The Art of the Cyber Jab: Using Defensive Cyberspace Operations-Response Action at Corps and Below

A Monograph

by

MAJ Tennille W. Scott
US Army

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

2018

REPORT DOCUMENTATION PAGE

Form Approved
0MB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
24-05-2018	Master's Thesis	JUL 2017 - MAY 2018

4. TITLE AND SUBTITLE

The Art of the Cyber Jab: Using Defensive Cyberspace Operations-Response Action at Corps and Below.

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

MAJ Tennille W. Scott

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

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

Defending networks, information systems, and data within the cyber domain are a necessity for ensuring freedom of maneuver for tactical elements. Defense-in-depth and line defense are forms of defense that the Department of Defense currently uses to conduct defensive cyberspace operations. However, operational and tactical commanders do not have the authorities or means to employ counter effects within cyberspace as they do within the physical domains. Case studies of the Russian attacks on Georgia in 2008 and Ukraine in 2014 demonstrate that passive defensive cyberspace operations are not sufficient to provide protection against a near-peer adversary with sophisticated cyber capabilities during combat operations. By providing an active capability, Defensive Cyberspace Operations-Response Action (DCO-RA) offers a possible solution to the problems of the inadequacy of passive defense at echelons corps and below.

15. SUBJECT TERMS

US Army; Cyberspace Operations; Defensive Cyberspace Operations-Response Action

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 Tennille Scott
(U)	(U)	(U)	(U)	37	19b. TELEPHONE NUMBER (Include area code)

Monograph Approval Page

Name of Candidate: MAJ Tennille W. Scott

Monograph Title: The Art of the Cyber Jab: Using Defensive Cyberspace Operations-Response Action at Corps and Below

Approved by:

_____, Monograph Director
Jacob A. Stoil, PhD

_____, Seminar Leader
Eric M. Remoy, 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

The Art of the Cyber Jab: Using Defensive Cyberspace Operations-Response Action at Corps and Below, by MAJ Tennille W. Scott, US Army, 37 pages.

Defending networks, information systems, and data within the cyber domain are a necessity for ensuring freedom of maneuver for tactical elements. Defense-in-depth and line defense are forms of defense that the Department of Defense currently uses to conduct defensive cyberspace operations. However, operational and tactical commanders do not have the authorities or means to employ counter effects within cyberspace as they do within the physical domains. Case studies of the Russian attacks on Georgia in 2008 and Ukraine in 2014 demonstrate that passive defensive cyberspace operations are not sufficient to provide protection against a near-peer adversary with sophisticated cyber capabilities during combat operations. By providing an active capability, Defensive Cyberspace Operations-Response Action (DCO-RA) offers a possible solution to the problems of the inadequacy of passive defense at echelons corps and below.

The primary obstacles to the implementation of DCO-RA as a viable solution are legal frameworks, capabilities, and the lack of direct precedent from which to learn. However, DCO-RA has analogies in the physical domains of warfare, counterfire and ballistic missile defense, that can provide guidance towards solving the problems of DCO-RA at the operational and tactical level. These analogies serve to demonstrate that the development and employment of DCO-RA is not an entirely new phenomenon of warfare, but rather an instance of a broader pattern. Overcoming an adversary is the art of combining what is possible with what is necessary to achieve defense. At some point the United States must stop being the world's cyber punching bag and counter its adversaries with a few cyber jabs of its own. This research demonstrates that DCO-RA, when fully and properly enabled, is capable of doing just that.

Contents

Acknowledgements

I would like to thank my monograph director, Dr. Jacob Stoil, and seminar leader, COL Eric Remoy, for their tireless assistance and guidance with this research project. I would also like to give a special thanks to my mentor and former SAMS graduate, COL(ret.) Dwayne Wagner, for his feedback, mentorship, and encouragement. To my battle buddies, MAJ Charles Slider, MAJ Jimmy McClain, MAJ Timothy Williams, MAJ Ryan Hand, and MAJ Elizabeth Marlin, your input, motivation, and shoulder to lean on has been invaluable. Last, but not least, I am blessed and grateful to have the love, patience and support of my family and friends, especially my two boys, Jaalen and Chrystopher.

Acronyms

ARCYBER	Army Cyber Command
BMD	Ballistic Missile Defense
BMDS	Ballistic Missile Defense System
CCDCOE	Cooperative Cyber Defense Center of Excellence
CEMA	Cyber Electromagnetic Activities
CERT	Computer Emergency Readiness Team
CSCB	CEMA Support to Corps and Below
CSIS	Center for Strategic and International Studies
CYBERCOM	US Cyber Command
DCO	Defensive Cyberspace Operations
DCO-RA	Defensive Cyberspace Operations-Response Action
DDoS	Distributed Denial-of-Service
DoD	Department of Defense
DODIN	DoD Information Network
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy
EW	Electronic Warfare
IPB	Intelligence Preparation of the Battlefield
ISR	Intelligence, Surveillance, and Reconnaissance
JTF	Joint Task Force
MDB	Multi-Domain Battle
NATO	North Atlantic Treaty Organization
NETCOM	US Army Network Enterprise Technology Command
OCO	Offensive Cyberspace Operations
OPLAN	Operation Plan

ROE	Rules of Engagement
SECDEF	Secretary of Defense
SOP	Standard Operating Procedure
SQL	Structured Query Language
SROE	Standing Rules of Engagement

Illustrations

Introduction

> We seem to be the cyber punching bag of the world…we get hit, and we don't retaliate … against the Russians, the North Koreans, the Chinese … they don't fear us.
>
> —Senator Dan Sullivan, US Senate Armed Service Committee

> History does not repeat, but it often rhymes.
>
> —Mark Twain

It is an undisputed and fundamental tenet of cyberspace operations that defense of networks, information systems, and data within the cyber domain are a necessity for ensuring freedom of maneuver. Commanders at corps and below do not have the authorities or means to employ counter effects within cyberspace as they do within the land domain. Defense-in-depth and line defense are forms of defense currently used to conduct defensive cyberspace operations but are not sufficient to provide protection against a near-peer with sophisticated cyber capabilities.[1] This research is significant because it will help develop a theory for active defensive cyberspace operations (DCO) in cyber warfare. It is relevant because a coherent, universally accepted approach for engaging adversaries, such as Russia and Islamic State of Iraq and the Levant, within the cyber domain, is underdeveloped.

Background and Problem

The Department of Defense (DoD) primarily employs defense-in-depth to defend in and through cyberspace. Defense-in-depth is a technique that implements layered protection that extends from the user, through information systems and out to the network. Defense-in-depth includes measures such as passwords, port security, firewalls, and intrusion detection systems. These methods are essentially forms of passive defense. At best, passive defensive measures alert

[1] The author observed this personally as an observation made while assigned to an Armored Brigade Combat Team during a National Training Center – Decisive Action rotation in 2013.

and deny intrusion attempts, but because network and system security is never one hundred percent effective, some intrusions are successful. Current doctrine limits response to incident response which are measures taken to protect networks by mitigating and denying further intrusions on friendly systems. At the time of a successful intrusion, actions to mitigate are moot, and a defender's actions are all reactive. If the defender is lucky, they can react before the network receives extensive damage. During combat operations, current defensive measures may not prove sufficient in a cyber attack. This paper will explore whether it is practical to add more active measures to the tools currently available for cyber defense. In particular, it will examine whether Defensive Cyberspace Operations-Response Action (DCO-RA) provides a valuable addition to cyber capabilities at the echelons of corps and below.

Russian cyber aggression against Georgia in 2008 and Ukraine from 2014 onwards demonstrates the intent of potential adversaries in making effective use of the cyber domain as well as the limited potential of purely defensive measures. The cyber attack against the DoD Joint Staff network in 2015, in which an adversary used a phishing campaign to exploit email servers, is indicative of the limitations and deficiencies of US passive defense. In that case, the inability of defenders to react in a timely manner resulted in the temporary shutdown of the entire network enclave.[2] The Joint Staff cyber attack also highlighted the passive and unaggressive mindset and policies of the US as it pertains to actions in cyberspace.

While commanders at corps and below have the authority to employ offensive effects to protect their force and achieve objectives in physical space, they lack similar power in the cyber domain. Counteraction is a common reaction mechanism in warfare within the physical domains, used as an inherent right to self-defense. Joint and Army doctrine identify an option for response in the cyber domain – DCO-RA. Joint Publication 3-12, *Cyberspace Operations*, defines DCO-

[2] Cory Bennett, "Pentagon Restores Hacked Network," The Hill, August 10, 2015, accessed April 23, 2018, http://thehill.com/policy/cybersecurity/250730-pentagon-restores-hacked-email-system.

RA as "deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend DoD cyberspace capabilities or other designated systems."[3] It is a subarea of cyber defense that remains theoretical. In essence, DCO-RA is a form of counteraction – a defensive response capability that employs offensive-like effects outside of the defended network.[4] Essentially, rather than purely protecting a defended network, DCO-RA targets the threat network that is attacking the defended network. This project will determine whether DCO-RA provides a viable option for commanders at corps and below in the event of a cyber attack.

In an article entitled "Cyberspace in Multi-Domain Battle," Lieutenant General Paul Nakasone, the nominee to be the next director of the National Security Agency and commander of CYBERCOM, and Major Charlie Lewis, cyber operations officer, emphasize that "One of the goals of the Department of Defense's (DoD) Cyber Strategy is the 'need to maintain viable cyber options' integrated into plans to achieve precise objectives."[5] By providing an active capability, DCO-RA could provide a solution to the problems of the inadequacy of passive defense. If viable, an active defense capability will give commanders the flexibility to respond to threats with actions in near real-time, reducing the likelihood of catastrophic compromise to information systems and data. The primary obstacles to the implementation of DCO-RA as a viable solution are legal frameworks, capabilities, and the lack of direct precedent from which to learn. However, all of the challenges to DCO-RA have analogies within that have already been addressed in the physical domains of warfare and can provide guidance towards solving the problems of DCO-RA.

---

[3] US Department of Defense, Joint Staff, Joint Publication (JP) 3-12 (Redacted), *Cyberspace Operations* (Washington, DC: Government Printing Office, 2013), II-3.

[4] US Department of the Army, Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: Government Printing Office, 2017), 1-8.

[5] Lieutenant General Paul M. Nakasone and Major Charlie Lewis, "Cyberspace in Multi-Domain Battle," *The Cyber Defense Review* 2, no. 1 (Spring 2017): 20.

Hypothesis

This project seeks to determine whether DCO-RA a viable option to employ at echelons corps and below during combat operations. Despite its potential challenges, DCO-RA may be a viable option for commanders at corps and below to respond to cyber attack, with highly restrictive conditions.

