Army Cyber Institute perfectly illustrates the threat that enemy EMSO poses to U.S./NATO in the future battlespace:

> Smart defense systems need to communicate, navigate, identify, and target. It does not matter how cyber secure our platforms are if we are denied access to electromagnetic spectrum. Every modern high tech weapon system is a dud

[141] Janes, "Borisoglebsk-2 Electronic Warfare Complex," 5 July 2021, https://customer.janes.com/Janes/Display/JC4IL0693-JC4IL

[142] U.S. Army TRADOC, "Borisoglebsk-2 (RB-301B) Russian Amphibious Multipurpose Jamming Complex," ODIN, OE Data Integration Network, accessed 10 October 2022, https://odin.tradoc.army.mil/

[143] Ruslan Minich, "Russia Shows its Military Might in the Black Sea and Beyond," *Atlantic Council*, 6 November 2018, https://www.atlanticcouncil.org/blogs/ukrainealert/russia-shows-its-military-might-in-the-black-sea-and-beyond/

[144] Janes, "Murmansk-BN Electronic Warfare System," 17 June 2022, https://customer.janes.com/Janes/Display/JC4IL1084-JC4IL

> without access to spectrum. The loss of spectrum will evaporate the American military might.[145]

The U.S. is slowly transitioning back to its advantage in this particular realm, but Russia's edge in EW capabilities reveal that in a near peer conflict, the West will no doubt be forced to relearn how to fight in a contested or denied communications environment. The final section of this work will explore resiliency and methods that Ukrainian troops have used since 2022 and provide recommendations for the West to contend with these threats.

[145]Jan Kallberg, "Why the Military Must Defend the Spectrum," *C4ISRNET*, 13 April 2015, <https://www.c4isrnet.com/opinion/the-compass/net-defense-blogs/2015/04/13/kallberg-why-the-military-must-defend-the-spectrum/>

IV. EXPLOITATION OF CYBERSPACE AND DIGITAL MEDIA IN RUSSIAN IW METHODOLOGY

A quote attributed to the father of Greek tragedy Aeschylus states that in war, truth is the first casualty. The obfuscation of truth, and weaponization of information during interstate conflict is neither new nor innovative concept. Its origins are traced to antiquity, and actively used as an instrument of power by both state and non-state actors alike.[146] Continuous Russian military aggression in the past fifteen years has emphasized the use of asymmetric and hybrid tactics; and evident amongst these tactics is a preeminence on exploiting cyberspace and other forms of digital media. And in a strategy that has become synonymous with *Information Warfare,* the Russian military has developed highly effective techniques, tactics, and procedures in exploiting this digital domain to inflict cognitive and psychological effects on their adversaries. These disruptive techniques began development after the Russian Revolution, and further perfected by the Soviets during the Great Patriotic War against Nazi Germany.[147] The conflicts in Georgia, Syria, and Ukraine demonstrate how the technologies have changed, but the methodology is similar, weaponizing digital media to conduct nefarious activities in the information domain.

The ongoing war in Ukraine has emphasized the use of the digital domain and cyber-attacks to facilitate information operations.[148] Russian cyber activities accompanying their invasion have not (least yet) matched up with "Cyber Pearl Harbor" predications and regarding their capabilities and willingness to attack national and civil infrastructure such as power grids and finance networks.[149] Despite this, observed Russian

[146] KJ Boyte, "An Analysis of the Social Media Technology, Tactics and Narratives Used to Control Perception in the Propaganda War Over Ukraine," *Journal of Information Warfare* 16, no. 1 (Winter 2017): 90.

[147] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*, (New York: Farrar Straus and Giroux, 2020); Taras Kuzio, "Old Wine in a New Bottle: Russia's Modernization of Traditional Soviet Information Warfare and Active Policies Against Ukraine and Ukrainians," *The Journal of Slavic Military Studies* 32, no, 4 (Winter 2019): 485–506.

[148] Piret Pernik, *Hacking for Influence: Foreign Influence Activities and Cyber-Attacks*, (Tallin, International Center for Defense and Security, February 2018).

[149] Erica D. Lonergan, Brandon Valeriano, et. al., "Putin's Invasion of Ukraine Didn't Rely on Cyberwarfare. Here's Why," *The Washington Post,* 7 March 2022; Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *The New York Times*, 11 October 2012.

cyber activities have parlayed more potent effects of a *different* form – in the informational and cognitive domain. As cyber expert Aaron Brantly argues, "[cyber] has been an auxiliary function… as minor operational or tactical shaping mechanism with limited successes to make the kinetic warfighting environment more and, at times, less permissible... Cyber-attacks have most impacted the information space."[150] Although the dearth of any major, geo-strategic level cyberattacks in the current Ukraine conflict [as of late] does not necessarily indicate a lack of capability, it encourages further analysis on the role that cyber and digital media play in influence and deception operations, and how the Kremlin's techniques of weaponizing digital media, and their nefarious activities in the information domain are *redefining* the modern battlespace.

For the purposes of this chapter's discussion, I make distinction between the non-kinetic, influence operations in cyberspace and Russian attacks on physical infrastructure mentioned above. I argue that beyond larger, geo-strategic level cyberattacks, it is the Kremlin's smaller-scale, malign activities for the purposes of influence campaigns, deception, and individual security that pose a *different*, but equally severe threat to force protection, military cohesion, and operational security (OPSEC). I argue that the ubiquity of servicemembers' Personally Identifiable Information (PII), the proliferation and widespread use of digital devices, and the ease at which the Kremlin (and other adversaries) can exploit these vulnerabilities poses a serious threat. This threat is far more difficult to see and trace than 'doomsday' type predictions listed above.[151] But as the following pages will show, it can be just as lethal, posing a severe risk to force and risk to mission for both the United States military and her NATO allies.

This chapter will explore how cyber, media exploitation, and Russian information operations are inextricably linked. I will first explain how the modern information environment, and the proliferation of digital media enables this exploitation for nefarious purposes. I will then continue to explore Russian and U.S. definitions of Information

[150] Aaron Brantly, "From the Foxhole: Cyber and Kinetic Conflict in Ukraine," *The Cyber Defense Review* 7, no. 2 (Spring 2022): 1–5.

[151] Emily O. Goldman and John Arquilla, eds., *Cyber Analogies*, a Technical Report for U.S. Cyber Command, NPS-DA-14-001 (Monterey, CA: Naval Postgraduate School, 2014): 11.

Warfare, and then examine specific examples from the 2008 Russo-Georgian War, the ongoing war in Ukraine, and others to explain how the Kremlin employs various means of digital media (namely, the internet, traditional media outlets and social media) in conjunction with military operations in attempts to achieve tactical level effects in the battlespace. Additionally, I will look at some critical vulnerabilities that state and non-state actors have already attempted, or successfully exploited that pose a significant threat to the U.S. military and our NATO allies in a potential near-peer conflict.

A. BACKGROUND: RUSSIAN IW AND THE EVOLUTION OF "HOMO DIGITALIS"

For the sake of clarity, it is important to distinguish these operations from the previously discussed methods of Russian Information Warfare, and why their strategy portends such a heavy emphasis on cyberspace and social media platforms. It is almost a truism that in the current age, the speed in which information travels has revolutionized the way in which wars are fought, tactical decisions are made, and armies maintained. The information networked capabilities we employ in the battlespace enable commanders to orchestrate logistics, fires, and maneuver with greater speed and accuracy than ever before imagined. Today, any military activity that does not touch the cyber domain in some form or another is almost thought of as an anachronism. Journalist David Patrikarakos identifies this phenomenon as *homo digitalis,* the "new breed of warriors in twenty-first century conflict, powerful globally connected individuals" whose reach easily extends to the personal lives of our servicemembers and domestic population.[152] This is of course facilitated through the ubiquity of smartphones, the internet, and other networked enabled platforms that have now become omnipresent in our daily lives.

The recently revised U.S. Joint Publication 3-04 *Information in Joint Operations* defines Operations in the Information Environment (OIE, formerly "IO") as "military actions involving the integrated employment of multiple information forces to affect

[152] 'Homo Digitalis' is a prevalent theme referenced in David Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in Twenty-First Century*, (New York: Basic Books, 2017), 9.

drivers of behavior."[153] This encompasses (often independent) and varying mechanisms; to include (as discussed in previous chapters) activities in the electronic spectrum (known as EW, or Electronic Warfare), Computer Network Operations (or Cyber), Military Deception (MILDEC), and Psychological Operations (also known as PsyOps, Military Information Support Operations, or MISO). Ultimately, as the DOD doctrinal definition describes, these mechanisms all have the same endstate, irrespective of method used, to achieve cognitive effects that paralyze enemy activity. With that in mind, the Kremlin has used highly adaptive methods in leveraging cyber operations by, though, and with social media platforms and other forms of digital media to exploit weaknesses, namely the cohesion and decision-making processes of their respective targets. Their methods have had varying degrees of success. But – they are nonetheless chilling, relatively low cost, and effective alternatives to more conventional (military) means in overcoming relative material weaknesses, and can also create *plausible deniability* for strategic effect.[154]

The distinction between the Western and Russian views on OIE are somewhat nuanced. Whereas the U.S. military "compartmentalizes" the different mechanisms of OIE as listed above, Russian information operations take a holistic methodology, employing a top down, "whole of society, whole of government approach," as articulated by General Valery Gerasimov in 2013.[155] The Russian framework (*informatsionnaya voyna*) is not limited to a strictly military concept, and can be employed via an array of methods.[156] This concept of IO is often employed in conjunction with *maskirovka,* (military deception) such as the deployment (and official denial of) the "Polite People" or "Little Green Men" under

[153] Joint Chiefs of Staff, *Information in Joint Operations*, JP 3-04 (Washington, DC: Joint Chiefs of Staff, 2022) GL-5; U.S. Department of Defense, *Dictionary of Military and Associated Terms*, (Washington, DC: Joint Chiefs of Staff, January 2021), 104. Note: The definition of "OIE" recently underwent multiple revisions, culminating with the publication of JP 3-04. Previous terminology includes Information Operations, defined as "the integrated employment of information related capabilities to influence, disrupt, corrupt, or usurp the decision making of adversaries while protecting our own."

