

US Army War College
USAWC Press

Monographs, Books, & Publications

3-18-2019

The Army Role in Achieving Deterrence in Cyberspace

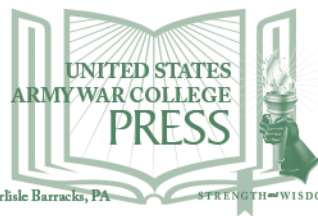
Jeffrey L. Caton

Follow this and additional works at: <https://press.armywarcollege.edu/monographs>

Recommended Citation

Jeffrey L. Caton, *The Army Role in Achieving Deterrence in Cyberspace* (US Army War College Press, 2019),
<https://press.armywarcollege.edu/monographs/380>

This Book is brought to you for free and open access by USAWC Press. It has been accepted for inclusion in Monographs, Books, & Publications by an authorized administrator of USAWC Press.



THE ARMY ROLE IN ACHIEVING DETERRENCE IN CYBERSPACE

Jeffrey L. Caton



The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a “think factory” for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.



The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.



The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.



The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.



The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.



The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE



The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

**Strategic Studies Institute
and
U.S. Army War College Press**

**THE ARMY ROLE IN ACHIEVING DETERRENCE
IN CYBERSPACE**

Jeffrey L. Caton

March 2019

The views expressed in this report are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. Authors of Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official U.S. policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This report is cleared for public release; distribution is unlimited.

This publication is subject to Title 17, United States Code, Sections 101 and 105. It is in the public domain and may not be copyrighted.

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5238.

This manuscript was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, <http://ssi.armywarcollege.edu/>, at the Opportunities tab.

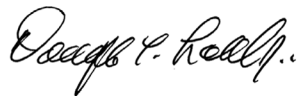
All Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications may be downloaded free of charge from the SSI website. Hard copies of certain reports may also be obtained free of charge while supplies last by placing an order on the SSI website. Check the website for availability. SSI publications may be quoted or reprinted in part or in full with permission and appropriate credit given to the U.S. Army Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, Carlisle, PA. Contact SSI by visiting our website at the following address: <http://ssi.armywarcollege.edu/>.

The Strategic Studies Institute and U.S. Army War College Press publishes a quarterly email newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on the SSI website at the following address: <http://ssi.armywarcollege.edu/newsletter/>.

ISBN 1-58487-798-7

FOREWORD

The U.S. tradition of pursuing national-level deterrence has developed and evolved significantly since the introduction of the Monroe Doctrine in 1823. Since the United States has stated publicly that it has vital interests in cyberspace, it is prudent for the Nation to achieve deterrence in this relatively new realm. In this monograph, Mr. Jeffrey L. Caton examines the implications for the U.S. Army to support such an endeavor. He analyzes existing policy and strategy documents, written at the departmental and executive level, as well as the international commitments that they may embody. He also explores the concepts of deterrence in cyberspace in the context of traditional deterrence utilizing all forms of national power, as well as aspects potentially unique to cyberspace. He argues that mechanisms of cyberspace deterrence exist whether we are aware of them or not, and that without proper coordination, such deterrence measures may escalate the conflict to levels undesired by either party. Further, he asserts that if military professionals do not seek to study these mechanisms, the Nation's military cyberspace operations may be conducted by those who are unenlightened as to the larger context and stakes of tactical- and operational-level cyber exchanges. Thus, this monograph aims to inform the ongoing activities of U.S. Cyber Command (USCYBERCOM) as well as individual Service cyberspace organizations.



DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

ABOUT THE AUTHOR

JEFFREY L. CATON is president of Kepler Strategies LLC, Carlisle, Pennsylvania, a veteran-owned small business specializing in national security, cyberspace theory, and aerospace technology. He is also an intermittent professor of program management with Defense Acquisition University. From 2007 to 2012, Mr. Caton served on the U.S. Army War College (USAWC) faculty, including as an associate professor of cyberspace operations and defense transformation chair. Over the past 9 years, he has presented lectures on cyberspace and space issues related to international security in the United States, Sweden, the United Kingdom, Estonia, Kazakhstan, and the Czech Republic, supporting programs such as the Partnership for Peace Consortium and the North Atlantic Treaty Organization Cooperative Cyber Defence Center of Excellence. His current work includes research examining the recent elevation of U.S. Cyber Command (USCYBERCOM) to a unified command as well as the evolving role of the U.S. Army with nuclear operations as part of the External Research Associates Program of the Strategic Studies Institute (SSI). Mr. Caton is also a member of the editorial board for *Parameters* magazine. He served 28 years in the U.S. Air Force working in engineering, space operations, joint operations, and foreign military sales, and commanded at the squadron and group level. Mr. Caton holds a bachelor's degree in chemical engineering from the University of Virginia, a master's degree in aeronautical engineering from the Air Force Institute of Technology, and a master's degree in strategic studies from the Air War College.

SUMMARY

Strategic deterrence has been a significant issue for the Department of Defense (DoD) for over 70 years, but many limit this concept to the use of nuclear weapons. The 2015 *DoD Cyber Strategy* explicitly calls for a comprehensive strategy to provide credible deterrence in cyberspace against threats from key state and nonstate actors. To be effective, such activities must be coordinated with ongoing deterrence efforts in the physical realm, especially those of near-peers impacting critical global regions such as China in the Asia-Pacific region and Russia in Europe. It is important for the Army to identify and plan for any unique roles that they may provide to these endeavors.

This monograph is divided into three major sections. The first section addresses the question: What is the current U.S. deterrence posture for cyberspace? The discussion will include an assessment of relevant current national and DoD policies and concepts as well as an examination of key issues for cyber deterrence found in professional literature. The second section examines the question: What are the Army's roles in cyberspace deterrence? It provides background information on how Army cyber forces operate and examines the potential contributions of these forces to the deterrence efforts prescribed in the *DoD Cyber Strategy*, as well as to broader DoD strategic deterrence efforts. The section addresses how the priority of these contributions may change with escalating levels of conflict. The final section provides recommendations for changing or adapting DoD and Army responsibilities to better define and implement the evolving concepts and actions supporting deterrence in the dynamic domain of cyberspace.

The discussion in this monograph is limited to unclassified and publicly available sources of information available before October 2017. Since some of the issues addressed herein are well documented in many sources, this monograph serves as a primer on current and future cyberspace deterrence activities for senior policymakers, decision makers, military leaders, and their staffs. This monograph includes recommendations related to strategic and regional applications for deterrence, potential synergy of various forms of military deterrence, and the possibility of creating a cyber-triad deterrence concept.

THE ARMY ROLE IN ACHIEVING DETERRENCE IN CYBERSPACE

Strategic deterrence has been a significant issue for the Department of Defense (DoD) for over 70 years, but many limit this concept to the use of nuclear weapons (or perhaps, the lack thereof). The April 2015 *DoD Cyber Strategy* emphasizes the increased need for credible deterrence in cyberspace:

In the face of an escalating threat, the Department of Defense [DoD] must contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key state and nonstate actors from conducting cyberattacks against U.S. interests. (p. 10)

Ideally, such deterrence must consider and address both state and nonstate actors. A cyber deterrence strategy must be coordinated with ongoing deterrence efforts in the physical realm, especially those of neighbors impacting critical global regions such as China in the Asia-Pacific region and Russia in Europe to be effective. It is important for the Army to identify and plan for any unique roles that they may provide to these endeavors.

This monograph is divided into three major sections. The first section addresses the question: What is the current U.S. deterrence posture for cyberspace? The discussion includes an assessment of relevant current national and DoD policies and concepts as well as an examination of key issues for cyber deterrence found in professional literature. The second section examines the question: What are the Army's roles in cyberspace deterrence? It provides background information on how Army cyber forces operate and examines the potential contributions of these forces to the deterrence efforts prescribed in the *DoD Cyber Strategy*, as well as to broader DoD strategic deterrence efforts.

This section addresses how the priority of these contributions may change with escalating levels of conflict. The final section provides recommendations for changing or adapting DoD and Army responsibilities to better define and implement the evolving concepts and actions supporting deterrence in the dynamic domain of cyberspace.

The discussion in this monograph is limited to unclassified and publicly available sources of information. Since some of the issues addressed herein are well documented in many sources, this study serves as a primer on current and future cyberspace deterrence activities for senior policymakers, decision-makers, military leaders, and their staffs.

CURRENT U.S. DETERRENCE POSTURE FOR CYBERSPACE

This section examines the current approach of the U.S. Government to cyberspace deterrence in three ways. First, it reviews national policy and strategy; next, it explores the relevant DoD policies and concepts; and finally, it surveys common issues and challenges contained in professional literature. Any mention of classical or traditional deterrence theory usually refers to the policies and strategies developed during the Cold War to guide the use of nuclear weapons. Unless otherwise noted, this monograph will use the current joint definition of deterrence as “the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits.”¹ Recognizing that operational deterrence is part of any joint campaign plan, this study emphasizes strategic level deterrence that provides the “backbone” deterrence that enables all global and regional operations.

National Deterrence Policy

What seems clear is that our adversaries have reached a common conclusion: that the reward for attacking America in cyberspace outweighs the risk. For years, cyber attacks on our Nation have been met with indecision and inaction. Our Nation has no policy and thus no strategy for cyber deterrence. This appearance of weakness has been provocative to our adversaries who have attacked us again and again with growing severity. Unless we demonstrate that the costs of attacking the United States outweigh the perceived benefits, these cyber attacks will only grow.²

—Senator John McCain, January 5, 2017

Senator McCain’s introductory comments at the start of a Senate Armed Services Committee testimony summed up his perspective on the serious nature of cyber deterrence. He indicated that the task went beyond mere cyber means, stating that successful cyber deterrence requires restored credibility of U.S. deterrence writ large. The senator then summed up perhaps the greatest challenge in this venture: “What is our theory of cyber deterrence, and what is our strategy to implement it?”³

Several U.S. Government leaders offered their assessments in response to these questions. Under Secretary of Defense for Intelligence, Marcel J. Lettre II, admitted that work remains in the refinement of a “national cyber policy framework” that has a foundation of denial, imposition of costs, and resilience.⁴ Director of National Intelligence, James R. Clapper, Jr., had a more pessimistic appraisal: “We currently cannot put a lot of stock, at least in my mind, in cyber deterrence.” He asserted that the “ephemeral” nature

of cyberspace limits the “substance and psychology” required for effective deterrence.⁵ Certainly, one might argue the antithesis of Clapper’s opinion, in that the very uncertain and unpredictable nature of cyber operations may add to its value. Admiral Michael Rogers, commander, U.S. Cyber Command (USCYBERCOM) noted that while defense is an integral part of a cyber deterrence strategy, defensive actions alone are not sufficient:

We have got to ask ourselves how do we change this broader dynamic . . . how do we convince nations and other actors that there is a price to pay for this behavior, that in fact it is not in your best interest.⁶

Senator McCain’s statement is accurate regarding the lack of a national cyber deterrence strategy; however, there is an official cyber deterrence policy. In December 2015, the White House submitted a policy report to Congress that “offers an initial roadmap for the United States Government’s departments and agencies to identify their role in the United States’ cyber deterrence efforts, to execute on specific lines of effort, and to develop plans for the future.”⁷

Figure 1 summarizes some of the key themes in current U.S. national cyber deterrence policy. Key tenets of the policy include:

improved defenses, more resilient architectures, and a range of options—cyber and non-cyber—to inflict costs and to hold accountable adversaries that choose to conduct cyber attacks or other malicious activity against U.S. interests.⁸

The policy rests upon deterrence by denial and deterrence by cost imposition, both of which are supported by whole-of-government and whole-of-nation

capabilities, declaratory statements and strategic communications, intelligence capabilities, international engagement, and research and development.⁹ Senator McCain criticized the policy for not introducing any new information as well as not providing details on how the Nation should “integrate ends, ways and means to meaningfully deter attacks in cyberspace.”¹⁰ While it is true that the policy did not provide an actionable strategy, it was nonetheless a vast improvement over the 2015 *National Security Strategy*, which was devoid of any reference to cyber deterrence.¹¹

Key Themes of Current U.S. National Cyber Deterrence Policy
<ul style="list-style-type: none"> ▪ Balanced combination of deterrence by denial and deterrence through cost imposition. ▪ Whole-of-government approach leveraging full range of national instruments of power: diplomatic, informational, military, economic, intelligence, and law enforcement. ▪ Tailorable to a specific situation and adversary; not “one-size-fits-all.” ▪ Extendable to international allies and partners. ▪ Part of a larger U.S. deterrence posture that includes a foundation of nuclear deterrence. ▪ Includes explicit declaratory statements in some U.S. cyberspace strategy documents. ▪ Widespread availability of cyberspace capabilities requires deterrence of nonstate actors in cyberspace.