Literature Review

The topic DCO-RA, a concept within a relatively new established domain of warfare poses several issues. The first glaring issue is that cyberspace operations are a sensitive topic with limited information at the unclassified level with respect to methods, sources, testing, and capabilities, for obvious reasons. The fact that DCO-RA is a defensive action that delivers offensive-like effects means the majority of the research is most likely at the classified levels. Another issue is that adversaries have revealed the inaptitude for nation-states to sufficiently protect themselves and successfully engage in a well-coordinated cyber attack during combat operations. As a result, there is not enough historical evidence within combat operations to conduct an analysis of DCO-RA. Despite these issues, there are works available to make a case for DCO-RA for cyberspace operations at corps and below.

Virtually all of the works in support of the topic are secondary sources. A North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Center of Excellence (CCDCOE) report on the cyber attacks against Georgia in 2008 and a report entitled "Defending the Borderland" that covers Ukraine's military experiences in the cyber domain provided the data for the case studies.[6] Joint and Army doctrine covered cyberspace and fire support operations. A paper written by James N. Rosenau entitled "Thinking Theory Thoroughly" provided the idea of

[6] Aaron F. Brantley, Nerea M. Cal, and Devlin P. Winklestein, *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW* (West Point, NY: Army Cyber Institute, 2017).

analyzing DCO-RA as an instance of a broader pattern and thus seeing DCO-RA as a form of counteraction analogous to other counteraction frameworks which exist in the physical domains.[7] The *DoD Law of War Manual* and the United States Army Judge Advocate General *Operational Law Handbook* offered an understanding of the legal aspect of cyberspace operations.[8] A Center for Strategic and International Studies report entitled "Offensive Cyber Capabilities at the Operational Level" was instrumental in examining the legal constraints of using offensive capabilities at the Joint Task Force (JTF) level and below.[9]

One work that was not in support of one of the areas of discussion is a Strategic Studies Institute report written by Colin Gray entitled "Making Strategic Sense of Cyber Power: Why the Cyber Sky is Not Falling."[10] In this report, Gray asserts the link between thinking about cyber strategically and tactically is missing, and that cyber strategy is analogous to other domain strategies, but a tactical analogy is sure to be misleading and wrong. Gray's viewpoint contradicts the comparison of DCO-RA to counteraction other frameworks as put forth in this research. However, this remains unproven.

The obvious missing literature for this topic is evidence of response action as well as significant discussion about using DCO-RA as an option to respond to cyber attack. Details about the doctrinal concept of DCO-RA in theory and practice is also not available. The reasons for this could be due to information held at official use and classified levels, that cyberspace operations is

---

[7] James Rosenau, "Thinking Theory Thoroughly," in *The Scientific Study of Foreign Policy* (London: Frances Pinter, 1980): 19-31.

[8] US Department of Defense, *Department of Defense Law of War Manual* (Washington, DC: Office of General Counsel, Department of Defense, 2016); US Army Judge Advocate General, *Operational Law Handbook*, 17th ed. (Charlottesville, VA: The Judge Advocate General's Legal Center and School, 2017).

[9] Maren Leed, *Offensive Cyber Capabilities at the Operational Level: The Way Ahead* (Washington, DC: Center for Strategic and International Studies, 2013).

[10] Colin Gray, *Making Strategic Sense of Cyber Power: Why the Cyber Sky is Not Falling*, (Carlisle, PA: US Army War College Press, April 2013).

relatively new, and the sense that DCO-RA is more trouble than it is worth at the operational and tactical levels.

Methodology

The research methodology is exploratory and conducted using document analysis and a structured approach to answer the research question. First, case studies of alleged Russian cyber aggression during combat operations is analyzed to explore the cyber operational threat environment where DCO-RA can potentially be employed. Second, it will provide a description of DCO-RA as currently defined in US Joint and Army doctrine. Third, it will determine the current situation of cyber defense within the DoD through the challenges DCO-RA present at corps and below. Last, it will present possible solutions for employing DCO-RA to evaluate its viability at corps and below.

The research is limited to the analysis of network-centric cyberspace operations at the operational and tactical levels of war that is provided at the unclassified level. It does not analyze electronic warfare which is currently included in the Cyber Electromagnetic Activities (CEMA) construct at corps and below. It also does not address the technical feasibility of conducting DCO-RA. The research explores concepts and capabilities that apply to the traditional physical domains (land, air, and sea) to analyze the applicability of extending these concepts and capabilities to the cyber domain for the purpose of using DCO-RA.

The research relies heavily on secondary and technical sources such as academic and scholarly articles, essays, research, technical books and articles, and after-action reports retrieved from sources like *Cyber Defense Review*, *Small Wars Journal*, Center for Army Lessons Learned, and Defense Technical Information Center, to name a few. It will draw on the material, primarily special reports, and news articles, relating to Russian cyber attacks against Georgia and Ukraine as evidence of Russia's ability and propensity to use offensive cyber within combat operations.

The research will also review technical literature accessed primarily through internet sources, like the Army War College Library, Google Scholar, and the Combined Arms Research Library databases, to determine the viability of DCO-RA as an option for commanders at corps and below.

Case Studies

This research presents case studies of the alleged Russian cyber attacks against Georgia in 2008 and Ukraine from 2014-2016, in which synchronized cyber campaigns were carried out prior to Russia's invasion of each country. These case studies highlight instances in which a peer adversary employed cyber attack capabilities simultaneously with a military invasion to achieve strategic and tactical objectives. State-on-state cyber attacks have occurred prior to this incident, but this case demonstrates the real-world application of the theoretical concept of cyber warfare within a hybrid warfare construct. In this cyber campaign, various methods were used to achieve specific effects which ultimately exploited Georgia's and Ukraine's inability to defend themselves from cyber attack that occurred in conjunction with military aggression.

Georgia 2008

The cyber campaign carried out against Georgia during the Russo-Georgian War in 2008 was a highly coordinated effort.[11] The cyber attacks began weeks prior to ground combat in the form of reconnaissance and probing activity discovered on the Georgian government's network infrastructure.[12] Days before the ground campaign, the attackers conducted distributed denial-of-service (DDoS), web defacement, and email spamming to create effects on Georgian infrastructure. According to security experts, the attacks occurred in two phases against strategic

[11] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media, 2012), 3.

[12] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, accessed August 1, 2017. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

targets.[13] The first phase consisted of distributed denial-of-service (DDoS) attacks against Georgian government and media websites.[14] The second phase expanded the attacks to include website defacement and spamming of Georgian educational and financial institutions and businesses, using Structured Query Language (SQL) injection and cross-site scripting as attack vectors.[15] DDoS and SQL injection are preferred methods of attack because of their simplicity, low overhead, access to target infrastructure, and difficulty for attribution.[16]

The series of attacks created effects in all three layers of cyberspace (physical, logical, and cyber persona) targeted at command and control of the Georgian internet infrastructure, confusion within the information environment, and uncertainty among the Georgian populace.[17] The DDoS attacks severely disrupted Georgian internet infrastructure and systems, including public services infrastructure (banking and media).[18] Attackers defaced several government websites, including the Georgian President and Ministry of Foreign Affairs, and targeted Georgian politicians in a spamming campaign. These activities degraded and disrupted communication and information flow within Georgia and between Georgia and the international community for several days.[19] It also attempted psychological effects on the Georgian populace.[20] Presumably, the objective of the campaign was to isolate and silence Georgia from the rest of the

---

[13] Captain Paulo Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," *Military Review* (November-December 2011): 63.

[14] Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," 63.

[15] Ibid., 64.

[16] A DDoS attack is a denial-of-service (DOS) technique used to deny electronic access to networks and systems by quickly flooding targets with a large concentration of traffic originating from various external nodes. A SQL injection is an attack where a user inputs data, typically to a web-based application, in an attempt to bypass validation to gain remote access to the server.

[17] Steven Blank, "Cyber War and Information War à la Russe," in *Understanding Cyber Conflict: Fourteen Analogies*, ed. George Perkovich and Ariel E. Levite (Washington, DC: Georgetown University Press, 2017): 88-89.

[18] Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*. (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2008), 16.

[19] Ibid., 15.

[20] Blank, "Cyber War and Information War à la Russe," 89.

world and create a paralysis effect on its government and armed forces prior to commencing combat operations.[21]

The Russian cyber attacks exposed Georgia's insufficient cyber defense capabilities. Georgia lacked the intelligence support (sensing and warning) necessary to provide indicators of a pending attack.[22] Without adequate intelligence that comes from network surveillance and monitoring, a cyber defender does not have the situational awareness needed to defend against cyber attack successfully. Georgia's internet infrastructure attempted some automated cyber defense by changing internet protocol addresses and hosts of a few websites; however, it was not sufficient to absorb the enormity of the attack.[23] Georgia's information technology professionals mitigated some effects by relocating websites and portals from compromised servers in Georgia to servers of partner nations and private companies.[24] This is a slow process that requires a high level of coordination and timing. Furthermore, Georgia's cyber professionals were not appropriately organized to respond to cyber attack. Computer Emergency Readiness Team (CERT)-Georgia, the organization that typically provided network security for higher education institutions, filled the role of a national CERT during the attacks.[25] Although Russia could only exploit Georgia's weak cyber defensive posture for a discriminate period of time, they were able to successfully time the effects of the cyber attacks to dominate in the physical and cyber domains simultaneously.[26] Georgia was not able to recover its cyberspace capabilities during this critical

[21] Blank, "Cyber War and Information War à la Russe," 90.

[22] Hollis, "Cyberwar Case Study," 8.

[23] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 14-15.

[24] Ibid., 14.

[25] Ibid., 14-15.

[26] Hollis, "Cyberwar Case Study," 8.

period of conflict.[27] Figure 1 is a pictorial representation of Georgia's DCO against Russia, including a failed DCO-RA attempt.[28]

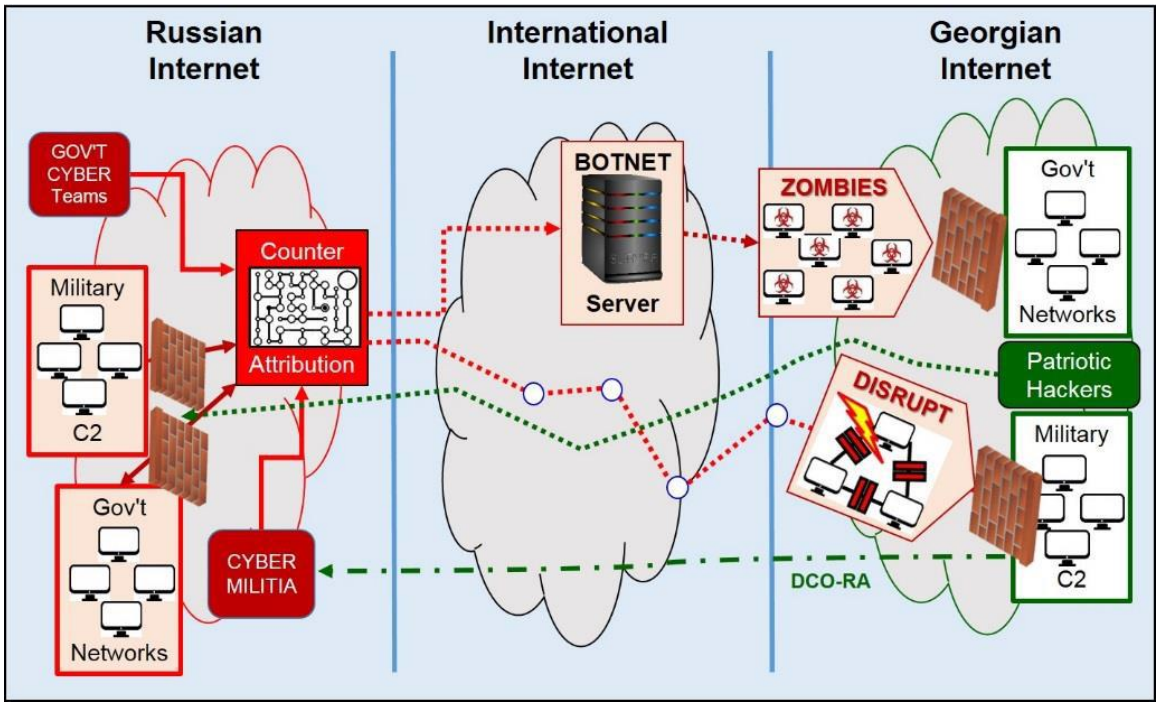

Figure 1. Georgian Defensive Cyberspace Operations. US Army War College, *Strategic Cyberspace Operations Guide,* 2016, 60.