[154] NJ Shallcross, "Social Media and Information Operations in the 21st Century," *Journal of Information Warfare* 16, no. 1 (Winter 2017): 4.

[155] Lincoln Flake, "Russia and Information Warfare: A Whole of Society Approach," *Lithuanian Annual Strategic Review* 18, no. 7 (May 2020): 163–75.

[156] Jonsson, *The Russian Understanding of War,* 94–7.

the false pretense of a military exercise, or simply denying their existence, as early statements from Vladimir Putin indicated during the opening days of the Ukraine conflict.

Through this, Kremlin seeks to create a "permissive information environment" in the battlespace in order to either create mass confusion, obfuscate intent, maximize ambiguity to shape public opinion, and present their narrative version of events as grounded in fact, demonstrated in the case studies listed herein.[157] The Kremlin employs these methods in a highly effective, mutual supporting manner to achieve this endstate (with often deadly results), via cyberspace and social media.

B. INFORMATION WARFARE IN THE 2008 RUSSO-GEORGIAN WAR

For a short, seemingly arbitrary regional border conflict in a part of the globe that most Americans could not find on a map, the Russo-Georgian War in late summer of 2008 is historically significant for several reasons. Not simply because it marked the first conventional war on European soil of the 21st Century, but that it witnessed the evolution of modern Russian IO tactics, and the first use of cyber and media influence in close coordination with a conventional military campaign.[158] By the time Russian mechanized and infantry forces (accompanied by state news reporters) maneuvered through the Roki Tunnel into the semi-autonomous zone of neighboring South Ossetia on 8 August 2008, a relentless cyber campaign against Georgian network infrastructure had been underway for several weeks, with the highest concentration of activity during the opening days of the conflict.[159]

Despite the sensationalized reports and analysis in the wake of the conflict, the cyber-attacks were determined to be geo-political in nature, not specifically in direct support of kinetic operations on the ground. It mainly consisted of Distributed Denial of Service (DDoS) attacks targeting government and public facing websites that were

[157] Mason Clark, "Russian Hybrid Warfare," *Institute for the Study of War* (September 2020), 18–19; Keir Giles, *Handbook of Russian Information Warfare*, (Rome: NATO Defense College, 2016), 22.

[158] Ronald Asmus, *A Little War that Shook the World: Georgia, Russia and the Future of the West*. (New York: Palgrave Macmillan, 2010)

[159] Sarah P. White, "Understanding Cyberwarfare: Lessons From the Russia-Georgia War." *Modern War Institute at West Point*. (March 2018): 1.

conducted as ancillary measures to the ground campaign to influence international public opinion. As such, these actions not only caused confusion within the Georgian military, its government and population, but promulgated the Russian narrative reported in the news media by regional and global outlets, with the intent to isolate the event from the West and delay response.[160] Additionally, due to the cyber-attacks on media outlets at the outset of the invasion, government officials were unable to get accurate information to the public, resulting in situations such as mass panic in Tbilisi on the night of August 10–11th in reaction to widely circulated rumors and disinformation regarding a Russian advance on the capital.[161] In total, approximately thirty five percent of Georgia's internet network infrastructure was taken down. A defacement of President Mikheil Saakashvili's website showed photos of him juxtaposed with Adolf Hitler, and DDoS and defacement activities were launched against no less than 54 Georgian news, government, and financial websites with periods lasting between two and six hours.[162] This created a great deal of confusion, panic, and ambiguity surrounding the events taking place on the ground and in the skies over Georgia.

Despite its introduction of a new form of warfare, the cyber-attacks conducted during the Russo-Georgian War were not about achieving decisive military objectives or attacking civilian infrastructure within the physical realm. They were part of a larger informational or psychological operations campaign, with the purpose of controlling the narrative and media reporting of the war, and the shaping of public and international opinion.[163] Fifteen years later, despite being ranked sixth in cyber capacity, the Kremlin is labeled as the second most aggressive state actor in cyberspace.[164] It can be argued that 2008 signaled the beginning of contemporary Russian information warfare.

---

[160] Nicholas Michael Sambaluk, *Weaponizing Cyberspace: Inside Russia's Hostile Activities*. (Santa Barbara, CA: Praeger Security International, 2022): 79–84.

[161] Ronald Deibert et al. "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War," *Security Dialogue* 43. no. 1 (February 2012): 12.

[162] White, 1.

[163] Lionel Beehner et al., *Analyzing Russian Way of War: Evidence from the 2008 Conflict with Georgia*, (West Point, NY: Modern War Institute, 2008), 60–3.

[164] Brandon Valeriano, Benjamin Jensen and Ryan Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*, (Cambridge: Oxford University Press, 2018), 110.

C. INFORMATION WAR AND "PINPOINT PROPAGANDA" IN UKRAINE: 2014 - PRESENT

If the events that transpired in Georgia served as a prologue to future Russian IW capabilities, the expertly orchestrated 2014 annexation of Crimea was its crown achievement. As the Kremlin's war against Ukraine (recently escalated to ground invasion) drags on in its eighth year, it has been characterized by a staggering amount of information operations (mainly distributed in the digital landscape and media) targeting the morale, trust, cohesion, and credibility of the Ukrainian population and their armed forces. Going back to its beginning in 2014, it was remarkable how the Russian military was able to annex the entire Crimean Peninsula without firing a shot, having achieved this tactical victory through a "digital blitzkrieg" of information operations, facilitated through its skillful employment and manipulation of social media and the internet.[165]

By March of 2014, Russia succeeded in achieving information dominance in Crimea through a highly sophisticated and multifaceted IO strategy. By severing its telecommunications infrastructure (to include fiber optic cables and cellular networks), the Peninsula was effectively cut off from the outside world prior to Russia even deploying its troops there.[166] Augmented by the Russian-owned companies that had already controlled a vast majority of Ukraine's Information Technology (IT) and telecommunications industry, their geographic boundaries proved a highly permissible information environment ripe for exploitation. This enabled the Kremlin to psychologically manipulate the masses with ease through the various forms of media, (with preeminence given to social media and internet).

Their IO campaign began as early as November of the previous year during the Euromaidan protests, when a pro-Russian proxy hacktivist group with ties to the Russian government, known as CyberBerkut (named for the former Ukrainian police unit) used a diverse toolkit of digital tactics in disseminating false disinformation and propaganda.

[165] U.S. Government Publication, *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014.* (Fort Bragg, NC: U.S. Army Special Operations Command, 2016.) 54–6.

[166] Azhar Unwala and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *Military Cyber Affairs* 1, no. 1 (2015): 4–6.

These ranged from botnet DDoS attacks, spear phishing of government and military officials, website defacements, and other digital publicity stunts with the aim of falsely leading the Ukrainian public and delegitimizing their government, NATO, and the West.[167] The Russian Federal Security Service (FSB) had unleashed a network of false media accounts (what has been termed Putin's "Troll Army") circulating false information and/or attacking any traditional news outlet that criticizes the Putin Regime.[168] "Fake news" stories purporting atrocities and war crimes were commonplace, such as the 2014 story of a boy crucified at the hands of Ukrainian troops that quickly went viral and was circulated throughout Russian, Ukrainian, and Western media outlets.[169]

As previously mentioned, harrowing (and deadly) forms of Russian information warfare were observed in Donbas as early as 2015. The close combination of kinetic fires, PsyOps, electronic signature detection and hijacking of soldiers' smartphones, deemed a "comprehensive fires package," is often accompanied by *pinpoint propaganda.*[170] This is demonstrated through Russian SMS text barrages containing disturbing messages such as: "They will find your body when the snow melts," or "Who is robbing your family while you are paid pennies waiting for your bullet?" followed by a volley of artillery fire on the unit position, often revealed through triangulation of cell phone signatures.[171] Now, many units have adapted, hardening their communications methods with foreign supplied encrypted radios, or even reverting to low-tech methods such as Soviet era wired field telephones.[172] Some of the innovative counter methods and resiliency will be briefly discussed in the final section.

---

[167] Maness, Valeriano, et. al., *Cyber Strategy,* 137–9.

[168] Robert Szwed, *Framing of the Ukraine-Russia Conflict in Online and Social Media*. (Riga: NATO Communications Center of Excellence, 2016), 54–6.

[169] T.S Allen and A.J Moore, "Victory Without Casualties: Russia's Information Operations," *Parameters* 48, no. 1 (Spring 2018): 66.

[170] Aaron Brantly, Nerea Cal, and Devlin Winkelstein, *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW*. (West Point, NY: The Army Cyber Institute): 28–9; Raphael Satter and Dmytro Vlasov. "Ukraine Soldiers Bombarded by 'Pinpoint Propaganda' Texts," *The Associated Press*, 11 May 2017, https://apnews.com/article/russia-kiev-ukraine-only-on-ap-archive

[171] Anonymous, "Enemy Armies with Black Mirrors," *The Economist* 439, no. 9246 (22 May 2021): 30; Sambaluk, *Weaponizing Cyberspace*, 86.

[172] Kenneth Rosen, "Kill Your Commanding Officer: On the Front Lines of Putin's Digital War With Ukraine," *Politico Magazine,* 15 Feb 2022.

