US Army War College
USAWC Press

Monographs, Books, & Publications

11-2-2017

# Evaluation of the 2015 DoD Cyber Strategy: Mild Progress in a Complex and Dynamic Military Domain

Jeffrey L. Caton

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

Recommended Citation
Jeffrey L. Caton, *Evaluation of the 2015 DoD Cyber Strategy: Mild Progress in a Complex and Dynamic Military Domain* ( US Army War College Press, 2017),
https://press.armywarcollege.edu/monographs/402

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.

UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH and WISDOM

# EVALUATION OF THE 2015 DOD CYBER STRATEGY: MILD PROGRESS IN A COMPLEX AND DYNAMIC MILITARY DOMAIN

Jeffrey L. Caton

U.S. ARMY WAR COLLEGE
SSI
STRATEGIC STUDIES INSTITUTE

# 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.

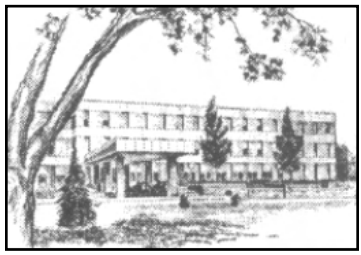
The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

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**

# EVALUATION OF THE 2015 DOD CYBER STRATEGY: MILD PROGRESS IN A COMPLEX AND DYNAMIC MILITARY DOMAIN

**Jeffrey L. Caton**

**November 2017**

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 17013-5010.

*****

This manuscript was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, *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: *ssi.armywarcollege.edu*.

*****

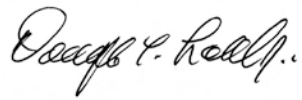
The Strategic Studies Institute and U.S. Army War College Press publishes a quarterly email newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic 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: *ssi.armywarcollege.edu /newsletter/*.

ISBN 1-58487-773-1

## FOREWORD

Cyberspace may be the ultimate dual-edged sword—the bright hope of its great intellectual and communicative potential is in contrast to its dark reality to enable havoc and destruction. In April 2015, then-Secretary of Defense Ashton Carter unveiled his department's new guidance on how the U.S. military should address the myriad challenges emerging in the cyberspace domain to a group of technology-savvy leaders gathered at Stanford University. The 2015 *Department of Defense (DoD) Cyber Strategy* builds upon the foundation of a 2011 strategy and stays true to its three primary missions, as well as overarching national security strategies—but can the new strategy work?

In this monograph, Mr. Jeffrey Caton explores various aspects of this question by examining the historical context, traditional strategy elements, subsequent DoD action, and whole-of-government approach contained within the 2015 *DoD Cyber Strategy*. He argues that positive assessments of the strategy's suitability, feasibility, and acceptability for implementation may be predicated upon the vagueness of the strategy's overarching intent. Further, he contends that the strategy is hampered by its own lack of clear end state, prioritization of efforts, and full context of the cyberspace realm writ large. Fortunately, Mr. Caton also provides recommendations for future cyberspace-related defense strategies in hope of improving their effectiveness.



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 2007-2012, Mr. Caton served on the U.S. Army War College (USAWC) faculty, including Associate Professor of Cyberspace Operations and Defense Transformation Chair. Over the past 7 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 on the nexus of cyberspace, space, and landpower doctrine issues 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 including command 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

In 2011, the Department of Defense (DoD) released its *Strategy for Operating in Cyberspace*, which officially recognized cyberspace as an operational domain akin to the traditional military domains of land, sea, air, and space. This monograph examines the 2015 *DoD Cyber Strategy* to evaluate how well its five strategic goals and associated implementation objectives define an actionable strategy to achieve three primary missions in cyberspace: defend the DoD network, defend the United States and its interests, and develop cyber capabilities to support military operations.

The topic of U.S. Federal cyberspace activities is well-documented in many sources, thus this monograph serves as a primer to provide senior policymakers, decision makers, military leaders, and their respective staffs with an overall appreciation for the complexities, challenges, opportunities, and risks associated with the development of military cyberspace operations. This report is limited to unclassified and open source information; any classified discussion must occur at another venue.

This monograph focuses on events and documents from the period of about 1 year before and 1 year after the 2015 strategy was released. This allows sufficient time to examine the key policies and guidance that influenced the development of the strategy, as well as follow-on activities for the impacts from the strategy. This inquiry has five major sections that utilize different frameworks of analysis to assess the strategy:

1. Prima Facie Analysis: This section is by intention only a superficial overview of the strategy. It explores the strategy and its public face as presented by DoD and addresses: What is the

stated purpose of the strategy? What are its content and key messages?

2. Historical Context Analysis: The official roots of the DoD cyber strategy go back more than a decade, and this section reviews the document's contents within the context of other key historical national defense guidance. The section focuses on two questions: Is this strategy consistent with previous strategies and current policies? What unique contributions does it introduce into the evolution of national security cyberspace activities?
3. Traditional Strategy Analysis: This section evaluates eight specific premises for good strategies that include the familiar elements of ends, ways, means, and risk. It also addresses three questions: Does the strategy properly address specific DoD needs as well as broader U.S. ends? Is the strategy appropriate and actionable? How may joint combatant commanders view the strategy?
4. Analysis of Subsequent DoD Action: This section explores the DoD cyber strategy's connections and influences to DoD guidance that followed its release. It will focus on two questions: How are major military cyberspace components—joint and Service—planning to implement the goals and objectives of the DoD cyber strategy? What plans has the Army put in place to support the strategy?
5. Whole of U.S. Government Analysis: This section examines DoD cyber activities from the perspective of a whole-of-government approach to national cybersecurity. This analysis focuses on two questions: Does the strategy support U.S.

Executive direction? Does the strategy integrate with other the cyberspace-related activities of other U.S. Government departments and agencies?

This monograph concludes with a section that integrates the individual section findings and offers recommendations to improve future cyberspace strategic planning documents.

## EVALUATION OF THE 2015 DOD CYBER STRATEGY: MILD PROGRESS IN A COMPLEX AND DYNAMIC MILITARY DOMAIN

In April 2015, the Department of Defense (DoD) released its second official cyberspace strategy to update the 2011 *Strategy for Operating in Cyberspace* and to present strategic goals and associated implementation objectives to achieve three primary missions in cyberspace: defend the DoD network, defend the United States and its interests, and develop cyber capabilities to support military operations. This monograph assesses the value of the new strategy utilizing five different frameworks of analysis: prima facie; historical context; traditional strategy elements; subsequent DoD action; and whole-of-government approach. This monograph focuses on events and documents from the timeframe of about 1 year before and 1 year after the 2015 strategy was released. This allows sufficient time to examine the key policies and guidance that influenced the development of the strategy, as well as follow-on activities for the impacts from the strategy. This monograph serves as a primer to provide senior policymakers, decision makers, military leaders, and their respective staff with an overall appreciation for complexities, challenges, opportunities, and risks associated with the development of military cyberspace operations.

### PRIMA FACIE ANALYSIS

Before delving into a detailed technical exploration of the strategy, let us first examine it through the eyes of a reader from the general public who may be unfamiliar with its background. Clearly, former Secretary of Defense (SECDEF) Ashton Carter considered such

an audience important when he stated that the strategy is "also a reflection of DoD being more open than before" during his public unveiling of the document at Stanford University.[1] This section explores the strategy and its public face as presented by the DoD and addresses the stated purpose of the strategy and its content and key messages. This section is by intention only a superficial overview of the strategy. Subsequent sections will explore the broader context and assess implications.

**Purpose and Content**

The 2015 *DoD Cyber Strategy* opens with a letter from Carter that clearly establishes his personal stake in the document—"I am invested in the success of this strategy and I will hold the Department accountable for meeting each goal and objective."[2] The letter also explains why the strategy was developed:

> The purpose of this cyber strategy, the Department's second, is to guide the development of DoD's cyber forces and strengthen our cyber defense and cyber deterrence posture. It focuses on building cyber capabilities and organizations for DoD's three cyber missions: to defend DoD networks; defend the U.S. homeland and U.S. national interested against cyberattacks of significant consequences; and support operational and contingency plans.[3]

The strategy, available for download from the official DoD website, is a 33-page document that is structured into 5 self-apparent main sections: Introduction, Strategic Context, Strategic Goals, Implementation Objectives, and Managing the Strategy, plus Carter's Prologue and a short Conclusion. The Introduction and Implementation Objectives comprise the bulk of the document (20 pages), and there are numerous

redundancies throughout.[4] The objectives are organized by their appropriate strategic goal, but there is no clear priority or balance regarding how the content material is presented (see Appendix 1). Thus, one may suspect that the document had different authors for each subsection that were merged together rather than integrated. The resulting collage of ideas and initiatives appears to be trying to cover all the bases vice focusing on a prioritized approach of applying limited resources to a boundless challenge. While these criticisms seem a bit pedantic to informed readers, the shortfalls in writing structure and continuity unwittingly may serve to muddy the intended messages.

In addition to the full strategy document, the DoD also posted a two-page fact sheet that presumably presents the key messages that the department wanted to communicate to the public. The fact sheet spells out the three primary missions and strategic goals as well as seemingly random examples of objectives. (Appendix 1 indicates which objectives were selected.) It cites "three major drivers" for the new strategy: a more severe and sophisticated cyber threat; Presidential direction to defend against cyberattacks; and development of the Cyber Mission Force (CMF). Consistent with the full document, the fact sheet sets the scope for achieving the strategy as "the next 5 years and beyond." It also dedicates a paragraph each to other themes: "building bridges to the private sector and beyond" and "deterrence is a key part of DoD's new cyber strategy."[5] Indeed, these two topics receive significant coverage in the strategy, but it is not evident why they were singled out in the fact sheet.

## Actions, Images, and Words

On April 23, 2015, Carter introduced his new cyber strategy to the public as part of a lecture at Stanford University in Palo Alto, California.[6] The selection of this venue in Silicon Valley, close to leading-edge technology and far away from Washington, DC, appeared to be no accident. Carter's speech focused on the history of successful technology partnering between the DoD, the private sector, and research institutions; and in the last quarter of it, he segued to cyberspace-related topics culminating with the announcement of a new strategy. His focus appeared to be tailored to the audience with many references to teamwork and cooperation, and asserted, "we have a unique opportunity to build bridges and rebuild bridges and renew trust."[7] Citing a previously undisclosed Russian intrusion into DoD networks, Carter made good on his claim in his strategy prologue to "seek to be open and transparent with the American people and the world about our capabilities and plans."[8]

To support the launch of the strategy, the DoD established a "Special Report" website that used links and images to state the purpose of the strategy clearly, as well as the three DoD primary cyber missions and CMF concept. The website also provided links to the document and fact sheet as well as links to the public websites of U.S. Cyber Command (USCYBERCOM), Army Cyber Command, U.S. Fleet Cyber Command, and Air Forces Cyber/24th Air Force. Perhaps most importantly, under a picture of the strategy's cover, the website conveyed a clear civil-military chain of command using pictures and statements of then-President Barack Obama, SECDEF Carter, and Commander, USCYBERCOM, Admiral Michael Rogers.[9]

Missing from the chain was the commander, U.S. Strategic Command; this inconsistency is discussed later in this monograph.