Ukraine 2014-2016

Russia's cyber attack on Ukraine from 2014-2016 resembled the attacks on Georgia in 2008, but were expanded in scale and scope, and included new methods. Prior to occupying Crimea, Russian forces were able to exploit and conduct monitoring and surveillance on Ukrainian internet and telephone communications lines.[29] In addition to network-centric attacks, such as DDoS and web defacement, Russian forces physically attacked communications

[27] Hollis, "Cyberwar Case Study," 5.

[28] United States Army War College, *Strategic Cyberspace Operations Guide* (Carlisle, PA: Center for Strategic Leadership, June 2016), 60.

[29] Shane Harris, "Hack Attack." Foreign Policy, March 3, 2014, accessed August 31, 2017, http://foreignpolicy.com/2014/03/03/hack-attack/.

infrastructure and systems, including military communications infrastructure.[30] Critical infrastructure was targeted with sophisticated malware.[31] Russian special forces also targeted communications systems via an electronic attack.[32] Signals intelligence was used to intercept signals and conduct man-in-the-middle attacks while social media intelligence used geotags to expose Ukrainian soldiers on the front lines.[33] There were also some indicators of hacked unmanned aerial vehicle systems.[34]

This operation produced effects similar to those of the Georgia 2008 attacks. Russia showed a pattern of degrading internal and external communications, disrupting command and control of the armed forces, targeting critical infrastructure, and conducting psychological operations. Russia attempted to blackout communications within Ukraine, and between Ukraine and the international community, however, a total blackout was not successful due to Ukraine's network architecture. Unlike Georgia whose internet links were terrestrial and only traversed Russia and Turkey, Ukraine has a more distributed terrestrial architecture and augments network communications with satellite communications.[35] Russia's effects on critical infrastructure were tied to achieving psychological effects on civilians in Ukraine. There were also effects within the information environment with the intent of psychological effects on Ukrainian Soldiers via social media operations.[36]

Like Georgia, the cyber attacks on Ukraine highlighted Ukraine's deficiencies in the area of cyber defense. Ukraine's inability to defend itself in cyberspace was largely due to constrained financial and human capital, its decentralized network architecture, and poor cyber defense

[30] Harris, "Hack Attack."

[31] Ibid. CrashOverrid (similar to Stuxnet)

[32] Ibid.

[33] Brantley, Cal, and Winklestein, *Defending the Borderland*, 25-26.

[34] Ibid., 30.

[35] Ibid., 26-29.

[36] Ibid., 25-26.

practices.[37] Ukraine lacks the equipment and trained personnel required to prevent persistent cyber attacks on critical communications links and critical infrastructure. Ukraine's decentralized network architecture supported redundant communications, but redundancy is a fail-safe measure to ensure availability, it is not an inherent preventive or protective cyber defense technique. Additionally, an accepted risk among leadership to trade security for convenience resulted in poor security best practices among users, which also added to the vulnerability of Ukraine's cyber defense posture.[38] Personal devices that function using unencrypted (unsecure) communications is standard practice within the military, especially at the tactical level.[39] This enabled Russian forces to locate Ukrainian soldiers on the front lines via geotagging on social media.[40] Although Ukraine displayed the ability to absorb and recover from cyber attack comparably better than Georgia did in 2008, like Georgia, Ukraine was not able to prevent Russia from using the cyber domain to achieve its objectives.

The two case studies lay the groundwork to explore the practicality for tactical commanders to use DCO-RA to engage and respond to cyber attack during combat operations against a near-peer adversary. The case studies also prove that adversaries have the ability and propensity to use offensive cyberspace operations to enable and support combat operations. Furthermore, they demonstrate the effectiveness of incorporating offensive cyberspace operations in time and space with combat operations and highlight the inefficiencies of passive cyber defense against a well synchronized multi-domain battle. This all serves to support the argument of the need for an effective capability at the tactical level to respond to cyber attacks.

---

[37] Brantley, Cal, and Winklestein, *Defending the Borderland*, 12.

[38] Ibid., 27.

[39] Ibid., 27.

[40] Ibid., 25-26.

The Issues of DCO-RA

The basic concept behind DCO-RA is counteraction outside of the defended friendly battlespace. Actions against a computer network include five types of denial effects: deny, degrade, disrupt, destroy, and manipulate.[41] Degrade and disrupt actions center on temporarily denying access to a network based on a percentage of capacity or amount of time, respectively. A destroy effect permanently and completely damages a network or its physical infrastructure, thereby maximizing denial of capacity and time. Finally, manipulation involves exploiting a network or systems to alter their function, process or product. If these actions were only targeted at enemy networks, DCO-RA would not present as complex a challenge. However, attacks may originate or be routed through a third-party network which would thus be on the receiving end of the DCO-RA effects. Figure 2 is a representation of cyber battlespace. The blue area depicts the friendly space, the red area illustrates the adversary space, and the gray portrays neutral space that

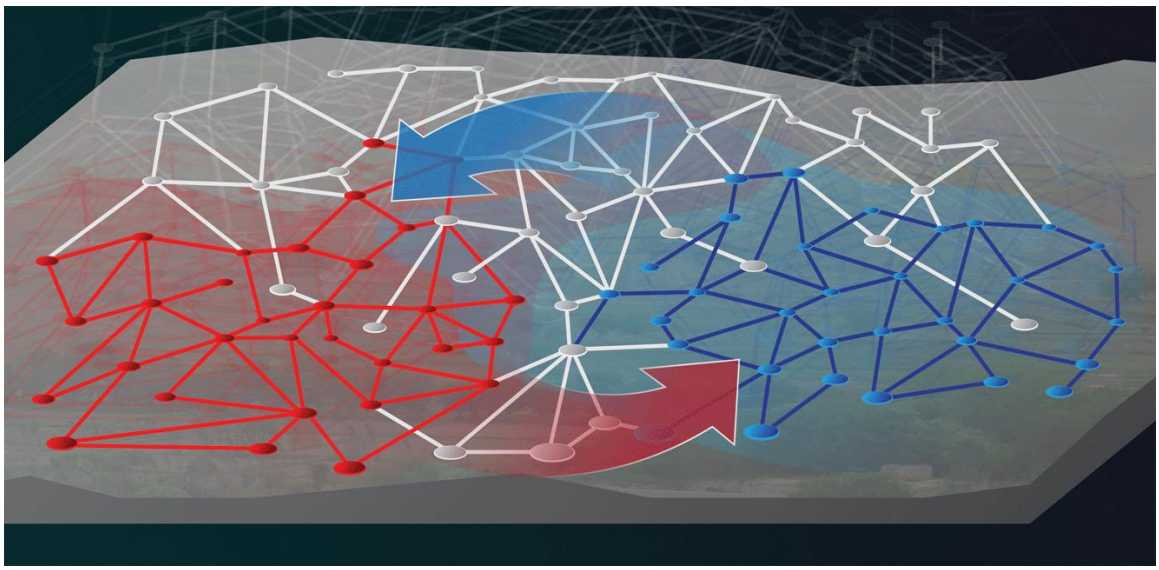

Figure 2. Cyber Battlespace. Alexander Kott, Ananthram Swami, and Bruce J. West, "The Internet of Battle Things," *Computer* 49, no. 12 (December 2016): 72.

[41] US Department of the Army, FM 3-12, *Cyberspace and Electronic Warfare Operations*, 1-10, 11.

is not owned by friendly or threat actors. This raises two challenges, one on the level of law and authorities required and one in terms of capabilities requirements. In addition to these, the lack of experience and precedent for DCO-RA leaves an uncomfortable degree of uncertainty.

Legal Challenges

Possibly the greatest limitation to conducting DCO-RA its legal basis. Attacking third-party networks has obvious ethical challenges. The networks from where an attack is originating might be contained in a hospital system, or school, or at the very least well integrated into the broader civilian network infrastructure. This challenge has resulted in significant legal constraints on the use of DCO-RA. The authorities for response action are synonymous with the authorities for offensive cyberspace operations, and as stated in the *2015 DoD Cyber Security Strategy*, authorities for a counterattack in cyberspace are held at the national strategic level with the Secretary of Defense (SECDEF) or President.[42] The US Army derives its legal authority for armed conflict from the DoD Law of War, which added cyberspace operations to its code in 2015.[43] In addition, the Standing Rules of Engagement (SROE)/Standing Rules of the Use of Force for US Forces provides guidance from the President and SECDEF to deployed US commanders on the use of force.[44]

As in the physical domains, the Law of War has a significant impact on commanders wishing to employ DCO-RA. The *DoD Law of War Manual* outlines cyber operations within the Just War framework (jus ad bellum and jus in bello), and thereby holds cyberspace operations to the principles of self-defense, necessity, discrimination, and proportionality. The last two of these pose a particular challenge in the cyber domain because they require attribution. Attribution presents a unique problem because unlike the physical domains, identification of a hostile actor

[42] US Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: Office of the Secretary of Defense, 2015): 5.

[43] US Department of Defense, *Department of Defense Law of War Manual 2015*, 1011.

[44] US Army Judge Advocate General, *Operational Law Handbook*, 77.

within the cyber domain is a time-consuming and inexact science.[45] Additionally, the ability to determine hostile intent is not as straightforward in cyberspace as it is in the physical domain. Joint doctrine defines hostile intent as "the threat of imminent use of force against the United States, US forces, or other designated persons or property."[46] In the cyber domain the same action or effect may be caused by benign or hostile intent, and until attribution is completed, it is impossible to know which the ultimate cause.[47] Furthermore, attacks from enemy militaries may originate from civilian networks and attackers have the ability to mask the real origin of the attack. DCO-RA may require activity in gray space (equivalent to neutral space) at which point laws of neutrality become a critical factor.