D. BLACK MIRRORS IN THE BATTLESPACE: DIGITAL MEDIA AND FUTURE IMPLICATIONS FOR THE WEST

Russian capabilities (and current observed trends) in the IO realm highlight some serious vulnerabilities that if Western military commanders are not adequately prepared, may potentially hinder the combat effectiveness of NATO/U.S. forces in a future near-peer fight. Irrespective of the level of target (Strategic, Operational and Tactical levels), Russian IO methods seek to disrupt the decision space of both military and political leadership. As the internet and digital media has now connected the battlefield in real time with a citizenry back home, this poses significant challenges for commanders. As media and diplomacy expert Philip Seib argues: "Information matters. How most people shape their attitudes about a war—support or opposition—is determined largely by the way the information is received about the particular conflict."[173]

The global community has already seen the consequences of proliferating digital information (to include photographs) in forward deployed areas and the severity it poses to not just operational security but also a politically fraught public opinion back home. The Abu Ghraib Scandal, and 2012 YouTube broadcast of U.S. Marine snipers desecrating Taliban corpses serve as examples. From a more technical point of view, digital images posted online pose significant concerns for operational security (known as OPSEC). While Vladimir Putin vehemently denied the existence of "Little Green Men" on the Crimean Peninsula in 2014, geo-tagged photos abounded on social media portraying Russian troops posing for selfies next to military hardware and equipment, thus quickly exposing and contradicting the lies perpetrated in official statements on behalf of their government.[174] In an attempt to further stymie the efforts of journalists and other collectors of open source intelligence (known as OSINT), Russian Parliament had prohibited its troops from possessing mobile phones or recording devices, with violators severely disciplined if

[173] Philip Seib, *Information at War: Journalism, Disinformation, and Modern Warfare*. (Cambridge, UK: Polity Press, 2021), 16.

[174] Christian Brose, "Move, Shoot, Communicate," in *The Kill Chain: Defending America in the Future of High-Tech Warfare*. (New York: The Hachette Group, 2020), 166–7.

caught.[175] However, Russian troops have been forced to rely on these devices in the recent campaign since late February 2022. Although the exact reasons for this reversal are unclear, this indiscretion has provided ample OSINT targeting opportunities for their Ukrainian adversaries.[176]

Accordingly, this tactic can prove a force for good, such as the Leicester stay-at-home father, turned cyber-sleuth Eliot Higgins, who, conducting his own investigation with Bellingcat, obtained open-source intelligence (OSINT) via metadata pulled from photographs taken by unwitting Russian troops, ultimately exposing their involvement in the downing of Flight MH17 over Eastern Ukraine in 2014.[177] But these activities also highlight even more potential opportunities for an adversary's IO apparatus, highlighting major security vulnerabilities for troops on the ground, to include jeopardization of their families back home. As media expert Susan L. Carruthers argues, the dangers posed by "non-professional image makers –most particularly the soldiers themselves" can produce volumes of content that can be easily turned against them, exploited, manipulated, and circulated by the enemy for their own purposes.[178]

Deepfakes, which can be highly realistic and convincing photos, audio, and video files, employ techniques in artificial intelligence known as deep learning (or machine learning) to create complete reconstructions of events or false ones.[179] These have been crafted for varying purposes, ranging from the benign, such as a break-dancing Vladimir Putin or the 2012 release of a fabricated video of U.S. Ambassador to Russia Michael

[175] Ivan Nechepurenko, "Russia Votes to Ban Smartphone Use by Military, Trying to Hide Digital Traces," *The New York Times*, 19 February 2019, https://www.nytimes.com/2019/02/19/world/europe/russia-military-social-media-ban.html

[176] Jeff Schogol, Russian Troops are Proving that cell phones in war zones are a very bad idea," *Task & Purpose*, 13 May 2022, https://taskandpurpose.com/news/russia-ukraine-cell-phones-track-combat/

[177] P.W Singer, and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*, (Boston, MA: First Mariner Books, 2019), 72–7.

[178] Susan L. Carruthers, "War in the Digital Age: Afghanistan and Iraq," in *The Media at War*, 2nd ed. (New York: Palgrave MacMillan, 2011), 241.

[179] Todd C. Helmus, *Artificial Intelligence, Deepfakes, and Disinformation: A Primer*, (Santa Monica, CA: RAND Corp, July 2022)

McFaul suggesting he was a pedophile in an attempt to discredit him.[180] Although this technology is still in its infancy, a potential "deepfake subterfuge" poses a major threat to military operations, especially in such a politically or culturally sensitive information environment.[181] Accordingly, the effects of digital "story wars," enhanced through faked videos in the information battlespace can easily determine the course of a fight just as swiftly as kinetic effects, proving that the weaponization of information, filtered through media (irrespective of its credibility) is more likely than not to be believed as fact by the audience receiving it. How would a deepfake photo or video of U.S. military personnel defiling a mosque or burning Korans be received by the Muslim community in a deployed area? How could this potentially affect military or civil operations with the local populace?

Former Commandant of the Marine Corps General Victor Krulak foresaw this dilemma over two decades ago when he wrote of the concept of "the Strategic Corporal." In a 1999 article penned in *Marine Corps Gazette,* Krulak calls on junior leaders to appropriately deal with "moral quandaries" one will often encounter on the battlefield. Accordingly, he claims the new, moral landscape demands of young troops to "confidently make well-reasoned and independent decisions under extreme stress—decisions that will likely be subject to the harsh scrutiny of both the media and the court of public opinion."[182] While this article was written in a world prior to the Post 9/11 counterinsurgency wars of the 21st century, his predictions quite accurately describe how the multidomain, information and sensor-saturated battlefields of modern war would play out—not to mention how easily it could be manipulated and exploited by the enemy.

Although the DOD has since attempted to embrace social media, the responsibility has fallen mostly within the realm of the respective services' Public Affairs Officers (PAOs). But an increasing distrust of the media, coupled with a distinct vulnerability and susceptibility to enemy exploitation of the DOD's hypersensitive, "corrosive over-

[180] Sami Quadri, "Former U.S. Ambassador says Russia is Using Deepfakes to Impersonate him," *The Evening Standard*, 1 October 2022, https://www.standard.co.uk/news/world/michael-mcfaul-ambassador-ukraine-russia-deepfakes-war-b1029502.html

[181] Justin Hauffe, "Don't Believe Your Eyes," *Proceedings* 147, no. 8, (August 2021).

[182] Victor Krulak, "The Strategic Corporal: Leadership in the Three Block War," *Marine Corps Gazette* 83, no. 1 (January 1999): 18–23.

response" approach to a politically fraught public opinion reveals an entirely new dimension that can be easily exploited by adversaries.[183] This new information environment demands a comprehensive approach that the West may not be adequately prepared for. Furthermore, this was explicitly identified in a recent Congressional report as a "critical vulnerability," with the potential to expose the U.S. military to new levels of nefarious IO conducted by foreign actors.[184] A recent article in *Proceedings* further illustrates this point in a vignette where a highly effective U.S. Naval commander is promptly removed from a combat situation due to a fabricated social media smear campaign exposing his email account, severely hindering operations and putting lives at risk.[185] Although fictitious, this scenario is highly plausible in today's media environment.

1. Algorithms, Social Engineering, And Microtargeting Of Military Personnel

As evident in these case studies, the Information Environment now extends down to the personal lives of U.S. servicemembers and their families. The ubiquity of smartphones, the internet, and other networked devices and applications enables the proliferation, mining, and harvesting of their personally identifiable information (PII). The Kremlin has proven (with ease) its ability to access this data, and further proves a major vulnerability for not simply servicemembers themselves, but military operations and cohesion, revealing a major national security threat if not comprehensively addressed.

Former FBI Director Christopher Wray warned of this threat in a 2020 Congressional Homeland Security Committee testimony: "If you are an American adult, it is more likely than not that China has stolen your personal data."[186] Referring specifically to the 2015 U.S. Office of Personnel Management (OPM) breach, and hacking of multiple

[183] Kate Bachelder Odell, "If War Comes, Will the U.S Navy Be Prepared?" *The Wall Street Journal*, 1 July 2021.

[184] U.S Congress, "A Report on the Fighting Culture of the United States Navy Surface Fleet." Conducted at the Direction of Senator Tom Cotton, Congressmen Jim Banks, Dan Crenshaw, and Mike Gallagher. 12 July 2021.

[185] Don Gomez, "Canceled in Combat: Get Ready for Smear War," *Proceedings* 147, no. 6 (June 2021)

[186] U.S Congress, House of Representatives, Committee on Homeland Security, "Worldwide Threats to the Homeland," 116th Cong., 2nd Session, 17 September 2020.

private firms such as Anthem and Equifax in 2014 and 2017, Wray claims, "[affects] nearly half of the American population and most American adults."[187] With the sheer volume of data existing on open source platforms, how can malign actors (like Russia's Internet Research Agency) harvest this data, and for what purpose?

Jessica Dawson, Army officer and researcher at the Army Cyber Institute has identified this trend of *microtargeting*, enabled by social media and the current advertising economy that collects massive amounts of PII data legally, and unabated by extremely loose regulatory controls within the tech industry. This "microtargeting" employs the same behavior predicting algorithms studied by Cambridge Analytica during the 2016 elections, exploiting marketing data that allows "individual level messaging to influence behavior, which can easily be leveraged for more insidious dis/misinformation campaigns."[188] The psychographic profiling and digital microtargeting employed by Cambridge Analytica had eerily similar parallels to military PsyOp and IO techniques, suggesting that these same methods used to influence elections could just as easily be used against our own military community.[189] The plethora of personal online data that servicemembers post in the social media ecosystem is a target rich environment for exploitation, by not only scammers but near peer adversaries abroad. Can exploitation of this data, obtained by malign actors through social media and other public forums have more profound effects than the previously mentioned cyber-attacks on physical infrastructure?

Military and government officials have long been ripe targets for foreign scammers, catfishing, blackmail and extortion schemes. This tactic has proven highly effective (and often deadly) in exploiting an often young, impressionable, and highly vulnerable demographic. In 2009, a U.S. cybersecurity firm was able to infiltrate the professional

[187] Wray Testimony, as quoted in Timothy McGeehan, "Web Storm Rising," *Proceedings 148*, no. 3 (March 2022)

[188] Jessica Dawson, "Microtargeting as Information Warfare," *The Cyber Defense Review* 6, no. 1 (Winter 2021): 64.