Figure 1. U.S. National Cyber Deterrence—Current Policy Focus

Much of the 2015 White House cyber policy was derived from the 2011 *International Strategy for Cyberspace*, which laid out policy priorities in the areas of

the economy, network protection, law enforcement, military operations, Internet governance, international development, and freedom and privacy.¹² More importantly, it dedicated a section to discuss dissuasion and deterrence with respect to protecting U.S. networks, which included a surprisingly frank declaratory statement:

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.¹³

The most recent update to the national cyber deterrence policy can be found in the March 2016 *Department of State International Cyberspace Policy Strategy*. It echoes the key themes of pursuing cyber deterrence through a combination of denial and cost imposition as well as the use of tailored approaches that leverage the full range of national instruments of power.¹⁴ The strategy also endeavors to provide the President with a wide range of options that leverage resources from the DoD, the Department of Justice, the Department of Homeland Security, and the Department of State.¹⁵

DoD Deterrence Policy and Concepts

In his April 2017 congressional testimony, General John Hyten, commander, U.S. Strategic Command (USSTRATCOM), provided a modern context for his command's primary mission:

in the 21st century, strategic deterrence is more than nuclear. It is the integration of all our capabilities in all domains across all the combatant commands, other governmental organizations, and alongside our allies.¹⁶

He also commented on the changing nature of deterrence from the perspective of our adversaries:

Well, I look at the evidence, and the evidence is when we de-emphasize nuclear weapons, both our primary adversaries, Russia and China, have both increased their focus on nuclear weapons... They also looked at now threatening space and threatening cyberspace. They went a significant direction and a different deterrent element than we did. So I believe you always have to look at your adversaries and understand what they do and then make sure you are in a position of strength relative to your adversaries. That is what deterrence is all about.¹⁷

General Hyten's remarks amplify some of the priorities that were established in the 2015 *National Military Strategy*, which put "Maintain a secure and effective nuclear deterrent" at the top of its list of joint force prioritized missions.¹⁸ While the 2015 strategy does discuss the importance of deterring potential adversaries in regional conflicts, it does not address any role of cyberspace activities in strategic or regional deterrence. This lack of emphasis is consistent with the content of the 2014 *Quadrennial Defense Review*, which averred that the foundational aspect of nuclear deterrence was "the ultimate protection against a nuclear

attack on the United States, and through extended deterrence, it also serves to reassure our distant allies of their security against regional aggression.”¹⁹ The 2014 review links space systems and missile defense to strategic deterrence but does not mention cyberspace operations in the same context.²⁰

The most recent DoD publication that deals directly with matters of military deterrence is the 2006 *Deterrence Operations Joint Operating Concept* (DOJOC).²¹ It was written before USCYBERCOM was formed and when key concepts related to cyberspace were discussed in terms of computer network operation that were a subset of joint information operations.²² The central idea of the DOJOC is presented in an end-ways-means paradigm. In this model, the end of joint deterrence operations is “to decisively influence the adversary’s decision-making calculus” toward a goal “to convince potential adversaries that courses of action that threaten US vital interests will result in outcomes that are decisively worse than they could achieve through alternative courses of action available to them.”²³ The DOJOC ways are a threefold set of actions that echo traditional deterrence actions: denying benefits, imposing costs, and encouraging adversary restraint.²⁴ Joint deterrence means are considered as four direct activities (force projection, active and passive defense, global strike, and strategic communication) and five enabling activities (global situational awareness, command and control, forward presence, security cooperation, and deterrence assessment).²⁵ For deterrence implementation, the DOJOC addresses the need to tailor deterrence operations to specific adversaries and strategic contexts as well as the practical matters of dealing with multiple decision makers in a dynamic and uncertain environment. Finally, the

document identifies anticipated sources of risk and provides a potential means of mitigation.²⁶

The DOJOC contains several overt references to cyberspace activities related to the global aspects of deterrence. In considering future adversaries, it notes the challenges presented by commercially available capabilities in cyberspace that can provide a global reach to nonstate actors.²⁷ The DOJOC also identifies cyber systems as a method to achieve Global Strike effects at high speeds over extended distances.²⁸ An illustrative example of deterrence provided in a DOJOC appendix presents an interesting role for cyberspace to sabotage adversary acquisition activities and undermine relationships with third-party actors.²⁹ In the self-assessment of how the DOJOC incorporates linkages to joint capability areas, it recognizes the growing significance of cyberspace activities, noting that the areas of joint information operations, public affairs operations, and shaping “do not adequately cover the emerging cyberspace warfare requirements.”³⁰ A significant challenge for evolving cyberspace deterrence will be to establish and ensure the credibility of threatened offensive applications. The DOJOC recommends, “Key elements of Global Strike capabilities should be periodically demonstrated openly on the world stage—to ensure adversary decision-makers fully comprehend the credible threats they face.”³¹ How does one accomplish this for offensive cyberspace operations (OCO) without revealing the vulnerabilities that the cyberweapon may exploit? Do more recent DoD documents address such issues?

The 2015 *DoD Cyber Strategy* emphasizes deterrence as an objective under its Strategic Goal III: “Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of

significant consequence.”³² One of the five objectives for this goal is for USSTRATCOM to “Assess DoD’s cyber deterrence posture and strategy” to determine in part if the DoD is building the right capabilities to deter key cyberspace threats, especially those associated with nonstate actors.³³ The *DoD Cyber Strategy* envisions three key elements of cyber deterrence: response, denial, and resilience. It notes that deterrence is not limited to military actions, but is achieved “through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems.”³⁴ Further, the strategy calls for collective deterrent efforts with other nations in its Strategic Goal V: “Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.”³⁵ Also, collaboration with private and whole-of-government is required to help face the challenge of attack attribution, which is “especially important for deterrence as activist groups, criminal organizations, and other actors acquire advanced cyber capabilities over time.”³⁶ The *DoD Cyber Strategy* concludes that a DoD cyberspace deterrence is not sufficient without a comprehensive national cyber deterrence strategy in place to guide the complex array of resources and methods available domestically and internationally.³⁷ Although the national cyber deterrence policy announced by the White House in December 2015 was a step in the right direction, no such comprehensive cyber deterrence strategy has come forth yet.

To more fully explore the concept of cyber deterrence, the Defense Science Board (DSB) conducted a 2-year study “to identify critical capabilities (cyber and

non-cyber) needed to support deterrence, warfighting, and escalation control against a highly cyber-capable adversary.”³⁸ The DSB *Task Force on Cyber Deterrence* report was published in February 2017, and it defines cyber deterrence as “the use of both deterrence by denial and deterrence by cost imposition to convince adversaries not to conduct cyber attacks or costly cyber intrusions against the United States.”³⁹ The DSB study addresses three types of adversaries: major powers/near-peer (China, Russia); lesser regional powers (Iran, North Korea); and other state and non-state actors who can stage “persistent cyber attacks and costly cyber intrusions.”⁴⁰ The report emphasizes that the aspects of denial and cost imposition should not be mutually exclusive; rather, both should be used in an appropriate balance of deterrence activities. Also, the report provides eight guiding principles to help define the context of its review and findings.⁴¹

The findings and recommendations of the 2017 DSB *Task Force on Cyber Deterrence* report are organized into three groups. The first, “Plan and Conduct Tailored Deterrence Campaigns,” emphasizes campaign planning and wargaming with combatant commands as well as the development of “an array of scalable offensive cyber capabilities.”⁴² The next group is “Create a Second-Strike Cyber Resilient ‘Thin Line’ Element of U.S. Military Forces,” which reaffirmed the findings of a 2013 DSB study by arguing that “Scalable military strike capabilities – including offensive cyber, non-nuclear long-range strike, and nuclear systems – are the foundation of U.S. deterrence by cost-imposition.”⁴³ To ensure such a force is up to the deterrence task at hand, the report advocates the development of a National Security Agency-based standing Red Team to test the capabilities of this combined strike force.⁴⁴ The final group of recommendations addresses the

need to “Enhance Foundational Capabilities” that include attribution determination, resiliency measures, and critical infrastructure protection.⁴⁵ The report also makes a brief mention of the need to pursue extended deterrence with allies and partners as well as the need for USCYBERCOM to continue to build a “top-notch cyber cadre.”⁴⁶

Many of the themes explored in the 2017 DSB report have their origin in the 2013 DSB *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, a study that set out “to improve the resilience of DoD systems to cyber attacks.”⁴⁷ The study categorized cyberthreats into six tiers that ranged from nuisance to existential, and its analysis expanded traditional deterrence concepts, noting that “the cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War.”⁴⁸ The report came to a similar conclusion, and it asserted a controversial view that “While the manifestation of a nuclear and cyber attack are very different, in the end, the existential impact to the United States is the same,” and could potentially be achieved through attacks on critical infrastructure.⁴⁹ To address this threat, the report argues that an effective response should include “elements of deterrence, mission assurances, and offensive cyber capabilities.”⁵⁰

With regard to national strategic deterrence, one of the 2013 DSB report’s key recommendations was to “Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary.”⁵¹ The report recommended that “to ensure the President has options beyond a nuclear-only response to a catastrophic cyber attack, the DoD must develop a mix of offensive cyber and high-confidence conventional capabilities.”⁵² Further, the report recommends

a strategy that emphasizes the use of OCO to deter upper tier cyberthreats and emphasizes defensive cyberspace operations (DCO) to minimize the impacts of medium- and lower-tier cyberthreats.⁵³ Finally, the report offers recommendations and suggested metrics for progress in the areas of deterrence, intelligence, world-class OCO and DCO, operational culture, and cyber resilience.⁵⁴

Key Issues for Cyberspace Deterrence

How is cyber deterrence viewed in the current dialogue within professional literature? With the growing popularity of the topic, this section cannot present a comprehensive assessment of the ongoing discourse. Instead, this section examines representative sources that offer varying perspectives of key issues for an emerging national cyber deterrence policy.

One of the most often quoted books in this subject area is Dr. Martin C. Libicki's 2009 *Cyberdeterrence and Cyberwar*, largely because it was one of the first publications to deal explicitly with deterrence in and through cyberspace. Written to inform Air Force leaders in the development of their fledgling cyber command, the study focuses on the policies surrounding conflict in cyberspace and "explores some key aspects of cyberwar to establish a framework for considering cyberdeterrence."⁵⁵ Libicki coins an interesting definition for cyber deterrence as "deterrence in kind to test the proposition that the United States, as [former commander USSTRATCOM] General Cartwright offered, needs to develop a capability in cyberspace to do unto others what others may want to do unto us."⁵⁶ Based on this perspective, Libicki limits his study to address mostly the principles of deterrence by punishment. Like former Director of National Intelligence Clapper,

he oversimplifies nuclear deterrence and asserts, “the ambiguities of cyberdeterrence contrast starkly with the clarities of nuclear deterrence.”⁵⁷ While declarations such as “operational cyberwar has an important niche role, but only that” may not stand the test of time, the analysis framework put forth by Libicki to explore “why cyberdeterrence is different” continues to have relevance in this dialogue.⁵⁸ Finally, *Cyberdeterrence and Cyberwar* offers one of the first analyses of active cyber retaliation and even potential escalation to cyberwar or general war.

In his Joint Advanced Warfighting School thesis, “Deterrence in Cyberspace,” Lieutenant Commander Matthew Rivera seeks to determine the areas of policy required to enable effective national cyberspace deterrence. He explores the history of nuclear deterrence and extracts relevant elements from that national experience to serve as a foundation for a national cyber deterrence policy. His study yields eight “aspects of deterrence” to consider: attribution, penalty, credibility, a definition of attack, dependency, counterproductivity, awareness, and futility.⁵⁹ Rivera then takes these aspects and explores how they are applied in existing executive policies and directives as well as those for the DoD and Department of Homeland Security. He provides readers with a useful matrix that cross-references the aspects against specific U.S. Government guidance documents in order to identify policy shortfalls.⁶⁰ Finally, Rivera uses the eight aspects as a framework to assess recent cyberspace attacks such as Stuxnet, Estonia, and Georgia. His recommendations include a call for the United States “to publicly demonstrate its cyber offensive capability” to convince potential adversaries that U.S. forces “can inflict significant damage in cyberspace.”⁶¹

In an award-winning essay for *Joint Force Quarterly*, Lieutenant Colonel Clorinda Trujillo, U.S. Air Force, explores “The Limits of Cyberspace Deterrence.” The author reviews the history of joint deterrence and notes that successful active deterrence—that is, deterrence by punishment—requires attribution, signaling, and credibility. Based on a review of the policy, the author lists seven proposed cyberspace deterrence options that emphasize defensive and passive means with no explicit mention of retaliation. The use of offensive cyberspace received only a passing mention, which is arguably a reduction in significance that does not match the literature reviewed.⁶² Trujillo argues there are several barriers to cyberspace deterrence, to include difficulty in attack attribution; the first-strike advantage that cannot be deterred; risk of asymmetric vulnerability to attack in cyberspace; credibility; and different risk tolerance than actions in the physical domain.⁶³ While presenting recommendations to improve cyber deterrence, Trujillo ponders if current efforts to consolidate DoD networks for enhanced defense also may centralize vulnerabilities for potential attackers—that is, efforts toward defense and resilience actually may be counterproductive.⁶⁴