Rules of engagement (ROE) for cyberspace operations present several issues when implemented at corps and below. The Army Judge Advocate General's *Operational Law Handbook* states "ROE are a commander's tool for regulating the use of force."[48] One issue for developing ROE for cyberspace operations is establishing a shared understanding and definition of actions that are considered force in cyberspace, for which there is little international or national consensus.[49] The *DoD Law of War Manual* attempts to classify illegal uses of force in cyberspace but does so in broad terms and using vague language, which could work in favor of an attacker or a defender. Adversaries are more likely to engage in cyber attack where the rules are still ambiguous. The second issue for ROE in DCO-RA is the SROE have not been updated since 2005 and therefore does not include an enclosure specific for cyberspace operations. A broad application of the SROE to cyberspace operations could result in serious legal ramifications for

[45] Ramberto A. Torruella, Jr., "Determining Hostile Intent in Cyberspace," *Joint Force Quarterly* 75, (4th Quarter 2014): 115.

[46] US Department of Defense, Joint Staff, JP 1-02, *DoD Dictionary of Military and Associated Terms* (Washington, DC: Government Printing Office, 2018), 105.

[47] Torruella, "Determining Hostile Intent in Cyberspace," 115-116.

[48] US Army Judge Advocate General, *Operational Law Handbook,* 77.

[49] Torruella, "Determining Hostile Intent in Cyberspace," 116.

tactical commanders, which may contribute to the risk-averse mindset of keeping DCO-RA at the strategic level.

Capability Challenges

Even if the legal framework existed to carry out DCO-RA, there would still be a challenge in the realm of capabilities. Personnel will cyber operational expertise is a critical factor for the DoD cyber force, and a scarce resource in the Army, especially at the tactical level.[50] Giving operational and tactical units the ability to conduct DCO-RA would necessitate training a significantly higher number of cyber personnel. As of now filling cyber positions in the DoD is already a challenge especially given the competition of the civilian sector.[51] The DoD pay structure and culture is less attractive than that of competing public and private sector entities. This makes recruiting and retaining service members who possess the knowledge, skills, and aptitude to conduct cyberspace operations problematic.[52] The degree of knowledge and skills required to conduct cyberspace operations on par with sophisticated adversarial cyber actors requires years of training and experience, but this level of expertise cannot be developed quickly.[53] Experienced DoD civilians and contractors currently augment the cyber force and in doing so fills some of the knowledge and skills gaps inherent in lesser experienced and qualified uniformed cyber warriors. However, the use of civilians in tactical and operational level combat could raise potential issues especially in terms of "trigger pulling."[54]

---

[50] Isaac R. Porche III et al., *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below* (Santa Monica, CA: RAND Corporation, 2017), 54.

[51] William Matthews, "Military Battles to Man its Developing Cyber Force," GovTechWorks, accessed August 22, 2017, https://www.govtechworks.com/military-battles-to-man-its-growing-cyber-force/#gs.dygJ=aA.

[52] Ibid.

[53] Kevin McCaney, "Army Proposes New Classification for Cyber Warriors," *Defense Systems*, September 5, 2014, accessed August 22, 2017, https://defensesystems.com/articles/2014/09/05/army-cyber-warrior-new-classification.aspx.

[54] Christopher Paul, Isaac R. Porche III, and Elliot Axelband, *The Other Quiet Professional* (Santa Monica, CA: RAND Corporation, 2014), 27.

Solving the problem of personnel will not by itself entirely overcome the challenge to developing adequate capabilities for the conduct of DCO-RA at all relevant echelons. Since DCO and offensive cyberspace operations (OCO) are treated as separate activities within Army cyber, this separation is also reflected in the way units that conduct cyberspace operations are organized. OCO is held at US Cyber Command (CYBERCOM), while DCO is executed by all service components.[55] The US Army Network Enterprise Technology Command (NETCOM) is the Army's network defenders and provides communications support to US Army Forces Command, the Army's primary warfighting units. NETCOM's responsibility as the Army's primary network defender has led to excessive centralization, making network response to regional or local incidents difficult and untimely.[56] Since only DCO is performed at the tactical level, the framework for external coordination, integration, and support required for DCO-RA is not inherent within units at corps and below. Additionally, a request for cyber effects from corps to CYBERCOM is a slow process with the potential to not meet the immediate needs of the commander in time and space. As indicated in Figure 3, DCO-RA, while a DCO mission, requires cyberspace attack actions which are tasked to the National Mission Teams, not the Cyber Protection Teams who are responsible for the DCO mission.[57] This necessitates an operational element at corps and below that integrates DCO and OCO to perform DCO-RA.

Enabling DCO-RA operations at corps and below would necessitate a change in organization that would also require a change in doctrine. Joint and Army doctrine provide definitions of DCO-RA and specify it as a Joint Force activity, but do not adequately describe

---

[55] Mark Pomerleau, "Here's How DoD Organizes Its Cyber Warriors," *Fifth Domain*, July 25, 2017, accessed November 12, 2017, https://www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/.

[56] J. Marcus Hicks, "A Theater-Level Perspective on Cyber," *Joint Force Quarterly* 76 (1st Quarter 2015): 58-63.

[57] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly* 73 (2nd Quarter 2014): 12-19.

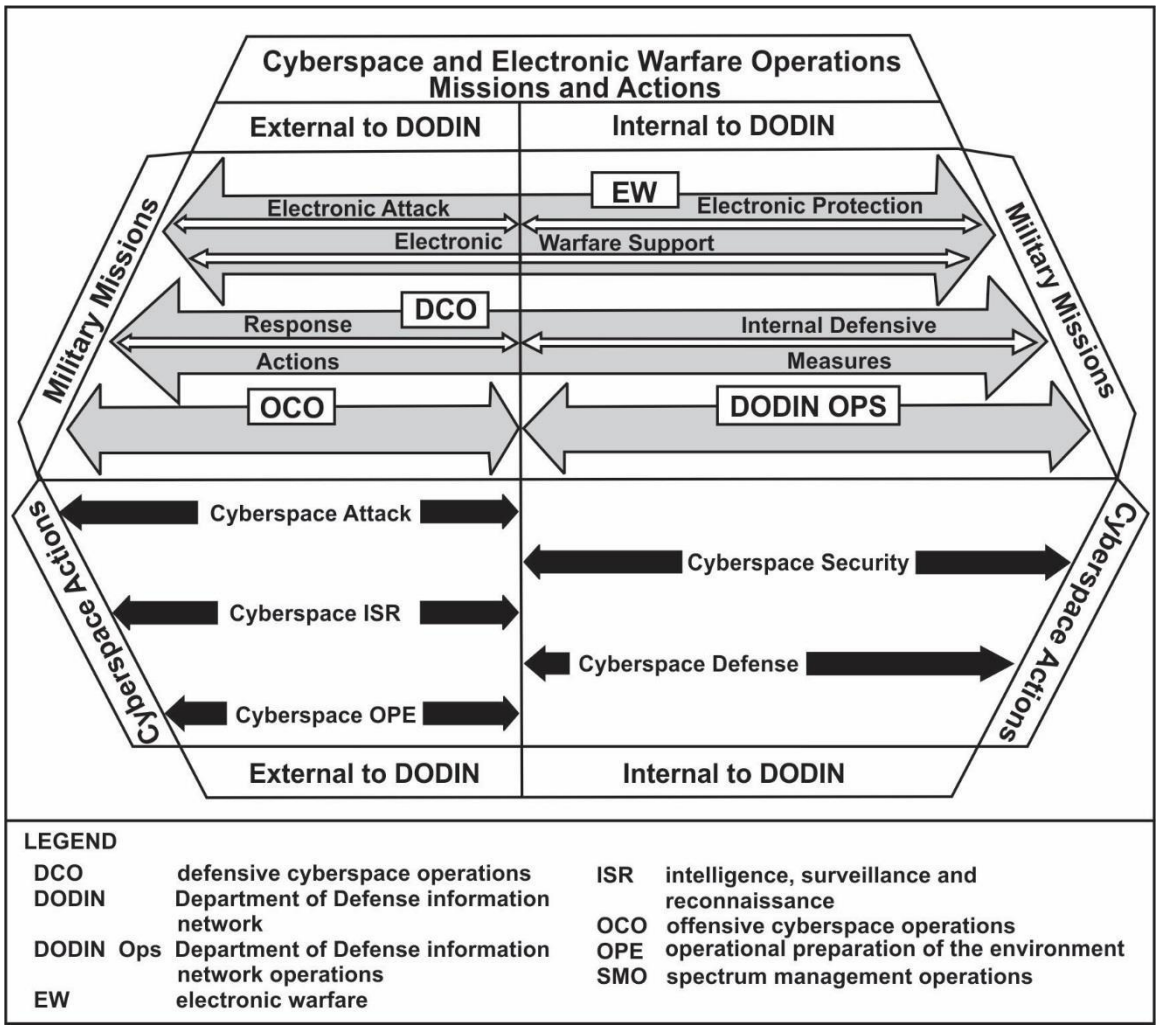

Figure 3. Cyberspace and Electronic Warfare Operations - Missions and Actions. US Department of the Army, FM 3-12, *Cyberspace and Electronic Warfare Operations*, 2017, 1-6.

specifics for its employment at the service level. Joint Publication 3-12 acknowledges some adversary actions can trigger DCO response actions (DCO-RA) necessary to defend networks, when authorized, by creating effects outside of the DoD Information Network (DoDIN).[58] Field Manual 3-12 recognizes that "DCO-RA is more aligned with OCO in execution, authorities, and techniques supporting the mission" and that Joint Forces provide DCO-RA support to

[58] US Department of Defense, JP 3-12, *Cyberspace Operations*, II-2.

commanders at corps and below.[59] More significantly, cyberspace operations are the only operations that separate offensive from defensive actions, for obvious reasons.

Effects outside of the DoDIN that are required to support Army operations and Joint Force Commander objectives are requested and delivered via OCO or DCO-RA missions.[60] This would have to change to enable DCO-RA at corps and below. Additionally, to achieve these effects commanders at corps and below conduct requires intelligence activities governed by Title 50. However, commanders generally are only situated to conduct Title 10 activities. Policy for conducting cyberspace operations in conjunction with unified land operations to achieve strategic objectives must consider both Title 10 and Title 50 activities, and the force must be organized to allow for this.