[189] Vian Bakir, "Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting," *Frontiers in Communication* 5, no. 67 (September 2020).

circles of military and intelligence personnel.[190] Hundreds were duped into inappropriately providing information to a fake LinkedIn online persona of a female posing as an MIT educated U.S. Navy civilian analyst out of Norfolk, Virginia. Known as "Robin Sage," this 28-day experiment netted highly alarming results. The avatar was able to gain access to official government email accounts, personal banking, and other highly sensitive information, proving how trust can be easily manipulated based on gender, occupation credentials via social media and open-source outlets, severely compromising OPSEC.[191]

A more recent study further explores this phenomenon against a small, geographically concentrated military population during a scheduled NATO exercise. In 2018, an experiment conducted by a "red team" of software engineers and researchers from the NATO StratCom Communication Center of Excellence sought to find out how easily servicemembers can be manipulated via social media and fake online personas.[192] During this large-scale exercise in Europe, they tested not only how much information they could pull from OSINT sources on the exercise itself, but whether or not they could influence and manipulate NATO troops' actions through social media catfishing and impersonation techniques. The results were quite concerning. Over a period of four weeks, the researchers were able to uncover and socially engineer the identities of more than 150 soldiers, exploit sensitive and compromising personal data, track unit movements and even lured individual troops into abandoning their duties and engage in "undesirable activities." This was all done with a small team and a budget of no more than $60 dollars.[193]

TikTok, a social media application whose widespread use is highly popular with servicemembers, has gained significant notoriety in the past year due to its parent company

[190] Katharina Krombholz et al., "Advanced Social Engineering Attacks," *Journal of Information Security and Applications* 22, (June 2015): 113–22.

[191] Thomas Ryan, "Getting in Bed with Robin Sage," *Provide Security LLC*., A paper presented at the 2010 Black Hat Conference, Las Vegas NV; Thierry Berthier and Bruno Teboul, "False Data and Fictitious Algorithmic Projections," in *From Digital Traces to Algorithmic Projections*, (London, UK: ISTE Press Ltd., 2019): 85–112.

[192] Sebastian Bay and Nora Biteniece, "The Current Digital Arena and its Risks to Serving Military Personnel." (Riga: NATO StratCom Center of Excellence, 2019).

[193] Issie Lapowsky, "NATO Group Catfished Soldiers to Prove a Point About Privacy," 18 February 2019, *Wired*, <https://www.wired.com/story/nato-stratcom-catfished-soldiers-social-media/>

ByteDance, and its lack of transparency in data privacy.[194] The app, which requires access to a smartphone's microphone and other functions, easily tracks its owner's location and collect voice and fingerprint data. In a recently uncovered leaked audio, a TikTok employee revealed that "Everything is seen in China," illustrating how the massive amount of user data harvested and stored in offshore servers is easily accessible to engineers in Beijing.[195] TikTok is not the only platform that tracks and harvests its users' data, with fitness apps and devices such as Strava (also very popular with servicemembers) were found tracking locations through GPS enabled metadata in forward deployed locations.[196]

Malign actors can easily find, socially engineer, and exploit this readily available (and openly shared) information to target servicemembers, their personal lives, and families. Russian hackers have been known to conduct such activities during major NATO exercises.[197] In multiple highly publicized instances, families of NATO servicemembers (and troops themselves) were on the receiving end of highly personalized forms of harassment and intimidation methods such as phone calls, hacking of smartphones, and face to face confrontations by strangers who possess their personal information.[198] In March 2015, the terrorist network ISIS published their infamous "Kill Lists" across social media outlets, containing the names, addresses, and photographs of hundreds of servicemembers and government officials. Despite this campaign being largely unsuccessful, it nevertheless gained enough traction to fuel a significant degree of fear and

[194] Joel Thayer, "TikTok Is Fun and Games Until China Wants Your Info," *The Wall Street Journal*, 22 July 2022.

[195] Emily Baker White, "Leaked Audio from 80 Internal TikTok Meetings Shows That U.S. User Data Has Been Repeatedly Accessed From China," 17 June 2022, *BuzzFeed News*, https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access

[196] Jeremy Hsu, "The Strava Heat Map and the End of Secrets," 29 January 2018, *Wired*, <https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy>

[197] Terri Shultz, "Russia is Hacking and Harassing NATO Soldiers, report says," 10 June 2017, *Deutche Welle News,* <https://www.dw.com/en/russia-is-hacking-and-harassing-nato-soldiers-report-says/a-40827197>

[198] Joseph V. Micallef, "Russian Harassment of NATO Personnel, Families: The Next Chapter in Information Warfare?" 3 *Military.com,* September 2019, https://www.military.com/daily-news/2019/09/03/russian-harassment-nato-personnel-families-next-chapter-information-warfare.html

change of behaviors within the military community, and could potentially be replicated at a far bigger scale.[199]

Although not a new nor unprecedented phenomenon, one example from over 30 years ago highlights the potential effects and the security vulnerabilities exposed from mining of publicly available information (often facilitated and enabled by mass media). In March 1989, the spouse of a prominent U.S. Navy Captain (who had been the target of extensive national media coverage) was the victim of a campaign of harassing visits and phone calls, leading up to an attack in which a pipe bomb in the undercarriage of her minivan exploded while at a stop light in San Diego, CA.[200] Her husband, Captain William C. Rogers, was the commander of the guided missile cruiser *USS Vincennes* which was involved in the accidental downing of Iranian Air Flight 655, killing all 290 civilian passengers on board.[201] Despite strong evidence, the FBI and NCIS could not conclusively attribute the bombing attack to retribution carried out by international terrorists. However, the investigation revealed that personal contact details as well as the location of their home was leaked by neighbors to suspected Iranian agents. Although an extreme case, this instance highlights the dangers of social engineering enabled by complicit media coverage and PII which is ever more prevalent and cheaper to obtain in the 21st Century.

In 1970, philosopher and media expert Marshall McLuhan predicted that the future of global conflict would be a continuous "guerilla information war, with no division between military and civilian participation."[202] Today, vulnerabilities and threats posed by the Kremlin's exploitation of cyberspace and digital media to military operational security is ever more foreboding. As Brantly argues: "Bits and bytes aren't taking out tanks, but they are slowly wearing down psychological walls."[203] Senior leaders and military experts

[199] Audrey Alexander and Bennett Clifford, "Doxing and Defacements, Examining the Islamic State's Hacking Capabilities," *Combating Terrorism Center at West Point Sentinel* 12, no. 4 (April 2019): 22–8.

[200] Jay Matthews, "Vehicle of Vincennes Skipper's Wife Bombed," *The Washington Post*, 11 March 1989.

[201] Will and Sharon Rogers, *Storm Center: The USS Vincennes and Iran Air Flight 655*. (Newport, RI: Naval Institute Press, 1992).

[202] Marshall McLuhan, *Culture Is Our Business*. (Eugene, OR: Wipf and Stock Publishers, 1970), 66.

[203] Brantly, "From the Foxhole," 5.

widely agree that Moscow is far ahead of the United States in terms of its information warfare capabilities and methodology, finding new and innovative ways to exploit not only cultural sensitivities but expose major weaknesses and paralyze command structures of their adversaries. Influence campaigns, waged by our adversaries in a future conflict scenario, facilitated by the long-eroded trust between the public, military and government, is a highly frightening prospect. It is evident from these case studies that cyberspace and digital media are key enablers for Russian Information Warfare, and the West's failure to adapt may prove to be its peril.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

This study examined three major components of Russian IW methodology: battlefield sensors, electronic warfare, and malign influence via cyberspace. These capabilities uncover not only trends in the changing character of warfare itself but offer a visceral glimpse into how information warfare may be prosecuted by the enemies of the U.S. in a future conflict. Additionally, these trends expose not only vulnerabilities in the West's own military apparatus, but also challenge long-held assumptions regarding *information dominance* that must be reexamined if we desire to maintain operational and technological primacy.

As previously discussed, the current phase of the Ukraine War is soon entering its tenth month. Despite their abysmal failures at the outset of this campaign, it would be foolhardy to rest upon laurels and dismiss the Russian military's performance at this stage, proffering their imminent defeat as a forgone conclusion. At the time of this writing, it appears that winter 2023 may precede a prolonged continuation of a bloody, bitter fight, reminiscent of a Dostoyevskian tragedy cold, bleak, and bereft of hope. As Dostoyevsky himself observed in 1870: "A human being living on the surface of the earth has no right to turn away and ignore what is happening on earth, and there are higher moral imperatives for this."[204]

Attempting to forecast future conflict can be a risky, and at best, nebulous endeavor.[205] Notwithstanding, the battlegrounds of Ukraine offer ample opportunity to not only examine the effects of these new technological innovations at the tactical and operational levels, but also their implications to the larger phenomenon of war itself. As such, an opportunity to conduct continued, scholarly research of the topics presented herein

[204] Note: human suffering is prevalent theme throughout Dostoyevsky's works, namely his 1880 novel. See Book V, Ch. IV of *The Brothers Karamazov*, trans. Constance Garnett (London, UK: William Heinemann Ltd, 1959), 244–272; For further analysis on this topic: Ani Kokobobo, "How Should Dostoevsky and Tolstoy be read during Russia's war against Ukraine?" *The Conversation*, 6 April 2022, https://theconversation.com/how-should-dostoevsky-and-tolstoy-be-read-during-russias-war-against-ukraine-179932

[205] Timothy L. Thomas, "Russian Forecasts of Future War," *Military Review* (May-June 2019): 84–93.

(as they unfold in real time on the ground and in the air) indisputably warrant further exploration and study as this war will likely rage into the spring.