The strategy includes 18 images spread roughly evenly throughout the document. Twelve of these are photographs with captions and source credit, and the other six are uncredited pictures that serve as background for section titles. A cursory review of these graphics reveal that they focus almost exclusively on themes related to the first and third primary missions as well as the first and second strategic goals. (See Appendix 2 for details.) The subjects of homeland defense, deterrence operations, and international partnerships are given short shrift in the visual communication realm of the strategy. An interesting artifact is that 50 percent of the captioned images are credited to U.S. Air Force (USAF) sources, and two of the section headings depict USAF cyberspace operations centers. From this, the uninformed reader may reasonably assume that the USAF is conducting the preponderance of DoD cyberspace operations.

The strategy's attempt to include external linkages to some of its key themes was patchy in places. It did a good job at identifying the explicit decision-making roles of the President of the United States (POTUS) and the SECDEF as well as references to the 2015 *National Security Strategy* (NSS) (still under development at the time) and the 2014 *Quadrennial Defense Review* (QDR). It also introduces the position of the Principal Cyber Advisor to the SECDEF established by the National Defense Authorization Act of 2014. However, it provided only two passing mentions of the 2011 *Department of Defense Strategy for Operating in Cyberspace*, neither of which provides an uninformed reader with any significant background of what the DoD had been

doing in cyberspace prior to April 2015.[10] Despite the focus on deterrence and the CMF, the strategy makes no mention of the development or practice of military doctrine or theory.[11]

### Summary

To a casual reader, the 2015 *DoD Cyber Strategy* starts off with a clear purpose and strong endorsement statement from Carter. Thereafter, the DoD's primary missions and strategic goals are stated explicitly, but the presentation of the context and implementation objectives is somewhat muddled with few specific details. The document's visual communication through captioned photographs provides little support for three of the five strategic goals. The document's conclusion devolves to a statement that offers no priorities and very little material that is unique to the cyber domain.

## HISTORICAL CONTEXT ANALYSIS

To understand better the content of the 2015 *DoD Cyber Strategy*, it is important to appreciate what has preceded it. The document infers that it is only the second DoD strategy related to cyberspace, thus only having a history back to 2011. However, the official roots of this strategy go back more than a decade and this section reviews the document's contents within the context of other key historical national defense documents. This section focuses on two questions: Is this strategy consistent with previous strategies and current policies? What unique contributions does it introduce into the evolution of national security cyberspace activities?

## Comparison to Previous Cyberspace Strategies

In his publication, *An Assessment of the Department of Defense Strategy for Operating in Cyberspace*, Dr. Thomas Chen provides an excellent summary of the evolution of cyberspace strategies from the 2003 Bush administration's *National Strategy to Secure Cyberspace*, through the 2006 *National Military Strategy for Cyberspace Operations*, and up to the 2011 *DoD Strategy for Operating in Cyberspace*. Based on this historical background, he then assesses each of the five strategic initiatives in the 2011 cyber strategy in terms of their significance and novelty as well as their practicality.[12]

Rather than repeat Chen's methodology, let us examine his observations and recommendations for their relevance to the new strategy. Table 1 lists verbatim, the strategic initiatives from the 2011 DoD cyberspace strategy with the strategic goals of the 2015 *DoD Cyber Strategy*. Several of Chen's observations regarding the 2011 strategy remain valid in the 2015 version: a focus on technology, resources, and cooperation; an emphasis on defense and prevention; and, mostly repeated themes with no surprises or controversies.[13] In fact, one could argue that all of the 2011 strategic initiatives provide the foundation for four of the 2015 strategic goals: initiatives 1 and 5 for goal I; initiative 2 for goal II; initiative 3 for goal III; and initiative 4 for goal V. The remaining 2015 goal, IV, addresses new material to the public DoD cyber dialogue that is addressed later in this section.

| *DoD Strategy for Operating in Cyberspace* (July 2011) Strategic Initiatives [14] | *The DoD Cyber Strategy* (April 2015) Strategic Goals [15] |
|---|---|
| 1. Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential. | I. Build and maintain ready forces and capabilities to conduct cyberspace operations. |
| 2. Employ new defense operating concepts to protect DoD networks and systems. | II. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions. |
| 3. Partner with other U.S. Government departments and agencies as well as the private sector to enable a whole-of-government cybersecurity strategy. | III. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence. |
| 4. Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity. | IV. Build and maintain viable cyber options and plans to use those options to control conflict escalation and to shape the conflict environment at all stages. |
| 5. Leverages the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation. | V. Build and maintain robust alliances and partnerships to deter shared threats and increase international security and stability. |

**Table 1. Comparison of Themes of DoD Cyberspace Strategies from 2011 and 2015.**

The 2015 strategy did make progress in five areas critiqued by Chen.[16] First, he noted that the 2011 strategy did not distinguish between types of adversaries, where the 2015 strategy discusses cyber threats in terms of state, nonstate, and criminal actors as well as combinations of the three.[17] However, the new strategy still does not offer specific initiatives to address these different adversaries.

Chen also noted that the 2011 strategy did not address offense, attribution, and implementation metrics. In the 2015 strategy, there is an explicit mention of U.S. offensive cyber capability, but no amplifying details are included.[18] On the other hand, the subject of attribution is discussed in great detail as a partnership between the DoD and the intelligence community with contributions from the private sector.[19] The new strategy names specific countries that have threatened the United States as well, and they will be addressed later. The 2015 strategy calls for the DoD to "propose, collect, and report a set of appropriate metrics to the Principle Cyber Advisor to measure the operational capacity of the CMF."[20]

A final area of progress for the 2015 strategy addresses Chen's observation that the 2011 strategy lacks discussion on the "rules for proper response to cyber attacks."[21] Part of the 2015 strategic goal IV requires the DoD to "accelerate the integration of cyber requirements into plans," and these plans "must outline and define specific cyberspace effects against targets."[22] More importantly, the new strategy also provides the philosophical unpinning that promulgates the lawful performance of cyberspace activities:

> To ensure that the Internet remains open, secure, and prosperous, the United States will always conduct

> cyber operations under a doctrine of restraint, as required to protect human lives and to prevent the destruction of property. As in other domains of operations, in cyberspace the Defense Department will always act in a way that reflects enduring U.S. values, including support for the rule of law, as well as respect and protection of the freedom of expression and privacy, the free flow of information, commerce, and ideas. Any decision to conduct cyber operations outside of DoD networks is made with the utmost care and deliberation and under strict policy and operational oversight, and in accordance with the law of armed conflict. As it makes its investments and builds cyber capabilities to defend U.S. national interests, the Defense Department will always be attentive to the potential impact of defense policies on state and non-state actors' behavior.[23]

## Ties to Current National Guidance

The 2015 *DoD Cyber Strategy* claims the "all of the goals and objectives within this strategy reflect the goals of the 2015 *United States National Security Strategy* [NSS] and the 2014 *Quadrennial Defense Review* [QDR]." An examination of the cyber-related excerpts from these documents validates this assertion in general terms, as illustrated with examples in Table 2 (see Appendix 3 for all relevant excerpts). Each of these purposeful documents dedicated a standalone paragraph to cyberspace issues: "Cybersecurity" in the NSS[24] and "Cyber" in the QDR.[25]

| *The DoD Cyber Strategy* (April 2015) Strategic Goals [26] | Supporting Excerpts from the 2015 NSS and the 2014 QDR [27] |
|---|---|
| I. Build and maintain ready forces and capabilities to conduct cyberspace operations. | NSS (p. 8):<br><br>We will protect our investment in foundational capabilities like the nuclear deterrent, and we will grow our investment in crucial capabilities like cyber; space; and intelligence, surveillance, and reconnaissance [ISR].<br><br>QDR (p. 33):<br><br>The Department of Defense will continue to invest in new and expanded cyber capabilities, building on significant progress made in recent years in recruiting, training, and retaining cyber personnel. A centerpiece of our efforts is the development of the Department of Defense Cyber Mission Force. |

**Table 2. Examples of Supporting Material for the 2015 DoD Cyberspace Strategy from Current National Security Documents.**

| | |
|---|---|
| II. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions. | NSS (p. 3):<br>We are fortifying our critical infrastructure against all hazards, especially cyber espionage and attack.<br>QDR (pp. 14-15):<br>We must be able to defend the integrity of our own networks, protect our key systems and networks, conduct effective cyber operations overseas when directed, and defend the Nation from an imminent, destructive cyberattack on vital U.S. interests. |
| III. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence. | NSS (p. 12):<br>Drawing on the voluntary cybersecurity framework, we are securing federal networks and working with the private sector, civil society, and other stakeholders to strengthen the security and resilience of U.S. critical infrastructure.<br>QDR (p. 15):<br>We support the Federal Government cybersecurity team and will continue working with the Department of Homeland Security (DHS) to improve critical infrastructure cybersecurity, and with DHS and the Federal Bureau of Investigation to support law enforcement activities. |

**Table 2. Examples of Supporting Material for the 2015 DoD Cyberspace Strategy from Current National Security Documents. (cont.)**

| | |
|---|---|
| IV. Build and maintain viable cyber options and plans to use those options to control conflict escalation and to shape the conflict environment at all stages. | NSS (p. 13):<br><br>We will defend ourselves, consistent with U.S. and international law, against cyber attacks and impose costs on malicious cyber actors, including through prosecution of illegal cyber activity.<br><br>QDR (p. 14):<br><br>The Department of Defense will deter, and when approved by the President and directed by the Secretary of Defense, will disrupt and deny adversary cyberspace operations that threaten U.S. interests. |
| V. Build and maintain robust alliances and partnerships to deter shared threats and increase international security and stability. | NSS (p. ii):<br><br>We are shaping global standards for cybersecurity and building international capacity to disrupt and investigate cyber threats.<br><br>QDR (p. 15):<br><br>Deterring and defeating cyber threats requires a strong, multi-stakeholder coalition that enables the lawful application of the authorities, responsibilities, and capabilities resident across the U.S. Government, industry, and international allies and partners. |

**Table 2. Examples of Supporting Material for the 2015 DoD Cyberspace Strategy from Current National Security Documents. (cont.)**

A new version of the *National Military Strategy* (NMS) followed the new cyber strategy about 2 months later. Surprisingly, cyberspace activities received relatively little emphasis. While the NMS did pick up the questionable party line regarding the North Korean hack of Sony Picture Cyberspace, cyberspace activities were not included as one of the 12 "Joint Force Prioritized Missions."[28] Further, the NMS did not dedicate a paragraph to cyberspace issues, and the text did not have any hint of linkage to the third primary mission in cyberspace (see Appendix 3 for all relevant excerpts). Simply put, the 2015 NMS presented military cyberspace activities as a step backward in the priority from the 2014 QDR and 2015 NSS.

