Limits of Decentralization: Streamlining the Dispersed Parts of the Information Whole

A Monograph

by

MAJ Ryan B. Min
US Army

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

2018

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
05-25-2018	Master's Thesis	JUN 2017 - MAY 2018

4. TITLE AND SUBTITLE
Limits of Decentralization: Streamlining the Dispersed Parts of the Information Whole

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
MAJ Ryan B. Min

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Advanced Military Studies Program / School of Advanced Military Studies

10. SPONSOR/MONITOR'S ACRONYM(S)

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

When the US Joint Staff introduced information as the newly incorporated Joint Function in 2017, it was a clear indication that the US military was aware of critical changes taking place within the contemporary operational environment. However, despite this recognition, the US military continues to disaggregate its information capabilities. This monograph argues that the US military must revisit and revise its current methods of dividing information into separate conduit and content-oriented fields. Specifically, this paper argues for the centralization of information operations task organizations in two ways. First, the information-related officer must be given command authority over all information related capabilities, in order to successfully synchronize and coordinate them. Second, the overall structure of information organization in the US military should be reworked so that both content and conduit are represented at the level of a combatant command. In juxtaposition to the current US construct, this monograph examines a case study of Russia's holistic organization of information, and notes how such a system of organizations could offer advantages to the United States.

15. SUBJECT TERMS
Information warfare; information operations; Russian information warfare; information content; information system; information revolution; organizational theory; organizational function; centralization; decentralization; departmentalization; decision-making; organizational structure; organizational hierarchy; organizational change; reorganization; streamlining organizations

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			MAJ Ryan B. Min
(U)	(U)	(U)	(U)	53	**19b. TELEPHONE NUMBER** *(Include area code)* 913-758-3300

Reset

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

Monograph Approval Page

Name of Candidate: MAJ Ryan B. Min

Monograph Title: Limits of Decentralization: Streamlining the Dispersed Parts of the Information Whole

Approved by:

_____, Monograph Director
Patricia J. Blocksome, PhD

_____, Seminar Leader
James M. DePolo, COL

_____, Director, School of Advanced Military Studies
James C. Markert, COL

Accepted this 24th day of May 2018 by:

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

Abstract

Limits of Decentralization: Streamlining the Dispersed Parts of the Information Whole, by MAJ Ryan B. Min, US Army, 53 pages.

When the US Joint Staff introduced information as the newly incorporated Joint Function in 2017, it was a clear indication that the US military was aware of critical changes taking place within the contemporary operational environment. However, despite this recognition, the US military continues to disaggregate its information capabilities. This monograph argues that the US military must revisit and revise its current methods of dividing information into separate conduit and content-oriented fields. Specifically, this paper argues for the centralization of information operations task organizations in two ways. First, the information-related officer must be given command authority over all information related capabilities, in order to successfully synchronize and coordinate them. Second, the overall structure of information organization in the US military should be reworked so that both content and conduit are represented at the level of a combatant command. In juxtaposition to the current US construct, this monograph examines a case study of Russia's holistic organization of information, and notes how such a system of organizations could offer advantages to the United States.

Contents

Acknowledgements

This monograph would not have been possible without the scrutinizing detail of Professor Misha Blocksome, who consistently maintained my writer's spirit despite its persistent block. I am also indebted to Colonel J. Michael DePolo for his continued support, as he instilled in me the professional guidance and perspective necessary for seeing through my research and writing. Both were critical to making this monograph. I also want to thank Lieutenant Colonel Amy Burrows and Ms. Monique Guerrero of Command and General Staff College for their insight and energy in directing my initial steps in this elusive search regarding 'information.' Lieutenant Colonel Burrows especially was a hub of historical organizational knowledge, which shaped much of my thinking concerning optimizing structure for the potential of the future. I would also like to thank the US Army Information Operations Proponent office here at Ft. Leavenworth for their hospitality despite my abrupt visit; this includes Dr. Robert Hill, Lieutenant Colonel Annie Pruitt, and Mr. Bob Meier. And last, but certainly not the least, I am indebted to my wife Mary for persevering through another one of my Army antics, overlooking my endless shortcomings, absenteeism—both in mind and body—and the neglect, which could not have been forgivable under any circumstance, but it was. She remains a testament to all things that represent the good of our Army families, that present, that quiet, and stoic with a heart. And to my children the ungrateful, I take the long view in investment.

Acronyms

ADP	Army Doctrine Publication
ADRP	Army Doctrine Reference Publication
ARCYBER	US Army Cyberspace Command
C2W	Command and Control Warfare
CNE	Cyberspace Network Exploitation
CNO	Cyberspace Network Operations
CO	Cyberspace Operations
COMCAM	Combat Camera
DARPA	Defense Advanced Research Projects Agency
DCO	Defensive Cyberspace Operations
DoD	Department of Defense
DoS	Department of State
DSB	Defense Science Board
EW	Electronic Warfare
FCC	Functional Combatant Command
FM	Field Manual
FMSO	Foreign Military Studies Office
IC	US Intelligence Community
ICT	Information Computer Technology
IO	Information Operations
IOWG	Information Operations Working Group
IRC	Information Related Capabilities
JP	Joint Publication
MILDEC	Military Deception
NCW	Network Centric Warfare

NSA	National Security Agency
OCO	Offensive Cyberspace Operations
PA	Public Affairs
PDD	Presidential Decision Directive
PO	Psychological Operations
SOC	Russian Special Operations Command
SOF	Special Operations Forces
UCC	Unified Combatant Command
USASOC	US Army Special Operations Command
USCYBERCOM	US Cyberspace Command
USSOCOM	US Special Operations Command
USSR	Union of Soviet Socialist Republics
USTRANSCOM	US Transportation Command
USG	United States Government

Introduction: Seventh Joint Function

On July 2017, the US Department of Defense's (DoD) Joint Staff published an update to its Joint Publication 1 (JP 1), *Doctrine for the Armed Forces of the United States*, where it presented 'Information' as a newly incorporated Joint Function, alongside traditional Joint Functions of 'Command and Control,' 'Intelligence,' 'Fires,' 'Movement and Maneuver,' 'Protection,' and 'Sustainment'.[1] While it will take time for the various subordinate military services, such as the US Army, to consider changes to their own corresponding Warfighting Functions, there is little doubt that the US military recognizes the evolving role of information in 21st century conflict.

However, information as a functional variable in military operations has consistently served as an enigma. Even within the construct of the D-I-M-E framework (Diplomacy-Information-Military-Economic), military researchers have found it challenging to quantitatively determine the value of information vis-à-vis more tangible variables such as diplomacy, military and economy.[2] Furthermore, the current operational environment has undoubtedly given new meaning to the role of information within the study of warfare. The rise of Russian military operations in the Balkans and the Baltics serve as an indicator of what may further come; and one cannot discount the evolution of the Russian state and its military in adapting their use of information since the early 2000s, leading to their full-blown invasion of Ukraine in 2014.[3]

---

[1] US Joint Chiefs of Staff, Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: US Joint Chiefs of Staff, 2017).

[2] Ibid., I-12 to I-14.

[3] Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations* (Washington, DC: US Defense Intelligence Agency, 2017); Keir Giles, *Assessing Russia's Reorganized and Rearmed Military*, Task Force on US Policy Toward Russia, Ukraine, and Eurasia (New York, NY: Carnegie Endowment for International Peace, 2017), accessed November 30, 2017, http://carnegieendowment.org/files/5.4.2017_Keir_Giles_RussiaMilitary.pdf; Maksymilian Czuperski Czuperski John Herbst, Eliot Higgins, Alina Polyakova, and Damon et al., *Hiding in Plain Sight: Putin's War in Ukraine* (Washington, DC: Atlantic Council, 2015), accessed December 30, 2017, http://www.atlanticcouncil.org/publications/reports/hiding-in-plain-sight-putin-s-war-in-ukraine-and-boris-nemtsov-s-putin-war; Maria Snegovaya, *Putin's Information Warfare in Ukraine*, Russia Report (Washington, DC: Institute for the Study of War, September 2015); Timothy Thomas, "Russia's Military

Russia's graduated military engagements offer an understanding of information's potential to be further integrated in a creative manner in military operations. Thus, information looks poised to play a greater role in the future of warfare in the 21st century. The recent change to Joint Publication 1 demands a reinvestigation of how modern militaries understand the future of information warfare, and what their own roles will be in such a future. In order to respond to such emergent changes in the global information environment, the US military faces the tasks of revisiting and analyzing the structure of its current organizational framework designed to take on that task of information.

DoD officially established US Cyberspace Command (USCYBERCOM) in 2010 in anticipation of its role in America's future in the operational environment.[4] Then, in 2017, they elevated USCYBERCOM to the level of a functional component command (FCC), further investing in the organization's expansion and readiness capability.[5] As a FCC, USCYBERCOM

Strategy and Ukraine: Indirect, Asymmetric—and Putin-Led," *The Journal of Slavic Military Studies* 28, no. 3 (July 3, 2015): 445–461; Jolanta Darczewska, *The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study*, Point of View (Warsaw, Poland: Center for Eastern Studies, May 2014), accessed October 7, 2017, https://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study.

[4] US Department of Defense, "DoD Announces First U.S. Cyber Command and First U.S. CYBERCOM Commander" (US Department of Defense, May 21, 2010), accessed September 27, 2017, http://archive.defense.gov/releases/release.aspx?releaseid=13551.

The origins of USCYBERCOM, however, date back to initial study groups led by DoD's Defense Science Board (DSB) under the Defense Advanced Research Projects Agency (DARPA). The initial research studies focused on defending computer networks. This focus primarily catered to DoD's Defense Information Security Agency, which focused on the protection of DoD signal communications systems. See US Department of Defense Science Board, *Information Warfare - Defense* (Washington, DC: Defense Science Board, November 1996); Leigh Armistead, ed., *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington, DC: Brassey's, 2004), 32–39; US Department of Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Defense Science Board, January 2013).

[5] US Joint Chiefs of Staff, JP 1, xvii-xviii, II-7, III-9 to III-12. FCC is a form of Unified Combatant Command, according to Joint Publication 1. FCCs provide a functional responsibility that traverses geographic boundaries, and often work in support of Geographic Combatant Commands, which are given traditional responsibility over a specified geographic area.

US Department of Defense, "DoD Initiates Elevation Process for U.S. Cyber Command to a Unified Combatant Command" (US Department of Defense, August 18, 2017), accessed October 27, 2017, https://www.defense.gov/News/News-Releases/News-Release-View/Article/1282920/dod-initiates-elevation-process-for-us-cyber-command-to-a-unified-combatant-com/; US Department of Defense, "Cyber Command Flexes New Acquisition Muscle" (US Department of Defense, October 12, 2017),

was able to rise to the national priority level of other combatant commands, such as US Special Operations Command (USSOCOM), US Strategic Command (USSTRATCOM), and US Transportation Command (USTRANSCOM).[6]

While this elevation to a FCC closely followed the recognition of the increased role of the cyberspace domain as a new battlespace of the future, the establishment and elevation of USCYBERCOM did not achieve a complete conceptualization of the whole of information warfare's future potential. As this monograph shows, USCYBERCOM's specific proclivity for technical innovation led it to inadvertently ignore the cognitive element of information and information warfare.[7] The rise of USCYBERCOM, with its focus on the means by which information is transmitted, limits the organization's ability to understand the full essence and potential of information warfare. Information warfare has traditionally been appreciated for the value of its content over the significance of its conduits. This monograph stresses that the technical emphasis advocated by USCYBERCOM leads to the neglect of support for the work of US forces undertaking message-focused and content-oriented information operations (IO). As long as current discussions concerning cyberspace operations exclude the prioritization of content over technical systems and means, DoD will miss the value of America's information warfare potential. This monograph focuses on potential ways that the US military can reorganize or

accessed October 27, 2017, https://www.defense.gov/News/Article/Article/1341201/cyber-command-flexes-new-acquisition-muscle/.

[6] Other FCCs include, US Special Operations Command (USSOCOM), US Strategic Command (USSTRATCOM), and US Transportation Command (USTRANSCOM). US Joint Chiefs of Staff, *JP 1*, xvii to xviii, II-7, III-9 to III-12.

[7] John Inglis et al., *Cyber-Enabled Information Operations* (Washington, DC: US Senate, 2017), accessed December 7, 2017, https://www.armed-services.senate.gov/hearings/17-04-27-cyber-enabled-information-operations; Rand Waltzman, *The Weaponization of Information, Testimony of Rand Waltzman* (Washington, DC: US Senate, 2017), accessed December 7, 2017, https://www.armed-services.senate.gov/hearings/17-04-27-cyber-enabled-information-operations; Rand Waltzman, "The U.S. Is Losing the Social Media War," *Time*, October 12, 2015, accessed December 7, 2017, http://time.com/4064698/social-media-propaganda/.

optimize itself in order to support the content, as well as the conduits, required for information warfare and its IO forces.

Literature Review

The general field of in IO literature within US defense industry and academia can be divided into the post-Cold War period and hybrid warfare phase.[8] While the post-Cold War period followed the end of the Cold War era in 1989, the new hybrid warfare phase begins in the mid-2000s, highlighted by Russia's intervention into Georgia and escalating with its invasion of Ukraine in 2014. Russia's use of IO in the annexation of the Crimean Peninsula, in particular, crystalized the importance of this type of information warfare threat in the eyes of Western democracies.[9]

Information Bifurcation

In its inception, the post-Cold War IO literature forecast a world full of new possibilities. It described future conflicts which took place within the growing digital landscape of the internet, a field that was experiencing continuous technological innovation. Nonetheless, amid this development, the literature remained too conceptual and abstract to envision a coherent path for

[8] While there are numerous studies that explore information warfare during the Cold War, this monograph focuses on security issues and context more appropriate to contemporary warfare. The advent of the information age includes rapid developments in information computer technologies. Much of this change accelerated after the Cold War in the 1990s, with massive acceleration of change in the 2000s.

[9] Michael Poznansky, "The Ordinary and Unique in Russia's Electoral Information Warfare Game," *War on the Rocks*, September 1, 2016, accessed July 20, 2017, https://warontherocks.com/2016/09/the-ordinary-and-unique-in-russias-electoral-information-warfare-game/; Maria Hellman and Charlotte Wagnsson, "How Can European States Respond to Russian Information Warfare? An Analytical Framework," *European Security* 26, no. 2 (March 1, 2017): 153–170; Keir Giles, "Countering Russian Information Operations in the Age of Social Media," *Council on Foreign Relations*, last modified November 21, 2017, accessed November 28, 2017, https://www.cfr.org/report/countering-russian-information-operations-age-social-media; Richard O. Hundley et al., eds., "Security in Cyberspace: Challenges for Society" (presented at the Security in Cyberspace: Challenges for Society, Santa Monica, CA: RAND Corporation, 1996).

future IO development worthy of military application. As the world wide web became further enmeshed in the everyday life of ordinary citizens, US defense industry analysts believed that there would be a progressively digitized security future which necessitated US adaptation towards computerized networks. While much of this cyber-focused digitization concept shaped DoD's focus on network-centric warfare (NCW), this literature primarily provided an appreciation of the technical aspects of the information environment. The research and analysis for NCW and information warfare focused on the futuristic elements of cyberspace as a technological revolution that would reshape future militaries in a technical sense, but failed to address in any depth the IO aspect of such NCW.