What immediate lessons can the West glean from these most recent case studies? First and foremost, the Russian military's failure to achieve its objectives in early 2022 clearly reflect a lack of planning (namely logistics, combined arms maneuver, and joint operations), a failure to heed actionable intelligence, the anticipation of stiff counter-resistance, and of course the national *will* of the Ukrainian people. Additionally, the 2009 "New Look" reforms failed to curtail rampant corruption and incompetence within its ranks that has evidently paralyzed its ability to operate as an effective fighting force. Triumphant from their "Little Green Men" success in 2014 and military adventurism in Syria, the Russian General Staff were not only overconfident in their ability to project power, but perhaps even befallen to their own *hubris*.[206]

In Greek mythology, *hubris* is inflated, excessive pride in one's own abilities that more often results in tragedy.[207] It is a similar, fatal hubris that H.R McMaster warns of in his memoir *Battlegrounds,* that not only led to U.S failure in Vietnam, but finds itself resurgent, out of complacency and overconfidence analogous to the United States' unrivaled primacy of the post-Cold War, post 9/11 eras.[208] While the counterinsurgency wars of the 21st Century closed with the tragic, yet anti-climactic exodus from Afghanistan in August 2021, the United States had already begun its pivot to strategic competition in the Indo-Pacific region. Accordingly, we must ask ourselves: Could the U.S. military suffer the same fate as Russia in a future conflict?

We must equally recognize our own failures to accurately assess the Russian military's capabilities. Since 2014, a great deal of attention is focused on drawing conclusions, both tactical and technical, from the case studies presented herein. Are these

[206] Seth Jones, "Russian Success in Syria: Will it Be a Pyrrhic Victory?" *CTC Sentinel* 12, no. 9 (October 2019): 1–9.

[207] Ivan Gomza, "Hubris of Mars: Insights on the Russo-Ukrainian War from Cases of Great Powers' Oversights," *Krytyka*, October 2022, https://krytyka.com/en/articles/hubris-of-mars-insights-on-the-russo-ukrainian-war-from-cases-of-great-powers-oversights

[208] H.R. McMaster, *Battlegrounds: The Fight to Defend the Free World*, (New York, NY: Harper Collins, 2020), 10–11.

implications for future conflict applicable outside of these combat theatres, or a different opponent? We must heed McMaster and Shore's warnings of mirror imaging. As one observer asks: "What if the analysts are seeing the lessons from Ukraine incorrectly, through lenses refracted by their own biases and hubris?"[209] Great care was undertaken throughout this research to avoid making analyses in isolation. However, despite incorrect estimates of Russia's military made prior to February 2022, some conclusions can be drawn from these recent case studies, asserted with a relative degree of certainty which can surely facilitate continued discussion and study.

It is considered a truism that peer/near peer adversaries (like Russia), who cannot compete symmetrically, will undoubtedly use various, disruptive means to gain relative advantage against the U.S./NATO. Those means can be encapsulated as follows:

(1) The West is likely to encounter, and must learn to cope in a highly contested, C2 degraded operational environment.

As modern communications technology has proved a force enabler in the rapid dissemination of information, precision fires, and heightened battlefield awareness— U.S commanders have grown accustomed, and sought even greater connectivity through robust, centralized military data networks, large bandwidth terminals with massive electronic signatures in pursuit of satellite enabled communications and navigation aids. Unsurprisingly, this vulnerability will also beget the enemy's *own* ability to degrade, deny, or exploit said connectivity and battlespace awareness. As commanders are now beginning to accept that reliance on logistical "Iron Mountains" of the past is no longer a realistic expectation, this logic must be applied to "C2 Iron Mountains" as well.[210] The recent focused investments in disruptive EMSO tech by Russia and China highlight this dilemma and may force a reckoning, not just with modernization of the U.S/NATO's own inventory, but perhaps extends beyond simply equipment. Military commanders will be forced to

[209] David Johnson, "Would We Do Better? Hubris and Validation in Ukraine," *War on the Rocks*, 31 May 2022, https://warontherocks.com/2022/05/would-we-do-better-hubris-and-validation-in-ukraine/

[210] Sydney Freedberg Jr., "No More Iron Mountains: Lighter Logistics Key to Multi-Domain Battle," *Breaking Defense*, 3 May 2017, https://breakingdefense.com/2017/05/no-more-iron-mountains-streamlined-logistics-key-to-multi-domain-battle/

adapt and learn to make decisions without all the information they want, when they want it, necessitating a difficult, and painful shift in expectations and even command culture, noted by former Vice Chairman John Hyten after an eye-opening 2021 wargaming exercise.[211] This can take multiple, innovative forms, envisioned in undertakings such as Army's Project Convergence, Navy's Project Overmatch, and improved integration with our allies and partners.

(2) The future operational environment will be saturated with sensor platforms and unmanned systems, rendering not only maneuver, but tactical cover and concealment extremely difficult.

The above trend has expanded to the air domain. Armed UAS, and low cost, replaceable off the shelf micro-UAS systems are now all but ubiquitous. One need not look beyond the headlines to understand that assumptions regarding air superiority will undoubtedly be challenged by a peer adversary. Loitering munitions and "kamikaze drones" only exacerbate persistent enemy threats from air. Like over-reliance on persistent communications, the ability to counter enemy ISR and direction-finding equipment via signature management and emissions control (EMCON), is a capability gap that commanders must continue to reinforce, improve upon, and demand down to the small unit level.[212] Recent, large-scale exercises such as the Marine Corps' MAGTF Warfighting Exercise (MWX-20) featured a renewed focus on (and challenges) reducing electronic signature management, radio discipline, and development of Standard Operating Procedures (SOPs) in pursuit of denying a notional enemy's ISR and electronic signature collection ability.[213] For the ground commander, the ability to shoot, move, and communicate is paramount to closing with and destroying the enemy. Tactical maneuver also requires effective cover and concealment and reinforcing basic measures of electronic camouflage, likely making the difference between mission success or failure. The Ukrainian military, forced to learn lessons paid in blood, have since employed low-tech,

[211] Copp, "It Failed Miserably," *Defense One*, 26 July 2021.

[212] Luke Clena, "Technical Signature Management for Small Units," *Marine Corps Gazette* 105, no. 5 (May 2021): 32–4.

[213] David J. Furness, "MWX 1–20 Summary from CG, 2d MARDIV," *Marine Corps Gazette* 104, no. 7 (July 2020): 8.

even primitive methods to evade detection and command and control forces at the lower levels. Now, relying less on easily detectable cellular phones and other "technological crutches," commanders have dusted off old techniques like morse code, antique Soviet-era TA-57 field telephones, and wired, landline communications.[214] An adage from the Cold War-era Second Offset Strategy proclaims: "what can be seen can be hit, and what can hit can be killed."[215] This of course now applies to emissions. Low-signature methods like these are by no means panacea solutions, but Ukrainian innovations in this regard must be further studied and explored.

(3) The enemy is likely to leverage cyberspace to employ malign influence campaigns, targeting not only domestic publics but servicemembers and military cohesion itself.

As Sun Tzu envisioned over two millennia ago: "supreme excellence consists in breaking the enemy's resistance without fighting."[216] With a politically fractured citizenry, coupled with an increasingly corrosive domestic media culture, this ultimately begs the seminal question of whether the U.S military (or the domestic public writ large) is even ready to 'win without fighting.' Active measures, malign influence, reflexive control – are tools effectively employed by nefarious actors that seek to exploit domestic strife, destroy allied partnerships, even internal military cohesion. This problem is by and large the most difficult to address of those previously discussed. In the increasingly connected global community, decisive blows of the next conflict will occur long before tactical strikes even begin.[217] At the strategic level, a digital "tug of war" competition to amplify fractured

[214] This is explored in a 2016 publication entitled "Russian New Generation Warfare Handbook," released by the U.S Army's now-divested Asymmetric Warfare Group. See also Nolan Peterson's interviews with Ukrainian troops in "Ukraine's Old School Answers to Russia's Modern Electronic Warfare Weapons," *Coffee or Die*, 7 February 2022, https://www.coffeeordie.com/ukraine-russia-electronic-warfare

[215] "Second Offset Strategy" was a concept attributed to former SecDef Harold Brown. See William E. DePuy, "Implications of the Middle East War on U.S. Army Tactics, Doctrine and Systems," in *Selected Papers of General William E. DePuy*, ed. Donald L. Gilmore and Carolyn D. Conway (Fort Leavenworth, KS: U.S. Army Combat Studies Institute, 1995), 85. See also Brian Kerg, "To Be Detected is to Be Killed," *Proceedings* 146, no. 12 (December 2020).

[216] Sun Tzu, *The Art of War*, ed. James Clavell (New York: Dell Publishing, 1983), 15.

[217] Charles Cleveland et al. *Military Strategy in the 21st Century: People, Connectivity, Competition*, (New York: Cambria Press, 2018), 4.

internal divisions, and affect strategic partnerships is not only precedented but should be anticipated. But at the micro level, Army IW expert Jessica Dawson identifies a critical vulnerability: enemy 'microtargeting' of our own military demographic.[218] Although the DOD has taken steps to increase awareness amongst troops regarding their PII, Dawson argues the algorithmic social media ecosystem, and targeted advertising economy represent a grave national security threat, easily exploited and must be taken seriously by the highest political leadership.

Like our own reckoning after the Vietnam War, the Soviet General Staff was forced to reexamine its own mistakes following their defeat and subsequent withdrawal from Afghanistan. In a well-documented post-mortem, the Generals concluded "the side with the greater moral commitment, stronger national will, and determination to survive" will always prevail.[219] In this new era of strategic competition, we are not yet at the mercy of our rivals, but we can be certain that we will not have the luxury to choose when, or where the next conflict will start. If the previous year has shown us anything, one lesson of warfare stands the test of time. Irrespective of the amount of technology and materiel superiority one nation brings to bear, it has been human *will* that determines national survival. Accordingly, it is not only our responsibility to heed these warnings from history, but must also recognize our own *hubris,* before it befalls *us*.