In a different *Joint Force Quarterly* article, “Rethinking the Cyber Domain and Deterrence,” Dr. Dorothy Denning challenges several fundamental aspects as well as implicit and explicit assumptions regarding cyber deterrence. Key tenets of the article are the fact that cyberspace—like the other operational domains—is a combination of natural (the electromagnetic spectrum for cyberspace) and manufactured structures and that deterrence focuses on influencing decisions and actions—the human elements.⁶⁵ Denning challenges the notion that “it is easier, cheaper, and faster

to act in cyberspace than in traditional domains,” arguing that “resources and skillsets matter as much in cyberspace as any other domain.”⁶⁶ Denning also discusses the concept of domain malleability and challenges the perception that cyberspace is more malleable than other domains, pointing out that significant changes in cyberspace are met with the inertia of standards, legacy software, equipment interoperability, and transmission protocols.⁶⁷

Regarding any comparison of cyber deterrence to nuclear deterrence, Denning asserts “the principles that have made nuclear deterrence effective for over half a century fall apart in cyberspace.”⁶⁸ She supports this position by arguing that nuclear deterrence was weapon-based, dependent on the nature of the weapon. However, Denning fails to examine the nuances and numerous manifestations of nuclear weapons, such as their platforms and delivery systems. In fact, there is no “specific type of weapon” upon which rests nuclear deterrence. Rather, nuclear weapons are part of a complex and still evolving force structure coupled with an equally complex command and control system, topped off by political and diplomatic discourse at the highest levels of governments—such a description may also apply to cyberspace. Therefore, is cyber deterrence domain- or weapon-based? Denning offers insights for both cases, first examining classes of cyberweapons that can support defensive and offensive cyberspace actions, and then identifying several established international regimes that may enable cyber deterrence.⁶⁹

Security expert Joseph S. Nye, Jr., examines the relevance of nuclear deterrence lessons in his 2011 *Strategic Studies Quarterly* article, “Nuclear Lessons for Cyber Security.” In contrast to Denning, Nye argues

that while cyber and nukes are different, their development and employment are similar and thus worthy of thoughtful consideration. He organized the article into four general lessons and six international cooperation lessons that include technology outpacing policy, complications due to civilian use, the role of arms control, and the complexity of deterrence in general.⁷⁰ His conclusion includes prudent advice for those who may summarily dismiss the lessons of nuclear deterrence learned during the Cold War, which continue to be valid:

It may help to put the problems of designing a strategy for cyber security into perspective, particularly the aspect of cooperation among states, if we realize how long and difficult it was to develop a nuclear strategy, much less international nuclear cooperation.⁷¹

In a more recent article in *International Security*, “Deterrence and Dissuasion in Cyberspace,” Nye considers a broader paradigm of deterrence that adds entanglement and norms to the classical military-focused means of punishment and denial.⁷² For an example of changing norms, Nye observes how tactical nuclear weapons were considered “normal” in 1950s Army doctrine, but that over time the norm has shifted to nonuse—actually, divestment—of these weapons.⁷³ However, he cautions that norms may be more difficult with cyberspace, noting, “unlike physical weapons, for example, it would be difficult to reliably prohibit possession of the whole category of cyber weapons.”⁷⁴ Since norms may vary for different nations and cultures, and since deterrence can be considered a psychological process, Nye advocates for tailored deterrence, because “a threat or defense or entanglement or norm that may deter some actors

may not deter others.”⁷⁵ For the deterrence of non-state actors, Nye argues that denial plays a larger role through the use of law enforcement measures as well as “robust cyber hygiene and defenses [that] may divert some nonstate actors to other acts and means.”⁷⁶ In his conclusion, Nye suggests that escalation ladder paradigms should be used with caution to avoid allowing “an opponent to game the outcome and try tactics just below the next rung.”⁷⁷ He closed by noting that the application of deterrence means in cyberspace requires discretion and prioritization based on their level of significance to national security.⁷⁸

ARMY ROLE IN CYBERSPACE DETERRENCE

What is in the Army’s collective toolkit with regard to cyberspace deterrence? This section first explores the Army’s concepts and forces being developed for cyberspace operations; and then it examines how these forces may be able to contribute to DoD cyberspace deterrence, as well as to broader DoD deterrence efforts. It also addresses how the Army may need to prioritize these contributions based on increasing levels of conflict escalation. The following discussion will address Army roles in deterrence at the operational and strategic levels; the tactical level will not be discussed to avoid the potential of revealing sensitive tactics, techniques, and procedures.

Cyberspace and Electromagnetic Activities (CEMA)

In February 2013, the Joint Staff published Joint Publication (JP) 3-12 (R), *Cyberspace Operations*, to provide guidance to the joint force for the planning, execution, and assessment of cyberspace operations. These operations were divided into three mission

areas: DCO, OCO, and Department of Defense information network (DODIN) operations. DCO was further divided into operations inside the DODIN as defensive cyberspace operations-internal defensive measures (DCO-IDM), and operations external to the DODIN as defensive cyberspace operations-responsive actions (DCO-RA).⁷⁹

In April 2017, the Army released Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations*, as the foundational doctrine to define how the Service will implement the missions first identified in JP 3-12 (R). As its title indicates, FM 3-12 describes the CEMA concept as a more holistic approach to cyberspace operations, as summarized in its foreword:

Incorporating cyberspace electromagnetic activities (CEMA) throughout all phases of an operation is key to obtaining and maintaining freedom of maneuver in cyberspace and the . . . [electromagnetic spectrum] while denying the same to enemies and adversaries. CEMA synchronizes capabilities across domains and warfighting functions and maximizes complementary effects in and through cyberspace and the . . . [electromagnetic spectrum]. Intelligence, signal, information operations . . . , cyberspace, space, and fires operations are critical to planning, synchronizing, and executing cyberspace and electronic warfare (EW) operations. CEMA optimizes cyberspace and EW effects when integrated throughout Army operations.⁸⁰

The CEMA concept includes five broad sets of cyberspace actions and three sets of EW actions. Like the joint DCO mission, some cyberspace and EW actions take place internal to the DODIN; others occur external to it. Table 1 lists all these actions and their locations with respect to the DODIN. For further details, appendix I of this volume provides the definitions for these actions as well as depicts their relationship with the joint cyberspace missions.

Cyberspace Actions	Electronic Warfare Actions
Actions Internal to DODIN	
<ul style="list-style-type: none"> • Cyberspace Defense • Cyberspace Security 	<ul style="list-style-type: none"> • Electronic Protection
Actions External to DODIN	
<ul style="list-style-type: none"> • Cyberspace Operational Preparation of the Environment (OPE) • Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR) • Cyberspace Attack 	<ul style="list-style-type: none"> • Electronic Attack
Actions Internal and External to DODIN	
	<ul style="list-style-type: none"> • Electronic Warfare Support • Spectrum Management Operations

Table 1. Army CEMA Operational Actions⁸¹

In addition to the CEMA relationship between cyberspace operations and EW, FM 3-12 includes a model of electromagnetic spectrum operations, which is comprised of overlapping activities of EW and spectrum management operations. These spectrum management operations activities enable the effective planning and execution not only of CEMA operations but also of joint operational use of the electromagnetic spectrum writ large. The functions of spectrum management operations include policy development, frequency assignment, spectrum management, frequency interference resolution, and host nation coordination.⁸² To support unified land operations, FM 3-12 describes CEMA Working Groups as the conduit to coordinate

and synchronize CEMA operations between different levels of command (such as between brigade combat teams and corps).⁸³ In joint operations, Army units may request CEMA support of joint cyberspace forces, such as cyber combat mission teams, using the cyber effects request format and electronic attack request format.⁸⁴

Army Cyberspace Forces

U.S. Army Cyber Command [ARCYBER] directs and conducts integrated electronic warfare [EW], information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.⁸⁵

ARCYBER is the Army's operational command for cyberspace operations as well as the service component command to USSTRATCOM for cyberspace. ARCYBER achieved its full operational capability in October 2010, and it is currently working to consolidate its headquarters to Fort Gordon, Georgia by 2020.⁸⁶ Fort Gordon is also the host for the U.S. Army Training and Doctrine Command's Cyber Center of Excellence, which provides training and doctrine development for the cyber branch.⁸⁷

ARCYBER forces are organized into four major units:

- Network Enterprise Technology Command (NETCOM) at Fort Huachuca, Arizona, which focuses on DODIN operations;⁸⁸
- 1st Information Operations Command at Fort Belvoir, Virginia, with a mission that includes OCO;⁸⁹

- Cyber Protection Brigade at Fort Gordon, Georgia, which conducts DCO and supports national critical infrastructure protection;⁹⁰ and,
- 780th Military Intelligence Brigade at Fort Meade, Maryland, which conducts signals intelligence and cyberspace operations.⁹¹

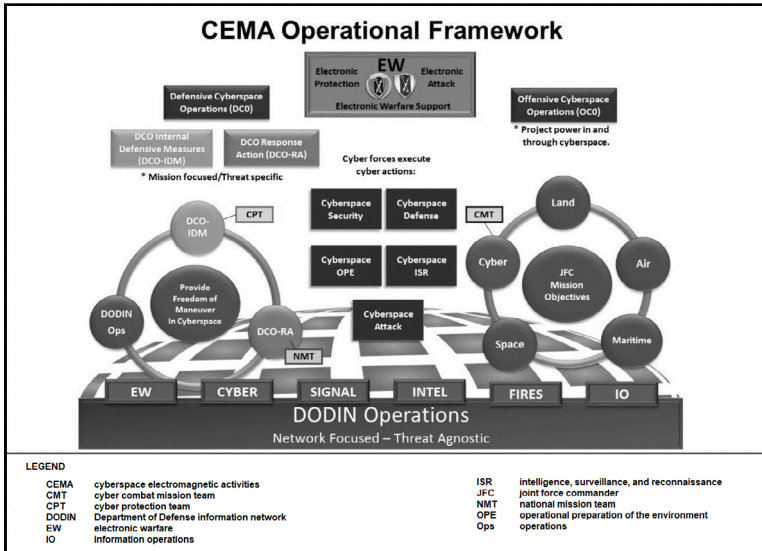
The activities of these units are monitored and controlled by the Army Cyber Operations and Integration Center, an operational unit within ARCYBER headquarters. ARCYBER also maintains a global presence and situational awareness in cyberspace through five regional cyber centers assigned to Europe, South-west Asia, Pacific, Korea, and the continental United States.⁹² As of May 2017, the Army cyber force had 2,331 Soldiers of an eventual ARCYBER force size that is planned to have over 3,800 military and civilian members with core cyber skills.⁹³

For joint cyberspace operations, ARCYBER is tasked to provide 41 teams to the USCYBERCOM cyber mission force (CMF) total of 133 teams. These teams work in concert to fulfill the USCYBERCOM mission:

USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks [DODIN] and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.⁹⁴

The 41 CMF teams of ARCYBER are broken down by function as 4 national mission teams, 3 national support teams, 8 cyber combat mission teams, 6 cyber support teams, and 20 cyber protection teams. Over 80 percent of the ARCYBER teams were mission ready in

May 2017, and all of the teams are expected to be fully operational by October 2018. Army total force units also contribute to the CMF mission, with the Army National Guard forming 11 cyber protection teams and the Army Reserve forming 10 cyber protection teams by 2021.⁹⁵ Another significant CMF role of ARCYBER is the leadership of one of the Joint Force Headquarters (JFHQ), Joint Force Headquarters-Cyber (JFHQ-C), which has the responsibility to support cyberspace activities at U.S. Northern Command, U.S. Central Command, and U.S. Africa Command.⁹⁶ Figure 2 depicts how national mission teams, cyber combat mission teams, and the cyber protection team elements of the CMF fit within the overall CEMA operational framework.



Source: U.S. Army.

Figure 2. Army CEMA Operational Framework⁹⁷

Army Contributions to DoD Cyber Strategy Deterrence Efforts

How do Army cyberspace forces contribute to cyberspace deterrence as envisioned in the response-denial-resilience paradigm of the 2015 *DoD Cyber Strategy*? Although FM 3-12 does not address cyberspace deterrence explicitly, it does discuss how CEMA operations support response and denial efforts with regard to adversary cyberspace actions. Also, while resiliency is not addressed directly, FM 3-12 does mention the need for forces to “adapt quickly and effectively to enemy and adversary presence inside cyberspace systems” as well as to “react to incidents, and then recover and adapt while supporting Army and joint forces from strategic to tactical levels while simultaneously denying adversaries effective use of cyberspace and the . . . [electromagnetic spectrum].”⁹⁸ Table 2 depicts how Army CEMA efforts best align with the three cyber strategy deterrence elements. Since it could be reasonably argued that every CEMA action can support each of the deterrence means, table 2 was built using each CEMA action only once to infer the way that it can best serve the collective goal of cyber deterrence.