Two of the primary advocates of this future cyberwar movement were John Arquilla and David Ronfeldt, former defense analysts at the RAND Corporation. Beginning with their 1993 report, *Cyberwar is Coming*, Arquilla and Ronfeldt emphasized the changing nature of warfare brought on by the advent of the information age and propelled by the possibilities of the internet.[10] The authors theorized about future wars with particular emphasis on the decentralized network-orientation of military organizations as opposed to traditional hierarchies. In 1996, they followed suit with another RAND study, *The Advent of Netwar*, where the authors furthered their thesis by emphasizing the flattened topography of information in the contemporary age.[11] Arquilla and Ronfeldt argued that the diminished cost of attaining information had a direct impact on existing power relationships both between and within states. As information networks expanded further through a dispersed organization, the power dynamic in international relations inevitably shifted to take on new forms. This forewarning surrounding the changing nature of both domestic and international power predicted alternate ways of challenging traditional global

[10] John Arquilla and David F. Ronfeldt, *Cyberwar Is Coming* (Santa Monica, CA: RAND Corporation, 1993).

[11] John Arquilla and David F. Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND Corporation, 1996).

powers via asymmetric means. Then, in 1997, Arquilla and Ronfeldt encapsulated their progressing thesis in a collection of chapters, *In Athena's Camp: Preparing for Conflict in the Information Age*, where they argued for the end of traditional state power dynamics based on the substantial democratization of human access to information. The authors saw a level playing field of human knowledge accessible to a wider global audience, which would serve as an impetus for change in the nature of wars in the post-Cold War aftermath.[12]

Much of Arquilla and Ronfeldt's focus on the information revolution was at its core a vehicle for championing the revolutionary role of cyberspace in future wars within networks—*netwars*. The authors emphasized the centrality of digital '*infowars,'* the authors' term for IO, in the 21st century. The advent of technology in the post-Cold War era witnessed massive change in the speed of information acquisition. However, the increasing connectivity of the digital network space also made humans much more vulnerable to adversarial actors with malicious intent. Therefore, it was of critical priority for the United States to discuss and pave a future strategy that could provide protection in the newly created space of the digital domain.

Yet, Arquilla and Ronfeldt's focus was heavily geared towards the technological advancement of the information conduit system, as opposed to the psychological and cognitive impact of information. In sum, these two prominent researchers focused their attention on the improving technologies and digital networks that would lead to a future full of offensive cyberattacks by highly specialized computer hackers and programmers, who would be the future elite warriors in America's military. Nevertheless, this research offered little information on the content of such *infowars*

[12] John Arquilla and David F. Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND Corporation, 1997). Also see John Arquilla and David F. Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy* (Santa Monica, CA: RAND Corporation, 1999).

Aside from the persistent research taking place at the civilian-led RAND Corporation during the 1990s, DoD also focused on generating its own ideas regarding IO. One particular discussion of note came from US Army War College's 1999 conference entitled "The Information Revolution and National Security" at Carlyle, Pennsylvania.[13] The conference participants delved into the question of national security in the face of the changing security dynamic brought on by what they regarded as the era of the information age. Topics ranged from integrating IO into the military decision-making processes, studying the role of information during strategic nuclear deterrence, finding advantages in the neutral terrain of the open source public domain, and managing perceptions via strategic communications and signaling.[14] Yet, the most revealing aspect of the Army War College's discussion was the concluding remarks, where participants identified a need to clearly define a working concept for *information warfare* as a coherent response and strategy to the ongoing information revolution taking place in the post-Cold War environment. To the participants, the concept of information warfare would inevitably require the transformation of the military organizations in the immediate future.[15]

The participating scholars felt a need to fulfill a void in the state of US information warfare strategy. They recognized the need to advance offensive action within a more networked and digitally advanced information domain. Yet, the common fallback solution to many of their discussions relegated information warfare to a language of technological systems. Such a vernacular focused on targeting the adversary's central information nodes while securing the United States' own network systems. In doing so, the information warfare discussion

---

[13] Thomas E. Copeland, ed., *The Information Revolution and National Security* (Carlisle, PA: Strategic Studies Institute, US Army War College, 2000).

[14] Ibid. Armistead, *Information Operations*, 124-137.

[15] In 1996, the Office of the Undersecretary of Defense for Acquisition, Technology and Logistics produced a report on the state US internet infrastructure protection. While it was an earlier study of information warfare than the conference at US Army War College, the report remained focused on the information systems aspect of US infrastructure defense. See US Department of Defense, Defense Science Board, *Information Warfare - Defense* (Washington, DC: Defense Science Board, November 1996).

concentrated on achieving dominance in the new domain of cyberspace. While this appreciation of power and superiority vis-à-vis another competing state power was a contribution in and of itself, the manner in which the dialogue for dominating new domains in the post-Cold War era narrowed the participants' understanding of information warfare to achieving dominance in the information domain, similar to the dominance required in land, air and sea domains. [16] The implication was that the rise of the cyberspace domain would begin a new arms race of increased budgets against another state. Yet, such analysis ignored the unique aspects of information as a domain. Unlike traditional domains of air, land and sea, information traversed through all of these domains without a clear distinction as to its boundary of responsibility. By equating the cyberspace domain as the representative domain of information warfare, the discussion narrowed the understanding of information to the realm of technical systems. Therefore, the US Army War College's focus on cyberspace as the new domain to be dominated, relegated the concept of American information warfare and IO, to a digitized future database system divorced from the actual content such campaigns would require. This lack of discussion on information content meant that the US military continued seeking technical solutions to respond to cyberspace challenges.

Nonetheless, at the turn of the 21st century, this technical prioritization would begin to change, as the field of IO started to give more emphasis to the information message, and as hybrid warfare activities began to take place around the globe. Scholars in the United States began to focus on clarifying the nuances of IO by differentiating between a concept reliant on the systems one employed via technological advancements—such as the digitized internet—versus a concept centered on traditional understanding of information—such as thematic ideas and human cognition—which affected the thought processes of human audiences. This delineation between

[16] Also see Stuart J. D. Schwartzstein, ed., *The Information Revolution and National Security: Dimensions and Directions*, vol. 18, 3 vols., Significant Issues Series (Washington, DC: Center for Strategic and International Studies, 1996).

systems technology and content orientation became further pronounced in a 2004 book entitled *Information Operations: Warfare and the Hard Reality of Soft Power*. Its editor, Leigh Armistead, examined the qualitative difference between the "military-technical" and the "informational-psychological" aspects of IO.[17] Referencing Russia's theoretical roots of IO thought, *Informatsionnaya Voina* (Information War), Armistead emphasized the psychological component of IO in relation to technological structures. [18] While this description of Russia's way of interpreting IO was not unique to Armistead's findings, *Warfare and Hard Realities of Soft Power* represented a new awareness in the field of American IO that appreciated the granularity between IO's technical futuristic framework and its content oriented human psychology.[19]

Another similar yet valuable US study on IO, published in 2005, was Emily Goldman's, *Information and Revolutions in Military Affairs*. Goldman, then-Director of USCYBERCOM and the National Security Agency Combined Action Group, approached the topic of information from a revolution in military affairs (RMA) perspective.[20] Goldman described RMA as a change in

---

[17] Armistead, *Information Operations*, 24-40.

[18] Ibid., 192–197. *Informatsionnaya Voina* had as much to do with studying the psychology of the human mind as it did with information as a warfare theory. The implications of such a theory pointed to manipulating and controlling the mind of a target audience, to the point where one could control their behavior based on deception and disinformation campaigns. While the ideas may have placed too much faith in the success these 'psychotronic' means, it nevertheless lent itself to other theories as well, such as 'reflexive control': the idea of causing a person to voluntarily make a predetermined choice designed by the influencer. See footnotes 10 to 12 in Ibid., 251. On further delineation of Russian concept of 'reflexive control', see Darczewska, *The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study*, 14–17; Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17 (2004): 237–256.

[19] Timothy Thomas, a former research analyst at US Army's Foreign Military Studies Office (FMSO) in Fort Leavenworth, Kansas, had taken note of these changes in Russian military philosophy, and contributed heavily to the wider body of US Army IO analysis. However, his distinction of IO as either being a system-based framework versus a content-based idea further bifurcated the holistic notion of information warfare in US military establishments. Russia's tendency to integrate and consolidate the separated information variables was merely a continuation of old Soviet practice. See Timothy Thomas' chapter, "Russian Information Warfare Theory: The consequences of August 2008" in Stephen Blank and Richard Weitz, eds., *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald* (Carlisle, PA: Strategic Studies Institute, US Army War College, 2010).

[20] Emily Goldman, *Information and Revolutions in Military Affairs* (London, UK: Routledge, 2015).

global technologies, that, when tied to military weaponry, inevitably transforms "the way wars are fought by the world's leading military powers."[21] RMAs have great effect on how society adapts to the new advantages as well as demands of the new technological advancement. Likewise information technology, alongside the information revolution, were integral parts of Goldman's conceptualization of IO and information warfare.[22] Goldman and her contributors posited that the concept of IO, in combination with the new cyberspace domain, would transform militaries around the world. This RMA would not only affect future militaries, but also cause greater societal trends in politics and economics.

Goldman categorically differentiated between the function of information as content and information technology as conduit. While the former related to the substance of the message and the inherent meaning of information affecting human psychology, conduits represented the physical and virtual medium of transferring information. This latter category was reminiscent of signals communication flow through cyberspace networks. Nonetheless, despite discussing the criterion of content inherent in IO, the authors focused on command and control warfare (C2W), which stresses attacks and disruptions on adversarial communication systems, rather than the content of those systems. While visionary in anticipating transformative change, *Information and Revolutions in Military* Affairs, similar to Arquilla and Ronfeldt's technological post-Cold War views, fell short of providing a thorough examination of the issues of content in US IO.[23]

---

[21] Ibid., 1.

[22] Ibid., 2–13. For a general overview of revolutionary literature concerning military affairs, see Clifford Rogers, ed., *The Military Revolution Debate: Readings on the Military Transformation of Early Modern Europe* (Boulder, CO: Westview Press, 1995); Richard O. Hundley, *Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us about Transforming the U.S. Military?* (Santa Monica, CA: RAND Corporation, 1999); Thierry Gongora and Harald Von Riekhoff, eds., *Toward a Revolution in Military Affairs? Defense and Security at the Dawn of the Twenty-First Century*, Contributions in military studies 197 (Westport, CT: Greenwood Press, 2000); MacGregor Knox and Williamson Murray, eds., *The Dynamics of Military Revolution, 1300-2050* (Cambridge, UK ; New York, NY: Cambridge University Press, 2001).

[23] For Goldman's recent comments on the command and control nature of cyberspace operations, see "Concurrent Session I: Cyber Weapons and Strategic Stability," in *Concurrent Session I: Cyber Weapons and Strategic Stability* (presented at the Carnegie International Nuclear Policy Conference 2017,

This differentiation between technology and content shaped how US IO and information-related organizations would be constructed during the early stages of the post-Cold War era. This divided US IO organizational efforts at the presidential level.[24] Content-oriented information was to be used in offensive manner against adversaries, affecting their decision making. Conversely, conduit-related information was defensive in nature; a cyberspace domain system of networks and nodes that were to be defended and protected against.[25] Admittedly, the initial attention during this IO organizational buildup was on the content-oriented offense of IO, which stressed the content of information. Information as a technical system was a secondary priority, to be further developed through research and development. Entities from the National Security Agency (NSA), Defense Science Board (DSB), DARPA, and the greater intelligence community (IC), all had large stakes in this defensive research and threat-protection. However, at this time, the primary direction of American IO and information warfare pointed initially towards the cognitive aspects of information warfare.

Therefore, in 1999, then-President Bill Clinton signed Presidential Decision Directive (PDD) 68 "International Public Information," as his executive action to establish a centralized national body that could coordinate all US government activities relating to information in

Washington, DC: Carnegie Endowment for International Peace, 2017), accessed January 7, 2018, http://carnegieendowment.org/2017/03/20/concurrent-session-i-cyber-weapons-and-strategic-stability-pub-67884.

USCYBERCOM Commander Admiral Michael Rogers was also interviewed by Retired Admiral James Stavridis at the WEST 2017 Conference sponsored by the US Naval Institute. This conference focused on future innovation and technology platforms. Both Rogers and Stavridis concentrate on the systems aspect of 'cyber warfare' without much discussion on the use of information in both defense and offense. See Admiral Michael Rogers, "Are We Organized and Aligned to Fight the Cyber War?," Youtube, February 23, 2017, accessed September 6, 2017, https://www.youtube.com/watch?v=d8WITQuOQFI.

[24] Armistead, *Information Operations*, 24–30, 124–133.

[25] Ibid., 32–40.

synchronized manner.[26] PDD 68 was an information content-oriented directive that was closely associated with Clinton's earlier PDD 56 "Managing Complex Contingency Operations," which recognized the strategic nature of change taking place within the post-Cold War security environment.[27]

PDD 68 relegated the "International Public Information" coordinating and executive authority to the Department of State (DoS) instead of the NSC. This delegation appeared inconsequential at first, yet by overly empowering one federal agency within a supposed whole of government IO approach, the Clinton Administration created unwanted bureaucratic challenges. The synchronization of diverging organizational priorities and culture, particularly between DoS and DoD, actually delayed IO synchronization and coordination.[28] For example, DoD had a vested stake in contributing to the rapid development of a military IO section. However, due to the procedural nature of DoS culture, actual coordination for productive IO outputs were never achieved.[29]

---

[26] US Office of the President of the United States, Presidential Decision Directive (PDD) 68: "International Public Information," *Federation of American Scientists*, last modified April 30, 1999, accessed January 7, 2018, https://fas.org/irp/offdocs/pdd68.htm.

[27] US Office of the President of the United States, Presidential Decision Directive (PDD) 56: "Managing Complex Contingency Operations," *Federation of American Scientists*, 56, last modified May 1997, accessed January 7, 2018, https://fas.org/irp/offdocs/pdd56.htm.

[28] Armistead also detailed the bureaucratic challenges faced by Bill Clinton's administration. However, Clinton's PPD-68: "International Public Information," fell short of developing the necessary framework for authorizing and enacting US IO in the strategic sense, due to its failure to understand the challenge of enacting a whole-of-government approach mandated to a self-interested DoS.

As a countermeasure, George W. Bush's administration attempted to regain the IO momentum from DoS via its creation of the Office of Strategic Influence in 2002 under DoD. However, this initiative was killed through by an intra-department battle led by its DoD public affairs supervisor, Assistant Secretary of Defense for Public Affairs (ASD/PA) Victoria Clarke. See Armistead, *Information Operations*, 133–137.