Historical Precedence and Analogies

One of the challenges to solving the issue of legal framework and capability when it comes to DCO-RA is the lack of immediately obvious historical precedent. This leads to a limited understanding of and skepticism concerning cyberspace operations, particularly OCO, within traditional warfare communities. Limited understanding can lead to risk aversion for commanders and therefore make a commander less likely to employ DCO-RA.[61] However, rather than thinking of DCO-RA as a wholly new phenomenon it is possible to understand it as analogous to a number of existing phenomena within the physical operational environment, or, essentially, as part of a larger pattern.[62] Doing so would not only help develop an understanding of DCO-RA but also contribute to solutions to the challenges of legal authority and capabilities. James McGhee, the legal advisor for Special Operations Command and former operational law attorney for the

[59] US Department of the Army, FM 3-12, *Cyberspace and Electronic Warfare Operations*, 1-10.

[60] Ibid.

[61] Williams, "Guide to Cyberspace Operations," 15-16.

[62] Rosenau, "Thinking Theory Thoroughly," 24.

Twenty-Fourth Air Force (Air Force Cyber Command), highlights the legal inconsistency in his article "Liberating Cyber Offense," by recognizing that "while the approval authority to conduct cyberspace operations outside of the DoDIN is high, similar approval for kinetic operations is much lower".[63] Counterbattery fire and ballistic missile defense (BMD) provide useful conceptual frameworks for response actions in general including DCO-RA. There are also other analogies that can help inform the development of DCO-RA.

No analogy is perfect; there are significant differences between the counteraction frameworks (counterfire and BMD) and DCO-RA. These include the incorporation of deterrence, the type of effects produced, and collateral damage. These counteraction strategies include some level of deterrence; however, it is currently debatable whether deterrence in cyberspace operations is plausible. Additionally, counteraction in the physical domains results in catastrophic kinetic effects, while DCO-RA produces non-kinetic effects that may be projected to the physical domains. These differences highlight areas that should be taken into consideration for developing a framework for DCO-RA since they can inform solutions for legal structures and capabilities. Yet, despite these differences, the similarities are sufficient to teach useful lessons for the development of DCO-RA.

Counterfire

Counterfire protects and gains freedom of maneuver for friendly forces by providing fires against the enemy indirect fire system.[64] The broad category of counterfire has two distinct subcategories, proactive and reactive counterfire. Proactive counterfire is the specific targeting of enemy indirect fire systems, including their command and control, sensors, and platforms before they engage friendly forces. Good intelligence is critical for enabling proactive counterfire.[65]

---

[63] James E. McGhee, "Liberating Cyber Offense," *Strategic Studies Quarterly* (Winter 2016): 48.

[64] US Department of the Army, FM 3-09, *Field Artillery Operations and Fire Support* (Washington, DC: Government Printing Office, 2014), 1-46.

[65] Ibid.

Reactive counterfire provides immediate indirect fire primarily in response to enemy indirect fire. It necessitates quick response capabilities for optimum effectiveness.[66] Planning considerations for counterfire include intelligence preparation of the battlefield (IPB), radar placement and zoning, terrain, and identification of high-payoff targets.[67] Depending on the placement of hostile fires, reactive counterfire runs the risk of causing significant collateral damage to civilian infrastructure and possibly lives. It also requires an immediacy of response which further increases these risks. Counterbattery fire addresses these tasks using doctrine, standard operating procedures (SOPs), and rules of engagement. The commander also assumes the risk for collateral damage through these measures.

The concept of fires and therefore by extension counterfire also exist within the conceptual realm of cyberspace operations. Cyberspace fires is a concept currently defined in joint doctrine as a "form of power projection" in and through cyberspace and by extension could also incorporate a concept for cyberspace counterfire.[68] In cyber operations, DCO-RA fills the role of cyberspace counterfire. Planning considerations such as IPB, placement of sensors for intelligence, surveillance, and reconnaissance (ISR), constructing terrain or network maps, and target nomination and synchronization all remain consistent with those of the physical domains.[69]

Counterbattery fire is used at the tactical level to protect the force against enemy indirect fires by locating and destroying the firing system. In cyberspace, this is akin to conducting reconnaissance and monitoring networks to destroy network infrastructures, such as routers, servers, and network sensors. Counterbattery fire and DCO-RA share several similarities: they both require extensive intelligence support and targeting synchronization and coordination, and both have the potential for collateral damage. The solutions presented to the challenges of

---

[66] US Department of the Army, FM 3-09, *Field Artillery Operations and Fire Support*, 1-46.

[67] Ibid., 1-48.

[68] US Department of Defense, Joint Staff, JP 3-12, *Cyberspace Operations*, II-9.

[69] US Department of Defense, Joint Staff, JP 3-12, *Cyberspace Operations*, II-3.

counterfire should also apply to the cyber domain. As counterfire uses SOPs and tailored ROE to mitigate the risk created by the potential for collateral damage, at a minimum, employing DCO-RA requires specific SOPs and ROE tailored to cyberspace operations.

Ballistic Missile Defense

BMD is a framework used in the land and air battlespace to counter the ballistic missile threat by intercepting the projectile. BMD was launched in the mid-1950s to counter the threat of Soviet intercontinental ballistic missiles.[70] The Ballistic Missile Defense System (BMDS) consists of an integrated, layered architecture that presents defenders with several opportunities to destroy missiles prior to reaching their targets.[71] There are four functions to defeat a ballistic missile: detection, discrimination (separating the missile from everything else), fire control (determining exactly where to intercept), and killing (hitting the missile with some type of interceptor). There are a number of challenges in successfully carrying out the BMD mission among those relevant to the case of DCO-RA are identifying when the launch happens, from where a launch occurs (attribution), and identifying the type of missile launched (discrimination).[72] For BMD it is necessary to address the challenges rapidly in order to develop an appropriate and effective response to a missile launch.

In order to overcome the key challenges of BMD, the BMDS architecture includes networked sensors and radars for target detection and tracking, interceptor missiles for destroying a ballistic missile via direct collision or an explosive blast fragmentation warhead, and a command, control, and management network.[73] Although some radars are strategically located outside of the United States and in partner nations, these systems are interconnected, with each

[70] Jonathan Masters, "Ballistic Missile Defense Systems," Council on Foreign Relations, August 2014, accessed January 27, 2018, https://www.cfr.org/backgrounder/ballistic-missile-defense.

[71] US Department of Defense Missile Defense Agency, "Fact Sheet: The Ballistic Missile Defense System," accessed January 27, 2018, https://www.mda.mil/global/documents/pdf/bmds.pdf.

[72] Masters, "Ballistic Missile Defense Systems."

[73] US Department of Defense Missile Defense Agency, "The Ballistic Missile Defense System."

rapidly adding vital information to create a total picture.[74] Figure 4 gives a pictorial representation of BMDS. The multi-system approach allows for the creation of integrated picture to reduce the chance that any individual component may be fooled or blinded. These sensor capabilities are integrated through a highly synchronized command and control network with explicit ROEs for responding to and engaging targets.[75] This allows units BMD missions to engage targets in time and space to achieve the desired effect.

A similar form of architecture could help address some of the challenges of attribution and characterization inherent in DCO-RA. DCO-RA attempts to counter malicious network activity against strategic or tactical targets in cyberspace. As such it has similar challenges to BMD, only in the cyber domain they are attributing malicious network activity to a threat actor (attribution) and determining the type of malicious activity (characterization). In order to mitigate the effects of these challenges, DCO-RA would need to rely on a robust layered system to include analyzing alerts and intelligence of a live attack from network monitoring tools. Network monitoring tools capture the data transiting a network for the purpose differentiating normal traffic from threat traffic. This takes the place of the sensors systems employed by BMD for the purpose of discrimination. In the cyber domain, attribution is more of a challenge and requires developing a layered intelligence picture which will need to be developed through an integrated multi-agency approach. BMD requires that some of the key sensor systems are located outside the United States, and DCO-RA also requires the integration of network sensors outside of the DoDIN.

As with the BMDS architecture, the 'sensors' responsible for attribution and characterization must be linked to an efficient command, control, and management. In the case

[74] US Department of Defense Missile Defense Agency, "Elements: Sensors," accessed January 27, 2018, https://www.mda.mil/system/sensors.html.

[75] Joshua Sanders, "Rules of Engagement Policies Automation For Ballistic Missile Defense System," (master's thesis, Naval Postgraduate School, 2009), accessed January 27, 2018, http://www.dtic.mil/dtic/tr/fulltext/u2/a514373.pdf.

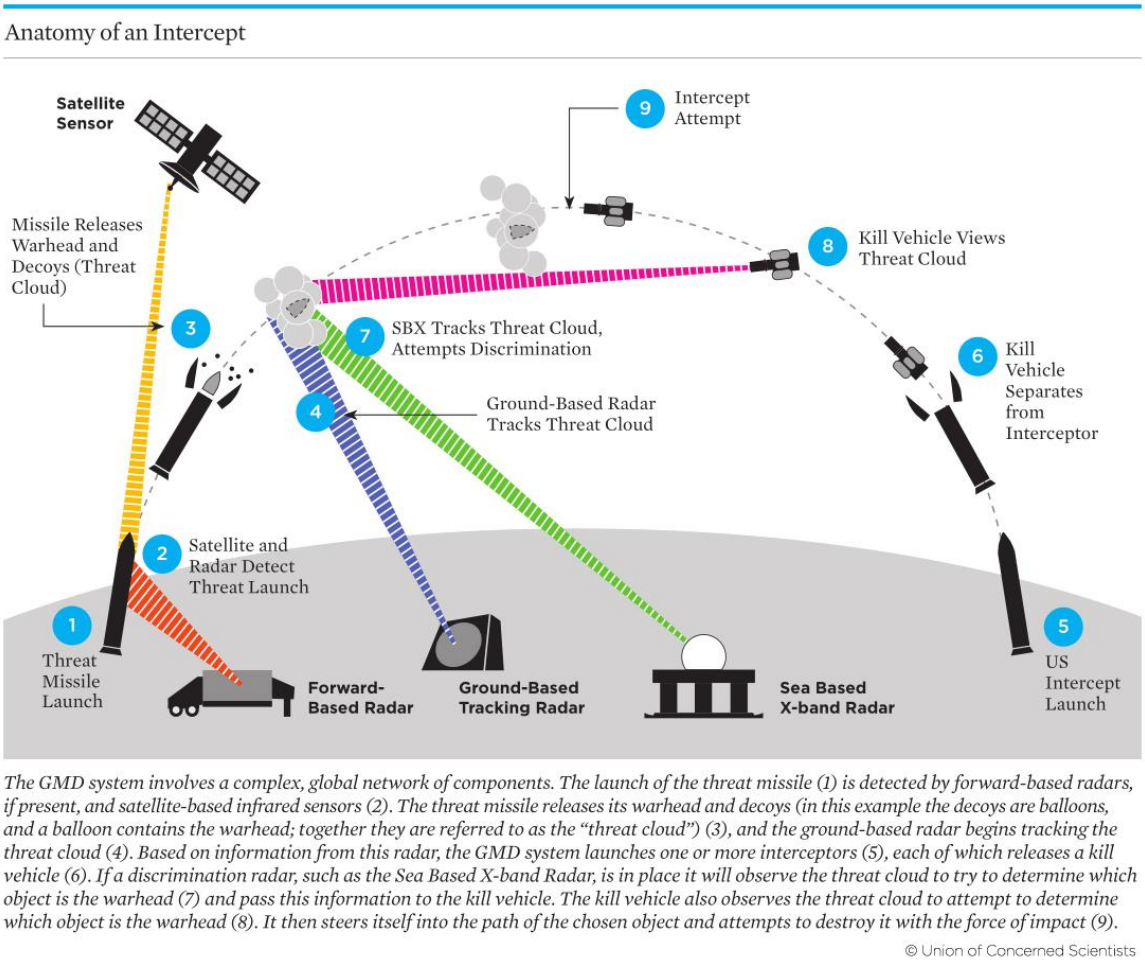

Figure 4. Anatomy of an Intercept. Union of Concerned Scientists, "How Does Missile Defense Work," accessed January 6, 2018, https://www.ucsusa.org/nuclear-weapons/missile-defense/how-gmd-missile-defense-works#.WrUPkExFzD4.

of DCO-RA, this requires a greater level of organizational integration because tactical and operational level cyber teams have limited access to much of the intelligence data produced by the strategic level sensors.[76] BMD units are enabled to view the information they need for targeting and in order to achieve a similar effect in the cyber domain units tasked with DCO-RA require the same.[77] In short, the case of BMD demonstrates that conducting DCO-RA requires a

[76] Porche et al., *Tactical Cyber*, 24.