Deterrence Element		Joint Cyberspace Domain Missions	Army Operational Contributions	
(Per 2015 DoD Cyber Strategy)	(Per 2006 DOJOC)		Army CEMA Operations	Army CMF Contributions
Response	Impose Costs	DCO-RA OCO	Cyberspace Attack Electronic Attack	4 national mission teams and 8 cyber combat mission teams
Denial	Deny Benefits	DCO-IDM DODIN Operations	Cyberspace Defense Cyberspace Security Electronic Protection Electronic Warfare Support	41 cyber protection teams: 20 Active Duty 11 National Guard 10 Reserve
Resilience	Encourage Restraint	DCO-IDM DODIN Operations	Cyberspace OPE Cyberspace ISR Electronic Warfare Support Spectrum Manage- ment Operations	3 national support teams and 6 cyber support teams

**Table 2. Army Contribution to
Cyberspace Deterrence**

Table 2 also depicts the broader aspect of DoD deterrence by associating the Army’s various CMF teams with the three cyberspace mission areas from JP 3-12 (R) (OCO, DCO, DODIN) as well as the three deterrence elements from the 2006 DOJOC (impose costs, deny benefits, and encourage restraint). The offensive nature of the national mission teams and cyber combat mission teams was clearly stated in open Congressional testimony by General Keith Alexander during his tenure as commander, USCYBERCOM, who noted: “this is an offensive team that the Defense Department would use to defend the Nation if it were attacked in cyber space.”⁹⁹ In addition, national support teams and cyber support teams are assigned to provide analytical and planning support to these mission teams, thus enhancing the resiliency of their

operations. The bulk of defense operations fall upon the cyber protection teams that are assigned to protect networks at Service cyberspace component commands, the JFHQ-C, the JFHQ-DODIN, and the Cyber National Mission Force headquarters.¹⁰⁰

Army Contributions to Broader DoD Deterrence Means

How can Army cyberspace operations contribute to joint deterrence operations? One way to address this question is to examine how CEMA activities can support the direct and enabling means of deterrence described in the 2006 DOJOC. Table 3 summarizes how specific CEMA activities align with specific deterrence means, with one column that considers cyberspace activities alone and a second column that considers additional activities that EW brings to the CEMA concept.

While these direct and enabling means are common to many other types of joint operations as well, the focus here is on the strategic ways of denying benefits, imposing costs, and encouraging restraint of the adversary. Accordingly, global situational awareness has a twofold goal: to determine the adversary's capabilities and to understand their perceptions of benefits and costs associated with not exercising restraint.¹⁰¹ Active and passive defenses allude to CEMA efforts, which enable net-centric forces, and they anticipate the potential use of advanced adversary weapons with wide area effects, such as electromagnetic pulse devices.¹⁰² For global strike, cyberspace operations are explicitly mentioned as part of actions employed over extended distances to meet urgent employment timelines and as "non-kinetic means . . . [that] may supplement US nuclear capabilities."¹⁰³

	Deterrence Means	Army Cyberspace Operation Contributions	
		Cyberspace Domain Operations	Multi-Domain Operations (CEMA)
Direct Deterrence Means	Force Projection	Cyberspace Attack Cyberspace OPE Cyberspace ISR	Electronic Attack: Electromagnetic Intrusion; Electronic Probing; and, Electromagnetic Deception.
	Active & Passive Defense	Cyberspace Defense Cyberspace Security	Electronic Protection: Electromagnetic Hardening; Electronic Masking; and, Emission Control. Electronic Attack: Countermeasures; Electromagnetic Deception; and, Electromagnetic Jamming. Electronic Warfare Support: Electronics Security.
	Global Strike	Cyberspace Attack	Electronic Attack: Countermeasures; Electromagnetic Intrusion; and, Electromagnetic Pulse.
	Strategic Communications	Cyberspace Defense Cyberspace Security	Electronic Warfare Support: Electronics Security.
Enabling Deterrence Means	Global Situational Awareness	Cyberspace ISR	Electronic Warfare Support: Electronic Intelligence; and, Electronic Reconnaissance.
	Command & Control	Cyberspace Defense Cyberspace Security	Electronic Protection: Electromagnetic Hardening; and, Wartime Reserve Modes. Electronic Warfare Support: Electronics Security.
	Forward Presence	Cyberspace OPE	Electronic Warfare Support: Electronic Intelligence; and, Electronic Reconnaissance. Electronic Attack: Electromagnetic Intrusion; and, Electronic Probing.
	Security Cooperation & Military Integration & Interoperability	Cyberspace OPE	Electronic Protection: Electromagnetic Compatibility; and, Electromagnetic Spectrum Management. Spectrum Management Operations.

Table 3. Army Contributions to Deterrence Means¹⁰⁴

In theory, Army CEMA activities can support all of the deterrence means in table 3, but such support may not be feasible based on the resources available. Thus, implementing CEMA actions requires balance and prioritization not only for immediate tactical and

operational needs but also for longer-term considerations of strategic deterrence. Also, the allocation of cyberspace resources must consider the degree to which specific military assets should be protected. The 2013 DSB report, *Resilient Military Systems*, cautioned:

Overextending cyber resiliency for all conventional capability will overwhelm DoD resources (technical, managerial, and financial). DoD must discipline itself to identify sufficient protected-conventional capability for assured operations.¹⁰⁵

Army Contributions Across Escalating Levels of Conflict

Deterrence is dynamic phenomena with the perspectives of decision makers subject to constant change based on actions and counteractions surrounding a given conflict. The 2006 DoD *Major Combat Operations Joint Operating Concept* supports this assertion, stating that “Tailored deterrence operations continue throughout the conflict to both deter the crisis (inter-war), and shape the adversary’s decision making process such that they do not take particular actions during the war (such as WMD [weapons of mass destruction] use).”¹⁰⁶ A more recent assessment is found in the November 2016 “Mad Scientist Conference” technical report by the U.S. Army Training and Doctrine Command G2, which notes that the cyber deterrence environment may involve:

a range of cross- and multi-domain deterrence tools [that] are emerging that may include sanctions, indictments, cyber retaliatory options, and even the threat of kinetic measures in response to cyber provocations.¹⁰⁷

The 2015 *DoD Cyber Strategy* acknowledges the challenges presented in conflict escalation through its fourth strategic goal: “Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.”¹⁰⁸ The implementation of this goal calls for the integration of cyber options into combatant command planning, assumedly through support from JFHQ-C cyber combat mission teams and cyber support teams.¹⁰⁹ But how should these planners model the contribution of cyber forces in varying levels of conflict escalation?

In his 2011 *Strategic Studies Quarterly* article, “Deterrence at the Operational Level of War,” Dr. James Blackwell examines how U.S. deterrence has changed since the Cold War. He contrasts the Cold War rationale actor model with the more contemporary behavioral model that seeks to understand the values, beliefs, and perspectives that shape adversary decision making. He also argues that models such as the Kahn Escalation Ladder that were designed to model the bipolar nature of the United States and the former Union of Soviet Socialist Republics relations might not do well in the current multipolar world. To address these changes in the deterrence environment, Blackwell offers “Ten Axioms for Campaign Planners” that address how to apply deterrence across all phases of joint operations.¹¹⁰

In contrast to Blackwell, a notional framework of analysis for active cyber defense application based on a modified Kahn ladder was proposed in the 2015 Strategic Studies Institute monograph, *Army Support of Cyberspace Operations: Joint Contexts and Global Escalation Implications*. In the updated paradigm, the seven crises regions of the Kahn model are simplified into

three areas—an upper half of conflict that deals with existential stakes (win or lose dynamics), a lower half of conflict that deals with theater or regional conflict (give and take dynamics), and a strategic warfare threshold that separates them (see figure 3 for a diagram of the modified Kahn ladder). Figure 4 depicts a possible progression of events across increasing intensity of conflict and degree of escalation with the strategic threshold characterized by cyberattacks on national critical infrastructure.¹¹¹

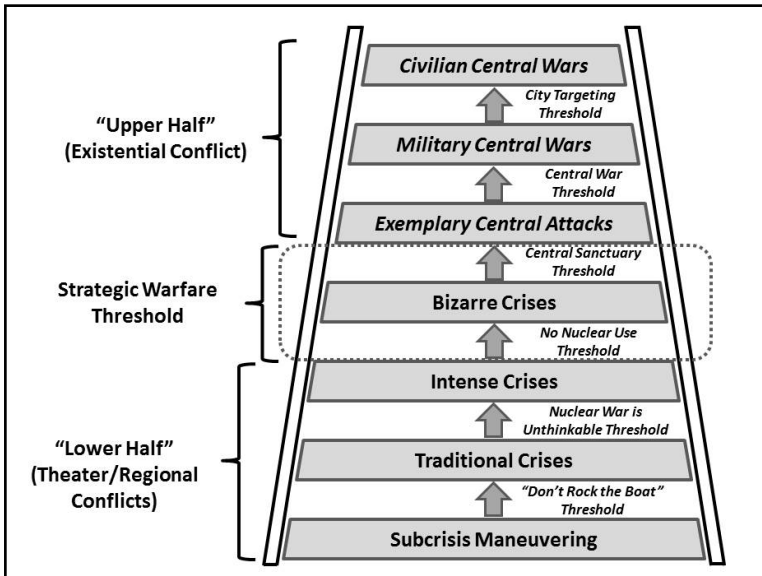


Figure 3. Modified Kahn Escalation Ladder¹¹²

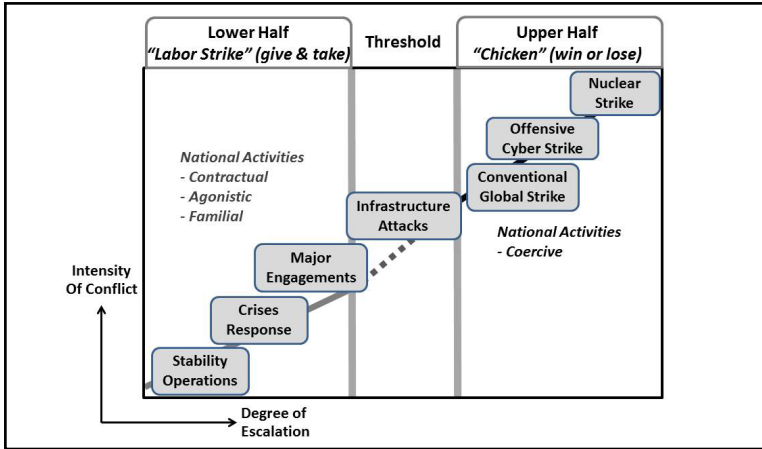


Figure 4. Dynamics of Conflict and Escalation¹¹³

How should Army cyber forces support the activities depicted in figure 4? As escalation increases the stakes involved with the conflict, the operational focus of Army cyberspace activity should adapt to best serve the strategic interests of the Nation. Table 4 provides an initial look at how the focus of Army support might change with conflict escalation; it is not presented as a solution, rather it is offered as a starting point for further dialogue. It proposes that the cyber deterrence priorities will be Response in the upper half of conflict, Denial in the threshold area, and Resilience in the lower half of conflict. Further development of this paradigm by cyber professionals should also consider the guiding principles of the 2017 DSB report on cyber deterrence, which include “deterrence by cost imposition requires credible response options at varying levels of conflict.”¹¹⁴

Escalation Ladders Area	Focus of Army Cyberspace Activity
Upper Half (Existential Conflict)	<p style="text-align: center;">Deterrence Priority: Response</p> <ul style="list-style-type: none"> • Cyberspace attack integrated with conventional and nuclear strike • Cyberspace defense and cyberspace security dedicated to nuclear and segmented conventional strike command and control • Cyberspace defense and cyberspace security reduced for some fielded forces to provide resources for priority response activities
Strategic Warfare Threshold	<p style="text-align: center;">Deterrence Priority: Denial</p> <ul style="list-style-type: none"> • Cyberspace defense and cyberspace security emphasize protection of national critical infrastructure • Cyberspace ISR and cyberspace OPE support the planning and application of DCO-RA measures
Lower Half (Theater/Regional Conflict)	<p style="text-align: center;">Deterrence Priority: Resilience</p> <ul style="list-style-type: none"> • Cyberspace ISR and cyberspace OPE emphasize enabling specific joint operating area or theater of operations • Cyberspace defense and cyberspace security emphasize protecting fielded joint forces

Table 4. Army Cyberspace Support in Simplified Escalation Ladder Areas

This section shows that the Army cyber forces can make significant contributions to U.S. cyberspace deterrence efforts as well as to broader U.S. strategic deterrence ventures. One of the greatest challenges facing Army leaders is how to balance and prioritize the almost unlimited demands of fulfilling military cyberspace missions with limited resources.

RECOMMENDATIONS

The concept of cyberspace deterrence is still in its infancy, and it is fraught with controversy regarding how to best proceed. This study has identified several key issues that should be included in the continued development and practice of cyberspace deterrence activities. This section offers suggestions to support the refinement of Army and DoD support to this endeavor.

Recommendation 1

The DoD and the Army should consider applications and implications of strategic OCO in synergy with the application of conventional and nuclear global strike.