A major theme missing from the 2015 *DoD Cyber Strategy* is the DoD Defense Innovation Initiative, more commonly referred to as the Third Offset Strategy.[29] The absence of this term is peculiar since Carter mentioned the concept of an offset strategy as part of his speech introducing the new cyber strategy.[30] Also, Deputy Secretary of Defense Bob Work clearly identified investment in cyber capabilities as an integral part of the Third Offset Strategy during a public speech in January 2015.[31] Inclusion of the Defense Innovation Initiative as part of the implementation objectives would strengthen significantly the linkage of the cyber strategy's strategic goal I to the larger DoD priorities.

**Summary**

The 2015 *DoD Cyber Strategy* does not contain any significant historical context regarding actions and accomplishments since the 2011 strategy. In fact, the 2015 strategy's five strategic goals remain largely unchanged from the 2011 strategy's five Strategic

Initiatives. Fortunately, the 2015 strategy's content is grounded firmly in guidance from the President via the 2015 NSS as well as from the SECDEF via the 2014 QDR. However, unlike the QDR and NSS, the 2015 NMS released shortly after the cyber strategy did not contain any unique content regarding cyberspace and did not list it among the prioritized joint missions. The cyber strategy appears to stay true to its 5-year scope of vision and does not discuss either any anticipated dynamics or changes of the cyberspace domain beyond 2020.

## TRADITIONAL STRATEGY ANALYSIS

Having established a basic understanding of the basic structure and historical context of the 2015 *DoD Cyber Strategy*, we will now evaluate it using traditional criteria for U.S. military strategy. The model for our analysis is that utilized by the U.S. Army War College (USAWC) that focuses on eight specific premises for good strategies that include the familiar elements of ends, ways, means, and risk. This section addresses three questions: Does the strategy properly address specific DoD needs as well as broader U.S. ends? Is the strategy appropriate and actionable? How may joint combatant commanders view the strategy?

### Grading the Strategy

There is no magic formula or standardized yardstick to determine the virtues of a given strategy. We will adopt a framework for our analysis that has decades of successful application in the USAWC curriculum. This model defines strategy as "the employment of the instruments (elements) of power (political/diplomatic, economic, military, and informational) to

achieve the political objectives of the state in cooperation or in competition with other actors pursuing their own objectives."[32] The model asserts that an effective strategy will achieve eight premises in its content and character: proactive and anticipatory; clear end state; appropriate balance of ends-ways-means; political purpose dominates; hierarchical; comprehensive in context; knowledge and analysis of environment; and consideration of risk as potential for failure.[33] Table 3 provides a visual summary of whether the 2015 *DoD Cyber Strategy* achieved, partially achieved, or failed to achieve each of these eight premises. Discussion to support each of these asserted evaluations follows.

| Strategy Premise | Not Achieved | Partially Achieved | Achieved |
|---|---|---|---|
| ➢ Proactive & anticipatory | | ◑ | |
| ➢ Clear end state | ○ | | |
| ➢ Balance as an integrated whole | | ◑ | |
| ➢ Political purpose dominate | | | ● |
| ➢ Hierarchical | | | ● |
| ➢ Comprehensive in context | | ◑ | |
| ➢ Knowledge & analysis of environment | | ◑ | |
| ➢ Consider risk as potential for failure | | ◑ | |

**Table 3. Evaluation of Strategy Premises.**

*Proactive and Anticipatory?*

Score: Partially achieved. While strategic goal IV does call for the integration of cyber options into plans to support the proactive role of shaping the conflict environment, the strategy provides little details

except that this integration needs to be accelerated. Otherwise, most of the objectives center on establishing and monitoring defensive perimeters around the DoD networks and establishing partnerships that should already exist. While some progress is being made, the rate of growth of strategy maturation is far less than rate of growth of cyberspace. The Internet population alone has grown by almost a billion users—about a 43 percent increase—since the 2011 *DoD Cyber Strategy* was released.[34]

*Clear End State?*

Score: Not Achieved. As discussed previously, the 2015 strategy provides excellent linkage to national security objectives as well as the U.S. goals and interests related to cyberspace. However, there is no clear end state expressed in the document's introduction or conclusion, and the sum of the five strategic goals does not equal an end state. The failure to achieve this critical element of communication is demonstrated by the overall weak language related to cyberspace in follow-on 2015 *National Military Strategy*.

*Appropriate Balance as an Integrated Whole?*

Score: Partially achieved. Although the strategy does not use the terminology of the ends-ways-means model in its text, it does address each of these elements conceptually. Table 4 provides examples of content in the 2015 *DoD Cyber Strategy* that support the model. This material is presented with no discussion on how they will be prioritized or integrated across the strategy writ large to assess potential gaps between "what is to be achieved and the concepts and resources available to achieve the objective."[35]

| | |
|---|---|
| **Ends**<br>***What is being accomplished?*** | • Three primary DoD missions in cyberspace.<br>• U.S. vital interests in cyberspace.<br>• U.S. core values. |
| **Ways**<br>***How is it being accomplished?*** | • Implement five strategic goals.<br>• Integrated and synchronized operations.<br>• Deterrence and doctrine of constraint. |
| **Means**<br>***What resources are being used?*** | • Cyber Mission Force.<br>• Joint Information Environment.<br>• Joint Force Headquarters for DoD information operations (JFHQ-DODIN). |

**Table 4. Examples of Ends, Ways, and Means in the 2015 *DoD Cyber Strategy*.**

The element of ends—what is being accomplished by the strategy—is addressed by the three primary DoD missions in cyberspace as well as by some of the national interests that they ultimately serve. Vital U.S. interests in cyberspace include "an open, secure, interoperable, and reliable Internet that enables prosperity, public safety, and the free flow of commerce and ideas."[36] According to the strategy, these interests "reflect core American values—of freedom of expression and privacy, creativity, opportunity, and innovation."[37]

The element of ways—how the strategy is being accomplished—includes processes described by the

five strategic goals. These processes emphasize the cyberspace operations that are integrated and synchronized with joint planning and operations working to form "the larger multi-mission U.S. military force to achieve synergy across domains."[38] In the subsequent DoD support for this notion, cyberspace operations receive significant attention in the 2016 joint staff planner's guide for cross-domain operations.[39] The strategy also emphasizes the incorporation of cyberspace operations into U.S. deterrence activities that include components of response, denial, and resiliency.[40] Finally, when the strategy calls for the judicious use of military cyberspace it means:

> to ensure that the Internet remains open, secure, and prosperous, the United States will always conduct cyber operations under a doctrine of restraint, as required to protect human lives and to prevent the destruction of property.[41]

The element of means—what resources are being used for the strategy—emphasizes personnel and infrastructure. The CMF is the linchpin for future DoD operations in cyberspace. The force is organized into 133 teams developed and trained for 4 task areas: defense of the network; national defense; combatant commander support; or general cyberspace support.[42] The strategy stresses that the success of the CMF depends on its ability to work with members of joint, interagency, international, and private sector teams. Although the strategy did address Joint Force Headquarters-DoD Information Networks (JFHQ-DODIN), it failed to mention the other three joint force headquarters designated to support specific combatant commands.[43] The infrastructure backbone for many DoD cyberspace operations will utilize the Joint Information Environ-

ment single security architecture which is designed to "enable a robust network defense and shift the focus from protecting service-specific networks and systems to securing the DoD enterprise in a unified manner."[44] To help coordinate the implementation of resources and program management for the DoD cyberspace activities, the strategy acknowledges the congressionally-directed requirement to establish the new position of Principal Cyber Advisor to the SECDEF.[45]

*Does Political Purpose Dominate?*

Score: Achieved. The strategy does an excellent job in establishing the U.S. constitutional tenet mandating the primacy of civilian control of military operations. The prelude to the introduction of the three primary missions in cyberspace captures this concept eloquently:

> The President has established principles and processes for governing cyber operations. The purpose of these principles and processes is to plan, develop, and use U.S. capabilities effectively, and to ensure that cyber operations occur in a manner consistent with the values that the United States promotes domestically and internationally.[46]

Further, the strategy also states that the President and SECDEF will direct the assessment of significant cyberattacks, the conduct of military cyberspace operations, and the delivery of public statements regarding cyberspace designed to enhance U.S. deterrence.[47]

*Is It Hierarchical – Does It Cascade from National Level Down?*

Score: Achieved. The last section's analysis of the strategy's linkage to national security documents revealed that the three primary DoD cyberspace missions and all the 2015 *DoD Cyber Strategy* strategic goals have traceable foundations to the 2014 QDR and 2015 NSS. Also, the strategy clearly decrees policy alignment with presidential guidance:

> Consistent with presidential guidance, DoD will align and simplify its cyber operations and cybersecurity policy management and identified gaps, overlaps, seams, conflicts, and areas in need of revision in current documentation.[48]

*Is It Comprehensive in Consideration of Context?*

Score: Partially achieved. The strategy does include a four-page section, "Strategic Context," that describes key cyber threats, malware proliferation, risk to DoD networks and infrastructure, and deterrence as well as an introduction that explains U.S. cybersecurity activities, DoD cyberspace missions, and the cyber mission force.[49] However, these discussions do not mention critical DoD stakeholders in cyberspace, such as the National Security Agency (NSA) and the Defense Information Systems Agency (DISA). There is no background provided to portray how the domain of cyberspace itself has changed since 2011—that is, the changes in its size in terms of users, devices, servers, data transfer rates, global memory capacities, and so forth. Perhaps of more concern is the dearth of material regarding the theory or doctrine of cyberspace operations.