[29] Ibid., 125–137. Certainly, the authors did not believe that such delay of US IO development was intentional. Rather, they emphasized that because one cabinet agency was given the final approval authority for national strategic IO, which in reality was an equally shared commodity to all federal agencies, the national approach to a holistic American IO hinged on DoS operating culture. This culture, defaulting to its internal processes and procedures, was not well suited to serve as the driving force for national offense in the information realm.

On the other hand, the task of defending US information networks against future adversaries and enemies slowly began to develop. Driven by the NSA and DoD, there was heavy investment into protecting the signals communications infrastructure of America's domestic networks. Yet, with the national directive to investigate the security of information computer systems (ICT) and the internet, DoD began to focus its energies towards the idea of cyberspace as a domain in need of protection.[30] By the 2010s, it was actually the defensive aspects of cyberspace as representing information warfare that gained broader national attention and priority within interagency discussions, and congressional legislation.[31]

Due to these issues, the defense and protection of information systems, which had originally been secondary to offensive information development, currently receive more organizational support, and attention as the representation of future IO and information warfare. The original bifurcation of information into the content-oriented and conduit-related parts has evolved into an organizational bifurcation with multiple stakeholders.

This paper questions whether such an organization structure for US military IO and information warfare are optimized for effective content-oriented information activities. However, prior to questioning the organizational makeup of US military forces geared towards contemporary IO and information warfare, this paper first reviews the theoretical field of modern

---

Ironically, while the offensive IO development was being stalled through interagency bureaucracy and sensationalized press coverage, the defense of IO/information warfare systems slowly began to emerge over the latter part of the 1990s and early 2000s. See Ibid., 21–33.

[30] Armistead, *Information Operations*, 23–24, 34–36; US Department of Defense Science Board, *Information Warfare - Defense*.

[31] US Department of Defense Science Board, *Advanced Cyber Threat*; US Department of Defense Science Board, *Capabilities for Constrained Military Operations* (Washington, DC: Defense Science Board, December 21, 2016), accessed December 2, 2017, https://www.acq.osd.mil/dsb/reports/2010s/DSBSS16_CMO.pdf; US Department of Defense Science Board, *Final Report of the Defense Science Board Task Force on Cyber Deterrence* (Washington, DC: Defense Science Board, February 2017), accessed December 9, 2017, https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

organizations, in order to understand how the composition and makeup of organizations affects coordination capacity.

Organizational Theory

In 1958, James March and Herbert Simon—interdisciplinary political scientists at Carnegie Mellon University in Pittsburgh, Pennsylvania—published *Organizations*, which became the cornerstone text for encapsulating organizational theory during the Cold War and throughout much of the post-Cold War period. March and Simon's book is not the first work in the field of organizational theory, but it provides an overview and continuation of a theory that began during the industrial revolution in the late 19th century by Frederick Taylor, Henri Fayol and others, who identified potential shifts in traditional hierarchical analysis of organizational behavior.[32]

Classical organizational theory described the 'scientific' aspects of an organization's architecture.[33] It emphasized hierarchical relationships to ensure efficient management from above. Deemed as the new science of sociology for organizing human beings for collective action solutions, classical theory advocated for centralizing organizations. This central organization would be best able to overcome the inefficiencies common to all organizations.[34]

---

[32] March and Simon allude to Luther Gulick (Columbia University) and Lyndall Urwick (British business theorist) of the early to mid-20th century as supplementary proponents of what became to be known as classical organizational theory, in their edited work *Papers on the Science of Administration*, New York, NY (1937). For a review of March and Simon's description of the classical school of thought, see James G. March and Herbert A. Simon, *Organizations*, 2nd ed. (Cambridge, MA: Blackwell Publishers, 1993), chapters 2 and 3.

[33] Ibid., 31–52. This notion of scientific management originates from Frederick Taylor, who was one of the original classical organizational theorists during the industrial revolution of early 20th century. Taylor focused on engineering human organizations that would be more efficient and precise in their industrial production. Much of the scientific origins of classical organizational theory stemmed from a desire to make human behavior more systematic in face of the industrial revolution. Also see Herbert A. Simon, *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations*, 4th ed. (New York, NY: Free Press, 1997), 26–28.

[34] March and Simon, *Organizations*, 31–52.

Classical organization theory complimented early 20th century sociology and thinking that stressed the management of human organizations through a more scientific and rational methodology. For instance, the classical school of organizational theory embraced the concept of division of labor stemming from traditional social economic theory. This notion of dividing organizational tasks into various sub-specialties had resonated with much of Western social sciences during the 19th and 20th century.[35] The idea in economics of the division of labor and specialization can be seen in the later development of organizational theory's concept of departmentalization. The separation of organizations by tasks and specialties, whether production oriented or management focused, found itself in line with well-established socio-economic principles.[36]

The most important theme to classical organizational theory was the central place hierarchies played in the overall design of organizations.[37] According to this theory, hierarchies streamlined the dispersal of data and information scattered throughout the organization. As it remained critical for organizations to make decisions necessary for collective action, classical theorists emphasized the primacy of hierarchies in providing order and prioritization. Standard operating procedures, for example, were classical tools for routinely consolidating vast quantities of information scattered throughout the management system's sub-departments. Yet these procedures tended to instill a culture of compartmentalization by inducing members within organizations to rely too heavily on the standard process, as opposed to actively working to coordinate information across departments.[38] While informal relationships were important in any

[35] Ibid., 179–182.

[36] Ibid., 40–48. The division of labor established within centralized organizations allowed the organization to adapt to the challenges of scale in a globalizing economy. By departmentalizing within organizations by function, organizations were able to maintain efficiency in production while responding to the fluctuations of market scale demand. Centralized hierarchies streamlined optimization and efficiency much needed in decentralized organizational states.

[37] Ibid., 211–221; Simon, *Administrative Behavior*, 4–5, 73–75, 192–197.

[38] March and Simon, *Organizations*, 41–47; Simon, *Administrative Behavior*, 30–31, 52–54.

human environment, classical theory stressed the organizational structure and its hierarchic formality. The action of streamlining dispersed information, in order to allow effective analysis and decision, remained the primary task for all organizations. An effective organization needed centralized structures that could enforce a logical system and process for consolidating information leading to timely decision.[39] Thus, classical organizations were pyramids which could integrate the growing phenomenon of complexity wrought by increasing specialization in a complex global market, while continuing to maintain central decision-making power and authority. This was the manner in which classical organizational theory believed organizations could manage the challenges of a fluctuating marketplace.[40]

However, March and Simon's *Organizations* differed from this literature, identifying the limitations of traditional classical organizational theory when exposed to globalizing market trends. In the authors' perspective, organizational firms had to deconstruct their departments and sub-departments if they were to remain relevant to the persistent demands of a volatile world system greatly affected by the information revolution.[41] March and Simon argued that business firms were failing in their adaptation despite their careful adoption of classical organizational theory's scientific prescripts. The authors pointed to early 20th century clinical data and experiments where organizational theorists had cautioned against adopting hierarchies to the detriment of human creativity.

---

[39] James G. March, *A Primer on Decision Making: How Decisions Happen* (New York, NY: Free Press, 2010), 140–172. It is important to note that the theory of hierarchies closely relate to the theory of power and determining where such power resides within a given organization. Within the classical school of thought, there is no question that one's power or authority to make a decision resides within a top-down organizational structure. For additional discussion on the evolution of traditional organizational theory, see Graham T. Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd ed. (New York, NY: Longman, 1999), 147–158.

[40] March and Simon, *Organizations*, 179–182. This latter notion of division of labor modeled itself after the classical economic theories of Adam Smith, and purported to incorporate his ideas of marketization into enlarged economies of scale necessary for modern business organizations.

[41] Ibid., 188–190; Simon, *Administrative Behavior*, 223–227.

Admittedly, while human capital and initiative were intangible in themselves, the case studies during the 1920's foreshadowed the rise of a new field within organizational theory that described how institutions could adapt and change to an evolving world.[42] These early findings suggested that organizations had to be more adept at incorporating the potential of the human individuality in the context of the collective organizational system.[43] March and Simon further emphasized that the future of information access would accelerate for the remainder of the 20th century, serving as impetus for further openness and change in how organizations were to restructure based on environmental realities.[44]

While March and Simon's view of the information age was still preliminary in context of how information communications systems would evolve into the 21st century, the authors presciently identified what would become known as the neoclassical perspective. The neoclassical theory of organizations emphasized the value of human creativity and initiative in context of organizational structures. It questioned the traditional practice of and value of hierarchies and argued that, in order to process growing amounts of information and data, institutions had to re-evaluate previous notions of power and authority. Deeming classical organizational theory to be overly optimistic in its scientific approach, the neoclassical perspective emphasized the challenge of cultivating human creativity and individuality in a

[42] For early micro-level observations made during the period of classical theory, see Mary Parker Follett and Pauline Graham, eds., *Mary Parker Follett - Prophet of Management: A Celebration of Writings from the 1920s*, Harvard Business School Press Classics (Boston, MA: Harvard Business School Press, 1995).

[43] Simon, *Administrative Behavior*, 183–185, 330; Mary Jo Hatch and Ann L. Cunliffe, *Organization Theory: Modern, Symbolic, and Postmodern Perspectives*, 2nd ed. (Oxford, UK ; New York, NY: Oxford University Press, 2006), 221–223; Follett and Graham, *Mary Parker Follett--Prophet of Management*.

[44] March and Simon, *Organizations*, 13–16. Simon, *Administrative Behavior*, 238–248. At the time, their definition of information acceleration was based on their witness of facsimiles and the growing number of land telephone lines within the United States.

vertical organizational construct.[45] In short, the neoclassical school suggested that the delegation of power and authority within centralized hierarchical structures should be relegated down to lower echelons.[46] This would let organizations capitalize on human capacity, making them more adaptable to the changing information environment.[47]

Overall, the idea of decentralization was the driving philosophy within the newly developed neoclassical school of thought where managers, acting as leaders, instilled greater trust to their subordinates. Power and authority, which had been centralized at the higher echelons of organizations, had to be spread throughout the hierarchical structure in order to enable

[45] March, *A Primer on Decision Making*, 33–35, 234–250. One of the main challenges of an evolving market economy was the speed and diffusion of information available to actors beyond traditional markets. While in the past, information served as a commodity, and access to business-oriented information remained controlled and selective, March and Simon noticed a change to the way businesses and human beings would have access to information in the future. In follow-on writings by the authors, and in the 1994 edition of *Organizations* March and Simon would further emphasize this information revolution via personal computers and facsimiles. They concluded that the information revolution would bring on unforeseen levels of access and speed in human processing, which inevitably affected the ways in business organizations would have to adapt in order to survive.

[46] March and Simon, *Organizations*, 182–192; Simon, *Administrative Behavior*, 185–197, 317–322.

[47] Certainly, March and Simon's call for horizontal organizational models was not as pronounced as what it would later become within the field of organizational theory in the decades to follow. Such emphasis on horizontal architecture, akin to networks, that placed the role of individuals at a higher value than traditional hierarchies, became more pronounced within the sub-genre school of organizational management. Nevertheless, March and Simon took note of this trend, which would lead to later neoclassical organizational theory advocating for the leveling of traditional structures into a more decentralized and democratic architecture.

subordinate actors to respond to the demands of a fluctuating market.[48] This neoclassical organizational theory became the new tradition in organizational theory.[49]

Much of this analysis and discussion took place before the rise of the internet. None of the neoclassical theorists foresaw the level of technological developments in information communications and massive increase in global interconnections. Nevertheless, neoclassicists were able to identify the weaknesses of existing tradition in the face of change to come: decision-making authorities had to be dispersed down to the right level of organizations.[50] In sum, while classic organizational theory promoted hierarchy in organizations, in neoclassical organizational theory, decentralization is embraced.[51] This shift in organizational theory was due to the

[48] Much of this sub-genre of organizational management is attributed to Peter Drucker of the Claremont Graduate School of Management in California. Drucker furthered the exploration of change and learned adaptation within organizations. For a succinct review of Peter Drucker's series of organizational management writings, see Peter F. Drucker, *Managing in a Time of Great Change* (New York, NY: Truman Talley Books/Dutton, 1995).

Others would contribute as well in the realm of leadership management and organizational change theory, particularly in the field of change management, with works by David Schon and John Kotter on instilling learning and cultural adaptation within institutions. Chris Argyris and Donald A. Schön, *Organizational Learning: A Theory of Action Perspective*, Addison-Wesley Organizational Development Series (Reading, MA: Addison-Wesley, 1978); John P. Kotter, *Power and Influence* (New York, NY: Free Press, 1985).

[49] Traditional notions of hierarchy diminished in importance in a world filled with rapid information which continued to splinter and multiply in terms of access and transfer. Decentralization as strategy became the mantra in a more open and flat economy. As the lines of communications and delivery of information and goods expanded further through the remainder of the 20th century, neoclassical notions of flattening vertical hierarchies became the new tradition in organizational theory.

[50] Neoclassical analysis paved the way for expansion within change management beyond the initial advocacy for decentralized processing and action at the sub-atomic level of central command and control. For studies on further progression of organizational theory and management following neoclassical theory, see Hatch and Cunliffe, *Organization Theory*, 41–56, 271–287.

[51] March and Simon, *Organizations*, 193–220. Neoclassical theory upheld the value of the human individual over the larger organization. Individual actors within organizations who exhibited creativity and initiative were the real source of potential to organizations. Neoclassical theory brought back the social human-ness of organizations back into the study of organizational theory. While certain powers and authorities remained at the hierarchical center, much of the transactional authorities for a decision leading to business action began to trickle down to the sub-component and individual level of the greater organization. Thus, organizations could rely on the subordinate members to act responsively based on the reality of their market environment and respond in timely fashion to the needs of a given business situation

recognition that while information was diffuse, and in need of consolidation, only decentralization would enable decisions to be made swiftly.

Within the military, this notion of decentralization has been in common usage over the past many decades. The US Army's use of 'Mission Command' is a clear product of the military's implementation of decentralization.[52] However, in terms of IO and information warfare activities, the military remains surprisingly hierarchical in terms of retaining its execution authorities and permission, while at the same time dispersing the whole of its IO function into disparate capabilities and organizations. In order to understand the parallels between organizational theory and its application to the US military, to the next section discusses the current structure of US IO organizations in support of American information warfare.