This recommendation should build upon earlier recommendations from the 2013 DSB study on resilient military systems (determine a mix of cyber, conventional, and nuclear capabilities¹¹⁵) as well as the 2017 DSB study on cyber deterrence (boost the cyber resilience of key U.S. strike systems¹¹⁶). Also, integrating these capabilities is consistent with the 2006 DOJOC tenet to integrate nuclear and non-nuclear strike operations in order to provide increased flexibility and credibility of U.S. deterrence writ large, which in turn reduces the likelihood of nuclear weapons use.¹¹⁷ With this model in mind, perhaps the mission statement of USCYBERCOM should be modified to add: "Provide direct support of U.S. strategic deterrence operations to include the protection of nuclear operations." Certainly, one can reasonably argue that this content is contained implicitly in the current USCYBERCOM mission statement. However,

since deterrence depends on perceptions and signaling, creating the explicit connection of military cyberspace operations to existential deterrence operations can only clarify the relationship and thus strengthen deterrence credibility.¹¹⁸

Recommendation 2

The Army Cyber Center of Excellence and ARCYBER should explicitly address how CEMA supports cyberspace-domain and multi-domain deterrence operations in the next iteration of FM 3-12.

The preface of the current FM 3-12 notes that the document not only addresses tactics and procedures for unified land operations and joint operations, but also “provides overarching guidance to commanders and staffs on Army cyberspace and electronic warfare [EW] operations at all echelons.” Its intended audience is “all members of the profession of arms” which includes joint and international forces as well as trainers and educators.¹¹⁹ Some CEMA actions, such as OCO, should be pursued with full knowledge of the broader context of ongoing cyber deterrence and national deterrence efforts – yet, FM 3-12 is deficient of this context. To properly inform the intended FM 3-12 audience, a distinct and concise discussion of cyber deterrence should be added to the next iteration of FM 3-12. This enhancement to Army doctrine would also support the 2015 *DoD Cyber Strategy* strategic goal task to “Assess DoD’s cyber deterrence posture and strategy.”¹²⁰ Also, a more informed body of professionals with respect to Army contributions to cyberspace deterrence can help USSTRATCOM and USCYBERCOM in their efforts to “determine whether DoD is

building the capabilities required for attributing and deterring key threats from conducting such [cyber] attacks and recommend specific actions that DoD can take to improve its cyber deterrence posture.”¹²¹

Recommendation 3

ARCYBER JFHQ-C should deliberately develop and conduct regionally-based cyberspace deterrence planning and operations.

ARCYBER JFHQ-C is responsible for providing and coordinating CMF teams that support U.S. Central Command, U.S. Africa Command, and U.S. Northern Command. The cyber combat mission teams and cyber support teams should advise their respective combatant command staffs in the planning of theater cyberspace operations that consider the holistic deterrence context of the region. This recommendation extends the discussion and findings of the 2017 DSB report on cyber deterrence in the area of “plan and conduct tailored deterrence campaigns” to go beyond the current potential adversary list (Russia, China, Iran, North Korea, and the Islamic State of Iraq).¹²² Of course, this recommendation also applies to the JFHQ-C support to all combatant commands.

Recommendation 4

The Army should continue to refine its CEMA construct to provide a more holistic approach to cyberspace operations.

Some of the confusion and controversy surrounding cyberspace deterrence may be a reflection of ill-defined notions with regard to what activities comprise cyberspace operations. The Army CEMA paradigm appears to offer planners an effective way of merging

cyberspace operations with those of EW and electro-magnetic spectrum operations. ARCYBER and the Cyber Center of Excellence should ensure that they are not only adapting the CEMA concept to capture improvements derived from operational experience (Army and joint), but that they are also developing relevant foundational theory.

Recommendation 5

The Army should support the DoD in the development of a comprehensive cyber deterrence strategy.

As promulgated in the 2015 *DoD Cyber Strategy*, the U.S. Government needs a comprehensive cyber deterrence strategy that deliberately integrates the elements of national power: diplomatic, informational, military, economic, financial, intelligence, and legal.¹²³ ARCYBER should support USCYBERCOM in developing and maintaining such a strategy, as well as adapt ARCYBER operations to best support the tenets of the comprehensive strategy when it is available. ARCYBER should also work with the Army foreign area officer branch to educate their officers in cyberspace operations so that foreign area officers can help enable strategic cyberspace deterrence efforts in the countries where they are posted.

Recommendation 6

The Army and the DoD should include the foundations of U.S. nuclear weapon employment and related strategic deterrence concepts at all levels of professional military education.

Some of the skepticism over the applicability of “classic nuclear deterrence theory” to cyberspace

deterrence may be due to widespread ignorance of nuclear operations. In his January 2017 Senate testimony, Director of National Intelligence James Clapper implied that nuclear deterrence theory is well understood and can be even be sensed tactilely, while cyberspace is “ephemeral.” Accordingly, he asserted, “We currently cannot put a lot of stock, at least in my mind, in cyber deterrence.”¹²⁴ But who is the “we” in his statements? Do Director Clapper and other U.S. senior leaders really claim to understand the tactical and operational mechanisms of nuclear weapon employment as well as their immediate and long-term global effects? Certainly, if current joint doctrine and professional military education is an indicator, then the answer is “no.” In fact, as critical thinkers, military professionals should consider the possibility that no one has truly understood nuclear deterrence.

Further, the Cold War success at avoiding a global catastrophe may have been a happy accident of history that has given the world a false sense of security regarding still-existing stockpiles that could devastate the world. In fact, one could argue that nuclear weapons systems and operations, in general, have been purposefully simplified by some leaders and analysts in order to enable self-delusion of understanding and claiming the “success of deterrence.” Given the stakes for failure, perhaps deterrence theory that addresses the existential realm of conflict should be given more time in doctrine and professional military education. This would set the proper foundation and context for the understanding of interlinked concepts such as cyberspace deterrence. In other words, one should first study nuclear deterrence more thoroughly to seek its proper relationship to newer concepts of deterrence before throwing it out as not applicable to cyberspace.

Recommendation 7

The Army and the DoD should consider the development of a cyber triad deterrence concept.

The 2003 Nuclear Posture Review proposed a “New Triad” for nuclear deterrence forces that consisted of non-nuclear and nuclear strike capabilities, defenses, and responsive infrastructure. While the “New Triad” was phased out in the 2010 Nuclear Posture Review, the paradigm may be useful for modeling cyberspace deterrence. The similar Cyber Triad would have OCO, DCO, and responsive network infrastructure as its three legs.¹²⁵ These three legs correlate well to the three primary cyberspace missions of JP 3-12 (R), and the Cyber Triad paradigm would focus on how to balance the mixture of forces to address a specific threat or situation.

CLOSING THOUGHTS

The U.S. tradition of pursuing national-level deterrence has developed and evolved significantly since the introduction of the Monroe Doctrine in 1823. Since the United States has publicly stated that it has vital interests in cyberspace, it is prudent for the Nation to achieve deterrence in this relatively new realm. This monograph examined the implications for the Army to support such an endeavor. It considered the existing policy and strategy documents written at the departmental and executive level as well as the international commitments and implications that they may embody. It also explored the concepts of deterrence in cyberspace in the context of traditional deterrence utilizing all forms of national power as well as aspects potentially unique to cyberspace.

Mechanisms of deterrence—military and national—exist whether we are aware of them or not. Without proper coordination, deterrence measures may escalate the conflict to levels undesired by either party. If military professionals do not seek to study these mechanisms, then the Nation’s military cyberspace operations may be conducted by those who are unenlightened as to the broader context and larger stakes of tactical- and operational-level exchanges. It is confusing enough to deal with leaders who chose to think that deterrence is dead, perhaps limiting their analysis to a nostalgic Cold War nuclear perspective. Adding cyberspace to the deterrence mix certainly makes matters more complex, but that is why the issue should not be ignored out of frustration; rather, it should be embraced out of sage consideration for the future.

ENDNOTES

1. *DOD Dictionary of Military and Associated Terms*, Washington, DC: Joint Chiefs of Staff, September 2018, p. 69, available from <http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-09-06-102155-910>, accessed November 2, 2018.

2. “Stenographic Transcript Before the Committee on Armed Services, United States Senate, Hearing To Receive Testimony on Foreign Cyber Threats to the United States,” 115th Congress, Sess. 1, January 5, 2017, p. 5, available from http://armed-services.senate.gov/imo/media/doc/17-01_01-05-17.pdf, accessed October 2, 2017, hereafter, “Stenographic Transcript, Foreign Cyber Threats,” January 5, 2017.

3. *Ibid.*, p. 6.

4. *Ibid.*, p. 16.

5. *Ibid.*, pp. 24, 43. The context surrounding Director of National Intelligence Clapper’s comments on cyber deterrence was:

Unlike nuclear weapons, cyber capabilities are difficult to see and evaluate and are ephemeral. It is accordingly very hard to create the substance and psychology of deterrence in my view.” (p. 24)

The point I was trying to make is that in the case of nuclear deterrence, there are instruments you can see, feel, touch, measure, weaponry. We have had a demonstration a long time ago of the impact of nuclear weaponry. And that is what creates both the physical substance of deterrence, as well as the psychology. And the problem with the cyber domain—it does not have those physical dimensions that you can measure, see, feel, and touch as we do with nuclear deterrence. (p. 43)

6. *Ibid.*, pp. 104-105. The context of Admiral Rogers’ comments on the role of defense in cyber deterrence includes:

So as we [Senate Armed Services Committee hearing attendees] talked about more broadly today, we have got to get better on the defensive side because part of deterrence is making it harder for them to succeed. I acknowledge that. But a defensive strategy alone is not going to work. It is a resource-intensive approach to doing business, and it puts us on the wrong end of the cost equation. That is a losing strategy for us, but it is a component of a strategy. (p. 104)

7. Untitled White House report on U.S. cyber deterrence policy, accessed through article link from Scott Maucione, “White House finally acquiesces to Congress on cyber deterrence policy,” Federal News Radio, December 29, 2015, available from <https://federalnewsradio.com/cybersecurity/2015/12/white-house-finally-acquiesces-congress-cyber-deterrence-policy/>, accessed October 13, 2017.

8. Lisa O. Monaco, “Administration Efforts on Cybersecurity: The Year in Review and Looking Forward to 2016,” White House Blog, February 2, 2016, available from <https://obamawhitehouse.archives.gov/blog/2016/02/02/administration-efforts-cybersecurity-year-review-and-looking-forward-2016>, accessed October 13, 2017.

9. Untitled White House report on U.S. cyber deterrence policy, p. 1.

10. Andrew Blake, "John McCain says White House's cyber deterrence policy comes up short," *The Washington Times*, January 15, 2016, available from <https://www.washingtontimes.com/news/2016/jan/15/john-mccain-says-white-houses-cyber-deterrence-pol/>, accessed October 13, 2017.

11. Barack Obama, *National Security Strategy*, Washington, DC: The White House, February 2015.

12. Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington, DC: The White House, May 2011.

13. *Ibid.*, p. 14.

14. *Department of State International Cyberspace Policy Strategy*, Washington, DC: Department of State, March 2016, pp. 1, 20-23, available from <http://state.gov/documents/organization/255732.pdf>, accessed September 30, 2017.

15. *Ibid.*, pp. 20-23. The strategy endeavors to provide options for the President:

The President has at his disposal a number of tools to carry out deterrence by denial. These include a range of policies, regulations, and voluntary standards aimed at increasing the security and resiliency of U.S. government and private sector computer systems. They also include incident response capabilities and certain law enforcement authorities, such as those used by the Department of Justice to take down criminal botnets. They include cyber threat information sharing mechanisms, as well as public-private partnerships. International cooperation is also a key element of the United States' strategy to respond to and prevent cyber incidents. The Department of Homeland Security's National Cybersecurity and Communications Integration Center . . . and law enforcement agencies frequently engage foreign counterparts to share information and coordinate operational assistance in responding to and mitigating malicious activities taking place from abroad. The Department of State can use its diplomatic channels, where appropriate, to bring a whole-of-government response to particular cyber incidents, and promote cooperation among policy makers in addressing these incidents. (pp. 20-21)

16. "Stenographic Transcript Before the Committee on Armed Services, United States Senate, Hearing to Receive Testimony on United States Strategic Command Programs," 115th Congress, Sess. 1, Washington, DC: U.S. Government Printing Office, April 4, 2017, p. 9, available from http://armed-services.senate.gov/imo/media/doc/17-31_04-04-17.pdf, accessed October 11, 2017.