[218] Jessica Dawson and Todd Arnold, "Eroding America from Within, Marketing Data threatens Military Cohesion," *C4ISRNET*, 15 February 2021, https://www.c4isrnet.com/opinion/2021/02/15/eroding-america-from-within-marketing-data-threatens-military-cohesion/

[219] The Russian General Staff, *The Soviet Afghan War: How a Superpower Fought and Lost*, trans. Lester Grau and Michael Gress (Lawrence, KS: University Press of Kansas, 2002), xiii

LIST OF REFERENCES

Adamsky, Dmitry. "Russian Lessons From the Syrian Operation and The Culture of Military Innovation." George C. Marshall European Center for Security Studies, *Security Insights* 47, (February 2020).

Ahmari, Sohrab. "Weekend Interview with Frederick B. Hodges: The View from NATO's Russian Front." *Wall Street Journal*, 7 Feb 2015.

Alexander, Audrey and Bennett Clifford. "Doxing and Defacements, Examining the Islamic State's Hacking Capabilities." *CTC Sentinel* 12, no. 4 (April 2019): 22–8.

Allen, T.S and A.J Moore. "Victory Without Casualties: Russia's Information Operations." *Parameters* 48, no. 1 (March 2018): 60–71.

Allen, John R., Ben Hodges, and Julian Lindley-French. *Future War and the Defense of Europe*. Oxford, UK: Oxford University Press, 2021.

Arquilla, John. *Bitskrieg: The New Challenge of Cyberwarfare*. Cambridge: Polity Press, 2021.

Asmus, Ronald. *A Little War that Shook the World: Georgia, Russia, and the Future of the West*. New York: Palgrave Macmillan, 2010.

Atherton, Kelsey D. "What to Know About the Russian Device Reportedly Captured in Ukraine." *The Center for Public Integrity*. 30 March 2022. https://publicintegrity.org/national-security/ukraine-in-crisis/what-to-know-about-the-russian-device-reportedly-captured-in-ukraine/

Baev, Pauk K. "The Trajectory of the Russian Military: Downsizing, Degeneration, and Defeat," in *The Russian Military: Power and Policy*, edited by Steven E. Miller and Dmitri Trenin. Cambridge, MA: The MIT Press, 2004.

Bakir, Vian. "Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting." *Frontiers in Communication* 5, no. 67 (September 2020).

Bardollar, Gil. "The Best of Both Worlds? Russia's Mixed Military Manpower System." *Center for Strategic & International Studies*. 23 September 2020. https://www.csis.org/blogs/post-soviet-post/best-or-worst-both-worlds

Bartles, Charles K. "Russian Combined Arms Armies Plan Electronic Warfare Battalions," Foreign Military Studies Office, *OE Watch* 8, no. 11 (November 2018).

Bay, Sebastian and Nora Biteniece. *The Current Digital Arena and its Risks to Serving Military Personnel*. Riga, Latvia: NATO StratCom Center of Excellence, 2019.

Beehner, Lionel, Liam Collins, Steve Ferenzi, Robert Person, and Aaron Brantly. *Analyzing the Russian Way of War: Evidence from the 2008 Conflict with Georgia*. West Point, NY: Modern War Institute at West Point. 2018.

Bendett, Samuel. "Strength in Numbers: Russia and the Future of Drone Swarms." *Modern War Institute at West Point*, 20 April 2021. https://mwi.usma.edu/strength-in-numbers-russia-and-the-future-of-drone-swarms/

Bendett, Samuel, Mathieu Boulegue, Richard Connolly, Margarita Konaev, Pavel Podwig, and Katarzyna Zysk. *Advanced Military Technology in Russia: Capabilities and Implications*. London, UK: Chatham House, 2021. https://www.chathamhouse.org/2021/09/advanced-military-technology-russia/03-putins-super-weapons

Bowen, Andrew S. *Russian Armed Forces: Military Modernization and Reforms*. CRS Report No. IF11603. Washington, DC: Congressional Research Service, 2020. https://crsreports.congress.gov/product/pdf/IF/IF11603

Boyte, K.J. "An Analysis of the Social-Media Technology, Tactics, and Narratives Used to Control Perception in the Propaganda War Over Ukraine." *Journal of Information Warfare* 16, no. 1 (Winter 2017): 88–111.

Brantly, Aaron. "From the Foxhole: Cyber and Kinetic Conflict in Ukraine." *The Cyber Defense Review* 7, no. 2 (Spring 2022): 1–5.

Brantly, Aaron, Nerea Cal, and Devlin Winkelstein. *Defending The Borderland: Ukrainian Military Experiences with IO, Cyber, and EW*. West Point, NY: The Army Cyber Institute, 2017.

Brose, Christian. *The Kill Chain: Defending America in the Future of High-Tech Warfare*. New York: The Hachette Group, 2020.

Bumiller, Elisabeth and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." *The New York Times*. 11 October 2012.

Carruthers, Susan. *The Media at War*. 2nd Edition. New York: Palgrave MacMillan, 2011.

Clark, Bryan. "The Fall and Rise of Russian Electronic Warfare." *IEEE Spectrum*. 30 July 2022. https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare

Clark, Colin. "Russia Widens EW War, 'Disabling' AC-130s in Syria." Breaking Defense. 24 April 2018. https://breakingdefense.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/

Clark, Mason. *The Russian Military's Lessons Learned in Syria: Military Learning and the Future of War Series*. Washington, DC: Institute for the Study of War, 2021.

Clark, Mason. *Russian Hybrid Warfare: Military Learning and the Future of War Series.* Washington, DC: Institute for the Study of War, 2020.

Clark, Mason and George Barros. "Russia's Zapad-2021 Exercise." *Institute for the Study of War*, 17 September 2021. https://www.understandingwar.org/backgrounder/russia%E2%80%99s-zapad-2021-exercise

Clausewitz, Carl von. *On War*, edited and translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

Clena, Luke. "Technical Signature Management for Small Units." *Marine Corps Gazette* 105, no. 5 (May 2021): 32–4.

Cleveland, Charles, Benjamin Jensen, Susan Bryant, and Arnel David. *Military Strategy in the 21st Century: People, Connectivity, and Competition*. New York: Cambria Press, 2018.

Collins, Liam and Harrison Morgan, "King of Battle: Russia Breaks Out the Big Guns." *Army,* (February 2019).

Copp, Tara. "It Failed Miserably: After Wargaming Loss, Joint Chiefs are Overhauling How the U.S. Military Will Fight." *Defense One*. 26 July 2021. https://www.defenseone.com/policy/2021/07/it-failed-miserably-after-wargaming-loss-joint-chiefs-are-overhauling-how-us-military-will-fight/184050/

Dawson, Jessica. "Microtargeting as Information Warfare." *The Cyber Defense Review* 6, no. 1, (Winter 2021): 63–76.

Dawson, Jessica, and Todd Arnold. "Eroding America from Within, Marketing Data threatens Military Cohesion." *C4ISRNET*. 15 February 2021. https://www.c4isrnet.com/opinion/2021/02/15/eroding-america-from-within-marketing-data-threatens-military-cohesion/

Deibert, Ronald, Rafal Rohozinski, and Masashi Crete-Nishihata. "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russa-Georgia War." *Security Dialogue* 43, no. 1 (February 2012): 3–24.

DePuy, William E. “Implications of the Middle East War on U.S. Army Tactics, Doctrine and Systems,” in *Selected Papers of General William E. DePuy*, edited by Donald L. Gilmore and Carolyn D. Conway. Fort Leavenworth, KS: U.S. Army Combat Studies Institute, 1995.

Dostoyevsky, Fyodor. *The Brothers Karamazov*, trans. Constance Garnett. London, UK: William Heinemann Ltd, 1959.

Episkopos, Mark. “Zapad: Russia Wants to be Ready for a War with NATO.” *The National Interest*. 21 September 2021. https://nationalinterest.org/blog/buzz/zapad-russia-wants-be-ready-war-nato-193859

Eversden, Andrew. “A Warning to DOD: Russia Advances Quicker than Expected on AI, Battlefield Tech.” *C4ISRNET*. 24 May 2021. https://www.c4isrnet.com/artificial-intelligence/2021/05/24/a-warning-to-dod-russia-advances-quicker-than-expected-on-ai-battlefield-tech/

Eversden, Andrew and Jaspreet Gil. “Why Hasn’t Russia used its Full Scope of Electronic Warfare?” *Breaking Defense*. 28 March 2022. https://breakingdefense.com/2022/03/why-hasnt-russia-used-its-full-scope-of-electronic-warfare

Facon, Isabelle. “Proliferated Drones: A Perspective on Russia.” *The Center for A New American Security*. 12 May 2016. http://drones.cnas.org/reports/a-perspective-on-russia/

Fitzgerald, Mary C. “The Soviet Military and the New ‘Technological Operation’ in the Gulf.” *Naval War College Review* 44, no. 4 (Autumn 1991): 16–43.

Flake, Lincoln. “Russia and Information Warfare: A Whole of Society Approach.” *Lithuanian Annual Strategic Review* 18, no. 7 (May 2020): 163–75.

Fox, Amos C. and Andrew J. Rossow. “Making Sense of Russian Hybrid Warfare: A Brief Assessment of the Russo-Ukrainian War.” *Association of the United States Army Institute of Land Warfare*, Land Warfare Paper No. 112, (March 2017).

Fox, Amos C. “Reflections on Russia’s 2022 Invasion of Ukraine: Combined Arms Warfare, the Battalion Tactical Group, and Wars in a Fishbowl.” *Association of the United States Army Institute of Land Warfare*, Land Warfare Paper No. 149, (September 2022).