How US Military Information Operations are Organized

According to Joint Publication (JP) 3-13, *Information Operations*, IO plays a critical role in providing situational awareness and understanding necessary for visualizing and shaping one's operational environment during joint operations.[53] The designated IO officer oversees the coordination and synchronization of all information-related activities by employing what are termed as Information Related Capabilities (IRC). IRCs include Public Affairs (PA), Psychological Operations (PO), Electronic Warfare (EW) and Cyberspace Operations (CO).[54]

---

[52] US Department of the Army, Army Doctrine Publication (ADP) 6-0, *Mission Command* (Washington, DC: Government Printing Office, 2012). US Army's doctrinal understanding of 'Mission Command' exemplifies much of the decentralized ideas of organizational theory. In order to capitalize on tactical initiative necessary for rapid analysis and decision-making in combat situations, 'Mission Command' advocates for subordinate commanders to seize initiative for relative advantage. Also see Clinton Ancker, "The Evolution of Mission Command in US Army Doctrine, 1905 to the Present," *Military Review* 93, no. 2 (April 2013): 42–52.

[53] US Joint Chiefs of Staff, Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: US Joint Chiefs of Staff, 2014), 3–13.

[54] Ibid., II-5 to II – 13; US Department of Defense, "DoD Strategy for Operations in the Information Environment" (US Department of Defense, June 2016), 3, accessed September 3, 2017, https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

The separation in these IRCs also correlate with distinct and codified branch separations in US Army's IO force structure. For example, the aforementioned IRCs of PA, PO, EW and CO are in themselves separate branches of US Army specialization. Furthermore, IO also remains a distinct functional entity, which maintains its occupational identity and proponent separate from the other Army branches relating to IRCs.[55] Thus not only are the US Army's information warfare capabilities separated between the signals conduit system and the information content creation; within the content-oriented division are further sub-divisions which only complicates the necessary communication and cohesion required for streamlined IO.[56]

IO officers serve as the focal point for IRCs, where they provide coordination and expertise across all the joint level staffs within a command as well as across interagency lines. The function of the IO officer is to consolidate and de-conflict the multiple information streams, in order to support or prosecute operations.[57] In this context, IO-trained personnel, as a functional branch, are responsible for synchronizing and coordinating multiple IO assets that they command. While joint doctrine specifies that IO functions are "not about ownership of individual capabilities," the IO officer, as the designated information entity, remains the functional focal point for a command's information-related operations.[58] Additionally, the IO officer oversees the IO working group (IOWG) in order to integrate necessary deception plans (MILDEC), utilize support of Combat Camera assets (COMCAM), and ensure OPSEC protection measures. The

---

[55] US Department of the Army, Field Manual (FM) 3-13, *Information Operations* (Washington, DC, Government Printing Office, 2016), 1-1 to 1-8.

[56] The first grouping of IRCs relate to traditional information content affecting human cognitive functions. The second set of IRCs relate to the signals conduit of information systems which enable communications transfer across various military domains. In doctrine, these technical systems of the latter IRC group belong to the J-6 staff group, which focuses on traditional signals communication, as opposed to the J-3 staff group, where the information content-oriented IRCs are.

[57] Ibid., 3–4; Even at the joint staff level of IO, similar conditions for synchronization and coordination exist for all services within the US military. See US Joint Chiefs of Staff, JP 1.

[58] US Joint Chiefs of Staff, *JP 1*, xi, I–5, II–5; US Department of the Army, FM 3-13, III–5.

IOWG attempts to de-conflict information issues in military operations and develops the greater information strategy for the command.[59]

In terms of IO integration, joint doctrine notes that such synchronization and collaboration should be conducted along the traditional staff levels of a military organization.[60] IO is coded as a J-39, which means that it is nested under the J-3 staff group. The J-3 staff is responsible for current military operations, both kinetic and non-kinetic.[61] Information serves as an operationalized function, where Army organizations enact IO as means of supplementing combat operations. Executing IO is an essential element of a commander's overall operational approach. In addition to fully non-kinetic operations utilizing information, both non-lethal and indirect IO methods for targeting adversaries serve as an important part of kinetic engagements. As a subsidiary staff under the J-3 division, IO, as a form of non-kinetic operations, are typically treated as a secondary concern to the kinetic J-3 priorities.[62] Despite this secondary status, joint doctrine assumes that IO will be able to seamlessly accomplish its mission. However, integrating IO priorities becomes extremely challenging in a resource and time-constrained environment.

To be sure, all staff functions within a given organization face the same constrained environment. It is debatable whether IO planners face challenges as coordinators and synchronizers of information that are any more challenging than other staff functions such as

---

[59] US Department of the Army, FM 3-13; US Department of the Army, Field Manual (FM) 3-53, *Military Information Support Operations* (Washington, DC: Government Printing Office, 2013).

[60] For instance, the Information Operations division within a given command organization is coded as S-39, indicating a sub-division of the overarching S-3 division. This makes logical sense in terms of integrating IO into standard US Army operations; however, given the limited time and space of any given combat operations, S-39 delegations are not afforded the necessary access and visibility to traditional S-3 and S-2 inter-operations.

[61] Traditional J-Staff Directorates range from J-1 to J-9. In order of typical priority for operations: J-3 (Operations), J-2 (Intelligence), J-4 (Sustainment), J-6 (Signal/Communications), J-1 (Personnel). Beyond these core J-Staff Directorates are J-5 (Future Plans), J-7 (Training), and J-9 (Civil-Military).

[62] Rod Thornton, "The Changing Nature of Modern Warfare," *The RUSI Journal* 160, no. 4 (September 2015): 42.

'Command and Control', 'Maneuver', 'Fires', and 'Logistics'. However, in a standard prioritization of kinetic and non-kinetic requirements, IO will inevitably take a secondary position in a military commander's cognitive thinking and prioritization.[63] This is somewhat to be expected, given that the military is an organization that has traditionally valued the lethal and kinetic aspects of its mission over the non-lethal aspects.[64]

While the initial divisions of the IRCs within US Army IO remained critical for developing the functional aspects of information capabilities, the US Army's ability to conduct and support information warfare has become diluted by the inability of the IO organizational structure to effectively coordinate and synchronize all necessary aspects of IRCs in a consolidated and holistic manner.[65] Ironically, persisting differentiation and organizational departmentalization amongst IRCs have increased bureaucracy and decreased organizational clarity.[66] In this current organizational framework, IO planners face difficulties in receiving resources for IRCs, and bringing them to the commander's attention.[67]

---

[63] Thomas Williams, "Strategic Leader Readiness and Competencies for Asymmetric Warfare," *Parameters* 33, no. 2 (Summer 2003): 27–29; Paul Kelley, Graham T. Allison, and Richard Garwin, *Nonlethal Weapons and Capabilities* (Washington, DC: Council on Foreign Relations, February 2004), 33, 38–39; David Galula, *Counterinsurgency Warfare: Theory and Practice*, New Edition. (Santa Barbara, CA: Praeger Security International, 2010), 77–85; Jeffery Underhill, "Are the Department of Defense Non-Lethal Weapon Capabilities Adequate for the 21st Century?" (US Army War College, 2006), 6–7, accessed July 20, 2017, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA448633; Janice H. Laurence, "Military Leadership and the Complexity of Combat Culture," *Military Psychology* 23, no. 5 (September 2011): 494–499.

[64] Williams, "Strategic Leader Readiness and Competencies for Asymmetric Warfare," 27–29; Kelley, Allison, and Garwin, *Nonlethal Weapons and Capabilities*, 33, 38–39; Underhill, "Non-Lethal Weapon Capabilities Adequate?," 10–11.

[65] US Joint Chiefs of Staff, *JP 1*, II-5 to II-13; US Department of the Army, FM 3-13, 1-7, 2-5.

[66] While this organizational dispersion may appear to be an exception to the more fluid organizational structure at subordinate service components of the DoD, one also realizes the very problem of coordination and synchronization. For instance, at the micro level of the US Army, the root of their IO decentralization problem stems from how the Army has constructed its IO-related branches, further exasperating compartmentalizing inefficiencies in its organizational processes.

[67] Nevertheless, the expectation for IRCs to effectively synchronize and coordinate all assets relating to IO will continue to be difficult due to the dispersion of its forces across the organization. Thus, being left to individualized specializations without a codified command organization to enforce the

Theory Development

Despite the progression of organizational theory from classical to neoclassical lines of thought, hierarchies within organizations continue to matter.[68] While flexibility and adaptability are important, it is through centralization that organizations are better able to consolidate information, analyze it, and prioritize its value.[69] The centralized venue for digesting data allows for responsive decision-making critical to military organizations in midst of combat.

A successful organization must account for varied specializations subordinate to its overall structure, but must balance the benefits of decentralization with the need for centralized control of processes. As organizational theorists have pointed out, subdividing the department specialties within a large organization remains necessary for developing a thorough understanding of specific areas.[70] Such departmentalization allows organizations to develop tailored capabilities as a part of its aggregated whole. Such functional departmentalization should allow adaptation and flexibility in an evolving environment.[71] And yet, there is a remarkable

---

streamlined logic of processes and action—characteristic of a centralized hierarchical authority—challenges the future of information despite its designation as the seventh joint function of the US military.

[68] March and Simon, *Organizations*, 144–149, 171–172, 190–192; Simon, *Administrative Behavior*, 52–54, 127; James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It*, New. (New York, NY: Basic Books, 2000), 14–28; Allison and Zelikow, *Essence of Decision*, 149–153, 156.

[69] March and Simon, *Organizations*, 211–216.

[70] Ibid., 40–44.

[71] Similarly, the departmentalization of IRCs in the Army remains critical for constructing a formidable US Army IO prepared to meet the complex challenges of a growing information environment greatly affected by cyberspace. It is necessary for exercising a comprehensive American information warfare strategy in context of future growth and development as a military force. One can attribute this tendency to decentralize US Army's IO into disaggregated IRCs to the persistent mantra of the Army's mission command philosophy. Taking its cues from the theories of decentralization and horizontal organization prescriptions advocated by the post-neoclassical organization theory academia, the mission command doctrine continues to inspire senior level discussions in the army enterprise.

The principle of decentralization as an idea stirs a certain sense of democratization which inevitably resonates with American audiences. Whether from neoclassical organization theory or supporters of army mission command concepts, the notion of leveling the communications and information playing field via a more equalized organizational structure wins the attention and support of both civilian and military thinkers.

difference between how private business organizations embrace the theoretical principles of decentralization as a renewed way of organizing, processing information, and making decisions compared to how the military has adopted the decentralized practice of delegation. Military organizations have typically been more hierarchical in their structure and their cultural identity.[72] Ironically, while US Army IO as a force faced much of the same challenges that initially affected the private business enterprise early at the onset of 20th century industrialization, the same lessons of balancing decentralized practice with centralized structure were not learned.

The practice of decentralization is less likely to be as applicable in the formal hierarchies of the military. In the case of the US Army, power and authority are principally based in a centralized command headquarters. It is the consolidation of power, authority, and ultimate responsibility for life-and-death situations that allow actual decision-making fundamental to the realms of war and conflict. The sheer nature of military reality demands adherence to orders during combat, and requires a form of more absolute control than that needed by business organizations.[73] One aspect of this limitation in theoretical decentralization is the unlikelihood of

---

For broadened discussion on 'mission command,' see Mark Milley, "AUSA 2016 Eisenhower Luncheon Address" (Washington, DC, October 4, 2016), http://wpswps.org/wp-content/uploads/2016/11/20161004_CSA_AUSA_Eisenhower_Transcripts.pdf; Mark Milley, "Commanders Series Event with Chief of Staff of the Army, General Mark Milley," May 4, 2017, accessed October 14, 2017, http://www.atlanticcouncil.org/events/past-events/commanders-series-event-with-chief-of-staff-of-the-army-general-mark-milley; David Barno and Nora Bensahel, "Six Ways to Fix the Army's Culture," *War on the Rocks*, last modified September 6, 2016, accessed July 14, 2017, https://warontherocks.com/2016/ 09/six-ways-to-fix-the-armys-culture/; David Barno and Nora Bensahel, "Three Things the Army Chief of Staff Wants You to Know," *War on the Rocks*, last modified May 23, 2017, accessed July 14, 2017, https://warontherocks.com/2017/05/three-things-the-army-chief-of-staff-wants-you-to-know/; Robert Phillipson, "Leeroy Jenkins and Mission Command," *Military Review Online Exclusive* (May 2017), accessed July 14, 2017, http://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2017-Online-Exclusive-Articles/Leeroy-Jenkins-and-Mission-Command/.

[72] US Joint Chiefs of Staff, *JP 1*, xxiii, II–18, IV-2 to IV – 20; Wilson, *Bureaucracy*, 14–28, 185–194; Allison and Zelikow, *Essence of Decision*, 158–159, 164–176; Morris Janowitz, "Changing Patterns of Organizational Authority: The Military Establishment," *Administrative Science Quarterly* 3, no. 4 (March 1959): 475–476.

[73] Wilson, *Bureaucracy*, 18, 105–106, 163, 185–194; Allison and Zelikow, *Essence of Decision*, 172–182; Simon, *Administrative Behavior*, 51–54, 179; March and Simon, *Organizations*, 55–66, 74–77, 171–172. See footnote 4 in, Janowitz, "Military Establishment," 475.

military command authority being fully delegated in decentralized fashion down to the sub-organizations of the operational and tactical realm. Operational abidance to rules of engagement, as well as strictly defined legal limitations in lethal operations and kinetic targeting, remain dependent on a higher command's authority and guidance. The identical mirroring of private business practice as prescribed by American neoclassical organizational theory and management naively discounts the sheer difficulty of implementation throughout its vertical rank structure.

Yet even beyond this differentiation of military and commercial organizations, organizational theorists have always agreed upon the preliminary structure required for streamlined information flow leading to shared understanding. Neither classical nor neoclassical organizational theory discounted the foundational role of structure leading to fluid and logical process for decision-making within an organization. Much of this vertical framework serves as the foundation for organizational decision-making.

This paper argues that the current decentralization of US Army IO's organizational architecture retards a command's potential to fully appreciate the information environment, conceptualize the various array of information data, and ultimately enact an effective information warfare strategy against rising near-peer adversaries. US Army IO forces are hampered by a decentralized structure which disaggregates its force capability within a growing and emerging domain that it is tasked to dominate.

In the past, the formalized framework of US Army's command and control structure has prepositioned it for operational success during combat.[74] The concept of decentralized military actions have only been possible due to an underlying foundation of US Army organizations as a centralized body. It has been the tradition of formalism, centralization and hierarchy, the theoretical framework criticized as antiquated by neoclassical organizational theorists, which has facilitated information sharing feasible throughout the Army via formally established

[74] Janowitz, "Military Establishment"; Wilson, *Bureaucracy*, 14–28, 185–194; Allison and Zelikow, *Essence of Decision*, 158–159; US Joint Chiefs of Staff, JP 1, xxiii, II–18.

communications channels. Therefore, centralized organizational frameworks continue to remain important, because they streamline information sharing and analysis, in order to produce timely decisions in complex security environments.