17. *Ibid.*, p. 40. General Hyten went on to note:

So I see a top tier cyber threat being Russia and China in particular because they have the ability to threaten the existence of this Nation. And so one of the reasons you have to be able to protect the nuclear command and control capability is that is fundamental to deterrence. If that is ever brought into question, that lowers our deterrent posture to top tier threats, and we have to make sure we never allow that to happen. (p. 47)

18. Chairman, Joint Chiefs of Staff, *The National Military Strategy of the United States of America, 2015: The United States Military's Contribution To National Security*, Washington, DC: Joint Chiefs of Staff, June 2015, p. 11. The strategy described nuclear deterrent efforts as:

Maintain a Secure and Effective Nuclear Deterrent. U.S. strategic forces are kept at the highest state of readiness, always prepared to respond to threats to the homeland and our vital interests. Accordingly, we are investing to sustain and modernize our nuclear enterprise. We continue to implement the 2010 Nuclear Posture Review and 2011 New START Treaty while ensuring our national defense needs are met. Concurrently, we are enhancing our command and control capabilities for strategic and regional nuclear forces. (p. 10)

19. Department of Defense (DoD), *Quadrennial Defense Review 2014*, Washington, DC: U.S. Government Printing Office, March 4, 2014, p. 13.

20. *Ibid.*, pp. 20, 32. Space systems and missile defense ties to deterrence are found in the following passages:

U.S. global communications and military operations depend on freedom of access in space, making security in this domain

vital to our ability to project power and win decisively in conflict. The Department will pursue a multi-layered approach to deter attacks on space systems while retaining the ability to respond, should deterrence fail. (p. 20)

Allied and partner acquisition of interoperable ballistic missile defense capabilities and participation in regional deterrence and defense architectures will counter the coercive and operational value of adversary ballistic missile systems as well. (p. 32)

21. *Deterrence Operations Joint Operating Concept*, Version 2.0, Washington, DC: Department of Defense, December 2006, available from http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_deterrence.pdf?ver=2017-12-28-162015-337, accessed September 27, 2017, hereafter, DOJOC.

22. Joint Chiefs of Staff, Joint Publication (JP) 3-13, *Information Operations*, Washington, DC: Joint Chiefs of Staff, February 13, 2006, pp. II-4–II-5. Computer Network Operations (CNO) was one of the five core functions of joint information operations; the other four were psychological operations, military deception, operations security, and electronic warfare (EW).

CNO is one of the latest capabilities developed in support of military operations. CNO stems from the increasing use of networked computers and supporting . . . [information technology] infrastructure systems by military and civilian organizations. CNO, along with EW, is used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure. For the purpose of military operations, CNO are divided into . . . [computer network attack, computer network defense], and related computer network exploitation . . . enabling operations. [Computer network attack] . . . consists of actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. [Computer network defense] . . . involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. [Computer network defense] . . . actions not only protect DOD systems from an external adversary but also from exploitation from

within, and are now a necessary function in all military operations. [Computer network exploitation] . . . is enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Note that due to the continued expansion of wireless networking and the integration of computers and radio frequency communications, there will be operations and capabilities that blur the line between CNO and EW and that may require case-by-case determination when EW and CNO are assigned separate release authorities.

The current version of JP 3-13 was released on November 27, 2012, and updated with change 1 on November 20, 2014; it purposefully removed the lexicon related to CNO.

23. DOJOC, p. 23.

24. *Ibid.*, pp. 24-28.

25. *Ibid.*, pp. 6, 28-44, 52-54.

26. *Ibid.*, pp. 44-52.

27. *Ibid.*, p. 15. The concept anticipates that commercially available capabilities will significantly increase the challenges to U.S. forces:

The proliferation of commercial dual-use technology, including the addition of satellite-assisted precision-guided weapons, will make this adaptation more feasible for a wider variety of potential adversaries. Additionally, commercially available information and cyber services (many enabled through common space systems) will provide an element of global reach for actors once limited to exerting only regional influence. The emergence of advanced capabilities and technologies such as computer network attack or directed energy weapons may permit future adversaries to achieve objectives once attainable only via the use of WMD [weapons of mass destruction].

28. *Ibid.*, p. 39.

29. *Ibid.*, pp. 62-64. Deterrence actions recommended in an example include: "Conduct CYBERSPACE WARFARE to

sabotage [e.g., discredit financial data] systems associated with Adversary X's WMD acquisition activities and undermine their support relationships with other third-party actors. (denying benefits)." (p. 64)

30. Ibid., p. 76.

31. Ibid., p. 41.

32. *The Department of Defense Cyber Strategy*, Washington, DC: Department of Defense, April 2015.

33. Ibid., pp. 25-26.

34. Ibid., p. 10.

35. Ibid., pp. 26-28.

36. Ibid., p. 12.

37. Ibid., p. 10. The call for a comprehensive cyber deterrence strategy is summarized as:

In the face of an escalating threat, the Department of Defense [DoD] must contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key state and non-state actors from conducting cyberattacks against U.S. interests. Because of the variety and number of state and non-state cyber actors in cyberspace and the relative availability of destructive cyber tools, an effective deterrence strategy requires a range of policies and capabilities to affect a state or non-state actors' behavior.

38. See the cover letter, "SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence," signed James N. Miller and James R. Gosler, to the DSB, *Task Force on Cyber Deterrence*, Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, February 2017, available from <http://www.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf>, accessed September 26, 2017.

39. DSB, *Task Force on Cyber Deterrence*, p. 3.

40. Ibid. The DSB report defines the two major types of cyber threats as:

Cyber Attack. For the purposes of this report, a cyber attack is any deliberate action that affects the desired availability and/or integrity of data or information systems integral to operational outcomes of a given organization. Not all cyber intrusions constitute attacks; indeed the vast majority do not. Cyber attacks may have temporary or permanent effects; they may be destructive of equipment or only disruptive of services; and they may be conducted remotely or by close access (including by insiders). In addition, while there is considerable attention given to cyber attacks focused on data and software-in-operation, supply chain vulnerabilities are of growing concern in a world where critical infrastructure is built and sustained through a global supply chain subject to malicious alteration across various phases of system life cycles [emphasis in original]. (pp. 2-3)

Costly Cyber Intrusions. Under our definitions, China's massive cyber theft of U.S. intellectual property and Russia's hack of U.S. political parties to facilitate information operations undermining confidence in U.S. elections represent costly cyber intrusions. The cyber intrusions in these cases did not affect the availability and/or integrity of U.S. data or information systems, and so do not constitute cyber attacks, but these intrusions did facilitate unacceptable actions by China and Russia that imposed respectively economic and political costs on the United States [emphasis in original]. (p. 3)

41. Ibid., pp. 6-8. The eight guiding principles of the report are:

The U.S. cyber deterrence posture must include both deterrence by denial and deterrence by cost imposition, with a different balance depending on the perpetrator and the severity of the attack to be deterred.

Deterrence by cost imposition requires understanding what key adversary decision makers value, holding that which they value at risk, and communicating (explicitly and/or implicitly by precedential action) the credible will and capability to respond.

Deterrence by cost imposition requires credible response options at varying levels of conflict.

In the event of a cyber attack on the United States (i.e., a failure of cyber deterrence), the question should not be whether to impose costs in response, but how and when to do so against the attacker, and how to connect the response to the attack.

The United States must clarify, first internally and then to potential adversaries, that it seeks to deter and will aim to impose countervailing costs in response to some forms of costly cyber intrusions.

Responding to adversary cyber attacks and costly cyber intrusions carries a risk of escalation (and quite possibly intelligence loss), but not responding carries near-certainty of suffering otherwise deterrable attacks in the future.

Reducing the vulnerability of U.S. critical infrastructure is essential not only to deterrence by denial, it also reinforces the credibility of U.S. threats to impose costs on attackers.

Although it may appear desirable in theory to find effective arms control approaches to stabilize the cyber balance between major powers—U.S.-Russia and U.S.-China—in practice cyber arms control is not viable, though norms and rules of the road may be both viable and highly valuable.

42. *Ibid.*, pp. 9-16.

43. *Ibid.*, p. 18.

44. *Ibid.*, p. 21.

45. *Ibid.*, pp. 25-28.

46. *Ibid.*, p. 28.

47. See the DSB report, co-chaired by James R. Gosler and Lewis Von Thae, DSB, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, Washington, DC: Defense Science Board, Department of Defense, January 2013, p. ii, available from <https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf>, accessed September 28, 2017.

48. Ibid., p. 31.

49. Ibid., pp. 6, 15. The report asserts that cyberattacks may constitute an existential threat:

The DoD should expect cyber to be part of all future conflicts, especially against near-peer and peer adversaries. This Task Force believes that full manifestation of the cyber threat could even produce existential consequences to the United States, particularly with respect to critical infrastructure. (p. 15)

50. Ibid., p. 31.

51. Ibid., p. 7.

52. Ibid., p. 8. The proposed response options available to the President would include:

Cyber offense may provide the means to respond in-kind. The protected conventional capability should provide credible and observable kinetic effects globally. Forces supporting this capability are isolated and segmented from general purpose forces to maintain the highest level of cyber resiliency at an affordable cost. Nuclear weapons would remain the ultimate response and anchor the deterrence ladder. This strategy builds a real ladder of capabilities and alleviates the need to protect all of our systems to the highest level requirements, which is unaffordable for the nation. Similar to the prior argument regarding the cyber resiliency of the nuclear deterrent, DoD must ensure that some portion of its conventional capability is able to provide assured operations for theater and regional operations within a full-spectrum, cyber-stressed environment.

53. Ibid., p. 32.

54. Ibid., p. 33. The seven report recommendations are:

1. Protect the Nuclear Strike as a Deterrent (for existing nuclear armed states and existential cyber attack).
2. Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary.

3. Refocus Intelligence Collection and Analysis to Understand Adversarial Cyber Capabilities, Plans and Intentions, and to Enable Counterstrategies.
4. Build and Maintain World-Class Cyber Offensive Capabilities (with appropriate authorities).
5. Enhance Defenses to Protect Against Low and Mid-Tier Threats.
6. Change DoD's Culture Regarding Cyber and Cyber Security.
7. Build a Cyber Resilient Force.

55. Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, CA: The RAND Corporation, 2009, p. 5. For a review of this book, see Jeffrey L. Caton, "Book Reviews: Cyberdeterrence and Cyberwar," *Strategic Studies Quarterly*, Vol. 5, No. 1, Spring 2011, pp. 148-150, available from <https://www.airuniversity.af.mil/SSQ/Display/Article/1063480/volume-05-issue-1-spring-2011/>, accessed October 13, 2017.

56. Libicki, p. 27.

57. *Ibid.*, p. xvi.

58. *Ibid.*, p. 39. The nine questions that Libicki explored to "differentiate cyberdeterrence from nuclear deterrence or general military deterrence" are:

[Critical questions:]

- Do we know who did it [attacked us]?
- Can we hold their assets at risk?
- Can we do so repeatedly?

[Ancillary questions:]

- If retaliation does not deter, can it at least disarm?
- Will third parties join the fight?
- Does retaliation send the right message to our own side?
- Do we have a threshold for response?
- Can we avoid escalation?
- What if the attacker has little worth hitting?

59. Matthew Rivera, "Deterrence in Cyberspace," Master of Science thesis, Hampton, VA: Joint Advanced Warfighting School, Joint Forces Staff College, June 2012, pp. 1, 6-14, available from <https://apps.dtic.mil/dtic/tr/fulltext/u2/a562428.pdf>, accessed December 7, 2018.

60. *Ibid.*, pp. 61-62.

61. *Ibid.*, p. 56.

62. Clorinda Trujillo, "The Limits of Cyberspace Deterrence," *Joint Force Quarterly*, Vol. 75, 4th Qtr., 2014, pp. 43-52, available from http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-75/jfq-75_43-52_Trujillo.pdf, accessed August 21, 2017. This essay won the Strategic Research Paper category of the 2014 Chairman of the Joint Chiefs of Staff Strategic Essay Competition. The author summarizes their review of existing policy as:

Based on this existing policy and doctrine and additional scholarly efforts, proposed cyberspace deterrent options include:

- develop policy and legal procedures
- develop other credible response options [which include offensive cyberspace actions]
- pursue partnerships
- secure cyberspace
- enhance resiliency
- strengthen defense
- conduct cyberspace deception. (p. 47)

63. *Ibid.*, pp. 47-49.

64. *Ibid.*, p. 49.

65. Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Force Quarterly*, Vol. 77, 2nd Qtr., 2015, pp. 8-15, available from http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_8-15_Denning.pdf, accessed September 28, 2017.

66. *Ibid.*, p. 10.

67. *Ibid.*, pp. 10-11.

68. *Ibid.*, p. 11.

69. *Ibid.*, pp. 12-15.

70. Joseph S. Nye, Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Vol. 5, No. 4, Winter 2011, pp. 18-35. The lessons put forth by Nye can be summarized as:

Some General Lessons. . . . Expect continuing technological change to complicate early efforts at strategy. . . . Strategy for a new technology will lack adequate empirical content. . . . New technologies raise new issues in civil-military relations. . . . Civilian uses will complicate effective national security strategies [emphasis in original]. (pp. 23-27)

International Cooperation Lessons. . . . Learning can lead to concurrence in beliefs without cooperation. . . . Learning is often lumpy and discontinuous. . . . Learning occurs at different rates in different issues of a new domain. . . . Deterrence is complex and involves more than just retaliation. . . . Begin arms control with positive-sum games related to third parties [emphasis in original]. (pp. 29-34)

71. *Ibid.*, p. 36.

72. Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3, Winter 2016/17, pp. 44-71. Nye defines entanglement as "the existence of various interdependences that make a successful attack simultaneously impose serious costs on the attacker as well as the victim." (p. 58)

73. *Ibid.*, p. 60.

74. *Ibid.*, p. 61.

75. *Ibid.*, p. 63. Although it may not be a recognized norm, Nye notes that "cyberattacks may be used for political signaling as well as physical destruction and disruption." (p. 49)

76. *Ibid.*, pp. 67-68. Note that Nye considers resilience to be a part of denial. (p. 56)

77. *Ibid.*, p. 70.

78. *Ibid.*, p. 71. Nye closes the article with practical advice for cyber deterrence planners:

Not all cyberattacks are of equal importance; not all can be deterred; and not all rise to the level of significant national security threats. The lesson for policymakers is to focus on the most important attacks and to understand the full range of mechanisms and contexts in which they can be prevented.

79. Joint Chiefs of Staff, JP 3-12 (R), *Cyberspace Operations*, Washington, DC: Joint Chiefs of Staff, original release February 5, 2013, updated as unclassified public document on October 21, 2014. Key definitions of joint cyberspace missions are:

defensive cyberspace operations [DCO]. Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems [emphasis in original]. (p. GL-4)

[Defensive Cyberspace Operations] Internal Defensive Measures [DCO-IDM]. Internal defensive measures are those DCO that are conducted within the DODIN [Department of Defense information network]. They include actively hunting for advanced internal threats as well as the internal responses to these threats. Internal defensive measures respond to unauthorized activity or alerts/threat information within the DODIN, and leverage intelligence, . . . [counterintelligence, law enforcement], . . . and other military capabilities as required [emphasis in original]. (p. II-3)

defensive cyberspace operation response action [DCO-RA]. Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense [DoD] cyberspace capabilities or other designated systems [emphasis in original]. (p. GL-4)

Department of Defense information network [DODIN] **operations**. Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense [DoD] networks to create and preserve information assurance on the Department of Defense information networks [emphasis in original]. (p. GL-4)

offensive cyberspace operations [OCO]. Cyberspace operations intended to project power by the application of force in or through cyberspace [emphasis in original]. (p. GL-4)

80. See John B. Morrison, Jr., "Foreword," in Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations*, Washington, DC: Headquarters, Department of Army, April 11, 2017, available from https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM%203-12%20FINAL%20WEB%201.pdf, accessed August 8, 2017, hereafter, FM 3-12.

81. FM 3-12, pp. 1-9-1-10, 1-25-1-31.

82. *Ibid.*, pp. 1-25, 1-34-1-35.

83. *Ibid.*, pp. 3-10-3-13.

84. *Ibid.*, pp. C-1-D-2. FM 3-12 appendix C provides an example of the cyber effects request format and appendix D provides an example of the electronic attack request format.

85. See the mission statement in "U.S. Army Cyber Command: The Nation's Army in Cyberspace," trifold, Fort Gordon, GA: U.S. Army Cyber Command, February 8, 2018, available from <http://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/1435502/us-army-cyber-command/>, accessed August 23, 2018.

86. U.S. Army Cyber Command (ARCYBER), "Ground-breaking marks 'leap forward' for Army cyberspace operations," U.S. Army, December 1, 2016, available from https://www.army.mil/article/178917/groundbreaking_marks_leap_forward_for_army_cyberspace_operations, accessed August 30, 2017. ARCYBER headquarters is currently split-based at Fort Belvoir, Virginia, Fort Meade, Maryland, and Fort Gordon, Georgia.

87. "Statement by Lieutenant General Edward C. Cardon, Commanding General, U.S. Army Cyber Command and Second Army before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, Operationalizing Cyberspace for the Services," 1st Sess., 114th Congress, March 4, 2015, p. 2, available from <https://docs.house.gov/>

meetings/AS/AS26/20150304/103093/HHRG-114-AS26-Wstate-CardonE-20150304.pdf, accessed September 13, 2017.

88. See more information at the official website, NETCOM. Army.Mil: U.S. Army Network Enterprise Technology Command, available from <http://netcom.army.mil/>, accessed August 22, 2017.

89. "Our Mission," 1st Information Operations Command, n.d., available from <http://www.1stiocmd.army.mil/Home/Mission>, accessed September 4, 2017.

90. Benjamin Leitzel and Anthony Allard, eds., *Strategic Cyberspace Operations Guide*, Carlisle, PA: Center for Strategic Leadership, U.S. Army War College, June 1, 2016, p. 120, available from <https://csl.armywarcollege.edu/usacsl/Publications/StrategicCyberspaceOperationsGuide2016.pdf>, accessed September 2, 2017.

91. "Welcome: Mission," 780th Military Intelligence Brigade, available from <https://www.inscom.army.mil/msc/780mib/>, accessed September 4, 2017.

92. FM 3-12, p. 3-3. ARCYBER RCCs are described as:

The regional cyber center is the single point of contact for operational status, service provisioning, incident response, and all Army network services in its assigned theater. It coordinates directly with tactical units to provide DODIN-A services, support to DODIN operations, and when required DCO to enable mission command and the warfighting functions.

93. "Statement by LTG Paul M. Nakasone, Commanding General, U.S. Army Cyber Command before the Subcommittee on Cybersecurity Committee on Armed Services, U.S. Army Cyber Posture," U.S. Senate, 1st Sess., 115th Congress, May 23, 2017, pp. 2, 12, available from <https://www.armed-services.senate.gov/download/?id=A19E0B4E-9DA3-4A42-8DFD-CED899D34851&download=1>, accessed August 15, 2017.

94. See the fact sheet, "U.S. Cyber Command (USCYBERCOM)," Official website of U.S. Strategic Command, September 30, 2016, available from <https://web.archive.org/web/20170925100958/http://www.stratcom.mil/media/factsheets/>

factsheet-view/article/960492/us-cyber-command-uscycbercom/, accessed August 23, 2018.

95. "Statement by LTG Paul M. Nakasone," pp. 2, 7.

96. "All Cyber Mission Force Teams Achieve Initial Operating Capability," news release, Fort Meade, MD: U.S. Cyber Command, October 24, 2016, available from <https://dod.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/>, accessed August 22, 2017. The responsibilities of the other three Joint Force Headquarters-Cyber (JFHQ-C) are divided amongst the other cyber Service component commands as follows: JFHQ-C Marine Forces Cyberspace Command: U.S. Special Operations Command; JFHQ-C Fleet Cyber Command: U.S. Pacific Command and U.S. Southern Command; and JFHQ-C Air Forces Cyber: U.S. European Command, U.S. Strategic Command, and U.S. Transportation Command.

97. Image modified from FM 3-12, p. vi.

98. FM 3-12, pp. 1-2, 1-5.

99. "Hearing to Receive Testimony On U.S. Strategic Command and U.S. Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2014 and the Future Years Defense Program," U.S. Senate, Committee on Armed Services, 113th Congress, Sess. 1, Washington, DC: U.S. Government Printing Office, March 12, 2013, pp. 8-9, available from <https://armed-services.senate.gov/imo/media/doc/13-09%20-%203-12-13.pdf>, accessed October 8, 2017. With regard to the offensive stance of some cyber combat mission teams, General Alexander stressed:

I would like to be clear that this team, this defend the Nation team, is not a defensive team; this is an offensive team that the Defense Department would use to defend the Nation if it were attacked in cyber space. 13 of the teams that we are creating are for that mission set alone. We're also creating 27 teams that would support combatant commands and their planning process for offensive cyber capabilities. Then we have a series of teams that would defend our networks in cyber space. Those three sets of teams are the core construct for what we're working with and the services to develop our cyber cadre.

100. *Defense Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened*, report GAO-17-512, Washington, DC: U.S. Government Accountability Office, August 2017, available from <http://gao.gov/assets/690/686347.pdf>, accessed August 22, 2017. Figure 1 of *Defense Cybersecurity* provides an organizational chart of the various cyber mission force (CMF) teams within the USCYBERCOM and DoD organizational and command structure.

101. DOJOC, p. 29.

102. *Ibid.*, p. 38. Although cyberspace operations are not mentioned explicitly in the discussion of active and passive defenses, cyberspace and electromagnetic activities (CEMA) efforts can provide significant support to net-centric force operational tenets as addressed below:

The increasingly net-centric joint force of the 21st Century will capitalize on passive defense achieved through widely dispersed forces. While still able to achieve operational objectives through their ability to more efficiently communicate, maneuver, and share a common operating picture, net-centric forces will present a less lucrative target for an adversary's WMD. However, because adversaries are more likely to use weapons capable of wide area effects (e.g., Electromagnetic Pulse . . .) to attempt asymmetric defeat of technologically superior US forces, improved weapons-effects hardening/survivability will be required for a broader range of joint force systems than required today. Effective interoperability, robustness, and functional redundancy between joint force units (particularly in the areas of ISR [intelligence, surveillance, and reconnaissance] and C2) will reduce the potential for single points of failure within complex systems and organizations, and ensure that critical C2 capabilities degrade gracefully. Information assurance for net-centric forces will ensure only trusted data are shared among users.

103. *Ibid.*, pp. 39-40.

104. Deterrence means are those prescribed in DOJOC, pp. 28-44.

105. DSB, *Resilient Military Systems*, p. 43. The report addresses the challenges with providing cyber resiliency to a specific set of conventional strike forces that directly support U.S. strategic deterrence efforts:

Furthermore, cyber resiliency can only be achieved by segmenting and isolating forces from general purpose forces. In the absence of a cyber threat, segmented forces are likely to possess slightly less capability than their non-segmented counterparts due to the isolation from every part of the supporting infrastructure which generates so much advantage to DoD. However, in the face of an adversary employing cyber, the segmented forces will provide far more capability than their non-segmented counterparts.

106. U.S. Joint Forces Command, *Major Combat Operations Joint Operating Concept*, Ver. 2.0, Washington, DC: Department of Defense, December 2006, p. 43, available from http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_combatops.pdf?ver=2017-12-28-162012-383, accessed October 1, 2017. This joint operating concept clearly identifies deterrence as an intimate part of conflict operations:

A critical element of deterrence is maintaining capable and rapidly deployable military forces and, when necessary, demonstrating the will to resolve conflicts decisively on favorable terms. This will require forces to operate in and from the global commons (space, international waters and airspace, and cyberspace) and effectively project and sustain forces in distant environments where adversaries may seek to deny us access. (p. 6)

107. *Mad Scientist: The 2050 Cyber Army Technical Report*, Joint Base Langley-Eustis, VA: U.S. Army Training and Doctrine Command G2, November 7, 2016, p. 25, available from <http://info.publicintelligence.net/USArmy-TRADOC-Cyber2050.pdf>, accessed October 8, 2016.

108. *The Department of Defense Cyber Strategy*, p. 14. The fourth strategic goal is described as:

During heightened tensions or outright hostilities, DoD must be able to provide the President with a wide range of options for managing conflict escalation. If directed,

DoD should be able to use cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities. As a part of the full range of tools available to the United States, DoD must develop viable cyber options and integrate those options into Departmental plans. DoD will develop cyber capabilities to achieve key security objectives with precision, and to minimize loss of life and destruction of property. To ensure unity of effort, DoD will enable combatant commands to plan and synchronize cyber operations with kinetic operations across all domains of military operations.

109. *Ibid.*, p. 26.

110. James Blackwell, "Deterrence at the Operational Level of War," *Strategic Studies Quarterly*, Vol. 5, No. 2, Summer 2011, pp. 30-51. The Ten Axioms for Campaign Planners listed below are addressed in:

Go to School on Deterrence and Nuclear Doctrine. . . .
Apply Deterrence in Each Phase of the Campaign. . . .
Do No Harm to the Stability of Central Strategic Deterrence. . . .
Understand the Limits of Conventional Deterrence. . . .
Plan for Operations on a Nuclear Battlefield. . . . Assess
the Credibility of Deterrence. . . . Beware the Potential for
Cascading Effects. . . . Leverage the Cognitive Domain of
War. . . . Do Not Assume Opponents without Fear Cannot Be
Deterred. . . . Develop Innovative Tactical and Operational
Forms. (pp. 36-49)

111. Jeffrey L. Caton, *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, January 2015, pp. 37-53.

112. This image is modified from "Figure 9. Modified Kahn Escalation Ladder," in Jeffrey L. Caton, *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, January 2015, p. 38.

113. *Ibid.*, p. 45. This figure is modified from "Figure 10. Relation of ACD to the Dynamics of Conflict and Escalation."

114. DSB, *Task Force on Cyber Deterrence*, p. 6.

115. DSB, *Resilient Military Systems*, p. 33. Recommendation number 2 of the report reads, "Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary."