Freedberg Jr., Sydney J. “U.S. Has Lost ‘Dominance in Electromagnetic Spectrum’: Shaffer.” *Breaking Defense*, 3 September 2014. https://breakingdefense.com/2014/09/us-has-lost-dominance-in-electromagnetic-spectrum-shaffer/

Freedberg Jr., Sydney. "No More Iron Mountains: Lighter Logistics Key to Multi-Domain Battle." *Breaking Defense*, 3 May 2017. https://breakingdefense.com/2017/05/no-more-iron-mountains-streamlined-logistics-key-to-multi-domain-battle/

Freeman, Suzanne B., and Katherine Kjellstrom Elgin. "What the Use of Russian Conscripts Tells Us About the War in Ukraine." *Politico Europe.* 17 March 2022. https://www.politico.eu/article/what-the-use-of-russia-conscripts-tells-us-about-the-war-in-ukraine/

Gaelotti, Mark. "Hybrid, Ambiguous, and Non-Linear? How New is Russia's New Way of War?" *Small Wars and Insurgencies* 27, no. 2 (2016)

Gaelotti, Mark. "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/

Giles, Keir. "Assessing Russia's Reorganized and Rearmed Military." Task Force White Paper, Carnegie Endowment for International Peace, 3 May 2017.

Giles, Keir. *Handbook of Russian Information Warfare*. Rome: NATO Defense College, 2016.

Giles, Keir. *The Next Phase of Russian Information Warfare*. Riga: NATO Strategic Communications Center of Excellence, 2016.

Glantz, David. "The Red Mask: The Nature and Legacy of Soviet Military Deception in the Second World War." *Intelligence and National Security* 2, no. 3 (1987).

Goldman, Emily and John Arquilla. *Cyber Analogies*. Report Number NPS-DA-14-001. Monterey, CA: Naval Postgraduate School, 2014.

Gomez, Don. "Canceled in Combat: Get Ready for Smear War." *Proceedings* 147, no. 6, (June 2021).

Gomza, Ivan. "Hubris of Mars: Insights on the Russo-Ukrainian War from Cases of Great Powers' Oversights." *Krytyka*, October 2022. https://krytyka.com/en/articles/hubris-of-mars-insights-on-the-russo-ukrainian-war-from-cases-of-great-powers-oversights

Grau, Lester and Charles K. Bartles. *The Russian Way of War: Force Structure, Tactics and Modernization of the Russian Ground Forces*. Fort Leavenworth, KS: U.S. Army TRADOC Foreign Military Studies Office, 2016.

Grau, Lester and Chuck Bartles. "Integration of Unmanned Aerial Systems Within Russian Artillery," *Fires Bulletin: A Joint Publication for U.S. Artillery Professionals*, (July-August 2016).

Grau, Lester and Charles Bartles. *The Russian Reconnaissance Fire Complex Comes of Age*. Oxford, UK: Oxford University Changing Character of War Centre, 2018.

Grisé, Michelle. *Rivalry in the Information Sphere: Russian Concepts of Information Confrontation*. RRA-198-8. Santa Monica, CA: RAND, 2022.

Hambling, David. "Ukraine's Bayraktar Drone Helped Sink Russian Flagship Moskva." *Forbes*. 14 April 2023. https://www.forbes.com/sites/davidhambling/2022/04/14/ukraines-bayraktar-drones-helped-destroy-russian-flagship/?sh=75f6d5c33a7a

Hauffe, Justin. "Don't Believe Your Eyes." *Proceedings* 147, no. 8 (August 2021).

Helmus, Todd. *Artificial Intelligence, Deepfakes, and Disinformation: A Primer*. PEA1043-1. Santa Monica, CA: RAND Corp., 2022.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, 6 January 2011. https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008

Hsu, Jeremy. "The Strava Heat Map and the End of Secrets." *Wired*. 29 January 2018. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy

Jasper, Scott. *Russian Cyber Operations: Coding the Boundaries of Conflict.* Washington: Georgetown University Press, 2020.

Janes. "Borisoglebsk-2 Electronic Warfare Complex/" 5 July 2021. https://customer.janes.com/Janes/Display/JC4IL0693-JC4IL

Janes. "Krasukha Series Radar Jammers." 25 February 2022. https://customer.janes.com/Janes/Display/JC4IL0650-JC4IL

Janes. "Leer-3 Electronic Warfare System." 2 May 2022. https://customer.janes.com/Janes/Display/JC4IA0399-JC4IA

Janes. "Murmansk-BN Electronic Warfare System." 17 June 2022. https://customer.janes.com/Janes/Display/JC4IL1084-JC4IL

Johnson, David. "Would We Do Better? Hubris and Validation in Ukraine." *War on the Rocks*, 31 May 2022. https://warontherocks.com/2022/05/would-we-do-better-hubris-and-validation-in-ukraine/

Johnson, Rob. "Dysfunctional Warfare: The Russian Invasion of Ukraine." *Parameters* 52, no. 2 (Summer 2022): 5–20.

Joint Chiefs of Staff. *Joint Air Operations*. JP 3-30. Washington, DC: Joint Chiefs of Staff, 2021. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf

Joint Chiefs of Staff. *Joint Electromagnetic Spectrum Operations.* JP 3-85. Washington, DC: Joint Chiefs of Staff, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf

Joint Chiefs of Staff. *Information in Joint Operations.* JP 3-04. Washington, DC: Joint Chiefs of Staff, 2022.

Jones, Seth. "Russian Success in Syria: Will it Be a Pyrrhic Victory?" *CTC Sentinel* 12, no. 9 (October 2019): 1–9.

Jonsson, Oscar. *The Russian Understanding of War: Blurring the Lines Between War and Peace*. Washington: Georgetown University Press, 2019.

Kahn, David. *Hitler's Spies: German Military Intelligence in World War II*. New York: Macmillan, 1978.

Kapusta, Philip. "The Grey Zone." *Special Warfare* 28, no. 4 (October 2015): 18–26.

Karber, Philip A. *Lessons Learned from the Russo-Ukrainian War: Personal Observations*. Prepared for Historical Lessons Learned Workshop, Johns Hopkins Applied Physics Laboratory and U.S. Army Capabilities Center. (6 July 2015).

Kallberg, Jan. "Why the Military Must Defend the Spectrum." *C4ISRNET*. 13 April 2015. https://www.c4isrnet.com/opinion/the-compass/net-defense-blogs/2015/04/13/kallberg-why-the-military-must-defend-the-spectrum/

Kallenborn, Zachary. "InfoSwarms: Drone Swarms and Information Warfare." *Parameters* 2, no. 52 (Summer 2022): 87–102.

Kjellen, Jonas. *Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces*. Report Number FOI-R-4625-SE. Stockholm: Swedish Defense Research Agency, 2018.

Kofman, Michael. "Syria and the Russian Armed Forces: An Evaluation of Moscow's Military Strategy and Operational Performance." in *Russia's War in Syria: Assessing Russian Military Capabilities and Lessons Learned*, edited by Robert E. Hamilton, Chris Miller, and Aaron Stein, 35–65. Philadelphia, PA: Foreign Policy Research Institute, 2020.

Kokobobo, Ani. "How Should Dostoevsky and Tolstoy be read during Russia's war against Ukraine?" *The Conversation*, 6 April 2022. https://theconversation.com/how-should-dostoevsky-and-tolstoy-be-read-during-russias-war-against-ukraine-179932

Krombholz, Katharina, Heidelinde Hobel, Markus Huber, and Edgar Weippl. "Advanced Social Engineering Attacks." *Journal of Information Security and Applications* 22 (June 2015): 113–122.

Krulak, Victor. “The Strategic Corporal: Leadership in the Three Block War.” *Marine Corps Gazette* 83, no. 1 (January 1999): 18–23.

Kuzio, Taras. “Old Wine in a New Bottle: Russia’s Modernization of Traditional Soviet Information Warfare and Active Policies Against Ukraine and Ukrainians.” *The Journal of Slavic Military Studies* 32, no. 4 (Winter 2019): 485–506.

Lannon, Gregory P. “Russia’s New Look Army Reforms and Russian Foreign Policy.” *The Journal of Slavic Military Studies* 24, no. 1 (Winter 2011): 26–54.

Lapaiev, Yuri. “EW Hype? The Reasons Behind the Limited Effectiveness of Russia’s Electronic Warfare in Ukraine.” *Eurasia Daily Monitor* 19, no. 51 (April 2022).

Lapowsky, Issie. “NATO Group Catfished Soldiers to Prove a Point About Privacy.” 18 February 2019. *Wired*. https://www.wired.com/story/nato-stratcom-catfished-soldiers-social-media/

Lonergan, Erica D., and Brandon Valeriano. “Putin’s Invasion of Ukraine Didn’t Rely on Cyberwarfare. Here’s Why.” *The Washington Post.* 7 March 2022. ProQuest.

Luzin, Pavel. *Electronic Warfare: Russia’s Approach*. Philadelphia, PA: The Foreign Policy Research Institute, 2022. https://www.fpri.org/article/2022/02/electronic-warfare-russias-approach/

Makichuk, Dave. “Lessons Learned from the Battle of Ukraine.” *Asia Times*. 31 October 2019. https://asiatimes.com/2019/11/lessons-learned-from-the-battle-of-ukraine/

Matthews, Jay. “Vehicle of Vincennes Skipper’s Wife Bombed.” *The Washington Post*, 11 March 1989. ProQuest.

Micallef, Joseph V. “Russian Harassment of NATO Personnel, Families: The Next Chapter in Information Warfare?,” *Military.com,* 3 September 2019. https://www.military.com/daily-news/2019/09/03/russian-harassment-nato-personnel-families-next-chapter-information-warfare.html

Minich, Ruslan. “Russia Shows its Military Might in the Black Sea and Beyond.” *Atlantic Council*. 6 November 2018. https://www.atlanticcouncil.org/blogs/ukrainealert/russia-shows-its-military-might-in-the-black-sea-and-beyond/

McCrory, Duncan. “Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States.” *The RU.S.I Journal* 165, no. 7, (Winter 2021): 34–44.

McDermott, Roger. “Does Russia Have a Gerasimov Doctrine?” *Parameters* 4, no, 1 (Spring 2016).

McDermott, Roger. *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*. Tallin: International Center for Defense and Security, Republic of Estonia Ministry of Defense, 2017.

McDermott, Roger. *Russia's Path to the High-Tech Battlespace*. Washington, DC: The Jamestown Foundation, 2022.