*Thorough Analysis and Knowledge of the Strategic Situation/Environment?*

Score: Partially achieved. In its section on Implementation Objectives, the strategy does discuss many internal and external factors that influence and have an impact on the strategic goals. However, it falls short of providing the specific examples, quantitative trends, and demographics necessary to analyze properly the magnitudes and directions of such influences. To its credit, the strategy forgoes the tired "cyber Pearl Harbor" admonishment. However, it only provides one explicit account of a cyberattack—the 2014 hack of Sony Picture attributed to North Korea and described as "one of the most destructive cyberattacks on a U.S. entity to date."[50] Perhaps the characterization of this example is a bit melodramatic in light of the costly compromises by Edward Snowden, the systematic theft of U.S. intellectual property by China, or even the mysterious Russian intrusion into the DoD networks revealed by Carter at the launch of the 2015 *DoD Cyber Strategy*.[51]

*Consider Risk as Potential for Strategy to Fail?*

Score: Partially achieved. The strategy is replete with references to risks from outside forces and entities that threaten cyberspace infrastructure and operations. Furthermore, the strategy proposes that "to mitigate these and other risks and improve U.S. national security, this strategy sets strategic goals for the Department to achieve, and prescribes objectives and metrics for meeting each goal."[52] This methodology of risk mitigation is presented in a piecemeal manner throughout the Implementation Objective, but risk is not discussed

at the enterprise level of the overall strategy. That is, the strategy does not explain how it will prioritize and balance its ends, ways, and means best to reduce the risk of failure.

**Summary**

The 2015 *DoD Cyber Strategy* addressed most of the premises of traditional military strategy to some degree, but failed to provide the most important element--a clear end state. This deficiency stifles any prioritization of effort and allows some of the goals and objectives to be interpreted or manipulated to suit or appease the purposes of many audiences. The strategy does an excellent job at stressing its subjugation to higher U.S. civilian authorities and their guidance. This strict adherence may hamper the strategy's ability to be proactive and anticipatory, thus making it a cautious and comfortable work at times that merely repeats the party line.

While the complexities of military cyberspace operations make it difficult for *The DoD Cyber Strategy* to provide a comprehensive context in a concise document, there should at least be some discussion of the theory and doctrine that form the foundation of these operations; this was not the case. The strategy did not fully describe the existing domain of cyberspace, and it did not analyze what changes may occur to its size and structure over the next 5 years.

While *The DoD Cyber Strategy* did include some general concepts that support an ends-ways-means paradigm, it did not provide any specific information that made it actionable. This dearth of detail on basic U.S. military cyberspace command and control structures diminishes its value to combatant commanders and their staffs.

## ANALYSIS OF SUBSEQUENT DOD ACTION

Having examined the contents of the 2015 *DoD Cyber Strategy* and its linkages to national security planning documents that preceded it, we now explore the strategy's connections and influences to DoD guidance that followed its release. This section will focus on two questions: How are major military cyberspace components—joint and Service—planning to implement the goals and objectives of *The DoD Cyber Strategy*? What plans has the Army put in place to support the strategy?

### USCYBERCOM Implementation

Less than 2 months after the release of the 2015 *DoD Cyber Strategy*, Admiral Rogers, Commander, USCYBERCOM, issued his vision and guidance document, *Beyond the Build: Delivering Outcomes through Cyberspace*.[53] Although his introductory letter directly ties this guidance to the DoD strategy, the content that follows is disappointing for anyone seeking details beyond generic slogans. Its central themes—"motivated by mission; powered by partnerships; oriented toward outcomes—we have a global mission that matters and an opportunity to serve our nation every day"[54]—offer nothing unique to the command or DoD cyberspace activities. The product does mention several key topics not found in the DoD strategy—ties to the NSA and the DISA, development of doctrine, and the fact that cyberspace is not a static domain in its size. It also includes a hierarchy of missions, imperatives, and enablers as summarized in Figure 1. Yet, these artifacts lack the practicality, priority, and precise language to yield any actionable guidance. One must ask, if the word "cyber" and "cyberspace" were removed from

Figure 1, could the remaining verbiage apply to any DoD organization?[55]

**Figure 1. Summary of Themes from The Commander's Vision and Guidance for U.S. Cyber Command (June 2015).[56]**

A more credible and actionable communique from Rogers is his congressional testimony in April 2016, a 1-year update of his USCYBERCOM vision.[57] While the threat landscape of named adversaries remained the same, other cyberspace incidents besides the Sony hack were presented—the theft of the personal infor-

mation of over 21 million Americans via compromised computers at the Office of Personnel Management, as well as the December 2015 cyberattack on Ukraine's power grid.[58] With regard to the means necessary to fulfill USCYBERCOM missions, Rogers noted that his command received a $466 million budget for FY 2016 and that the CMF development stood at 123 of 133 teams formed. He noted progress in several areas critical to CMF operations: training, sustainment, capabilities, innovation, and culture. He acknowledged the role that Third Offset Strategy would play in his command:

> USCYBERCOM stands ready to help develop and deploy the new cyber capabilities entailed in the Third Offset, particularly hardened command and control networks and autonomous countermeasures to cyber attacks.

He also expressed his gratitude for being granted limited authority by the National Defense Authorization Act of 2016 as a Command Acquisition Executive.[59] Ideally, this will improve the speed and agility of procuring capabilities for the command.

**Derivative Strategic Planning Documents**

Two significant DoD initiatives followed the 2015 *DoD Cyber Strategy* to address resource management issues of improving the integrity of the network infrastructure and personnel operating on it. First, the DoD Cybersecurity Discipline Implementation Plan was developed in October 2015 to help achieve *The DoD Cyber Strategy* Strategic Goal II (defend the DoD information network). Its stated purpose is "to mitigate risks and operationalize cyber readiness reporting for the information systems they own, manage, or lease

for mission assurance through DRRS [Defense Readiness Reporting System]."[60] The implementation plan is a very actionable document and includes appendices that codify priorities, sequence of tasks, and traceability of the plan's requirements with overarching DoD cybersecurity requirements.[61] Second, the DoD Cybersecurity Culture and Compliance Initiative (DC3I) was directed by Chairman of the Joint Chiefs of Staff, General Martin Dempsey and SECDEF Carter in September 2015 to "transform DoD cybersecurity culture by improving individual human performance and accountability in mutual support of *The DoD Cyber Strategy*."[62] It also supports Strategic Goal II by establishing five operational excellence principles—Integrity, Level of Knowledge, Procedural Compliance, Formality and Backup, and a Questioning Attitude—to be inculcated across the DoD cyber enterprise. The DC3I identifies four distinct groups within the enterprise—leaders, provider, cyber warriors, and users—and 11 short-term tasks to make the initiative actionable.[63]

In his April 2016 congressional testimony, Rogers noted that "USCYBERCOM comprises a headquarters organization and seven components: the Cyber National Mission Force, the Joint Force Headquarters-DoD Information Networks, plus joint force headquarters and growing forces," which are part of the individual Service cyber commands as well as that of the Coast Guard.[64] Each of these USCYBERCOM components has published strategy-planning documents with mostly implicit linkage to the 2015 *DoD Cyber Strategy*. The titles of these documents are summarized in Table 5 with excerpts that describe the purpose or focus of the work. The reader should note that these documents are available on official public websites, and thus some of these papers may not be under the

direct purview of the component. While it is beyond the scope of this monograph to analyze these works in detail, it is apparent from a cursory review that the focus of the documents aligns with existing organizational and Service cultures and what they can contribute to joint operations. While many of them include strategic goals, none of them had direct reference to the strategic goals of the DoD strategy.

| USCYBERCOM Component Affected | Strategic Planning Document |
|---|---|
| Cyber National Mission Force | *DoD Cyberspace Workforce Strategy* (December 2013):<br><br>This document is the Department's strategy for transforming its cyberspace workforce of military (active/reserve) and civilian personnel and includes approaches to recruit, train, and retain staff in a competitive national environment. Additionally, many of the principles and tenets within this document will hold true for the contract services supporting the Department's cyberspace workforce personnel. Successful execution of this cyberspace workforce strategy requires coordinated action across the Department, the Office of Personnel Management (OPM), agencies, industry partners, and academia, while keeping Congress informed.[65] |

**Table 5. Derivative Strategic Planning Documents.**

| | |
|---|---|
| Joint Force Headquarters-DoD Information Networks | Defense Information Systems Agency Strategic Plan 2015-2020 (June 2015):<br>We will continue to lead the DoD cyberspace and information technology optimization efforts. This includes eliminating Department duplication of effort, capitalizing on the range of commercial cloud solutions, and maintaining the operational cyberspace integrity of the DoDIN services we defend, operate, and assure. Our agile enterprise will emphasize on-demand, real-time, 24x7, secure access and availability.<br>Over the next several months, DISA will:<br>• Evolve the JFHQ-DODIN<br>• Deploy and operationalize the Joint Regional Security Stacks (JRSS) platform<br>• Continue to implement our reorganization<br>• Maintain our superior delivery of capability to our mission partners<br>• Enhance mobility and collaboration capabilities.[66] |

**Table 5. Derivative Strategic Planning Documents. (cont.)**

| | |
|---|---|
| Army Cyber/Second Army | *Army Network Campaign Plan: 2020 & Beyond* (February 2015):<br><br>This campaign plan supports mission readiness by providing the vision and direction that set conditions for and lay a path to *Network 2020 and Beyond*, thereby unifying efforts to provide a modern network that meets the Army's warfighting and business needs, today and tomorrow.<br><br>The network envisioned spans all Army operations, from administrative operations in garrison to the most forward-deployed soldier at the tactical edge. Army users expect to access the network securely at the point of need—and that the network will deliver. For this reason, the network must be highly responsive, providing the information necessary to execute decisive actions anytime, anywhere and on any device. It also must enable command posts to be mobile, agile, modular, scalable and survivable in support of continuous mission command to win in the complex world in which the Army operates.[67] |

**Table 5. Derivative Strategic Planning Documents. (cont.)**

| | |
|---|---|
| Marine Forces Cyberspace | Marine Corps Concept for Cyberspace Operations (October 2015):<br><br>Addresses the cyberspace capabilities the Marine Corps will need to support missions as part of a joint force and meet requirements of the combatant commanders. It stresses that commanders must integrate cyberspace capabilities into the operational plans across the warfighting functions and domains, and shows that integration and synchronization of cyberspace and electromagnetic spectrum operations will be critical to mission success.[68] |
| Fleet Cyber Command/Tenth Fleet | *U.S. Fleet Cyber Command/TENTH Fleet Strategic Plan 2015-2020* (May 2015):<br><br>This strategic plan emphasizes the warfighting aspects of this command—both offensive and defensive—while still recognizing the significant ways in which other warfighters rely on our effectiveness in the confluence of cyberspace, the electromagnetic spectrum, and space.[69] |