116. DSB, *Task Force on Cyber Deterrence*, p. 17. In discussion of the report principle to "Create a Second-Strike Cyber Resilient 'Thin Line' Element of U.S. Military Forces," the integration of cyberspace, conventional, and nuclear strike is presented as:

DoD must therefore devote urgent and sustained attention to boosting the cyber resilience of key U.S. strike systems (cyber, nuclear, non-nuclear) – including essential supporting forces and critical infrastructure to ensure we maintain credible response capabilities. **Without such measures, the United States will not be able to effectively deter the most sophisticated large-scale cyber attacks. . . . 2.1 Establish a Highly Cyber Secure/Resilient 'Thin Line' of Strategic Offensive Cyber, Nuclear, and Non-Nuclear Long-Range Strike Capability. . . . Scalable military strike capabilities – including offensive cyber, non-nuclear long-range strike, and nuclear systems – are the foundation of U.S. deterrence by cost-imposition. These strike capabilities will be targeted by major powers' cyber (and other) programs, and must both be resilient and perceived as such. For these systems, a perception of vulnerability is dangerous and destabilizing [emphasis in original].** (pp. 17-18)

117. DOJOC, pp. 39-42.

Improving our capability to integrate nuclear and non-nuclear strike operations should further enhance these [advanced conventional kinetic and non-kinetic] capabilities. Providing the President an enhanced range of options for both limiting collateral damage and denying adversaries sanctuary from attack will increase the credibility of US nuclear threats, thus enhancing deterrence and making the actual use of nuclear weapons less likely. (p. 40)

118. *Ibid.*, pp. 41-42. In the discussion of using Global Strike to encourage adversary constraint, the document notes that:

In many cases where the adversary is convinced that the cost of aggression or coercion will be a response using nuclear Global Strike, other considerations tend to pale in comparison. However, when an adversary perceives truly severe consequences of restraint, and doubts US willingness to use nuclear weapons, deterrence could fail despite our nuclear capabilities. (p. 42)

119. FM 3-12, p. iv.

120. *The Department of Defense Cyber Strategy*, pp. 25-26. The cited task falls under “Strategic Goal III: Be Prepared to Defend the U.S. Homeland and U.S. Vital Interests from Disruptive or Destructive Cyberattacks of Significant Consequence.” The text of the task is:

Assess DoD’s cyber deterrence posture and strategy.

Building off of the Defense Science Board’s [DSB] Task Force on Cyber Deterrence, U.S. Strategic Command (USSTRATCOM), in coordination with the Joint Staff and the Office of the Secretary of Defense, will assess the Department of Defense’s [DoD] ability to deter specific state and non-state actors from conducting cyberattacks of significant consequence on the U.S. homeland and against U.S. interests, to include loss of life, significant destruction of property, or significant impact on U.S. foreign and economic policy interests [emphasis in original].

121. *Ibid.*, p. 26.

122. DSB, *Task Force on Cyber Deterrence*, pp. 9-13. The report offers guidance for developing tailored deterrence campaigns:

The U.S. cyber deterrence posture must be ‘tailored’ to cope with the range of potential attacks that could be conducted by each potential adversary. And it must do so in contexts ranging from peacetime to ‘gray zone’ conflicts to crisis to war. Clearly, for U.S. cyber deterrence (as with deterrence more broadly), one size will not fit all.

Conducting detailed advance planning for responses to every plausible cyber attack, with every potential adversary in every conceivable scenario, is neither possible nor necessary. Nor is it feasible to have in hand the ‘optimal’ response

to each hypothetical attack scenario. However, it is both possible and essential to conduct systematic planning and wargaming, to establish clear employment and declaratory policies, and to establish priorities for the development of a range of potential cyber and non-cyber (and military and non-military) responses to cyber attacks. (p. 9)

123. *The Department of Defense Cyber Strategy*, p. 10. A comprehensive U.S. cyber deterrence strategy should address:

As DoD builds its Cyber Mission Force [CMF] and overall capabilities, DoD assumes that the deterrence of cyberattacks on U.S. interests will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems. The deterrence of state and non-state groups in cyberspace will thus require the focused attention of multiple U.S. government departments and agencies. The Department of Defense [DoD] has a number of specific roles to play in this equation.

124. "Stenographic Transcript, Foreign Cyber Threats," January 5, 2017, p. 23.

125. Kevin R. Beeker, "Strategic Deterrence in Cyberspace: Practical Application," Graduate Research Project, No. AFIT/ICW/ENG/09-01, Wright-Patterson Air Force Base, OH: Air Force Institute of Technology, June 2009, pp. 18-20, available from <http://www.dtic.mil/dtic/tr/fulltext/u2/a502250.pdf>, accessed September 29, 2017.

APPENDIX I

See table I-I for a description of the specific cyberspace actions of U.S. Army Cyberspace and Electromagnetic Activities (CEMA) and table I-II for descriptions of Army CEMA electronic warfare actions. Figure I-I depicts the cyberspace and electronic warfare operations relationship with the joint cyberspace missions.

Cyberspace Actions	Description
Cyberspace Defense	Cyberspace defense are actions normally taken within the DOD [Department of Defense] cyberspace for securing, operating, and defending the DODIN [Department of Defense information network] against specific threats. The purpose of cyberspace defense includes actions to protect, detect, characterize, counter, and mitigate threats. (p. 1-9)
Cyberspace Operational Preparation of the Environment (OPE)	Cyberspace OPE consists of the non-intelligence enabling activities for the purpose of planning and preparing for ensuing military operations. Cyberspace OPE requires forces trained to a standard that prevents compromise of related intelligence collection operations. (p. 1-10)
Cyberspace Security	Cyberspace security actions are those taken within a protected network to prevent unauthorized access to, an exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Cyberspace security activities include vulnerability assessment and analysis, vulnerability management, incident handling, continuous monitoring, and detection and restoration capabilities to shield and preserve information and information systems. (p. 1-10)
Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR)	Cyberspace ISR is an intelligence action conducted by the . . . [joint force commander] authorized by an execute order or conducted by attached signals intelligence . . . units under temporary delegated . . . [signals intelligence] operational tasking authority. Cyberspace ISR includes activities in cyberspace conducted to gather intelligence required to support future OCO [offensive cyberspace operations] or DCO [defensive cyberspace operations]. These activities support planning and execution of current and future cyberspace operations. (p. 1-9)
Cyberspace Attack	Cyberspace attack is a cyberspace action that creates various direct denial effects in cyberspace (for example, degradation, disruption, or destruction) and manipulation that leads to denial, that is hidden or that manifests in the physical domains. The purpose of cyberspace attack is the projection of power to provide an advantage in cyberspace or the physical domains for friendly forces. (p. 1-10)

Table I-I. Army CEMA Cyberspace Actions¹

Electronic Warfare Actions	Description
Electronic Protection	
<p>[Electronic protection] involves actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the . . . [electromagnetic spectrum] that degrade, neutralize, or destroy friendly combat capability. For example, . . . [electronic protection] includes actions taken to ensure friendly use of the . . . [electromagnetic spectrum], such as frequency agility in a radio or variable pulse repetition frequency in radar. Commanders should avoid confusing . . . [electronic protection] with self-protection. Both defensive . . . [electronic attack and electronic protection] protect personnel, facilities, capabilities, and equipment. However, . . . [electronic protection] protects from the effects of . . . [electronic attack] (friendly and enemy) and electromagnetic interference, while defensive . . . [electronic attack] primarily protects against lethal attacks by denying enemy use of the . . . [electromagnetic spectrum] to guide or trigger weapons. (p. 1-28)</p>	
Electromagnetic compatibility	The ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response. (p. 1-29)
Electromagnetic hardening	Action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and and/or shielding against undesirable effects of electromagnetic energy. (p. 1-29)
Electromagnetic spectrum management	Planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures. (p. 1-29)
Electronic masking	The controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electronic warfare support measures . . . [signals intelligence] without significantly degrading the operation of friendly systems. (p. 1-29)
Emission control	The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. mutual interference among friendly systems; and/or c. enemy interference with the ability to execute a military deception plan. (pp. 1-29-1-30)

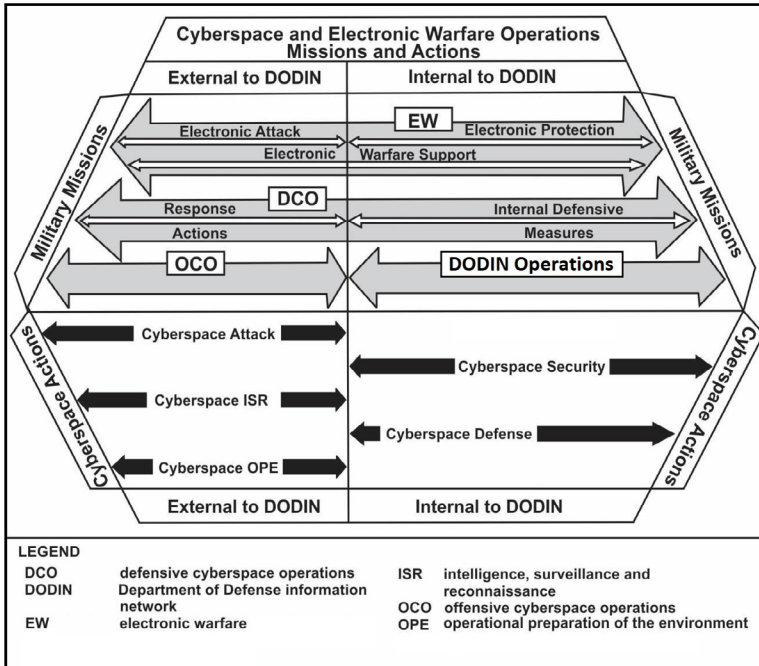
Table I-II. Army CEMA Electronic Warfare Actions²

Electronic Warfare Actions	Description
Wartime reserve modes	Characteristics and operating procedures of sensors, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. (p. 1-30)
Electronic Attack [Electronic attack] involves the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. . . . [Electronic attack] includes – <ul style="list-style-type: none"> • Actions taken to prevent or reduce an enemy’s effective use of the . . . [electromagnetic spectrum]. • Employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism. • Offensive and defensive activities, including countermeasures. (p. 1-26) 	
Countermeasures	Form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (p. 1-27)
Electromagnetic deception	Electromagnetic deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy’s combat capability. (p. 1-27)
Electromagnetic intrusion	Intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. (p. 1-28)
Electromagnetic jamming	The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy’s effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy’s combat capability. (p. 1-28)

**Table I-II. Army CEMA Electronic Warfare Actions
(cont.)**

Electronic Warfare Actions	Description
Electronic probing	Intentional radiation designed to be introduced into the devices or systems of potential enemies for the purpose of learning the functions and operational capabilities of the devices or systems. (p. 1-28)
Electromagnetic pulse	The electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges. (p. 1-28)
Electronic Warfare Support	
[Electronic warfare support] involves actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. . . . [Electronic warfare support] enables U.S. forces to identify the electromagnetic vulnerability of an enemy's or adversary's electronic equipment and systems. Friendly forces take advantage of these vulnerabilities through EW [electronic warfare] operations. (p. 1-30)	
Electronic Intelligence	Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (p. 1-30)
Electronic Reconnaissance	The detection, location, identification, and evaluation of foreign electromagnetic radiations. (p. 1-30)
Electronics Security	The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations, e.g., radar. (p. 1-31)
Spectrum Management Operations (SMO)	
Spectrum management is the operational, engineering, and administrative procedures to plan, coordinate, and manage use of the electromagnetic spectrum and enables cyberspace, signal and EW operations. Spectrum management includes frequency management, host nation coordination, and joint spectrum interference resolution. Spectrum management enables spectrum-dependent capabilities and systems to function as designed without causing or suffering unacceptable electromagnetic interference. Spectrum management provides the framework to utilize the electromagnetic spectrum in the most effective and efficient manner through policy and procedure. (p. 1-34)	

**Table I-II. Army CEMA Electronic Warfare Actions
(cont.)**



Source: U.S. Army.

Figure I-I. Army Cyberspace and Electronic Warfare Operations – Missions and Actions³

ENDNOTES - APPENDIX I

1. Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations*, Washington, DC: Headquarters, Department of Army, April 11, 2017, pp. 1-9-1-10, available from https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM%203-12%20FINAL%20WEB%201.pdf, accessed August 8, 2017, hereafter, FM 3-12.

2. FM 3-12, pp. 1-25-1-34.

3. Image modified from FM 3-12, p. 1-6.

U.S. ARMY WAR COLLEGE

**Major General John S. Kem
Commandant**

**STRATEGIC STUDIES INSTITUTE
AND
U.S. ARMY WAR COLLEGE PRESS**

**Director
Professor Douglas C. Lovelace, Jr.**

**Director of Research
Dr. Steven K. Metz**

**Author
Jeffrey L. Caton**

**Editor for Production
Dr. James G. Pierce**

**Publications Assistant
Ms. Denise J. Kersting**

**Composition
Mrs. Jennifer E. Nevil**



U.S. ARMY



FOR THIS AND OTHER PUBLICATIONS, VISIT US AT
<https://www.armywarcollege.edu/>

ISBN 1-58487-798-7



9

9 0000 >



This Publication



SSI Website



USAWC Website