McDermott, Roger N. "Russia's Electronic Warfare Capabilities as a Threat to GPS." *Eurasia Daily Monitor* 18, no. 40 (March 2021).

McDermott, Roger N. "Russia's Armed Forces Enhance UAV Strike Capability." *The Eurasia Daily Monitor* 18, no. 148 (Fall 2021).

McDermott, Roger N. *Russia's Perspectives on Network Centric Warfare: The Key Aim of Serdyukov's Reform*. Ft. Leavenworth, KS: Foreign Military Studies Office, 2011.

McDermott, Roger N. "Russian UAV Technology and Loitering Munitions." *The Eurasia Daily Monitor* 18, no, 72 (May 2021).

McDermott, Roger N., Bertil Nygren, and Carolina Vendil Pallin, eds. *The Russian Armed Forces in Transition: Economic, Geopolitical, and Institutional Uncertainties*. New York: Routledge, 2012.

McGeehan, Timothy. "Web Storm Rising." *Proceedings* 148, no. 3 (March 2022).

McLeary, "Report: Russia's Winning the Electronic War." *Foreign Policy*. 21 October 2015. https://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/

McLuhan, Marshall. *Culture Is Our Business*. Eugene, OR: Wipf and Stock Publishers, 1970.

McMaster, H.R. *Battlegrounds: The Fight to Defend the Free World*. New York: Harper Collins, 2020.

Nadimi, Farzin. "Iranian Drones to Russia: Capabilities and Limitations," *The Washington Institute for Near East Policy*. 1 August 2022. https://www.washingtoninstitute.org/policy-analysis/iranian-drones-russia-capabilities-and-limitations

Nechepurenko, Ivan. "Russia Votes to Ban Smartphone Use by Military, Trying to Hide Digital Traces." *The New York Times*. 19 February 2019. ProQuest.

Newdick, Thomas. "Russia Provides a Glimpse of Its Orion Drone Executing Combat Trials in Syria." *The Drive*. 22 February 2021. https://www.thedrive.com/the-war-zone/39381/russia-provides-a-glimpse-of-its-orion-drone-executing-combat-trials-in-syria

Odell, Kate Bachelder. “If War Comes, Will the U.S Navy Be Prepared?” *The Wall Street Journal*. 1 July 2021.

Oliker, Olga. *Russia’s Chechen Wars 1994–2000: Lessons from Urban Combat*. Report Number MR-1289. Santa Monica, CA: RAND, 2001.

Őze, Zoltán. “Special Features of the Russian-Ukrainian Armed Conflict,” *Hadmérnök* 15, no. 1 (May 2020).

Ozkarasahin, Sine. “Can Iranian Drones Respond to Putin’s Call for Help?” *Eurasia Daily Monitor* 19, no. 112 (July 2022)

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

Pernik, Piret. *Hacking for Influence: Foreign Influence Activities and Cyber-Attacks.* Tallinn, International Center for Defense and Security, 2018.

Petersen, Nolan. “Ukraine’s Old School Answers to Russia’s Modern Electronic Warfare Weapons.” *Coffee or Die*. 7 February 2022. https://www.coffeeordie.com/ukraine-russia-electronic-warfare

Pomerleau, Mark. “U.S. is ‘outgunned’ in electronic warfare, says cyber commander.” *C4ISRNET*. 10 August 2017. https://www.c4isrnet.com/show-reporter/technet-augusta/2017/08/10/us-is-outgunned-in-electronic-warfare-says-cyber-commander/

Quadri, Sami. “Former U.S. Ambassador says Russia is Using Deepfakes to Impersonate him.” *The Evening Standard*. 1 October 2022. https://www.standard.co.uk/news/world/michael-mcfaul-ambassador-ukraine-russia-deepfakes-war-b1029502.html

Renz, Bettina. *Russia’s Military Revival*. Cambridge, UK: Polity Press, 2018.

Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar Straus and Giroux, 2020.

Rogers, Will and Sharon Rogers. *Storm Center: The USS Vincennes and Iran Air Flight 655*. Newport, RI: Naval Institute Press, 1992.

Rosen, Kenneth. “Kill Your Commanding Officer: On the Front Lines of Putin’s Digital War With Ukraine.” *Politico Magazine.* 15 February 2022.

Russian General Staff. *The Soviet Afghan War: How a Superpower Fought and Lost*. Translated and edited by Lester Grau and Michael Gress. Lawrence, KS: University Press of Kansas, 2002.

Sun Tzu. *The Art of War.* Edited by James Clavell. New York: Dell Publishing, 1983.

Sambaluk, Nicholas Michael. *Weaponizing Cyberspace: Inside Russia's Hostile Activities*. Santa Barbara, CA: Praeger Security International, 2022.

Satter, Raphael and Dmytro Vlasov. "Ukraine Soldiers Bombarded by 'Pinpoint Propaganda' Texts." *The Associated Press*. 11 May 2017.

Schogol, Jeff. "Russian Troops are Proving that Cell Phones in War Zones are a Very Bad Idea." *Task & Purpose*. 13 May 2022. https://taskandpurpose.com/news/russia-ukraine-cell-phones-track-combat/

Scott, Richard. "Tuning In, Turning On: Russia Brings Radio Electronic Combat to the Fore." *Journal of Electromagnetic Dominance* 43, no. 11 (December 2020).

Seely, Robert. "Defining Contemporary Russian Information Warfare." *The RUSI Journal* 162, no. 1 (Spring 2017).

Seib, Philip. *Information at War: Journalism, Disinformation, and Modern Warfare.* Cambridge, UK: Polity Press, 2021.

Seligman, Laura. "Huge Problem: Iranian Drones Pose New Threat to Ukraine." *Politico*. 26 September 2022. ProQuest.

Sergey Sukhankin. "Blind, Confuse, Demoralize: Russian Electronic Warfare Operations in Donbas." *The Jamestown Foundation.* 27 August 2021. https://jamestown.org/program/blind-confuse-and-demoralize-russian-electronic-warfare-operations-in-donbas/

Shallcross, N.J. "Social Media and Information Operations in the 21st Century." *Journal of Information Warfare* 16, no. 1 (Winter 2017): 1–12.

Shore, Zachary. *Blunder: Why Smart People Make Bad Decisions*. New York, NY: Bloomsbury, 2008.

Shultz, Terri. "Russia is Hacking and Harassing NATO Soldiers, report says." *Deutche Welle News,* 10 June 2017. https://www.dw.com/en/russia-is-hacking-and-harassing-nato-soldiers-report-says/a-40827197

Singer, P.W and Emerson T. Brooking. *LikeWar: The Weaponization of Social Media*. Boston, MA: First Mariner Books, 2019.

Sprengel, Frank Christian. *Drones in Hybrid Warfare: Lessons From Current Battlefields.* Hybrid CoE Working Paper 10. Helsinki: The European Centre of Excellence for Countering Hybrid Threats, 2021.

Stoner, Kathryn E. *Russia Resurrected: Its Power and Purpose in a New Global Order.* New York: Oxford University Press, 2021.

Szwed, Robert. *Framing of the Ukraine-Russia Conflict in Online and Social Media*. Riga: NATO Communications Center of Excellence, 2016.

Thayer, Joel. "TikTok Is Fun and Games Until China Wants Your Info." *The Wall Street Journal*. 22 July 2022.

Theohary, Catherine. *Defense Primer: Information Operations*. CRS Report No. IF10771. Washington, DC: Congressional Research Service, 2020. https://crsreports.congress.gov/product/pdf/IF/IF10771/8

Thomas, Timothy. "The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia." *Journal of Slavic Military Studies* 22, (2009): 31–67.

Thomas, Timothy. *Russia's Electronic Warfare Force: Blending Concepts with Capabilities*. Report Number 19–2714. McLean, VA: MITRE Center for Technology and National Security, 2020.

Thomas, Timothy. *Advanced Weaponry and Russian Military Art of War*. Report Number 20–1890. McLean, VA: MITRE Center for Technology and National Security, 2020.

Thomas, Timothy. *Russian Electronic, Information, Navigation, and Reconnaissance Strike and Fire Operations: Definitions and Use*. Report Number 20–3186. McLean, VA: MITRE Center for Technology and National Security, 2020.

Thomas, Timothy. "Russian Forecasts of Future War." *Military Review* (May-June 2019): 84–93.

Trenin, Dmitri. "The Revival of the Russian Military: How Moscow Reloaded." *Foreign Affairs* 95, no. 3 (May-June 2016): 23–9.

Trevithick, Joseph. "Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio Virus." *The Drive*. 30 October 2019. https://www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics-including-radio-virus

Turunen, Andreas. "The Broader Challenge of Russian Electronic Warfare Capabilities," in *Improvisation and Adaptability in the Russian Military: A Report of the CSIS Russia and Eurasia Program,* edited by Jeffrey Mankoff, 13–21. Washington, D.C: Center for Strategic and International Studies, 2020.

Unwala, Azhar and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict." *Military Cyber Affairs* 1, no. 1 (2015).

Urcosta, Ridvan Bari. “The Revolution in Drone Warfare: The Lessons from the Idlib De-Escalation Zone.” *The Air Force Journal of European, Middle Eastern, and African Affairs* 2, no. 3. (August 2020).

Valeriano, Brandon, Benjamin Jensen and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion*. Cambridge: Oxford University Press, 2018.

Watling, Jack. “Just How Tall are Russian Soldiers?” *The RUSI Journal* 24, (March 2022).

Westwood, James T. “Soviet Electronic Warfare: Theory and Practice,” *Jane’s Soviet Intelligence Review* 1, no. 9 (September 1989).

White, Emily Baker. “Leaked Audio from 80 Internal TikTok Meetings Shows That U.S. User Data Has Been Repeatedly Accessed from China.” *BuzzFeed News*, 17 June 2022. https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access

White, Sarah P. *Understanding Cyberwarfare: Lessons From the Russia-Georgia War*. West Point, NY: Modern War Institute at West Point, 2018.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California