[77] US Department of Defense Missile Defense Agency, "Elements: Command and Control, Battle Management, and Communications (C2BMC)," accessed January 27, 2018, https://www.mda.mil/system/c2bmc.html.

robust sensing architecture that consists of integrated network sensors as well as an operational-level command and control platform that is synchronized across multiple echelons and organizations.

Other Analogies

In addition to counteraction frameworks, there are other activities in the physical domain which provide useful analogies on which to build DCO-RA. These can help conceptualize the development of a framework for DCO-RA are the evolution of warfighting forces and the development of strategic cyberweapons. The United States established the US Air Force and the Special Operations Force to meet the demands of future war (airpower and irregular warfare). Likewise, the necessity for using cyber power and maintaining superiority in cyberspace is becoming a reality in warfare. Additionally, the development and employment of the Stuxnet virus as a means to disarm Iranian nuclear proliferation illustrates the value and appropriateness of active defense when incorporated within a well-constructed strategic narrative.[78] Stuxnet is a perfect example of how cyberweapons can be used to employ DCO-RA.[79] These commonalities reinforce the idea that the development and employment of DCO-RA is not an entirely new phenomenon of warfare, but simply challenges the current understanding and reality of active defense within cyberspace operations.

Solutions

DCO-RA has an inherent level of uncertainty because of its blurred lines between DCO and OCO, but there are solutions to overcome the legal and capabilities challenges of using DCO-RA at the tactical level. As previously discussed there are physical domain analogies that can help

[78] P.W. Singer, "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons," *Case Western Reserve Journal of International Law* 47, no. 1 (Issue 1, Spring 2015): 84-86.

[79] Ibid., 84-86.

with this. A framework for conducting DCO-RA that parallels current counteraction theories and doctrine in the physical domains will provide familiarity and a level of comfort to tactical commanders of non-cyber elements at corps and below. In particular, counterfire provides simplicity and the best visual representation equivalent to DCO-RA in cyberspace: enemy targets are located and fired upon, some are destroyed, and collateral damage may result. It also incorporates processes from other warfighting functions, such as ISR and targeting. While counterfire helps conceptualize responding to high volume and rapidly successive attacks, such as DDoS and brute force attacks, BMD is best for understanding how to effectively build unity of effort across multiple entities and echelons and differentiating between when to use automation versus human interaction. BMD is a more deliberate form of counteraction, but it also responds to a higher-level threat and requires coordination and synchronization across multiple organizations.

Other solutions that are necessary before any enabling change can occur include shifting perspectives, updating legal frameworks, and fulfilling necessary resource requirements. A shift in mindset about the cyber domain will allow leaders to overcome some of the uncertainty of conducting offensive-like cyberspace operations at the tactical level. Such a shift will also empower US Army Cyber Command (ARCYBER) leadership to develop its force as necessary to accomplish their unique mission. In addition, expanded and updated legal frameworks and authorities for conducting cyberspace operations similar to operations in the physical domains at the tactical level will provide commanders the authority needed to include DCO-RA in their operations. Moreover, addressing capabilities deficiencies in the areas of doctrine, organization, and personnel will give tactical commanders the ability to leverage the cyber domain to conduct operations.

Capabilities Solutions

As previously mentioned the United States is currently under-resourced to implement DCO-RA fully. However, there are several options for addressing capabilities challenges. The

first aspect of the challenge of capabilities is one of doctrine and organization. Within doctrine, DCO-RA requires a distinct process and description of the transition between DCO and OCO. DCO and OCO are treated as two isolated activities, which was possibly a matter of simplicity rather than out of strict necessity at the inception of CYBERCOM. Continuing to keep these areas separate at the operational and tactical levels, where defense and offense are mutually supporting activities in time and space, is counterproductive. The previously presented case studies suggest there is a thin line between cyber defense and counteraction against adversaries who effectively integrate offensive cyberspace operations with combat operations.

ARCYBER has made significant progress in the area of organization. The CEMA support to corps and below (CSCB) initiative is in its third year. This concept has made strides to support commanders at corps and below with an added capability for cyberspace operations at the tactical level. Recent efforts are mostly in the area of electronic warfare (EW). This is a necessary capability since tactical communications platforms primarily rely on satellites for wide-area network transport.[80] However, because all of the tactical battle command systems are net-centric, EW dominance alone will not give tactical commanders freedom of maneuver in cyberspace. Furthermore, a RAND study found that due to time and space requirements, an element acting as reachback support is not sufficient.[81] For this reason, CSCB should experiment with using a combined-cyber squad/team composed of a combination of defensive, offensive and support roles to enable combat operations.

Another area of challenge within the realm of capability is that of personnel. As already discussed, there are not enough cyber personnel assigned to the tactical echelons to carry out DCO-RA. The CSCB initiative is also solving some of the personnel barriers by temporarily augmenting tactical commanders with offensive cyber teams and cyber planners during training

[80] US Army Program Executive Office Command Control Communications-Tactical, "Mission Network," updated March 2017, accessed November 12, 2017, http://peoc3t.army.mil/wint/inc2.php.

[81] Porche et al., *Tactical Cyber*, 11.

rotations. In addition, the Electronic Warfare occupation specialties are merging into the Cyber Branch which also fills the demand for cyber planners and operators within tactical formations, though there remains a question as to whether the addition of Electronic Warfare specialists to the cyber capability will result in sufficient cyber-trained personnel. The Army is also pressing forward on a Cyber Direct Commissioning initiative to bring in experienced civilians with cyber-related skills and abilities as Lieutenants.[82] Additionally, Congress also recently passed a measure to let the DoD bypass ordinary federal hiring and pay procedures to make it a more competitive employer of cyber specialists.[83] This program, the DoD Cyber Excepted Service provides "flexibilities for recruitment, retention, and development of cyber professionals across DoD."[84] Though the Army is making good progress to resolve its cyber personnel problem, it could also develop an outside research and development group that is not subject to security clearance requirements. This type of organization could leverage civilian talent to fulfill some the Army's unclassified research needs.

Legal Solutions

The legal challenges barring the employment of DCO-RA at the tactical and operational levels are partly real and partially illusory. In July 2013, a Center for Strategic and International Studies (CSIS) study team consisting of members from the military, government, and private industry was established to explore the viability of offensive cyber capabilities at the JTF level

[82] Lauren C. Williams, "Army Looks To Tap Civilian Talent," FCW, December 5, 2017, accessed March 31, 2018, https://fcw.com/articles/2017/12/05/cyber-civilian-army-hire.aspx.

[83] Jared Serbu, "Full Implementation of DoD's Cyber Excepted Service Still a Year Away," Federal News Radio, November 7, 2017, accessed March 31, 2018, https://federalnewsradio.com/dod-reporters-notebook-jared-serbu/2017/11/full-implementation-of-dods-cyber-excepted-service-still-a-year-away/.

[84] US Department of Defense, "DoD CES Personnel System Fact Sheet," August 2017, accessed March 31, 2018, https://www.cpms.osd.mil/content/documents/CyberOneStop/CES/CESOverviewFactSheet.pdf.

and below.[85] One of the findings of this project was a consensus among legal and policy experts

> "that while current practice may be to hold approval authorities at very high levels, the potential for commanders at any level to utilize offensive cyber tools during approved military operations is not in fact constrained by either policy or law, as long as existing processes are adhered to."[86]

If this is true, then expanding authorities for OCO to tactical commanders is plausible, and the legal hurdles to conduct DCO-RA at corps and below may not be as high as previously presumed. This research proposes three possibilities for clearing the legal hurdles: establishing precise terms for force in cyberspace; adjusting DCO-RA to current portions of the *DoD Law of War*; and requesting DCO-RA approvals within already existing Operational Plans (OPLANs). These alternatives would help shape the ROE required to conduct DCO-RA at corps and below.

The first step toward a shared understanding of cyberspace operations within armed conflict is defining force in cyberspace. A clear understanding of force in cyberspace sets the stage for determining necessity, discrimination, and proportionality, as well as identifying conditions for self-defense, which are all required for just war. The Tallinn Manual 2.0 could prove useful to this end. The Tallinn Manual 2.0 is an unofficial document written by experts with NATO CCDCOE and attempts to apply international law to cyberspace operations and codify rules that should be followed.[87] These rules include international responsibility, the use of force, hostile activity, and neutrality to name a few. The Tallinn Manual is not legally binding and therefore only provides a theoretical concept for operating legally in cyberspace. The Schmitt Analytical Framework is another tool that may be useful to apply to anticipatory self-defense scenarios where there is a perceived imminent threat.[88] The Schmitt Framework uses seven

---

[85] Leed, *Offensive Cyber Capabilities at the Operational Level*, 2.

[86] Ibid., 4.

[87] NATO Cooperative Cyber Defence Centre of Excellence, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Factsheet," accessed January 6, 2018, https://www.ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf.

[88] US Army Judge Advocate General, *Operational Law Handbook*, *17th ed*., 7.

factors to gauge hostile intent: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[89] These two documents taken together provide a useful foundation for understanding the potential legal nature of the cyber environment. This combined with understanding analogous physical situations such as counterfire will allow for the development of ROE relevant to DCO-RA.