This monograph argues that US Army IO must consider centralizing its task organization in order to streamline all of its disparate capabilities. It remains bureaucratically ineffective and divisive for IO forces to maintain their organizational separation within the holistic realm of information warfare. Distinctly codifying the responsibility of coordination and synchronization away from IRCs such as PA, PO, EW, and CO only complicates the interrelated parts of an operation. As a first step, the US military must reconsider the purpose and role of the IO proponent. The US Army IO officer's designated task of synchronization and coordination is not enough to streamline the disparate capabilities spread throughout the force. Instead, the functional concept of information requires command authority over all IRCs; this would overcome the challenge of information authorities and permissions that are otherwise not often delegated down to the subordinate commands. The information-related officer must have organizational autonomy in order to enact a coherent information warfare strategy. To champion decentralization of activities, without identifying a central source of authority to oversee and shape the direction of those activities, does not solve the information challenge of contemporary warfare.[75]

Additionally, with the recent rise of USCYBERCOM, focused on the conduit systems of information, there has been no corresponding organizational structure developed for information content. Such a condition only exacerbates the difficulties of US Army IO in achieving a cohesive

[75] It is no surprise that coordination responsibilities are not technical occupational skills but qualities and skillsets inherent to all forms of occupation within the US Army. In many ways, distinctly codifying the responsibility of coordination and synchronization away from existing IRCs such as PA, PO, EW and CO further complicates the interrelated parts of an information endeavor that is in dire need of revision. It is no wonder why many defense analysts call for a more cohesive and effective information strategy, while failing to realize the problem of dispersion in its IO organizational structure. See Giles, "Countering Russian Information Operations in the Age of Social Media"; Waltzman, *Weaponization of Information*; Waltzman, "The U.S. Is Losing the Social Media War."

strategy to confront real world near-peer adversaries. Senior leaders must reconsider how to provide a coherent organizational structure that supports both conduit and content. USCYBERCOM could be given additional taskings and responsibilities to oversee information messaging activities. Alternatively, the US military could create a new FCC that focuses on all aspects of content, comparable to the USCYBERCOM's focus on conduit activities. By implementing one of these options, the US military would gain more robust capabilities and provide a centralizing structure to oversee and support both content-oriented and systems-technical military personnel.

By addressing the issue of decentralization through new authorities and organizational structures, the US military can mitigate the challenges facing current IO and information warfare capabilities. A US Army IO, which can seamlessly command all the IRCs, will be able to mitigate the unnecessary bureaucracy which appears prevalent in the present force structure. By either expanding USCYBERCOM or developing a new FCC focused on the content orientation of information, the US military will be better able to support all aspects of information warfare. In order to demonstrate what a more centralized IO and information warfare capabilities could look like, and what they would be capable of, this paper examines the case study of Russia.

The current American adaptation towards the realities of the information revolution stand in stark contrast to Russia's understanding of information and adaptation of its warfare practices within that domain. While the US has resorted to a domain-specific organization, a USCYBERCOM designated for cyberspace superiority and dominance, Russia has blended the technical-system and political-psychological aspects of IO to enrich a greater understanding and way of its information warfare. The Russian military adaptation to the globalized information environment offers an alternative conceptualization of information warfare and of the organization of information capabilities.

Case Study: Russian Information Hybridization

On April 27, 2007, Russian military forces conducted distributed denial of service (DDoS) attacks on Estonia's internet servers.[76] Official Estonian entities, such as its parliamentary *Riigikogu* and subordinate ministries, became inundated with internet attacks, which degraded its public infrastructure and essential services. Estonian private banks and news organizations were targeted as well, preventing ordinary citizens from carrying on daily economic activities and degrading the quality of business and commerce within their local communities.[77] While the origin of this interstate dispute supposedly stemmed from the relocation of a World War II monument symbolizing Russian historic contributions to the area, the actual intent was clear: it was an explicit showcase of Russian state and military power within cyberspace for the purposes of disrupting and degrading another state's internal security and sovereignty.[78]

Despite this display of Russian asymmetric capability however, many of the leaders in Western democracies regarded Russia's cyberattack as an isolated event and overlooked its implications.[79] Then, in 2008, Russia orchestrated a more comprehensive cyberattack against Georgia in attempt to seize the South Ossetia and Abkhazia provinces. In this conflict, Russia

---

[76] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 17, 2007, sec. World news, accessed November 30, 2017, http://www.theguardian.com/world/2007/may/17/topstories3.russia.

[77] A.J.C. Selhorst, "Russia's Perception Warfare: The Development of Gerasimov's Doctrine in Estonia and Georgia and Its Application in Ukraine," *Militaire Spectator* 185, no. 4 (2016): 154–155; Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia."

[78] Stephen Herzog, "Country in Focus: Ten Years After the Estonian Cyberattacks," *Georgetown Journal of International Affairs* 18, no. 3 (Fall 2017): 67–78; Cory Welt, *Russia: Background and U.S. Policy* (Washington, DC: Congressional Research Service, August 21, 2017), accessed November 30, 2017, https://fas.org/sgp/crs/row/R44775.pdf.

[79] Herzog, "Ten Years After"; Deutsche Welle, "Spiegel: NATO Unprepared If Russia Moved into Baltic Members," *DW*, last modified May 18, 2014, accessed December 30, 2017, http://www.dw.com/en/spiegel-nato-unprepared-if-russia-moved-into-baltic-members/a-17643795; Bernd Riegert, "Opinion: NATO Needs to Rethink Its Strategy," *DW*, last modified June 5, 2014, accessed December 30, 2017, http://www.dw.com/en/opinion-nato-needs-to-rethink-its-strategy/a-17614273.

demonstrated military hybridization of lethal and non-lethal activities, coordinating cyberattacks, an information propaganda campaign, and kinetic military actions.[80]

To be sure, the new Russian model of war during the 2008 Georgian crisis was filled with mistakes and shortcomings. Senior Russian military leaders later attested to their failures in enacting a more comprehensive information campaign alongside ground tactical combat operations.[81] In fact, during the Georgian invasion, Russian officials were caught off guard by Georgian civilian media organizations who rose to the challenge of countering Russian military propaganda and disinformation.[82] By contesting Russian military IO with commercial media, Georgians multiplied their information dissemination capability.[83] Private Georgian citizens, acting as self-interested internet vigilantes, countered Russian information and messaging. This adaptive and impromptu cohesion of public, government, and citizen actors enabled Georgia to defend its domestic information environment while gathering public support from external states. Georgia won support from both the Caucasus region states and the international community. This

[80] Cory Welt, *Russia: Background and U.S. Policy* (Washington, DC: Congressional Research Service, August 21, 2017), 25–27, 37–44, accessed November 30, 2017, https://fas.org/sgp/crs/row/R44775.pdf; F. Stephen Larrabee et al., *Russia and the West After the Ukrainian Crisis: European Vulnerabilities to Russian Pressures* (Santa Monica, CA: RAND Corporation, 2017), 10, 51–52; Ariel Cohen and Robert Hamilton, *The Russian Military and the Georgia War: Lessons and Implications* (Carlisle, PA: Strategic Studies Institute, US Army War College, June 2011), 63–66.

[81] Emilio Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," *Parameters* 47, no. 2, Innovations in Warfare and Strategy (2017): 59–62; Tor Bukkvoll, "Russia's Military Performance in Georgia," *Military Review* 89, no. 6 (December 11, 2009): 57; Bettina Renz and Rod Thornton, "Russian Military Modernization," *Problems of Post-Communism* 59, no. 1 (February 2012): 45–46.

[82] Jolanta Darczewska, *The Devil Is in the Details: Information Warfare in the Light of Russia's Military Doctrine*, Point of View (Warsaw, Poland: Centre for Eastern Studies, May 19, 2015), 24, 32–37; Jolanta Darczewska, *Active Measures: Russia's Key Export*, Point of View (Warsaw, Poland: Centre for Eastern Studies, May 30, 2017), 45–47.

[83] Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," 52–54; Maria Haigh, Thomas Haigh, and Nadine Kozak, "Stopping Fake News: The Work Practices of Peer-to-Peer Counter Propaganda," *Journalism Studies* (April 25, 2017): 20–21.

support aided in the eventual defeat and withdrawal of Russian forces, though Russia continues in a partial occupation of South Ossetia and Abkhazia.[84]

The coordinated synchronization of cyberattacks and computer viruses caught Western security and defense analysts off guard.[85] In many respects Russia's methodical orchestration of conventional attacks coupled with non-lethal and non-kinetic activities stood as an anomaly to the American counterterrorism mindset steeped in the Global War on Terror. Western security and defense analysts had to revise their outlook, which was anchored to the non-state actor paradigm of global Islamic terrorism. However, based on Russia's actions, analysts now needed to reorient back to state versus state conflict.[86]

In February 2014, Russia initiated offensive operations into Ukraine by sending preliminary forces into the Crimean Peninsula.[87] The Russian state combined its special

---

[84] Emilio Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," *Parameters* 47, no. 2, Innovations in Warfare and Strategy (2017): 52–54; Edward Lucas and Peter Pomeranzev, *Winning the Information War* (Washington, DC: Center for European Policy Analysis, August 2, 2016), 11–13.

[85] Anne Applebaum, "World Inaction: Russia Invades Georgia While the West Watches," *Slate Magazine*, last modified August 8, 2008, accessed October 10, 2017, http://www.slate.com/articles/news_and_politics/foreigners/2008/08/world_inaction.html; C.J. Chivers, "In Georgia and Russia, a Perfect Brew for a Blowup," *New York Times* (New York, NY, August 10, 2008), sec. Europe, accessed October 10, 2017, https://www.nytimes.com/2008/08/11/world/europe/11ticktock.html.

[86] John Mearsheimer, "Back to the Future," *International Security* 15, no. 1 (Summer 1990): 5–56; John Mearsheimer, Stanley Hoffman, and Robert Keohane, "Back to the Future, Part II: International Relations Theory and Post-Cold War Europe," *International Security* 15, no. 2 (Fall 1990): 191–199; John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York, NY: W. W. Norton and Company, 2003); Bettina Renz and Hanna Smith, *Russia and Hybrid Warfare - Going Beyond the Label*, Aleksanteri Papers (Helsinki, Finland: Kikimora Publications, University of Helsinki, 2016), 18–21, accessed July 21, 2017, https://helda.helsinki.fi/handle/10138/175291.

[87] US DoD's Quadrennial Defense Review (QDR) was published on March 4, 2014 in the midst of ongoing Russian military operations in Ukraine, which had begun February 21. The language of QDR 2014 underestimated the actual level of Russian military aggression in its sphere of influence, and ultimately failed to identify Russia as an adversary intent on challenging the international system. Within the language of QDR 2014, the authors proposed to "cooperate with Russia" and "engage [them] constructively" in order to "increase transparency." The descriptions were heavily diplomatic, and QDR 2014 made no distinction between the type of challenges posed by Russia and China to global security. Rather, the QDR addressed China with a slightly more threat-centric language, despite its strategic focus on economic growth. QDR 2014 would be the last publication before DoD's decision to transition its strategy publications to classified versions of the National Defense Strategy and National Military Strategy. US Department of Defense, *Quadrennial Defense Review 2014*, Special Report (Washington, DC: US Department of Defense, March 4,

operations forces (SOF) with conventional military follow-on forces during the subsequent months. The United States and Western European nations took no military action, hoping that Russia's military actions were based on misunderstandings between the two states.[88] Most policymakers remained cautious, hesitating to call out Russia for violating international law.[89] As Russia's president, Vladimir Putin, methodically denied Russian military presence in the Ukrainian territory, the Crimea Peninsula was effectively annexed by the summer of 2014.[90] This annexation of Crimea dispelled any previous doubt of Russia's territorial ambitions and strategic intention.[91]

The Holistic View of Information

From the information perspective, Russia's successes in these conflicts originated from their ability to conceptualize the idea of information as a whole within the context of military operations. While earlier Russian information theory subdivided information into subcomponents of information-psychological content versus conduit-technical systems for analysis, that

---

2014), 28, 36, 57. Also see Free Russia Foundation's timeline and analysis of Vladimir Putin's decision cycle and Russian military presence in Ukraine from mid-February 2014 and on, in Ilya Yashin and Olga Shorina, *Putin.War: Based on Materials from Boris Nemtsov* (Moscow, Russia: Free Russia Foundation, 2015), accessed December 30, 2017, http://4freerussia.org/putin.war/Putin.War-Eng.pdf.

[88] Kylie MacLellan, "'Complacent' NATO Unprepared for Russian Threat: British Lawmakers," *Reuters*, last modified July 31, 2014, accessed December 30, 2017, https://www.reuters.com/article/us-ukraine-crisis-britain-nato/complacent-nato-unprepared-for-russian-threat-british-lawmakers-idUSKBN0FZ2M920140731; Klaus Jansen, "NATO Members Mull Rearmament," *DW*, last modified July 5, 2014, accessed December 30, 2017, http://www.dw.com/en/nato-members-mull-rearmament/a-17616328.

[89] MacLellan, "'Complacent' NATO Unprepared for Russian Threat"; Jansen, "NATO Members Mull Rearmament."

[90] Czuperski et al., *Hiding in Plain Sight*. For details on deliberate denial of Russian presence in Crimea and Donbass region, see, Yashin and Shorina, *Putin.War: Based on Materials from Boris Nemtsov*, 14–22.

[91] Tor Bukkvoll, "Why Putin Went to War: Ideology, Interests and Decision-Making in the Russian Use of Force in Crimea and Donbas," *Contemporary Politics* 22, no. 3 (September 2016): 267–282; Tor Bukkvoll, "Off the Cuff Politics—Explaining Russia's Lack of a Ukraine Strategy," *Europe-Asia Studies* 53, no. 8 (December 2001): 1141–1157.

subdivision was not maintained during information warfare; information was not to be disaggregated during military action.[92] Both Russian information theory and military thought applied information in holistic terms against adversaries. Arguably, the success of Russian IO resulted from their ability to re-consolidate the bifurcated sub-elements of information into a whole during the course of military offense. This merger of conduit systems alongside the narrative message and information content embodies a persistent trend within Russian hybrid warfare theory.[93] The Russian concept of hybrid warfare went beyond the simple amalgamation of traditional and irregular warfare. True hybridization included the holistic integration of information which was in itself a unified whole, with content intertwined alongside conduit.

According to Jolanta Darczewska of the Centre for Eastern Studies, Russian IO does not separate the employment of information for psychological effect from the technical advantages of the conduit system during actual execution. In fact, Darczewska argues that modern, post-Cold War Russian IO remains a continuation of the ideological and disinformation practices historically dominant within Soviet information doctrine.[94] Certainly advances in technology and innovation have expanded Russia's use of information in the 21st century. However, Darczewsak

[92] Armistead, *Information Operations*, 192–197. The political-psychological dimensions of Russian information warfare revealed a profound connectedness between Russia's military operations and greater national strategy. Furthermore, Russia's graduated acceptance of hybrid warfare concepts necessitated a symbiotic integration between the political and military entities. By understanding the psychological elements of action—whether military or not—as being directly tied to the greater strategy of the state, Russian IO never separated politics from military action. For the delineation of Russia's renewed forms of warfare, see Timothy Thomas, "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking," *The Journal of Slavic Military Studies* 29, no. 4 (October 2016): 560–567.