**Table 5. Derivative Strategic Planning Documents. (cont.)**

| | |
|---|---|
| Air Forces Cyber/24th Air Force | *Air Force Information Dominance Flight Plan: The Way Forward for Cyberspace IT in the United States Air Force (May 2015):*<br><br>Aligns the strategies and objectives of the Air Force and DoD, to include the *DoD Cyber Strategy* and the Air Force's Strategic Master Plan (SMP). This plan refocuses our Cyber workforce on executing, enhancing, and supporting Air Force core missions. This change in focus is critical as it strengthens our understanding of how cyberspace/ Information Technology (IT) capabilities contribute to overall DoD operations and encourages the rapid development and integration of Air Force IT/cyberspace capabilities in support of joint warfighters and in the face of real and dangerous cyber threats to our core missions.[70] |

**Table 5. Derivative Strategic Planning Documents. (cont.)**

| | |
|---|---|
| U.S. Coast Guard Cyber | *U.S. Coast Guard Cyber Strategy* (June 2015):<br><br>To operate effectively within the cyber domain, and to counter and protect against maritime cyber threats over the next decade, the Coast Guard's Cyber Strategy emphasizes three strategic priorities: Defending Cyberspace, Enabling Operations, and Protecting Infrastructure.<br><br>This Strategy provides a framework for the Coast Guard's efforts in the cyber domain over the next 10 years, which will be essential to ensuring our Nation's security and prosperity in the maritime environment. This framework will enable success across all Coast Guard mission areas and will support all aspects of our "Prevent-Respond" core operational concept. It is aligned with current governing Executive directives, policies, and laws, including . . . the *DoD Cyber Strategy of 2015*.[71] |

**Table 5. Derivative Strategic Planning Documents. (cont.)**

The Army has published several cyberspace-planning documents that address not only the 5-year scope of the DoD strategy but also ones that look decades into the future.[72] In an article addressing the 2015 *DoD Cyber Strategy*, Lieutenant General Robert Ferrell, Army Chief Information Officer/G-6 (CIO/G-6), noted that the Army's role in implementing the strategy requires a coordinated team effort within the department:

> To shape acquisition and resourcing strategies and to help build next generation cyber capabilities, our Army

> team has a partnership between the U.S. Army Cyber Command/Second Army, HQDA G-2, HQDA G/3-5-7, the Assistant Secretary of the Army for Acquisition, Logistics and Technology, the Program Executive Offices and the CIO/G6. This enhanced partnership will help provide our forces flexible options to shape and dominate the cyberspace domain.[73]

As identified in Table 5, the *Army Network Campaign Plan* sets the stage by defining lines of effort to achieve network end states. This foundation plan is augmented by more detailed implementation guidance documents that distinguish primary and supporting efforts and define priority activities for near-term (2016-2017)[74] and mid-term (2018-2022).[75]

In March 2016, the CIO/G-6 released *Shaping the Army Network: 2025-2040* to provide the long-term strategic direction with six focus areas: dynamic transport; computing and edge sensors; data to decisive action; human cognition enhancement; robotics and autonomous operations; and cybersecurity and resiliency.[76] These focus areas represent a more holistic view of possible future operations in and through cyberspace. To help make the guidance actionable, the document includes a matrix to indicate its alignment with joint capability areas. It also provides a summary chart that identifies the ends-ways-means strategy to support the envisioned mission command network.[77] Other critical supporting strategies include the *Army Cloud Computing Strategy* (March 2015)[78] and the *Army Data Strategy* (February 2016)[79] as well as the *U.S. Army Cyber Center of Excellence Strategic Plan* (September 2015), which addresses how the center will lead efforts to "develop concepts, doctrine, requirements, integrate cyberspace operations and train Soldiers and leaders."[80]

## Summary

All major components of USCYBERCOM have released strategic planning products that complement the 2015 *DoD Cyber Strategy.* As may be expected, these documents often reflect Service-specific approaches, resources, and biases. The Army appears to have a good set of supporting strategies in place that include not only near-term guidance for Army cyber operations but also long-term guidance out to 2040. Unfortunately, the USCYBERCOM *Commander's Vision and Guidance* is heavy on jargon and light on actionable detail—it reads more like a marketing brochure than a serious work of strategic planning. The commander's testimonies before Congress provide much better insight into the current and future activities of USCYBERCOM.

## WHOLE OF U.S. GOVERNMENT ANALYSIS

The 2015 *DoD Cyber Strategy* avers that when conducting military cyberspace operations,

> the Defense Department cooperates with agencies of the U.S. Government with the private sector, and with our international partners to share information, build alliances and partnerships, and foster norms of responsible behavior to improve global strategic stability.[81]

This section examines this claim by analyzing the DoD's cyber activities from the perspective of a whole-of-government approach to national cybersecurity. This analysis focuses on two questions: Does the strategy support U.S. Executive direction? Does the strategy integrate with other cyberspace-related activities of other U.S. Government departments and agencies?

## Executive Direction

The Obama administration clearly advocated for a whole-of-government approach to U.S. national cybersecurity and put it at the top of its list of principles to employ to the cybersecurity challenge along with "network defense first . . . protection of privacy and civil liberties . . . public-private collaboration . . . [and] international cooperation and engagement."[82] Indeed, the 2015 *DoD Cyber Strategy* includes several references to these principles in its Strategic Context and Implementation Objectives chapters. Previous sections of this monograph explored how *The DoD Cyber Strategy* is linked to national security plans and strategies—documents that are more philosophical than directive. We now look at directives, laws, and implementation activities that require action from the DoD (and other parts of the U.S. Federal Government) to turn the various strategies into reality.

The Obama administration also listed five cybersecurity priorities in addition to its employment principles. Table 6 compares these priorities with the five strategic goals from the 2015 *DoD Cyber Strategy* and provides examples of recent Executive direction that affect DoD activities. There is excellent alignment between concepts in the presidential priorities and those in the DoD's cyber strategic goals, although their order of presentation is different. A review of the details in the examples of Executive direction reveals the common themes of interagency teamwork as well as partnership with private sector to coordinate cyber incident responses and implement data sharing.

| *The DoD Cyber Strategy* (April 2015) Strategic Goals[83] | Obama Administration Cybersecurity Priority [84] and Supporting Executive Direction |
|---|---|
| I. Build and maintain ready forces and capabilities to conduct cyberspace operations. | 5. Shaping a cyber-savvy workforce and moving beyond passwords in partnership with the private sector.<br>• Federal Cybersecurity Workforce Strategy (July 2016)<br>An OPM-led team recommended that NIST, DoD, and DHS convene to determine what actions are required for each work role with a specific interest on major talent gaps for both federal employees and contractor employees, in order to fully utilize the existing retention and talent development opportunities. Enterprise-wide workforce planning includes efforts to incorporate certifications and training opportunities so that cybersecurity professionals remain knowledgeable about emerging trends in their area(s) of responsibility, with these and other professional development opportunities serving as retention strategies.[85] |

**Table 6. Linkage of Presidential Direction to the 2015 *DoD Cyber Strategy*.**

| | |
|---|---|
| II. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions. | 4. Securing federal networks by setting clear security targets and holding agencies accountable for meeting those targets.<br>• Executive Order 13718 "Commission on Enhancing National Cybersecurity" (February 2016)<br>The Commission will make detailed recommendations to strengthen cybersecurity in both the public and private sectors while protecting privacy, ensuring public safety and economic and national security, fostering discovery and development of new technical solutions, and bolstering partnerships between federal, state, and local government and the private sector in the development, promotion, and use of cybersecurity technologies, policies, and best practices.[86]<br>• Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Government (October 2015)<br>Strengthening the cybersecurity of federal networks, systems and data is one of the most important challenges we face as a Nation. As a result, the Federal Government is bringing significant resources to bear to ensure cybersecurity remains a top priority. This includes strengthening government-wide processes for developing, implementing, and institutionalizing best practices; developing and retaining the cybersecurity workforce; and working with public and private sector research and development communities to leverage the best of existing, new, and emerging technology.[87] |

**Table 6. Linkage of Presidential Direction to the 2015 *DoD Cyber Strategy*. (cont.)**

| | |
|---|---|
| III. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence. | 1. Protecting the country's critical infrastructure—our most important information systems—from cyber threats.<br>• Executive Order 13691 "Promoting Private Sector Cybersecurity Information Sharing" (February 2015)<br>Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.[88]<br>• Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" (February 2013)<br>To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary [of Homeland Security], consistent with 6 U.S.C. 143 and in collaboration with the Secretary of Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.[89] |

**Table 6. Linkage of Presidential Direction to the 2015 *DoD Cyber Strategy*. (cont.)**

| | |
|---|---|
| IV. Build and maintain viable cyber options and plans to use those options to control conflict escalation and to shape the conflict environment at all stages. | 2. Improving our ability to identify and report cyber incidents so that we can respond in a timely manner.<br><br>• PPD-41 "United States Cyber Incident Coordination" (July 2016)<br><br>This Presidential Policy Directive (PPD) sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities. For significant cyber incidents, this PPD also establishes lead federal agencies and an architecture for coordinating the broader Federal Government response. It also requires the Departments of Justice and Homeland Security to maintain updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents to the proper authorities.[90]<br><br>• Executive Order 13694 "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (April 2015)<br><br>All property and interests in property that are in the United States . . . of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in . . . any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.[91] |

**Table 6. Linkage of Presidential Direction to the 2015 *DoD Cyber Strategy*. (cont.)**

| | |
|---|---|
| V. Build and maintain robust alliances and partnerships to deter shared threats and increase international security and stability. | 3. Engaging with international partners to promote internet freedom and build support for an open, interoperable, secure, and reliable cyberspace.<br>• Executive Order 13687 "Imposing Additional Sanctions with Respect to North Korea" (January 2015)<br>I, BARACK OBAMA, President of the United States of America, find that the provocative, destabilizing, and repressive actions and policies of the Government of North Korea, including its destructive, coercive cyber-related actions during November and December 2014, actions in violation of UNSCRs 1718, 1874, 2087, and 2094, and commission of serious human rights abuses, constitute a continuing threat to the national security, foreign policy, and economy of the United States, and hereby expand the scope of the national emergency declared in Executive Order 13466 of June 26, 2008, expanded in scope in Executive Order 13551 of August 30, 2010, and relied upon for additional steps in Executive Order 13570 of April 18, 2011.[92]<br>• International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (May 2011)<br>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.[93] |

**Table 6. Linkage of Presidential Direction to the 2015 *DoD Cyber Strategy*. (cont.)**

A comprehensive summary of cybersecurity–related legislative actions compiled by the Congressional Research Service noted, "despite many recommendations made over the past decade, most major legislative provisions relating to cybersecurity had been enacted prior to 2002."[94] This drought of congressional legislation ended within months of the 2015 *DoD Cyber Strategy* release as the 113th Congress passed five major bills in December 2014 and the 114th Congress passed a four-part cybersecurity division within the Consolidated Appropriations Act in December 2015.[95] Most of these laws emphasize interagency efforts to pursue national cybersecurity activities that include information sharing and voluntary inclusion of the private sector.