An alternative option is to leverage the rules of the *DoD Law of War Manual* to develop limited, small-scale operations under DCO-RA initially. For example, the *DoD Law of War Manual* section 'Cyber Operations and Jus in Bello,' identifies cyber operations that are not considered attack and therefore not subjected to the rules of attack.[90] These operations are: "defacing a government webpage; a minor, brief disruption of internet services; briefly disrupting, disabling, or interfering with communications; and disseminating propaganda."[91] So DCO-RA operations that employ limited disrupt or manipulate effects might be classified as response action, and concurrently not be considered an attack operation. They might, therefore, be below the threshold of some restrictive authorities or constraints. Figure 5 provides an example of a cyber response spectrum that planners at corps and below could use to determine the DCO-RA activities that do not require the higher authorizations inherent to offensive cyber operations.

The last option is an idea put forth by the CSIS study team from their project to examine offensive capabilities at the operational level. The study team found that the same process for "narrowly constructed" approvals could be considered for broader approvals.[92] Meaning essentially, a JTF commander could request to employ offensive cyber capabilities within an OPLAN, as part of an ongoing or future campaign, which ultimately gets approved as an

---

[89] Torruella, "Determining Hostile Intent in Cyberspace," 118.

[90] US Department of Defense, *Department of Defense Law of War Manual, 2015*, 1022.

[91] Ibid.

[92] Leed, *Offensive Cyber Capabilities at the Operational Level*, 4-5.

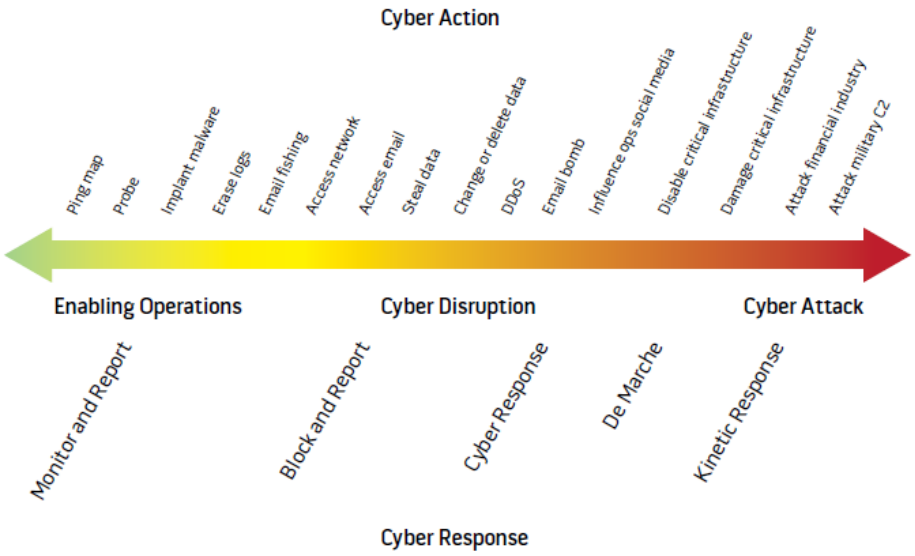

Figure 5. Example of Brown-Tullos Cyber Action Response Spectrum. Torruella, "Determining Hostile Intent in Cyberspace," 121.

Execute Order.[93] Theoretically, a corps commander should be able to do the same.

Whether one of these potential options is selected or whether the way forward is a combination of all three, in order to conduct DCO-RA it is critical to establish clear and explicit legal terms for operating in cyberspace. This will allow for the construction of proper authorities and ROE to conduct DCO-RA at the tactical level in much the same way as proper authorities and ROE enable the use of counterfire in the physical domain. Establishing such ROE will enable commanders at corps and below to conduct DCO-RA within the required short time window. In short, the frameworks to do this already exist and are evidence that solving the legal issues for DCO-RA is a matter of the United States getting out of its own way.

Mindset Shift

For DCO-RA to become a reality at the tactical level, military and political leaders will have to challenge their views and shift their perspective. First, US political and military leaders

[93] Leed, *Offensive Cyber Capabilities at the Operational Level*, 5.

should take the cyber threat as seriously as physical threats.[94] This will require establishing, in distinct terms, what constitutes acts of force in the cyber domain. The United States has been overly passive in response to cyber attacks, which has opened the door for its adversaries to become increasingly aggressive.[95] In the face of cyber attacks, the United States has focused inward on defense, instead of imposing consequences on its adversaries.[96] Meanwhile, the passive mindset has enabled adversaries to not only prep the cyber battlefield, but, as the Georgia and Ukraine case studies demonstrated, also practice their tactics, techniques, and procedures at will. This is also evident in more recent cyber attacks against the United States.[97]

Command and control is another area that requires a mindset adjustment, especially among military leaders. US military leaders are accustomed to a hierarchical command structure that has one commander in authority over an organization and battlespace. Employing DCO-RA at the tactical level is just one facet of multi-domain battle (MDB). MDB requires "resilient formations" that conduct "semi-independent" operations within an expanded battlespace.[98] This arrangement of cyber-land battle may work best under a co-command relationship, a marriage of sorts, where responsibilities are delineated between the cyber and land/air/sea commander. A co-commander structure might ultimately relieve any anxiety of the land/air/sea commander to make decisions within a domain which they may not fully understand.

Finally, if the goal is to build a premier cyber force that is comparable to the land, air, and sea forces, there has to be an acceptance that the cyber force culture will be different from

---

[94] US Department of the Army, FM 3-12, *Cyberspace and Electronic Warfare Operations*, 1-20, 21.

[95] Arthur Herman, "Wanted: A Real National Cyber Action Plan," *National Review*, February 11, 2016, accessed March 31, 2018, https://www.nationalreview.com/2016/02/cyber-defense-what-we-are-missing/.

[96] Ibid.

[97] Doug Olenick, "Cyber Enemies of the United States," *SC Magazine*, May 9, 2017, accessed March 31, 2018, https://www.scmagazine.com/cyber-enemies-of-the-united-states/article/650736/.

[98] Nakasone and Lewis, "Cyberspace in Multi-Domain Battle," 20.

that of the traditional force. For example, some cyber warriors may not meet the traditional appearance and fitness standards. The mental and intellectual skills and abilities required to outmatch adversaries in cyberspace is high in demand but low in supply among traditional soldiers. As Senator Claire McCaskill, who is a member of the Senate Armed Services Committee put it "we need to get the best and brightest. I am not sure that's always the guy who can do the most sit-ups."[99] In addition, the garrison offices and field operating spaces for traditional combat units may not be conducive to a cyber team to train and operate on a daily basis. Some training and operations may occur at public locations or other types of facilities and may require soldiers to be inconspicuously dressed instead of wearing a uniform. This challenge is not entirely alien to the current military, several specialties such as Special Forces and human intelligence already require similar accommodations.[100] Another area of cultural difference is the intermingling among ranks. It is not uncommon for a commissioned officer and non-commissioned officer to work side-by-side or even for a commissioned officer to be subordinate to a warrant or non-commissioned officer during a cyber mission. This too is not entirely unique within the Army as Special Forces and other such specialized branches at times may operate in a similar manner.[101] Adapting this shift in mindset will create an environment to better grow and maintain the cyber force which will provide the personnel necessary to carry out DCO-RA at the echelons of corps and below.

The potential solutions of DCO-RA discussed above include developing a framework consistent with counterfire and BMD, altering perspectives, expanding legal structures, and focusing efforts to provide needed resources. While some of the solutions presented are based on analysis derived from existing concepts, such as counteraction in the physical domains, other

---

[99] Jesse Bogan, "Military Culture Must Change to Keep the Best Cyber Warrirors: Senator," Military.com, accessed March 31, 2018, https://www.military.com/daily-news/2016/08/30/military-culture-must-change-keep-best-cyber-warriors-senator.html.

[100] Paul, Porche, and Elliot, *The Other Quiet Professional*, 35-38.

[101] Paul, Porche, and Elliot, *The Other Quiet Professional*, 35-36.

solutions are based on results from independent studies (i.e., the CSIS study team) and ongoing experiments (i.e., CSCB). Taken together, the solutions demonstrate that the challenges of employing DCO-RA at the operational and tactical level are solvable and does not require entirely new science. They support the premise that DCO-RA can be a viable option at corps and below.

Conclusion

Over the past decade, the United States witnessed and experienced increasing cyber activity and cyber-aggression by its adversaries, to include state and non-state actors, as well as state-sponsored hackers. For example, Russia, through its campaigns against Georgia in 2008 and Ukraine in 2014, has shown the ability and propensity to synchronize cyber attacks in conjunction with combat operations. US Army operational and tactical units conduct defensive cyberspace operations to defend against cyber attack using a defense-in-depth strategy that is enabled by supporting network architecture and infrastructure. The tactics and techniques used within the defense-in-depth strategy consist of active and passive actions taken within the defended network. However, as the cases of Georgia and Ukraine demonstrated all too clearly, such actions may be necessary, but they are not sufficient. DCO-RA may provide the missing piece of the defense puzzle.

Defenders at the operational and tactical level are not authorized to respond to attacks outside of the defended network where most attacks originate and therefore cannot conduct DCO-RA. As such, the current passive defensive approach presents challenges for commanders at corps and below. They lack authorities and capabilities required to effectively engage adversaries in cyberspace which means they cannot dominate the cyber domain to during combat operations.

Although, DCO-RA, gives commanders and cyber defenders at corps below the ability to respond to cyber attacks, implementing it is not without challenges. Some of these challenges are inherent to DCO-RA itself, while others are center on fitting within the broader structure of the

Army. Among this issue is the lack of historical precedent for using DCO-RA in combat, which results in limited understanding and skepticism of its potential as a warfighting capability. Second, there are resource deficiencies which preclude employing DCO-RA. These exist in the areas of doctrine, organization, personnel. Finally, legal constraints which include limited authorities and ROEs limit the practicality of DCO-RA as a tool for corps and below. The present utility of DCO-RA is further diminished and constrained by an overall lack of consensus of how the concept of force applies within cyberspace. In spite of these issues, there is still a need to respond to cyber attack at the tactical level, and DCO-RA fulfills this need. This research analyzed the issues of DCO-RA to determine whether DCO-RA could be a viable solution for commanders at corps and below.

The findings support the hypothesis that DCO-RA is potentially a viable solution for operational and tactical elements. First, analogies to similar activities within the physical domains demonstrate that although DCO-RA in warfare is an unfamiliar concept, its underlying phenomenon, counteraction, is not. Two counteraction concepts and frameworks, counterfire and BMD, can inform theories for action and employment for DCO-RA at corps and below. Second, legal frameworks and authorities can be adjusted as necessary to achieve military objectives, and there is broad consensus among legal and policy experts that nothing precludes leaders from doing so. Third, the DoD has a process and framework (Joint Capabilities Integration Development System [JCIDS] and the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy [DOTMLPF-P] Framework) to identify and fulfill specialized capabilities requirements, and the Army is currently addressing some of these areas with the CSCB initiative. Finally, implementing the solutions that will enable DCO-RA at corps and below require leaders to change their mindset about this unique domain of warfare. There must be an acceptance that an elite cyber force will look different from the traditional combat force and that building it will require doing things differently.