[93] Bettina Renz, "Russia and 'Hybrid Warfare,'" *Contemporary Politics* 22, no. 3 (September 2016): 283–300; Renz and Smith, *Going Beyond the Label*; Keir Giles, "Handbook of Russian Information Warfare" (NATO Defense College Fellowship Monograph, NATO Defense College, 2016); Thomas, "The Evolution of Russian Military Thought."

[94] Jolanta Darczewska, *The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study*, Point of View (Warsaw, Poland: Center for Eastern Studies, May 2014); Jolanta Darczewska, *The Devil Is in the Details: Information Warfare in the Light of Russia's Military Doctrine*, Point of View (Warsaw, Poland: Centre for Eastern Studies, May 19, 2015).

argues that the use of cyberspace and the digital domain continues to remain subordinate to the greater purpose of Russian information warfare which targets the cognitive perceptions and psychology of its intended audience. In many respects, this holistic appreciation of the information environment remains a continuation of ideological warfare reminiscent of the East versus West paradigm at the height of the Cold War. While the 1990s appeared to have had brought an end to Communist history, Darczewska contends that Russia has remained unchanged in its mindset of challenging the current international system for the purposes of degrading Western democracies.[95]

Maria Hellman and Charlotte Wagnsson of the Swedish Defence University argue that Russian revisionist aspirations seek to delegitimize the core democratic values of European democracies, and that information serves as a tool for countering Western culture. Hellman and Wagnsson contend that the Russian narrative takes precedence over the technological innovations within information systems conduits, despite the Russian development of these technologies.[96] They emphasize the primacy of information content which supersedes the conduit system; Russia views the conduit as merely a means to the end. Thus, not only does Russian information warfare combine the divided aspects of information during military operations, it prioritizes the content of information as being more critical than the technical system of information due to the psychological value and impact of the former over the latter.[97] In this respect, Russian information warfare emphasizes the message of information over its medium—the content over the actual system—just the opposite of the current US prioritization of cyberspace operations.

---

[95] Jolanta Darczewska, *The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study*, Point of View (Warsaw, Poland: Center for Eastern Studies, May 2014); Jolanta Darczewska, "The Information War on Ukraine: New Challenges" (presented at the Great Debate Paper, Paris, France: Cicero Foundation, 2014).

[96] Hellman and Wagnsson, "How Can European States Respond to Russian Information Warfare? An Analytical Framework," 154.

[97] Darczewska, *Active Measures*; Darczewska, *The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study*.

Russian Centralization of Information

In Russia, information is not only centralized in its conceptual understanding but is also centralized between the differentiated levels of IO capabilities available to the state. This streamlined vertical organizational structure enables analysis, production, and dissemination, and is the central characteristic of Russian IO. Such centralization can be seen in the relationship between the government and the Russian media. It can also be seen in the organizational hierarchies within the Russian bureaucracy.[98]

Russia's current use and reliance on state-sponsored media broadcast companies such as RT (formerly known as Russia Today) and RIA *Novosti*, are examples of the heavily streamlined structure and approach which allow the Russian state to combine the effects of information at the strategic level, to the events of the tactical and operational levels of war.[99] Following lessons learned from Georgia in 2008, RT made major adjustments in how it reported ongoing military operations. These changes helped RT became a dominant news source in Russia's invasion of Ukraine in 2014, and continued to control the regional media environment during Russia's military operations in Ukraine's Donbas region.[100]

---

[98] Consider Vladimir Putin's quote emphasizing the importance of centralized command and control for decision-making in 2014: "I gave the orders and instructions to the Ministry of Defense…to deploy a special division of the Main Intelligence [Directorate] together with naval infantry forces and paratroopers…Do you know what our advantage was? It was the fact that I managed this personally. Not because I did everything correctly, but because, when the highest authorities of the state do this, it's easier for the enforcers to do their work." In Yashin and Shorina, *Putin.War: Based on Materials from Boris Nemtsov*, 15.

[99] Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War," *The New York Times*, September 13, 2017, sec. Magazine, accessed October 8, 2017, https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html; Digital Forensics Research Lab, "Question That: RT's Military Mission," *@DFRLab*, last modified January 8, 2018, accessed February 8, 2018, https://medium.com/dfrlab/question-that-rts-military-mission-4c4bd9f72c88.

[100] Maria Snegovaya, *Putin's Information Warfare in Ukraine*, Russia Report (Washington, DC: Institute for the Study of War, September 2015), 15–19; Timothy Thomas, "Russia's Military Strategy and Ukraine: Indirect, Asymmetric—and Putin-Led," *The Journal of Slavic Military Studies* 28, no. 3 (July 3, 2015): 446, 456; NATO Strategic Communications Centre of Excellence, "Analysis of Russia's Information Campaign against Ukraine" (NATO Strategic Communications Centre of Excellence, 2014), 2–3, accessed July 22, 2017, https://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine; Jolanta Darczewska, "The Information War on Ukraine," 8, 11–13.

While RT and RIA *Novosti* are in some ways equivalent to international news agencies such as CNN or BBC, both RT and RIA *Novosti* remain state-funded entities who are not sheepish about disclosing their offensive mission. According to numerous interviews, both RT and RIA *Novosti* seek to voice the Russian story and perspective in a global media environment.[101] RT specifically seeks to fight in the narrative space to support the overall goals of the Russian state.[102] Thus, RT's core function becomes part and parcel to the strategic goals and purposes of the Russian government; the media organization serves as a combative arm of Russian strategy during the course of military operations, as showcased in Georgia and Ukraine. As RT's Chief Editor Margarita Simonyan openly advocates, RT's mission is to "weaponize its use of information" for the purposes of advancing the Russian narrative.[103]

In addition to the coordination between media and governmental organizations, Russia also appears to be streamlining IO structures within the government. Details on much of Russia's organization of information capabilities is limited. However, one area that is somewhat visible is the Russian military restructuring, specifically its structural changes to Russian *Spetsnaz*. In 2013, Russia's Ministry of Defense established a Special Operations Command (SOC) akin to USSOCOM.[104] The intent behind this centralization was the internal bureaucratic challenge

---

[101] Margarita Simonyan, "RT's Editor-in-Chief on Election Meddling, Being Labeled Russian Propaganda," January 7, 2018, accessed January 25, 2018, https://www.cbsnews.com/news/rt-editor-in-chief-on-election-meddling-russian-propaganda-label/; Stephen Ennis, "Kremlin's Global Media Operation Under the Spotlight," *BBC News* (London, UK, November 16, 2014), sec. Europe, accessed October 25, 2017, http://www.bbc.com/news/world-europe-30040363.

[102] Simonyan, "Election Meddling and Russian Propaganda."

[103] Rutenberg, "RT, Sputnik and Russia's New Theory of War"; Simonyan, "Election Meddling and Russian Propaganda."

[104] Defense Intelligence Agency, *Russia Military Power*; Tor Bukkvoll, "Russian Special Operations Forces in Crimea and Donbas," *Parameters* 46, no. 2 (Summer 2016): 13–21; Tor Bukkvoll, "Military Innovation Under Authoritarian Government - the Case of Russian Special Operations Forces," *Journal of Strategic Studies* 38, no. 5 (August 26, 2015): 602–625; US Army Special Operations Command, *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014* (Fort Bragg, NC: US Army Special Operations Command, 2015).

presented by a dispersed *Spetsnaz* force.[105] Prior to the creation of SOC, *Spetsnaz* had brigades spread across the country, an organizational structure that created problems of synchronization. *Spetsnaz* were located not only within the Main Intelligence Directorate, but also within Russia's Federal Security Service and Foreign Intelligence Service. These three interagency entities are all outside of the Ministry of Defense structure. The driving purpose of SOC was thus to enable the streamlining and centralization of disparate *Spetznaz* capabilities spread throughout the country, which were in dire need of a formalized system for communication and information sharing.[106]

Furthermore, Russia's conception of SOF incorporates its intelligence assets in a holistic manner alongside its operations. Darczewska attributes this to the current structure being the progeny of Soviet information warfare, which arose from the USSR's centralized union of intelligence and psychological warfare units.[107] When Russian forces attempt to conduct perception management and deception operations during information warfare, the authorities and permissions necessary for such IO already exist within the command structure of SOC and the Main Intelligence Directorate.[108] The authorities for IO do not have to be coordinated from a separate intelligence entity. Thus, Russia's holistic understanding of IO includes the functions of intelligence, which is organizationally integrated with military operations.

While there has been an intense academic attention paid to Russian information warfare since Crimea in 2014, in conjunction with the more popular study of hybrid warfare, much of Russia's use of IO nevertheless remains opaque to Western study.[109] Some see this

---

[105] Bukkvoll, "Russian Special Operations Forces in Crimea and Donbas," 13–15.

[106] Ibid., 15; Bukkvoll, "Military Innovation Under Authoritarian Government - the Case of Russian Special Operations Forces," 602–605.

[107] Darczewska, *Active Measures*, 12–27.

[108] Renz and Smith, *Going Beyond the Label*, 26–30; Bettina Renz, "Russian Military Capabilities after 20 Years of Reform," *Survival* 56, no. 3 (July 2014): 67; Bettina Renz, "Russia's 'Force Structures' and the Study of Civil-Military Relations," *Journal of Slavic Military Studies* 18, no. 4 (January 25, 2005): 563, 571–574.

[109] Renz and Smith, *Going Beyond the Label*, 18; Renz, "Russia's 'Force Structures,'" 560.

impenetrability as an inheritance from Russia's history as a communist society, and modern Russian society simply continues that lack of transparency as a way of life.[110] Yet, it has also been Russia's familiarity with autocratic rule and governance which may have allowed it to centralize its practice of information warfare for the purposes of Russian strategy.[111]

Summary of Findings

The post-Cold War evolution of Russian information warfare has been a learning process for the Russian state. Since its Estonian intervention in 2007, Russia has had to endure its own trial and error leading through Georgia in 2008 and thereafter. What Western institutions have regarded as a seemingly successful Russian information warfare, has been a work-in-progress development. Russia's efforts were neither prescient in strategy nor boilerplate in doctrine from their beginnings in 2007.[112] Russians have pushed the envelope of their information warfare practice despite heavy losses in information credibility and blowback to state legitimacy.[113] Therefore, while it is important to learn from the Russian implementation of IO and information warfare, it is also important to note that this Russian way of war is not without potential setbacks. However, in terms of a holistic understanding of information, and organizational structures to support that interconnected view, Russia does offer some valuable lessons.

---

[110] Darczewska, *Active Measures*, 35–36, 60–63.

[111] Bukkvoll, "Military Innovation Under Authoritarian Government - the Case of Russian Special Operations Forces," 620.

[112] Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," 59–62; Darczewska, *Active Measures*, 45–47; Renz and Thornton, "Russian Military Modernization," 45–46; Bukkvoll, "Russia's Military Performance in Georgia," 57.

[113] Keir Giles and Andrew Monaghan, *Russian Military Transformation - Goal in Sight?*, The Letort Papers (Carlisle, PA: Strategic Studies Institute, US Army War College, May 2014).

In terms of this holistic understanding of information, contemporary theory and practice of Russian information warfare models itself after the nation's traditional understanding of information warfare dating back to the USSR.[114] Much of that understanding emphasized the cognitive approach to conducting IO, which placed the role of perception management and psychological warfare at the forefront of information warfare. While Russia's way of information warfare emphasized the advantages and developments garnered through technological innovation, ultimately, the strength of their IO was through the combined exercise of the content and conduit of information.

In addition to this holistic interpretation of information, the modern Russian state today also conducts information warfare in a much more streamlined fashion due to the centralization of its military and state apparatus.[115] This latter form of holism is an additional important component of Russia's practice of information warfare, based on an organizational structure that has much more fusion between the political and the military aspects. Furthermore, contemporary Russian information concepts capture a large swath of intelligence activities and collections, which in the US are typically an integrated but distinct field of military operations, remaining separate from US IO force structures. The field of Russian intelligence remains part and parcel of the larger whole of Russian information warfare, which mitigates the challenges of authorities and delegation that are common in the decentralized American military IO organization.

---

[114] Darczewska, *Devil Is in the Details*; Darczewska, *The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study*; Keir Giles, *Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, Research Paper (London, UK: Chatham House, The Royal Institute of International Affairs, March 2016); Timothy Thomas, "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking," *Journal of Slavic Military Studies* 29, no. 4 (October 14, 2016): 554–575.

[115] Bukkvoll, "Why Putin Went to War"; Bukkvoll, "Military Innovation Under Authoritarian Government - the Case of Russian Special Operations Forces"; Gustav Gressel, "Russia's Quiet Military Revolution, and What It Means for Europe," *European Council on Foreign Relations*, no. 143, Policy Brief (October 2015): 18; Bettina Renz, "Putin's Militocracy? An Alternative Interpretation of Siloviki in Contemporary Russian Politics," *Europe-Asia Studies* 58, no. 6 (September 2006): 903–924; Renz, "Russia's 'Force Structures.'"

In sum, Russia offers an alternative view of IO, conducted by both the military and political apparatus, which has strong implications for the future of information warfare. Through its way of conceptualizing information as a whole, and the manner in which it has streamlined its decision-making by lateral and vertical centralization, the contemporary Russian security apparatus has adapted and evolved to the demands of the post-Cold War information age. However, this type of all-encompassing framework seems unlikely to develop in the current organizational context of US DoD, given that the US military has yet to even centralize or consolidate the multiple sub-functions of information into one cohesive and functional entity.

Conclusion

Despite the overarching concept of information as the new Joint Function, US DoD continues to disaggregate information into two parts: content and conduit. This can be seen in the established organizational path set for USCYBERCOM, and the continued separation of US military IO forces responsible for information content. However, the challenge of streamlining organizational functions and processes in the contemporary era will continue to persist as long as the US military continues to disaggregate the information specialties across its organization.[116] It has been the American tendency to formalize the sub-components of information warfare and further separate the capabilities within IO, as opposed to centralizing all of its activities into one functional element of American strategic and military power. This may prevent the United States from readily meeting the challenges of 21st century information warfare.

Prior to the advent of organizational management and change management within organizational theory, American scholars valued the role hierarchies and structures played in the construction of organizations. Even neoclassical organizational theory, which stresses decentralized networks and adaptation, still notes the importance of an underlying hierarchy.

[116] US Department of Defense, *Summary of the 2018 National Defense Strategy* (Washington, DC: US Department of Defense, 2018), 7, 10–11.

While the concept of organizational decentralization may make organizations more flexible and adaptive, the benefits garnered through decentralized structures cannot be supported without some establishing hierarchy.