In concert with these numerous cybersecurity laws, President Obama initiated the Cybersecurity National Action Plan (CNAP) in February 2016 that includes near- and long-term activities:

> to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security.[96]

Specific CNAP actions include the establishment of a Commission of Enhancing National Cybersecurity (see Executive Order 13718 in Table 6) and two proposed budget increases for fiscal year (FY) 2017: $3.1 billion for an Information Technology Modernization Fund as part of an overall federal cybersecurity funding amount of $19 billion (over 35 percent more than FY 2016).[97] It is unclear if any of these increases will be allocated to the DoD's activities.

The 2015 *DoD Cyber Strategy* infers that federal budget trends may negatively impact strategy implementation:

> Although DoD has prioritized the allocation of resources in its budget to develop cyber capabilities, continued fiscal uncertainty requires that DoD plan to build its cyber capabilities under a declining overall defense budget.[98]

In fact, a congressional fact sheet on the FY 2016 National Defense Authorization Act asserts that the budget fully resources and authorizes USCYBERCOM, Service cyber commands, and cyber science and technology initiatives.[99] Further, the DoD budget request for FY 2017 included $6.7 billion for "strengthening cyber defenses and increasing options available in case of a cyber-attack."[100] The DoD Comptroller asserts that such funding is sufficient to execute the 2015 cyber strategy, support the CMF, and develop offensive cyber capabilities.[101]

**Interdepartmental and Interagency Efforts**

Coordination and interaction in support of cyberspace-related goals among federal agencies within the U.S. Government has occurred continuously for more than a decade. As stressed in the presidential direction, congressional acts, and the 2015 *DoD Cyber Strategy*, a significant portion of these activities center on the three key themes of cyber incident handling, information sharing, and private-public partnerships.

*Cyber Incident Handling*

The formal coordination of national cyber incidents goes back at least as far as 2010, when three important events occurred: the completion of a Memorandum of Agreement between the DoD and the DHS, which included the establishment of the National Cybersecurity and Communications Integration Center (NCCIC); the release of the interim version of the National Cyber Incident Response Plan (NCIRP); and the establishment of Cyber Storm exercises to test and refine NCIRP processes.[102] Although evolutionary progress was made over the intervening years, no new NCIRP was ever published.

On July 2016, Obama released Presidential Policy Directive 41 (PPD-41), "United States Cyber Incident Coordination."[103] This directive provides principles for handling incident response—which include unity of government effort—and the three concurrent lines of effort for response activities. The lines of effort are threat response activities led by the Department of Justice (DoJ)/Federal Bureau of Investigation (FBI); asset response activities led by DHS; and intelligence support and related activities led by the Office of the Director of National Intelligence (ODNI). PPD-41 differentiates between routine and significant cyber events, with the latter being the focus of Federal Government actions:

> While the vast majority of cyber incidents can be handled through existing policies, certain cyber incidents that have significant impacts on an entity, our national security, or the broader economy require a unique approach to response efforts. These significant cyber incidents demand unity of effort within the Federal Government and especially close coordination between the public and private sectors.[104]

The 2015 *DoD Cyber Strategy* also uses the notion of "cyberattacks of significant consequence" in its description of the second DoD mission.[105] When a significant cyber event has been identified officially, PPD-41 calls for a Cyber Unified Coordination Group (UCG) that:

> shall serve as the primary method for coordinating between and among federal agencies in response to a significant cyber incident as well as for integrating private sector partners into incident response efforts, as appropriate.[106]

Existing DoD cyber incident roles and responsibilities are codified in Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B (July 10, 2012), *Cyber Incident Handling Program*, a manual that "specifies its major processes, implementation requirements, and related U.S. Government interactions."[107] The manual includes several concepts found in PPD-41, such as the Cyber UCG (p. F-6) and work with DHS and other federal agencies under the role of Defense Support of Civil Authorities (DSCA) (p. A-5).[108] One challenge noted in the CJCSM is that the DoD and the DHS have different categorization systems for cyber incidents, although the goal is to agree to common definitions.[109]

Per PPD-41, the DoD will participate in the Cyber Response Group (CRG), which will "coordinate the development and implementation of the Federal Government's policies, strategies, and procedures for responding to significant cyber incidents" as well as resolve issues elevated to it by subordinate bodies (such as a Cyber UCG) and coordinate communications strategies for significant cyber incidents.[110] PPD-41 maintains the DoD as the sector-specific agency (SSA) for significant cyber incidents affecting the Defense

Industrial Base (DIB) as well as SECDEF as the federal lead "for managing the threat and asset response to cyber incidents affecting the DoD Information Network, including restoration activities, with support from other federal agencies as appropriate."[111]

For other agencies, PPD-41 calls for incorporation of cyber incident response into training and exercise programs by each SSA. It directs the DHS and DoJ to lead the SSAs to develop a new concept of operations that "shall further develop how the Cyber UCG and field elements of the federal coordination architecture will work in practice for significant cyber incidents."[112] This concept of operations should fulfill some of the requirements of the Cybersecurity Act of 2015.

Finally, PPD-41 directs the development of a new National Cyber Incident Response Plan lead by DHS with support from the Attorney General, SECDEF, and SSAs. The new response plan should satisfy requirements of National Cybersecurity Act of 2014.[113]

In practice, the DoD still has some work to do with its internal coordination of cyber incidents. In a report published 3 months before PPD-41, the Government Accountability Office (GAO) noted, "[the] DoD's guidance does not clearly define DSCA roles and responsibilities for domestic cyber incidents."[114] The official DoD response concurred with the GAO findings and agreed to update guidance to clarify the specific roles and responsibilities as well as command relationships necessary to provide DCSA support for significant cyber incident response.[115]

*Information Sharing*

In February 2013, two important documents were released by the White House that included provisions for enhanced information sharing to support national cyber security. The first was PPD-21, "Critical Infrastructure Security and Resilience," which included "Enable Efficient Information Exchange by Identifying Baseline Data and Systems Requirements for the Federal Government" as one of its three strategic imperatives.[116] This initiative expressed the value of sharing threat and vulnerability information internally amongst federal agencies as well as externally with private sector owners and operators of critical infrastructure.[117] The second document was Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," focused on:

> *Policy*. In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible [emphasis in original].[118]

Subsequent refinements to this information sharing process include the February 2015 presidential direction to form the Cyber Threat Intel Integration Center (CTIIC) to:

> serve as the national cyber threat intelligence center to 'connect the dots' within government regarding malicious foreign cyber threats to the nation so that relevant departments and agencies are aware of these threats in as close to real time as possible.[119]

Part of the CTIIC function will be to support "U.S. Cyber Command in its mission to defend the nation from significant attacks in cyberspace."[120] To satisfy the requirements of the Cybersecurity Information Sharing Act of 2015, a joint report authored by the DNI, DHS, DoD, and DoJ in February 2016 summarized the current mechanisms for sharing cyber threat information with both federal and non-federal entities. For the DoD, the report included the contributions of the voluntary DIB Cybersecurity Program as well as those of the DoD Defense Cyber Crime Center (DC3).[121] The report also highlighted the benefits of organizations such as Information Sharing and Analysis Centers (ISACs) established in 1998 to "help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards."[122]

Based on feedback from non-federal entities, the DHS and DoJ published updated guidance on sharing cyber threat indicators and defensive measures in June 2016.[123] The preferred method of information sharing is the DHS Automated Indicator Sharing (AIS) program that provides the capability that "enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed."[124]

*Public-Private Partnerships*

An official White House blog article chronicling cybersecurity successes of 2015 and challenges for 2016 highlighted the desire of the administration to partner with the private sector not only for information sharing, but also to achieve a national unity of effort for cybersecurity:

> Companies, organizations, and government agencies should be prepared to respond to and recover from incidents. . . . But just as we are dedicated to sharing appropriate information with the private sector to better defend against cyber threats, we also stand ready to provide assistance to the private sector. . . . In 2016, we will refine our policies and procedures to further strengthen our unity of effort response, whether it is helping a Federal agency or a private company.[125]

This concept of public-private partnerships is essential to both the cyber incident response and information sharing already discussed. The focus of the DoD's cyberspace-related efforts with the private sector is on the DIB, but it may be called upon to support other private sectors if directed.

An important organization for DoD cybersecurity activities with the DIB is the Damage Assessment Management Office (DAMO) which "works in close cooperation with the participating DIB companies to review and assess cyber incidents on their networks that involve DoD information."[126] Formed in 2008, the DAMO tracks the review of potential information compromises in the DIB and works with the DC3 to conduct damage assessments. The DoD Chief Information Officer manages the DIB Cyber Security/Information Assurance Program to provide industry with threat indicator databases and assistance.[127] While this effort is fixated on the large defense contractors, the DoD acknowledges the need to expand these programs to the numerous small businesses within the DIB, as recommended in a September 2015 GAO report.[128]

The DoD's work with the DIB also involves innovation ventures, such as the Defense Innovation Unit Experimental (DIUx) initiative which may include support of cyberspace portions of the Third Offset

Strategy.[129] Such efforts may be supported by existing programs such as the Software and Supply Chain Assurance Forum and the National Cybersecurity Center of Excellence.[130] Science and technology projects may be influenced by the 2016 *Federal Cybersecurity Research and Development Strategic Plan*.[131]

**International Efforts**

Strategic Goal V of the 2015 *DoD Cyber Strategy* strives to build international alliances and partnerships that involve significant coordination with the DoS. In Table 6, Obama published an international cyberspace strategy in 2011 that focused on achieving prosperity, security, and openness. In March 2016, the DoS published their *International Cyberspace Policy Strategy* as part of the reporting requirements from the cyberspace-related sections of the Consolidated Appropriation Act of 2016. Its stated purpose is to provide status on the implementation of the President's strategy and to address three themes: international law, confidence building measures, and norms of state behavior. The strategy acknowledges the importance of "working in partnership with other federal departments and agencies" toward accomplishing collective goals.[132] Two areas of particular relevance to DoD cyber strategy are deterrence and international norms. We now examine how the DoS strategy addresses these topics.