This project makes a few recommendations for future research. One is investigating the technical feasibility of DCO-RA as well as options for offensive cyber tools for use at corps and below, areas which the CSIS study team also undertook. Another is exploring ways that DCO-RA can be applied to EW and information operations. Army Cyber is releasing a DOTMLPF-P assessment of its CSCB pilot in fiscal year 2018.[102] The results can help inform solutions for using DCO-RA within EW. The last recommendation is examining the organizational structures and processes required to enable national strategic intelligence support and targeting support to echelons corps and below for the purpose of employing DCO-RA.

Russian aggression in the cyber domain over the past decade show that mere passive response to cyber attack is not sufficient to prevail against a well-rehearsed adversary that combines offensive cyberspace operations with combat operations. Fear of the unknown cannot be an excuse for idleness, and the US cannot afford to be "cyber punching bags" in combat.[103] Inactivity is not an option. Lieutenant General Nakasone told senators in a confirmation hearing March 1, 2018 "As cyberspace develops, the longer that we have inactivity, the longer our adversaries are able to establish their own norms – and I think that is very, very important that we realize that."[104] This sentiment resonates with Moltke in his statement that "omission and inactivity are worse than resorting to the wrong expedient."[105] While DCO-RA may not be a perfect solution, as its analogies in the physical domain demonstrate, perfection is not always necessary. Overcoming an adversary is the art of combining what is possible with what is necessary to achieve defense. At some point the US must stop being the world's

[102] Mark Pomerleau, "What Can Cyber Do For You, The Commander," *Fifth Domain*, December 15, 2017, accessed March 31, 2018, https://www.fifthdomain.com/electronic-warfare/2017/12/15/what-can-cyber-do-for-you-the-commander/.

[103] *Hearing Before the Committee on Armed Services United States Senate: Nominations*, US Congress, March 1, 2018.

[104] Ibid.

[105] Strategy by Design, "Von Moltke on Strategy," Strategic Thinking, accessed March 31, 2018, http://www.strategybydesign.org/von-moltke-the-elder-on-strategy/.

cyber punching bag and counter its adversaries with a few cyber jabs of its own. This research demonstrates that DCO-RA, when fully and properly enabled, is capable of doing just that.

Bibliography

Bennett, Corey. "Pentagon restores hacked network." The Hill. August 10, 2015. Accessed April 23, 2018. http://thehill.com/policy/cybersecurity/250730-pentagon-restores-hacked-email-system.

Blank, Steven. "Cyber War and Information War à la Russe." In *Understanding Cyber Conflict: Fourteen Analogies*, edited by George Perkovich and Ariel E. Levite, 81-98. Washington, DC: Georgetown University Press, 2017.

Bogan, Jesse. "Military Culture Must Change to Keep the Best Cyber Warriors: Senator." Military.com. August 30, 2016. Accessed March 31, 2018. https://www.military.com/daily-news/2016/08/30/military-culture-must-change-keep-best-cyber-warriors-senator.html.

Brantley, Aaron F., Nerea M. Cal, and Devlin P. Winklestein. *Defending the Borderland: Ukrainian Military Experiences with IO. Cyber. and EW*. West Point, NY: Army Cyber Institute, 2017. Accessed August 31, 2017. http://www.dtic.mil/dtic/tr/fulltext/u2/1046052.pdf.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, CA: O'Reilly Media, 2012.

Gray, Colin. *Making Strategic Sense of Cyber Power: Why the Cyber Sky is Not Falling*. Carlisle, PA: US Army War College Press, April 2013. Accessed September 12, 2013. https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1147.

Harris, Shane. "Hack Attack." Foreign Policy. March 3, 2014. Accessed August 31, 2017. http://foreignpolicy.com/2014/03/03/hack-attack/.

Herman, Arthur. "Wanted: A Real National Cyber Action Plan." *National Review*. February 11, 2016. Accessed March 31, 2018. https://www.nationalreview.com/2016/02/cyber-defense-what-we-are-missing/.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*. January 6, 2011. Accessed August 1, 2017. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

Hicks, J. Marcus. "A Theater-Level Perspective on Cyber." *Joint Force Quarterly* 76 (1st Quarter 2015): 58-63.

Kott, Alexander. Ananthram Swami, and Bruce J. West. "The Internet of Battle Things." *Computer* 49, no. 12 (December 2016): 70-75.

Leed, Maren. *Offensive Cyber Capabilities at the Operational Level: The Way Ahead*. Washington, DC: Center for Strategic and International Studies, 2013. Accessed November 12, 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf.

Masters, Jonathan. “Ballistic Missile Defense Systems.” Council on Foreign Relations. August 2014. Accessed January 27, 2018. https://www.cfr.org/backgrounder/ballistic-missile-defense.

Matthews, William. “Military Battles to Man its Developing Cyber Force.” GovTechWorks. Accessed August 22, 2017. https://www.govtechworks.com/military-battles-to-man-its-growing-cyber-force/#gs.dygJ=aA.

McCaney, Kevin. “Army Proposes New Classification for Cyber Warriors.” *Defense Systems*. September 5, 2014. Accessed August 22, 2017. https://defensesystems.com/articles/2014/09/05/army-cyber-warrior-new-classification.aspx.

McGhee, James E. “Liberating Cyber Offense.” *Strategic Studies Quarterly* (Winter 2016): 46-63.

Nakasone, Lieutenant General Paul M., and Major Charlie Lewis. “Cyberspace in Multi-Domain Battle.” *The Cyber Defense Review* 2, no. 1 (Spring 2017): 15-24.

NATO Cooperative Cyber Defence Centre of Excellence. “Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Factsheet.” Accessed January 6, 2018. https://www.ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf.

Olenick, Doug. “Cyber Enemies of the United States.” *SC Magazine*. May 9, 2017. Accessed March 31, 2018. https://www.scmagazine.com/cyber-enemies-of-the-united-states/article/650736/.

Paul, Christopher, Isaac R. Porche III, and Elliot Axelband. *The Other Quiet Professional*. Santa Monica, CA: RAND Corporation, 2014. Accessed January 18, 2017. https://www.rand.org/content/dam/rand/pubs/research_reports/RR700/RR780/RAND_RR780.pdf.

Pomerleau, Mark. “Here’s How DoD Organizes Its Cyber Warriors.” *Fifth Domain*. July 25, 2017. Accessed November 12, 2017. https://www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/.

———. “What Can Cyber Do For You, The Commander?” *Fifth Domain*. December 15, 2017. Accessed March 31, 2018. https://www.fifthdomain.com/electronic-warfare/2017/12/15/what-can-cyber-do-for-you-the-commander/.

Porche III, Isaac R., Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick. *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*. Santa Monica, CA: RAND Corporation, 2017. Accessed November 12, 2017. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1600/RAND_RR1600.pdf.

Rosenau, James. “Thinking Theory Thoroughly.” In *The Scientific Study of Foreign Policy*, 19-31. London: Pinter, 1980.

Sanders, Joshua. “Rules of Engagement Policies Automation for Ballistic Missile Defense System.” Master’s thesis, Naval Postgraduate School, 2009. Accessed January 27, 2018. http://www.dtic.mil/dtic/tr/fulltext/u2/a514373.pdf.

Serbu, Jared. “Full Implementation Of DoD’s Cyber Excepted Service Still A Year Away.” Federal News Radio. November 7, 2017. Accessed March 31, 2018. https://federalnewsradio.com/dod-reporters-notebook-jared-serbu/2017/11/full-implementation-of-dods-cyber-excepted-service-still-a-year-away/.

Shakarian, Captain Paulo. “The 2008 Russian Cyber Campaign Against Georgia.” *Military Review* (November-December 2011): 63-68.

Singer, P.W. “Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons.” *Case Western Reserve Journal of International Law* 47, no. 1 (Issue 1, Spring 2015).

Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2008. Accessed August 31, 2017. http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-attack-NATO-Aug-2008.pdf.

Torruella, Jr., Ramberto A. “Determining Hostile Intent in Cyberspace.” *Joint Force Quarterly* 75 (4th Quarter 2014): 114-121.

Strategy by Design. “Von Moltke on Strategy.” Strategic Thinking. Accessed March 31, 2018. http://www.strategybydesign.org/von-moltke-the-elder-on-strategy/.

Williams, Brett T. “The Joint Force Commander’s Guide to Cyberspace Operations.” *Joint Force Quarterly* 73 (2nd Quarter 2014): 12-19.

Williams, Lauren C. “Army Looks To Tap Civilian Talent.” FCW. December 5, 2017. Accessed March 31, 2018. https://fcw.com/articles/2017/12/05/cyber-civilian-army-hire.aspx.

Union of Concerned Scientists. “How Does Missile Defense Work.” Accessed January 6, 2018. https://www.ucsusa.org/nuclear-weapons/missile-defense/how-gmd-missile-defense-works#.WrUPkExFzD4.

US Army Judge Advocate General. *Operational Law Handbook*. 17th ed. Charlottesville, VA: The Judge Advocate General’s Legal Center and School, 2017.

US Army Program Executive Office Command Control Communications-Tactical. “Mission Network.” updated March 2017. Accessed November 12, 2017. http://peoc3t.army.mil/wint/inc2.php.

US Army War College. *Strategic Cyberspace Operations Guide*. Carlisle, PA: Center for Strategic Leadership, June 2016.

US Congress. Senate. *Hearing Before the Committee on Armed Services United States Senate: Nominations*, March 1, 2018. Accessed March 31, 2018. https://assets.documentcloud.org/documents/4407097/United-States-Senate-Armed-Services-Committee.pdf.

US Department of the Army. Field Manual (FM) 3-09, *Field Artillery Operations and Fire Support*. Washington, DC: Government Printing Office, 2014.

———. Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations*. Washington, DC: Government Printing Office, 2017.

US Department of Defense. "DoD CES Personnel System Fact Sheet." August 2017. Accessed March 3, 2018. https://www.cpms.osd.mil/content/documents/CyberOneStop/CES/CESOverviewFactSheet.pdf.

———. *The Department of Defense Cyber Strategy*. Washington, DC: Office of the Secretary of Defense, 2015.

———. *Department of Defense Law of War Manual*. Washington, DC: Office of General Counsel, Department of Defense, 2016.

———. Joint Staff. Joint Publication (JP) 1-02, *DoD Dictionary of Military and Associated Terms*. Washington, DC: Government Printing Office, 2018.

———. Joint Staff. Joint Publication (JP) 3-12 (Redacted), *Cyberspace Operations*. Washington, DC: Government Printing Office, 2013.

US Department of Defense Missile Defense Agency. "Fact Sheet: The Ballistic Missile Defense System." Accessed January 27, 2018. https://www.mda.mil/global/documents/pdf/bmds.pdf.

———. "Elements: Command and Control. Battle Management. and Communications (C2BMC)." Accessed January 27, 2018. https://www.mda.mil/system/c2bmc.html.

———. "Elements: Sensors." Accessed January 27, 2018. https://www.mda.mil/system/sensors.html.