As American information warfare forces continue to separate its IO, PA, PO, EW and CO forces into different branches with different organizational support structures, there is less room for US military adaptation to address the realities of today's operational environment. While organizational parochialism is natural during a process of military adaptation, in order for American information warfare to be effective, this monograph argues that the US military must revisit and revise its current methods of separating its IO forces into the systems-technical and the content-oriented fields. Specifically, this paper argues that US DoD should centralize IO task organization in two ways. First, the information-related officer must be given command authority over IRCs, in order to successfully synchronize and coordinate them. Second, the overall structure of US DoD information organization should be reworked so that both content and conduit are represented at the FCC level.

As discussed in the case study of Russian information warfare, Russian theory and concepts have always delineated the psychological aspects of information content from the technicalities of its conduit. While the disaggregation of information between its information-psychological and conduit system remained useful in developing future capabilities for the information age, Russian information theory did not advocate the complete separation of the information variables during the actual course of war. In fact, Russian information warfare practices still regard information as being part of a greater system of warfare. This holistic viewpoint allowed Russian hybrid warfare to shape the operational environment with great effectiveness. Through its tendency to conceptualize the whole of information alongside its tendency for organizational centralization the current Russian practice of information warfare offers an alternative structure for information organization.

The identification of information as the new Joint Function within US DoD is a positive step for understanding the role of information. However, the task of organizational adaptation to fully integrate this function remains undone. Continuing to question the working framework of American IO's coordination and synchronization mission in the face of complex changes taking place within a digitized information domain remains the central task in understanding how the US military can successfully adapt to the contemporary information environment.

Bibliography

Admiral Michael Rogers. “Are We Organized and Aligned to Fight the Cyber War?” Youtube, February 23, 2017. Accessed September 6, 2017. https://www.youtube.com/watch?v=d8WITQuOQFI.

Allison, Graham T., and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis*. 2nd ed. New York, NY: Longman, 1999.

Ancker, Clinton. “The Evolution of Mission Command in US Army Doctrine, 1905 to the Present.” *Military Review* 93, no. 2 (April 2013): 42–52.

Applebaum, Anne. “World Inaction: Russia Invades Georgia While the West Watches.” *Slate Magazine*. Last modified August 8, 2008. Accessed October 10, 2017. http://www.slate.com/articles/news_and_politics/foreigners/2008/08/world_inaction.html.

Argyris, Chris, and Donald A. Schön. *Organizational Learning: A Theory of Action Perspective*. Addison-Wesley Organizational Development Series. Reading, MA: Addison-Wesley, 1978.

Armistead, Leigh, ed. *Information Operations: Warfare and the Hard Reality of Soft Power*. Washington, DC: Brassey’s, 2004.

———, ed. *Information Warfare: Separating Hype from Reality*. Washington, DC: Potomac Books, 2007.

Arquilla, John, and David F. Ronfeldt. *Cyberwar Is Coming*. Santa Monica, CA: RAND Corporation, 1993.

———, eds. *In Athena’s Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND Corporation, 1997.

———. *The Advent of Netwar*. Santa Monica, CA: RAND Corporation, 1996.

———. *The Emergence of Noopolitik: Toward an American Information Strategy*. Santa Monica, CA: RAND Corporation, 1999.

Associated Press. “Top U.S. Intelligence Official: Russia Stopped Hacking After U.S. Warnings.” *RadioFreeEurope/RadioLiberty*. Last modified November 17, 2016. Accessed September 6, 2017. https://www.rferl.org/a/clapper-russia-hacking-warnings/28124781.html.

Barno, David, and Nora Bensahel. “Six Ways to Fix the Army’s Culture.” *War on the Rocks*. Last modified September 6, 2016. Accessed July 14, 2017. https://warontherocks.com/2016/09/six-ways-to-fix-the-armys-culture/.

———. “Three Things the Army Chief of Staff Wants You to Know.” *War on the Rocks*. Last modified May 23, 2017. Accessed July 14, 2017. https://warontherocks.com/2017/05/three-things-the-army-chief-of-staff-wants-you-to-know/.

Bartles, Charles. “Getting Gerasimov Right.” *Military Review* 96, no. 1 (February 28, 2016): 30–38.

Betz, David. “The More You Know, the Less You Understand: The Problem with Information Warfare.” *Journal of Strategic Studies* 29, no. 3 (August 16, 2006): 505–533.

Blank, Stephen, and Richard Weitz, eds. *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*. Carlisle, PA: Strategic Studies Institute, US Army War College, 2010. Accessed July 29, 2017.

Bukkvoll, Tor. “Military Innovation Under Authoritarian Government - the Case of Russian Special Operations Forces.” *Journal of Strategic Studies* 38, no. 5 (August 26, 2015): 602–625.

———. “Off the Cuff Politics—Explaining Russia’s Lack of a Ukraine Strategy.” *Europe-Asia Studies* 53, no. 8 (December 2001): 1141–1157.

———. “Russia May Gain Small and Lose Big.” *POLITICO*. Last modified March 19, 2014. Accessed March 22, 2017. https://www.politico.eu/article/russia-may-gain-small-and-lose-big/.

———. “Russian Special Operations Forces in Crimea and Donbas.” *Parameters* 46, no. 2 (Summer 2016): 13–21.

———. “Russia’s Military Performance in Georgia.” *Military Review* 89, no. 6 (December 11, 2009): 57.

———. *The Russian Defence Industry – Status, Reforms and Prospects*. Kjeller, Norway: Norwegian Defence Research Establishment. Accessed June 3, 2013. https://www.ffi.no/no/Rapporter/13-00616.pdf.

———. “Why Putin Went to War: Ideology, Interests and Decision-Making in the Russian Use of Force in Crimea and Donbas.” *Contemporary Politics* 22, no. 3 (September 2016): 267–282.

Carnegie Endowment for International Peace. *Concurrent Session I - Cyber Weapons and Strategic Stability*. Webpage Video. Vol. Concurrent Session 1. Carnegie International Nuclear Policy Conference, 2017. Accessed September 6, 2017. http://carnegieendowment.org/2017/03/20/concurrent-session-i-cyber-weapons-and-strategic-stability-pub-67884.

Chen, Adrian. “The Agency.” *The New York Times*, June 2, 2015, sec. Magazine. Accessed July 28, 2017. https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

Chivers, C.J. “In Georgia and Russia, a Perfect Brew for a Blowup.” *New York Times*. New York, NY, August 10, 2008, sec. Europe. Accessed October 10, 2017. https://www.nytimes.com/2008/08/11/world/europe/11ticktock.html.

Cohen, Ariel, and Robert Hamilton. *The Russian Military and the Georgia War: Lessons and Implications*. Carlisle, PA: Strategic Studies Institute, US Army War College, June 2011.

Copeland, Thomas E., ed. *The Information Revolution and National Security*. Carlisle, PA: Strategic Studies Institute, US Army War College, 2000.

Czuperski, Maksymilian Czuperski, John Herbst, Eliot Higgins, Alina Polyakova, and Damon, John Herbst, Eliot Higgins, Alina Polyakova, and Damon Wilson. *Hiding in Plain Sight: Putin’s War in Ukraine*. Washington, DC: Atlantic Council, 2015. Accessed December 30, 2017.

http://www.atlanticcouncil.org/publications/reports/hiding-in-plain-sight-putin-s-war-in-ukraine-and-boris-nemtsov-s-putin-war.

Darczewska, Jolanta. *Active Measures: Russia's Key Export*. Point of View. Warsaw, Poland: Centre for Eastern Studies, May 30, 2017. Accessed November 13, 2017. https://www.osw.waw.pl/en/publikacje/point-view/2017-05-30/active-measures-russias-key-export.

———. *Russia's Armed Forces on the Information War Front*. OSW Studies. Warsaw, Poland: Centre for Eastern Studies, June 27, 2016. Accessed October 7, 2017. https://www.osw.waw.pl/en/publikacje/osw-studies/2016-06-27/russias-armed-forces-information-war-front-strategic-documents.

———. *The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study*. Point of View. Warsaw, Poland: Center for Eastern Studies, May 2014. Accessed October 7, 2017. https://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study.

———. *The Devil Is in the Details: Information Warfare in the Light of Russia's Military Doctrine*. Point of View. Warsaw, Poland: Centre for Eastern Studies, May 19, 2015. Accessed November 13, 2017. https://www.osw.waw.pl/en/publikacje/point-view/2015-05-19/devil-details-information-warfare-light-russias-military-doctrine.

———. "The Information War on Ukraine: New Challenges." Paris, France: Cicero Foundation, 2014. Accessed November 13, 2017. http://www.cicerofoundation.org/lectures/Jolanta_Darczewska_Info_War_Ukraine.pdf.

Defense Intelligence Agency. *Russia Military Power: Building a Military to Support Great Power Aspirations*. Washington, DC: US Defense Intelligence Agency, 2017.

Dempsey, Judy. "NATO Is Unprepared for Conflict With Russia." *Carnegie Europe*. Last modified August 19, 2015. Accessed December 30, 2017. http://carnegieeurope.eu/2015/08/19/nato-is-unprepared-for-conflict-with-russia-pub-61058.

Deutsche Welle. "Spiegel: NATO Unprepared If Russia Moved into Baltic Members." *DW*. Last modified May 18, 2014. Accessed December 30, 2017. http://www.dw.com/en/spiegel-nato-unprepared-if-russia-moved-into-baltic-members/a-17643795.

Digital Forensics Research Lab. "Question That: RT's Military Mission." *@DFRLab*. Last modified January 8, 2018. Accessed February 8, 2018. https://medium.com/dfrlab/question-that-rts-military-mission-4c4bd9f72c88.

Drucker, Peter F. *Managing in a Time of Great Change*. New York, NY: Truman Talley Books/Dutton, 1995.

Ducheine, Paul, and Frans Osinga, eds. *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities to Crises*. Hague, Netherlands: T.M.C. Asser, 2017.

Ennis, Stephen. "Kremlin's Global Media Operation Under the Spotlight." *BBC News*. London, UK, November 16, 2014, sec. Europe. Accessed October 25, 2017. http://www.bbc.com/news/world-europe-30040363.

Follett, Mary Parker, and Pauline Graham, eds. *Mary Parker Follett - Prophet of Management: A Celebration of Writings from the 1920s*. Harvard Business School Press Classics. Boston, MA: Harvard Business School Press, 1995.

Franke, Ulrik. *War by Non-Military Means*. Swedish Defense Research Agency, March 2015.

Galbraith, Jay R., and Edward E. Lawler. *Organizing for the Future: The New Logic for Managing Complex Organizations*. 1st ed. The Jossey-Bass Management. San Francisco, CA: Jossey-Bass Publishers, 1993.

Galula, David. *Counterinsurgency Warfare: Theory and Practice*. New Edition. Santa Barbara, CA: Praeger Security International, 2010.

Giles, Keir. *Assessing Russia's Reorganized and Rearmed Military*. Task Force on US Policy Toward Russia, Ukraine, and Eurasia. New York, NY: Carnegie Endowment for International Peace, 2017. Accessed November 30, 2017. http://carnegieendowment.org/files/5.4.2017_Keir_Giles_RussiaMilitary.pdf.

———. "Countering Russian Information Operations in the Age of Social Media." *Council on Foreign Relations*. Last modified November 21, 2017. Accessed November 28, 2017. https://www.cfr.org/report/countering-russian-information-operations-age-social-media.

———. "Handbook of Russian Information Warfare." NATO Defense College Fellowship Monograph, NATO Defense College, 2016.

———. *Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. Research Paper. London, UK: Chatham House, The Royal Institute of International Affairs, March 2016.

Giles, Keir, and Andrew Monaghan. *Russian Military Transformation - Goal in Sight?* The Letort Papers. Carlisle, PA: Strategic Studies Institute, US Army War College, May 2014.

Goldman, Emily. *Information and Revolutions in Military Affairs*. London, UK: Routledge, 2015.

Goldman, Emily, and John Arquila, eds. *Cyber Analogies*. Monterey, CA: Naval Postgraduate School, 2014. Accessed August 12, 2017.

Gongora, Thierry, and Harald Von Riekhoff, eds. *Toward a Revolution in Military Affairs? Defense and Security at the Dawn of the Twenty-First Century*. Contributions in military studies 197. Westport, CT: Greenwood Press, 2000.

Gressel, Gustav. "Russia's Quiet Military Revolution, and What It Means for Europe." *European Council on Foreign Relations*, no. 143. Policy Brief (October 2015): 18.

Haigh, Maria, Thomas Haigh, and Nadine Kozak. "Stopping Fake News: The Work Practices of Peer-to-Peer Counter Propaganda." *Journalism Studies* (April 25, 2017).

Hatch, Mary Jo, and Ann L. Cunliffe. *Organization Theory: Modern, Symbolic, and Postmodern Perspectives*. 2nd ed. Oxford, UK ; New York, NY: Oxford University Press, 2006.

Hellman, Maria, and Charlotte Wagnsson. “How Can European States Respond to Russian Information Warfare? An Analytical Framework.” *European Security* 26, no. 2 (March 1, 2017): 153–170.

Herzog, Stephen. “Country in Focus: Ten Years After the Estonian Cyberattacks.” *Georgetown Journal of International Affairs* 18, no. 3 (Fall 2017): 67–78.

Hundley, Richard O. *Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us about Transforming the U.S. Military?* Santa Monica, CA: RAND Corporation, 1999.

Hundley, Richard O., Robert Anderson, John Arquilla, and Roger C. Molander, eds. “Security in Cyberspace: Challenges for Society.” Santa Monica, CA: RAND Corporation, 1996.

Iasiello, Emilio. “Russia’s Improved Information Operations: From Georgia to Crimea.” *Parameters* 47, no. 2. Innovations in Warfare and Strategy (2017).

Inglis, John, Michael Lumpkin, Rand Waltzman, and Clint Watts. *Cyber-Enabled Information Operations*. Washington, DC: US Senate, 2017. Accessed December 7, 2017. https://www.armed-services.senate.gov/hearings/17-04-27-cyber-enabled-information-operations.

Inkster, Nigel. “Information Warfare and the US Presidential Election.” *Survival* 58, no. 5 (November 2016): 23–32.

Janowitz, Morris. “Changing Patterns of Organizational Authority: The Military Establishment.” *Administrative Science Quarterly* 3, no. 4 (March 1959): 473–493.

Kelley, Paul, Graham T. Allison, and Richard Garwin. *Nonlethal Weapons and Capabilities*. Washington, DC: Council on Foreign Relations, February 2004. Accessed January 5, 2018. https://www.cfr.org/report/nonlethal-weapons-and-capabilities.

Knox, MacGregor, and Williamson Murray, eds. *The Dynamics of Military Revolution, 1300-2050*. Cambridge, UK ; New York, NY: Cambridge University Press, 2001.

Kofman, Michael. “The ABCs of Russian Military Power: A Primer for the New Administration.” *National Interest* (February 2, 2017). Accessed August 29, 2017. http://nationalinterest.org/print/feature/the-abcs-russian-military-power-primer-the-new-19299.