*Deterrence*

The concept of achieving deterrence in cyberspace was formalized in the 2011 international strategy with the inclusion of a declaratory statement of U.S. willingness to respond to hostile acts in this new domain as it would in the traditional domains (see excerpt in

Table 6). *The DoD Cyber Strategy* carries forward the essence of the deterrence concepts from the President's international strategy, noting, the "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."[133] The DoS strategy reflects the President's December 2015 cyber deterrence policy that maintains the flexibility to use multiple methods:

> The United States works to counter threats in cyberspace through a whole-of-government approach that brings to bear its full range of instruments of national power and corresponding policy tools—diplomatic, informational, military, economic, intelligence, and law enforcement—as appropriate and consistent with applicable law.[134]

The new deterrence policy envisions the use of a combination of the methods of denial and cost imposition implemented using the various policy tools. Of course, there is no cookbook solution; each application of deterrence measures must be based on the merits of the specific situation.[135] Denial measures seek to reduce the incentive for potential adversaries to attack cyberspace assets, in large part by "increasing the security and resiliency of U.S. Government and private sector computer systems."[136] If required, the approach of applying cost imposition measures may require more direct action by DoD:

> Military capabilities also provide an important set of options for deterring and responding to malicious cyber activity. As with all of the other tools described above, the United States has made clear for some time that just because an attack takes place in cyberspace does not mean a lawful and appropriate response must be conducted through cyber means.[137]

*International Norms*

The 2015 *DoD Cyber Strategy* acknowledges that one of DoD's important cyberspace activities is to "foster norms of responsible behavior to improve global strategic stability."[138] The DoS strategy also strives to achieve peace and stability:

> While emphasizing that existing international law applies to state behavior in cyberspace, the Department of State has pioneered the promotion of a framework of shared voluntary norms to guide state behavior in peacetime, and advanced the development of practical cyber confidence building measures (CBMs) to reduce risk, with the objective of establishing a coalition of states in support of that framework.[139]

This concept of U.S. "cyber diplomacy" has three key elements—international law, responsible state behavior, and CBMs. In implementing this concept, the DoS plans to use bilateral and multilateral engagements to construct international consensus toward an admirable end state:

> The United States has developed and is promoting a strategic framework of international cyber stability, designed to achieve and maintain a peaceful cyberspace environment where all states are able to fully realize its benefits, where there are advantages to cooperating against common threats and avoiding conflict, and where there is little incentive for states to engage in disruptive behavior or attack one another.[140]

Juxtaposed to this ideal worldview is the realization that military cyberspace capabilities are proliferating, and the dual-use nature of military technology inherently is destabilizing.[141] However, if military conflict in cyberspace does occur, it should still adhere to

international norms, such as those expressed in vehicles such as the United Nations (UN) Charter, the *Tallinn Manual,* and the Laws of Armed Conflict.[142] In fact, the United States must realize that its military will be establishing de facto norms by what it does in cyberspace.

*Global Environment: Allies and Adversaries*

Despite their concentration on the international aspects of cyberspace, neither the DoD nor DoS strategies provide much detail on the population of cyberspace users. A comparison of the population of Internet users by country in 2010 with those in 2015 reveals global dynamics that should be considered in any cyberspace strategy. Table 7 lists the countries with the top ten Internet user populations in 2015, the collective population of which comprises about 59 percent of the world's Internet users. The top five nations remained the same from 2010 to 2015—China, India, United States, Brazil, and Japan—but the percent of growth in India was over 300 percent. The combined Internet population of China and India is over one billion users—more than the total of the remaining top 10 countries. Nigeria and Indonesia each more than doubled their number of Internet users and China, Brazil, and Russia each grew more than 50 percent, while the United States, Japan, Germany, and the United Kingdom each had moderate grow of less than 20 percent.

| Country | Millions of Internet Users in 2015 (Global Ranking) | Millions of Internet Users in 2010 (Global Ranking) | Percent Change |
|---|---|---|---|
| China | 674 (1) | 420 (1) | + 60 |
| India | 354 (2) | 81 (4) | + 337 |
| United States | 281 (3) | 240 (2) | + 17 |
| Brazil | 118 (4) | 76 (5) | + 55 |
| Japan | 115 (5) | 99 (3) | + 16 |
| Russia | 103 (6) | 60 (7) | + 72 |
| Nigeria | 93 (7) | 44 (10) | + 111 |
| Indonesia | 73 (8) | 30 (16) | + 143 |
| Germany | 72 (9) | 65 (6) | + 11 |
| United Kingdom | 59 (10) | 51 (8) | + 16 |

**Table 7. Populations of Internet Users in 2010 and 2015.[143]**

**Friends and Allies**. The 2015 *DoD Cyber Strategy* provides only general statements regarding how it will build international partnerships. Priority of effort is equally vague, with the strategy mentioning the importance of the Five Eyes treaty and North Atlantic Treaty Organization alliance as well as the regions of the Middle East, Asia-Pacific, and Europe with no amplifying details. From this, one could infer that the continents of Africa and South America offer little value to U.S. mil-

itary cyberspace operations. As may be expected, the DoS *International Cyberspace Policy Strategy* provides significantly more detail on U.S. diplomatic ventures with other nations by citing specific accomplishments and plans vice broad concepts of engagement.

The DoS strategy focuses on four of the prominent actors in cyberspace—China, Russia, Brazil, and India—all of which also happen to be in the top six countries in terms of Internet user populations. Interestingly, the DoS notes, "the Brazilian approach to policy related to international security in cyberspace is shaped by a number of factors, including its emerging cyber military capabilities and policies."[144] Brazil is also a democratic nation with many national values aligned with those of the United States including "its willingness to affirm the applicability of international law to state behavior in cyberspace."[145] For India, the world's largest democracy, the DoS strategy observes, "the United States has a vibrant channel for engaging India on international security and other cyber policy issues, through the U.S.-India Cyber Dialogue." The framework of this bilateral endeavor echoes principles and concerns of the United States and designates 21 main areas of cooperation, including "developing a common and shared understanding of international cyber stability, and destabilizing cyber activity."[146]

**Potential Adversaries**. The 2015 *DoD Cyber Strategy* provides more specific information than the 2011 version, actually identifying four potential adversary nations by name—China, Russia, Iran, and North Korea—as well as the nonstate actor of the Islamic State in Iraq and the Levant (ISIL).[147] However, only China receives further treatment in the strategy as a dedicated implementation objective under Strategic Goal V. The objective calls for the DoD to strengthen its cyber dia-

logue with China "to reduce the risks of misperception and miscalculation that could contribute to escalation and instability."[148] The DoD strategy relegates Russia to a mere endnote that may unwittingly worsen an already tenuous situation:

> If and when U.S.-Russia military relations resume, as a part of broader interagency efforts DoD will seek to develop a military-to-military cyber dialogue with Russia to foster strategic stability in cyberspace.[149]

The *Department of State International Cyberspace Policy Strategy* also dedicates more content to China than any other country and asserts the following regarding its view of international norms:

> China has affirmed that international law applies in cyberspace, but has not been willing to affirm more specifically the applicability of the law of armed conflict or other laws of war, because it believes it would only serve to legitimize state use of cyber tools as weapons of war.[150]

Despite the diplomatic rhetoric, the 2015 *U.S.-China Economic and Security Review* report to Congress concludes, "the Chinese government appears to believe that it has more to gain than to lose from its cyber espionage and attack campaigns."[151] Contrary to the DoD strategy's view of Russia, the DoS strategy claims that it has:

> found common ground with the United States approach of promoting the applicability of international law to state conduct in cyberspace, as well as voluntary, non-binding norms of state behavior in peacetime.[152]

Perhaps to temper this remark, the DoS strategy goes on to note that "Russia and China are the most assertive states advancing alternative visions for international stability in cyberspace and seeking to sway undecided states in regional and multilateral venues."[153]

**Summary**

The 2015 *DoD Cyber Strategy* has excellent linkage to presidential and congressional directives, policies, and laws; this enhances its credibility with domestic and international audiences. The federal budget appears to provide adequate funding to implement the activities outlined in the strategy.

A spate of laws passed by Congress in 2014 and 2015 provided the foundation for much of the current interagency work on cybersecurity. The DoD roles and responsibilities to support this legislation focus on the areas of cyber incident response, information sharing, and public-private partnering. The DoD also has primary responsibility for helping to protect DIB critical infrastructure and may be called upon to perform DCSA operations to help defend cyber-related infrastructure in other sectors. These activities are consistent with implementation objectives found in strategic goals I and II.

Compared to the *Department of State International Cyberspace Policy Strategy*, the DoD strategy is vague regarding its international activities and priorities. Fortunately, both strategies address cyberspace-related deterrence issues in a manner consistent with the latest presidential policy. Unfortunately, neither strategy attempts to capture the changing nature of cyberspace and how it may affect elements of national power.

## SUMMARY

This section summarizes the key findings from the assessment of the 2015 *DoD Cyber Strategy* accomplished utilizing five individual analytical frameworks. It also identifies and integrates common themes that may emerge from these different perspectives.

### Strengths

*Primacy of Civilian Authority*

*The DoD Cyber Strategy* presents a firm and consistent portrayal of U.S. civilian control of military cyberspace operations through the President and SECDEF as well as adherence to legislative direction and guidance for cybersecurity activities. It also expresses the mandate of DoD activities in cyberspace to support enduring U.S. values of freedom, prosperity, and respect for international law.

*Deterrence*

*The DoD Cyber Strategy* significantly expands the discussion of cyberspace activities as they relate to U.S. national deterrence policies over the mere mention of the topic in the previous strategy. The strategy includes the key elements of response, denial, and resilience, coupled with the doctrine of constraint and use of all elements of national power. This depiction of deterrence is consistent not only with the President's 2011 *International Strategy for Cyberspace*, but also with the updated tenets of U.S. cyber policy as described in the DoS 2016 *International Cyberspace Policy Strategy.*

*Derivative Strategies*

*The DoD Cyber Strategy* spawned a series of Service-specific supporting guidance and planning documents. The Army CIO/G-6, Army Cyber Command, and Army Cyber Center of Excellence have strategic planning publications in place that provide actionable detail and some prioritization to the myriad tasks required to operationalize cyberspace for the soldier. Collectively, these derivative strategies bring together a diverse group of Army stakeholders and capabilities—cyber, signal, intelligence, and electronic warfare—to enable mission command in joint operations that may cross many domains.

**Areas of Concern**

*Lack of Clear End State*

*The DoD Cyber Strategy* does not contain an explicit or implicit end state toward which to orient its five strategic goals. The need for a clear vision to explain the fundamental purpose of the strategy is essential, given the public nature of its release and its anticipated domestic and international readership.