Kotter, John P. *Power and Influence*. New York, NY: Free Press, 1985.

Larrabee, F. Stephen. “Russia, Ukraine, and Central Europe: The Return of Geopolitics.” *Journal of International Affairs* 5 (Spring 2010). Accessed July 22, 2017. https://jia.sipa.columbia.edu/russia-ukraine-and-central-europe-return-geopolitics.

Larrabee, F. Stephen, Stephanie Pezard, Andrew Radin, Nathan Chandler, Keith Crane, and Thomas Szayna. *Russia and the West After the Ukrainian Crisis: European Vulnerabilities to Russian Pressures*. Santa Monica, CA: RAND Corporation, 2017. Accessed December 15, 2017. https://www.rand.org/pubs/research_ reports/RR1305.html.

Laurence, Janice H. “Military Leadership and the Complexity of Combat Culture.” *Military Psychology* 23, no. 5 (September 2011): 489–501.

Lucas, Edward, and Peter Pomeranzev. *Winning the Information War*. Washington, DC: Center for European Policy Analysis, August 2, 2016. Accessed December 9, 2017. http://cepa.org/reports/winning-the-Information-War.

MacFarquhar, Neil. "A Powerful Russian Weapon: The Spread of False Stories." *New York Times*, August 28, 2016, sec. Europe. https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html.

MacLellan, Kylie. "'Complacent' NATO Unprepared for Russian Threat: British Lawmakers." *Reuters*. Last modified July 31, 2014. Accessed December 30, 2017. https://www.reuters.com/article/us-ukraine-crisis-britain-nato/complacent-nato-unprepared-for-russian-threat-british-lawmakers-idUSKBN0FZ2M920140731.

March, James G. *A Primer on Decision Making: How Decisions Happen*. New York, NY: Free Press, 2010.

March, James G., and Herbert A. Simon. *Organizations*. 2nd ed. Cambridge, MA: Blackwell Publishers, 1993.

Mearsheimer, John. "Back to the Future." *International Security* 15, no. 1 (Summer 1990): 5–56.

Mearsheimer, John, Stanley Hoffman, and Robert Keohane. "Back to the Future, Part II: International Relations Theory and Post-Cold War Europe." *International Security* 15, no. 2 (Fall 1990): 191–199.

Mearsheimer, John, Bruce Russett, and Thomas Risse-Kappen. "Back to the Future, Part III: Realism and the Realities of European Security." *International Security* 15, no. 3 (Winter 1990/1991): 216–222.

Milley, Mark. "Commanders Series Event with Chief of Staff of the Army, General Mark Milley," May 4, 2017. Accessed October 14, 2017. http://www.atlanticcouncil.org/events/past-events/commanders-series-event-with-chief-of-staff-of-the-army-general-mark-milley.

———. "Eisenhower Luncheon Address." Washington, DC, October 4, 2016. Accessed September 14, 2017. https://www.ausa.org/events/ausa-annual-meeting-exposition/sessions/eisenhower-luncheon.

Morgan, Wesley. "U.S. Army Unprepared to Deal with Russia in Europe." *POLITICO*. Last modified September 2, 2017. Accessed December 30, 2017. https://www.politico.com/story/2017/09/02/army-study-173rd-airborne-brigade-europe-russia-242273.

NATO Strategic Communications Centre of Excellence. "Analysis of Russia's Information Campaign against Ukraine." NATO Strategic Communications Centre of Excellence, 2014. Accessed July 22, 2017. https://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine.

Nikolsky, Alexey. "Little, Green and Polite: The Creation of Russian Special Operations Forces." In *Brothers Armed: Military Aspects of the Crisis in Ukraine*. 2nd ed. East View Press, 2015.

Nimmon, Ben. "Question That: RT's Military Mission." *Digital Forensics Research Lab*. Last modified January 8, 2018. Accessed February 28, 2018. https://medium.com/dfrlab/question-that-rts-military-mission-4c4bd9f72c88.

Pallin, Carolina Vendil. “Internet Control Through Ownership: The Case of Russia.” *Post-Soviet Affairs* 33, no. 1 (2017): 16–33.

Phillipson, Robert. “Leeroy Jenkins and Mission Command.” *Military Review Online Exclusive* (May 2017). Accessed July 14, 2017. http://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2017-Online-Exclusive-Articles/Leeroy-Jenkins-and-Mission-Command/.

Pomerantsev, Peter, and Michael Weiss. *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. Special Report. New York, NY: Institute of Modern Russia, 2014.

Poznansky, Michael. “The Ordinary and Unique in Russia’s Electoral Information Warfare Game.” *War on the Rocks*, September 1, 2016. Accessed July 20, 2017. https://warontherocks.com/2016/09/the-ordinary-and-unique-in-russias-electoral-information-warfare-game/.

Renz, Bettina. “Putin’s Militocracy? An Alternative Interpretation of Siloviki in Contemporary Russian Politics.” *Europe-Asia Studies* 58, no. 6 (September 2006): 903–924.

———. “Russia and ‘Hybrid Warfare.’” *Contemporary Politics* 22, no. 3 (September 2016): 283–300.

———. “Russian Military Capabilities after 20 Years of Reform.” *Survival* 56, no. 3 (July 2014): 61–84.

———. “Russia’s ‘Force Structures’ and the Study of Civil-Military Relations.” *Journal of Slavic Military Studies* 18, no. 4 (January 25, 2005): 559–585.

———. “Russia’s Modernized Military: Lessons from Crimea and Syria.” *Russian Analytical Digest*, no. 196 (December 26, 2016): 14.

———. “Why Russia Is Reviving Its Conventional Military Power.” *Parameters* 46, no. 2 (Summer 2016): 14.

Renz, Bettina, and Hanna Smith, eds. *After “Hybrid Warfare”, What Next?: Understanding and Responding to Contemporary Russia*. Helsinki, Finland: Office of the Prime Minister, Finland, 2016. Accessed July 21, 2017. https://helda.helsinki.fi/handle/10138/175284.

———. *Russia and Hybrid Warfare - Going Beyond the Label*. Aleksanteri Papers. Helsinki, Finland: Kikimora Publications, University of Helsinki, 2016. Accessed July 21, 2017. https://helda.helsinki.fi/handle/10138/175291.

Renz, Bettina, and Rod Thornton. “Russian Military Modernization.” *Problems of Post-Communism* 59, no. 1 (February 2012): 44-54.

Riegert, Bernd. “Opinion: NATO Needs to Rethink Its Strategy.” *DW*. Last modified June 5, 2014. Accessed December 30, 2017. http://www.dw.com/en/opinion-nato-needs-to-rethink-its-strategy/a-17614273.

Rogers, Clifford, ed. *The Military Revolution Debate: Readings on the Military Transformation of Early Modern Europe*. Boulder, CO: Westview Press, 1995.

Rutenberg, Jim. “RT, Sputnik and Russia’s New Theory of War.” *The New York Times*, September 13, 2017, sec. Magazine. Accessed October 8, 2017. https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html.

Scales, Robert. “Clausewitz and World War IV.” *Military Psychology* 21, no. 1 (2009): 23–35.

Schwartzstein, Stuart J. D., ed. *The Information Revolution and National Security: Dimensions and Directions*. Vol. 18. 3 vols. Significant Issues Series. Washington, DC: Center for Strategic and International Studies, 1996.

Selhorst, A.J.C. “Russia’s Perception Warfare: The Development of Gerasimov’s Doctrine in Estonia and Georgia and Its Application in Ukraine.” *Militaire Spectator* 185, no. 4 (2016): 148–164.

Simon, Herbert A. *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations*. 4th ed. New York, NY: Free Press, 1997.

Simonyan, Margarita. “RT’s Editor-in-Chief on Election Meddling, Being Labeled Russian Propaganda,” January 7, 2018. Accessed January 25, 2018. https://www.cbsnews.com/news/rt-editor-in-chief-on-election-meddling-russian-propaganda-label/.

Sinovets, Polina, and Bettina Renz. *Russia’s 2014 Military Doctrine and Beyond: Threat Perceptions, Capabilities and Ambitions.* Research Paper. Rome, Italy: NATO Defense College, July 2015. http://odcnp.com.ua/images/pdf/rp_117.pdf.

Snegovaya, Maria. *Putin’s Information Warfare in Ukraine*. Russia Report. Washington, DC: Institute for the Study of War, September 2015.

Sorcher, Sara. “Poll: NATO Is Unprepared to Counter Russia.” *Defense One*. Last modified April 19, 2014. Accessed December 30, 2017. http://www.defenseone.com/politics/2014/04/poll-nato-unprepared-counter-russia/83404/.

Stahl, Roger. “Weaponizing Speech.” *Quarterly Journal of Speech* 102, no. 4 (July 29, 2016): 376–395.

Thomas, Timothy. “Russia’s Information Warfare Strategy: Can the Nation Cope in Future Conflicts?” *The Journal of Slavic Military Studies* 27, no. 1 (January 2, 2014): 101–130.

———. “Russia’s Military Strategy and Ukraine: Indirect, Asymmetric—and Putin-Led.” *The Journal of Slavic Military Studies* 28, no. 3 (July 3, 2015): 445–461.

———. “Russia’s Reflexive Control Theory and the Military.” *Journal of Slavic Military Studies* 17 (2004): 237–256.

———. “The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking.” *Journal of Slavic Military Studies* 29, no. 4 (October 14, 2016): 554–575.

Thornton, Rod. “The Changing Nature of Modern Warfare.” *The RUSI Journal* 160, no. 4 (September 2015): 40–48.

Traynor, Ian. “Russia Accused of Unleashing Cyberwar to Disable Estonia.” *The Guardian*, May 17, 2007, sec. World news. Accessed November 30, 2017. http://www.theguardian.com/world/2007/may/17/topstories3.russia.

Underhill, Jeffery. “Are the Department of Defense Non-Lethal Weapon Capabilities Adequate for the 21st Century?” US Army War College, 2006. Accessed July 20, 2017. http://www.dtic.mil/get-tr-doc/pdf?AD=ADA448 633.

US Army Special Operations Command. *“Little Green Men”: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*. Fort Bragg, NC: US Army Special Operations Command, 2015.

US Department of Defense. “Cyber Command Flexes New Acquisition Muscle.” US Department of Defense, October 12, 2017. Accessed October 27, 2017. https://www.defense.gov/News/Article/Article/1341201/cyber-command-flexes-new-acquisition-muscle/.

———. “DoD Announces First U.S. Cyber Command and First U.S. CYBERCOM Commander.” US Department of Defense, May 21, 2010. Accessed September 27, 2017. http://archive.defense.gov/releases/release.aspx?releaseid=13551.

———. “DoD Initiates Elevation Process for U.S. Cyber Command to a Unified Combatant Command.” US Department of Defense, August 18, 2017. Accessed October 27, 2017. https://www.defense.gov/News/News-Releases/News-Release-View/Article/1282920/dod-initiates-elevation-process-for-us-cyber-command-to-a-unified-combatant-com/.

———. “DoD Strategy for Operations in the Information Environment.” US Department of Defense, June 2016. Accessed September 3, 2017. https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

———. *Quadrennial Defense Review 2014*. Special Report. Washington, DC: US Department of Defense, March 4, 2014. Accessed December 30, 2017. https://www.defense.gov/News/Special-Reports/QDR/.

———. *Summary of the 2018 National Defense Strategy*. Washington, DC: US Department of Defense, 2018.

US Department of Defense Science Board. *Capabilities for Constrained Military Operations*. Washington, DC: Defense Science Board, December 21, 2016. Accessed December 2, 2017. https://www.acq.osd.mil/dsb/reports/2010s/DSBSS16_CMO.pdf.

———. *Final Report of the Defense Science Board Task Force on Cyber Deterrence*. Washington, DC: Defense Science Board, February 2017. Accessed December 9, 2017. https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

———. *Information Warfare - Defense*. Washington, DC: Defense Science Board, November 1996.

———. *Resilient Military Systems and the Advanced Cyber Threat*. Washington, DC: Defense Science Board, January 2013.

US Department of the Army. Army Doctrine Publication (ADP) 3-0, *Operations*. Washington, DC: Government Printing Office, 2016. Accessed July 24, 2017.

———. Army Doctrine Publication (ADP) 6-0, *Mission Command*. Washington, DC: Government Printing Office, 2012.

———. Army Doctrine Reference Publication (ADRP) 6-0, *Mission Command*. Washington, DC: Government Printing Office, 2012.

———. Field Manual (FM) 3-0, *Operations*. Washington, DC: Government Printing Office, 2017.

———. Field Manual (FM) 3-13, *Information Operations*. Washington, DC: Government Printing Office, 2016.

———. Field Manual (FM) 3-53, *Military Information Support Operations*. Washington, DC: Government Printing Office, 2013.

———. Field Manual (FM) 6-0, *Command and Staff Organization and Operations*. Washington, DC: Government Printing Office, 2014.

US Joint Chiefs of Staff. Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*. Washington, DC: US Joint Chiefs of Staff, 2017.

———. Joint Publication (JP) 3-13, *Information Operations*. Washington, DC: US Joint Chiefs of Staff, 2014.

US Office of the President of the United States. Presidential Decision Directive (PDD) 56: "Managing Complex Contingency Operations." *Federation of American Scientists*. Last modified May 1997.

———. Presidential Decision Directive (PDD) 68: "International Public Information." *Federation of American Scientists*. Last modified April 30, 1999.

Waltzman, Rand. "The U.S. Is Losing the Social Media War." *Time*, October 12, 2015. Accessed December 7, 2017. http://time.com/4064698/social-media-propaganda/.

———. *The Weaponization of Information, Testimony of Rand Waltzman*. Washington, DC: United States Senate, 2017. Accessed December 7, 2017. https://www.armed-services.senate.gov/hearings/17-04-27-cyber-enabled-information-operations.

Welt, Cory. *Russia: Background and U.S. Policy*. Washington, DC: Congressional Research Service, August 21, 2017. Accessed November 30, 2017. https://fas.org/sgp/crs/row/R44775.pdf.

Williams, Thomas. "Strategic Leader Readiness and Competencies for Asymmetric Warfare." *Parameters* 33, no. 2 (Summer 2003): 19–35.

Wilson, James Q. *Bureaucracy: What Government Agencies Do and Why They Do It*. New. New York, NY: Basic Books, 2000.

Yashin, Ilya, and Olga Shorina. *Putin.War: Based on Materials from Boris Nemtsov*. Moscow, Russia: Free Russia Foundation, 2015. Accessed December 30, 2017. http://4freerussia.org/putin.war/Putin.War-Eng.pdf.

"Concurrent Session I: Cyber Weapons and Strategic Stability." In *Concurrent Session I: Cyber Weapons and Strategic Stability*. Washington, DC: Carnegie Endowment for International Peace, 2017. Accessed January 7, 2018. http://carnegieendowment.org/2017/03/20/concurrent-session-i-cyber-weapons-and-strategic-stability-pub-67884.