*No Prioritization of Efforts*

*The DoD Cyber Strategy* lays out 30 implementation objectives, several with multiple subtasks, and makes mention of budget concerns that may affect progress of these tasks. However, it offers no sense of priority to guide the strategy implementation to apply limited resources to boundless problems.

*Lack of Full Context*

*The DoD Cyber Strategy* does have a section called Strategic Context, but it serves mostly as a snapshot of the current manifestation of cyberspace threats and risks. It fails to provide any significant historical information or provide any baseline definition of the bounds of the cyberspace domain. Without such information, the strategy focuses on the present without thoughtful consideration of the past or future.

**Recommendations for Improvement**

Future versions of *The DoD Cyber Strategy* or similar derivative strategies should consider incorporating the following recommendations to improve their effectiveness:

- Provide a balanced and integrated hierarchy of end state, goals, and implementing objectives as well as explicit priorities for resources.
- Include a concise team line of past and future milestones and key guidance documents to help define the context of the current strategy.
- Provide specific examples of DoD responses to cyberattack or other cyber-incidents with clear ties to the strategy's goals and objectives. The example of the Sony hack in the 2015 strategy was confusing since it did not mention any DoD involvement in its resolution.
- Deliberately integrate and synchronize the actions, images, and words of the public released strategy document to better support the DoD's strategic communication goals.

In addition to these recommended structural changes, future DoD cyber strategy should also incorporate the following topics in its content:

- Address each Service and other major component's unique focus and contribution to the DoD cyberspace team.
- Include specific details on the organizations and processes that provide support to combatant commanders.
- Discuss the dynamic context of U.S. Government guidance and policy refinement that may be driven by events and decisions from executive, legislative, interagency, international, and commercial fora.
- Address the fundamental characterizations that define cyberspace domain and how they may change in the future as well as the implications of this change.
- Promote a dedicated effort to pursue cyberspace theory.

**Closing Remarks**

In evaluating the 2015 *DoD Cyber Strategy* from a holistic perspective, one must ask the simple question: Can the strategy work? It appears to be suitable in the sense that its individual goals all support DoD cyberspace operations as well as the greater needs of U.S. national security. It appears to be feasible since external Federal Government authorities are providing the funding and other resources necessary for its implementation. It appears to be acceptable since it has broad support from the executive, legislative, and interagency organizations of the U.S. Government. However, such positive assessments of suitability, feasibility, and

acceptability may be predicated upon the vagueness of the strategy's overarching intent. Without a clear end state, the strategy runs the risk of achieving objectives that may diverge from each other, eventually weakening the ability to achieve integrated and synchronized DoD cyberspace operations as well as activities of the U.S. Government writ large.

To be fair, the 2015 *DoD Cyber Strategy* is no worse than many similar government documents and presents progress in many areas over its 2011 predecessor. However, this progress was firmly planted in safe and comfortable themes that offered little in the way of where DoD cyberspace operations have been and where they are going. Worse, it implicitly treats cyberspace as a static domain that is well understood and characterized by the DoD, when in fact it should be considered a complex adaptive system that merits deliberate and significant study to define its fundamental nature. In the end, the 2015 *DoD Cyber Strategy* is a mild evolution of incremental efforts struggling to characterize an operational domain that is growing in size and complexity in ways that have yet to be understood.

## ENDNOTES

1. Ashton Carter, "Drell Lecture: 'Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity'," Stanford, CA: Stanford University, available from *defense.gov/DesktopModules/ArticleCS/Print.aspx?PortalId=1&ModuleId=2575&Article=606666*, accessed August 24, 2016.

2. *The DoD Cyber Strategy*, Washington, DC: U.S. Department of Defense, April, 2015, p. ii.

3. Ibid., p. ii.

4. Ibid. Examples of redundant material in the Implementing Objectives include the task to assess Cyber Protection Team capabilities listed under different objectives on pp. 20 and 21, as well as a repeated task to assess DFARS rules on p. 23.

5. "Fact Sheet: The Department of Defense (DoD) Cyber Strategy, April 2015," available from *defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf*, accessed October 23, 2015.

6. Cheryl Pellerin, "Carter Unveils New DoD Cyber Strategy in Silicon Valley," *DoD News*, April 23, 2015, available from *defense.gov/DesktopModules/ArticleCS/Print.aspx?PortalId=1&ModuleId=753&Article=604511*, accessed August 17, 2016.

7. Carter, "Drell Lecture."

8. *The DoD Cyber Strategy*, p. ii; and Carter, "Drell Lecture." Secretary Carter's account of the Russian cyber intrusion follows:

> So today, for example, I want to disclose a recent instance that helps illustrate the cyber threat we face today and what to do about it. It's never been publically reported, and it shows how rapidly DoD can detect, attribute, and expel an intruder from our military networks—in this case, unclassified ones.
>
> Earlier this year, the sensors that guard DoD's unclassified networks detected Russian hackers accessing one of our networks. They'd discovered an old vulnerability in one of our legacy networks that hadn't been patched.
>
> While it's worrisome they achieved some unauthorized access to our unclassified network, we quickly identified the compromise, and had a team of incident responders hunting down the intruders within 24 hours. After learning valuable information about their tactics, we analyzed their network activity, associated it with Russia, and then quickly kicked them off the network, in a way that minimized their chances of returning.

9. *The DoD Cyber Strategy*, available from *defense.gov/News/Special-Reports/0415_Cyber-Strategy*, accessed September 9, 2016. The website has been online in this format since at least August 16, 2015, per a search of archived websites using the Internet Archive

Wayback Machine. The specific search result is available at *web.archive.org/web/20150816023321/http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy*, accessed August 25, 2016.

10. *The DoD Cyber Strategy*, pp. 3, 33. The only two mentions of the previous DoD cyberspace strategy are:

> The May 2011 Department of Defense Strategy for Operating in Cyberspace guided the Defense Department's cyber activities and operations in support of U.S. national interests over the last four years. (p. 3)

> Since developing its first cyber strategy in 2011, the Defense Department has made significant progress in building its cyber capabilities, developing its organizations and plans, and fostering the partnerships necessary to defend the country and its interests. More must be done. (p. 33)

11. Ibid. The word "doctrine" appears twice in the document (see below), but not in an actionable sense that could be applied to the tactical and operational implementation of the strategy.

> To ensure that the Internet remains open, secure, and prosperous, the United States will always conduct cyber operations under a doctrine of restraint, as required to protect human lives and to prevent the destruction of property. (p. 6)

> Through the course of this strategy, as part of the U.S.-China Defense Consultative Talks and related dialogues, such as the Cyber Working Group, DoD will continue to hold discussions with China to bring greater understanding and transparency of each nation's military doctrine, policy, roles and missions in cyberspace. (p. 28)

12. Thomas M. Chen, *An Assessment of the Department of Defense Strategy for Operating in Cyberspace*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, September 2013. The evolution of cyberspace strategies is found on pp. 3-7, and a list of key national security strategy documents and their sources is included in the appendix (pp. 45-46).

13. Ibid., pp. 29-30.

14. *DoD Strategy for Operating in Cyberspace*, Washington, DC: Department of Defense, July 2011, p. i.

15. *The DoD Cyber Strategy*, p. iii.

16. Ibid., p. 30. The following two bullets from Chen's observations actually contain five different topics:

> The strategy does not distinguish between different types of adversaries—nation-states, foreign intelligence, hacktivists, criminals, hackers, terrorists—nor does the strategy address initiatives for specific types of adversaries.
>
> The unclassified version of the strategy neglects to address important issues: offense; attribution; rules for proper response to cyber attacks; and metrics of progress toward implementation. (p. 30)

17. *The DoD Cyber Strategy*. Specific discussion of types of adversaries is included in the Introduction and Strategic Context sections, as illustrated below:

> State and non-state actors conduct cyber operations to achieve a variety of political, economic, or military objectives. In conducting their operations, they may strike at a nation's values as well as its interests or purposes. (p. 1)
>
> Potential state and non-state adversaries conduct malicious cyber activities against U.S. interests globally and in a manner intended to test the limits of what the United States and the international community will tolerate. Actors may penetrate U.S. networks and systems for a variety of reasons, such as to steal intellectual property, disrupt an organization's operations for activist purposes, or to conduct disruptive and destructive attacks to achieve military objectives. (p. 9)
>
> In addition to state-based threats, non-state actors like the Islamic State in Iraq and the Levant (ISIL) use cyberspace to recruit fighters and disseminate propaganda and have declared their intent to acquire disruptive and destructive cyber capabilities. Criminal actors pose a considerable threat in cyberspace, particularly to financial institutions, and ideological groups often use hackers to further their political objectives. State and non-state threats often also blend together; patriotic entities often act as cyber surrogates

> for states, and non-state entities can provide cover for state-based operators. This behavior can make attribution more difficult and increases the chance of miscalculation. (p. 9)

18. Ibid., p. 29.

19. Ibid., pp. 11-12. The strategy included these details regarding the envisioned teamwork to achieve attribution of cyberattacks:

> Attribution is a fundamental part of an effective cyber deterrence strategy as anonymity enables malicious cyber activity by state and non-state groups. On matters of intelligence, attribution, and warning, DoD and the intelligence community have invested significantly in all source collection, analysis, and dissemination capabilities, all of which reduce the anonymity of state and non-state actor activity in cyberspace. Intelligence and attribution capabilities help to unmask an actor's cyber persona, identify the attack's point of origin, and determine tactics, techniques, and procedures. Attribution enables the Defense Department or other agencies to conduct response and denial operations against an incoming cyberattack.
>
> Public and private attribution can play a significant role in dissuading cyber actors from conducting attacks in the first place. The Defense Department will continue to collaborate closely with the private sector and other agencies of the U.S. Government to strengthen attribution. This work will be especially important for deterrence as activist groups, criminal organizations, and other actors acquire advanced cyber capabilities over time. (pp. 11-12)

20. Ibid., p. 19.

21. Chen, p. 30.

22. *The DoD Cyber Strategy*, p. 26.

23. Ibid., p. 6.

24. Barack Obama, *National Security Strategy*, Washington, DC: The White House, February 2015, pp. 12-13.

25. Department of Defense (DoD), *Quadrennial Defense Review 2014*, Washington, DC: U.S. Government Printing Office, March 4, 2014, pp. X, 33.

26. *The DoD Cyber Strategy*, p. iii.

27. Obama, *National Security Strategy*; Department of Defense, *Quadrennial Defense Review 2014*.

28. 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, pp. 2, 11. The 12 Joint Force Prioritized Missions are:

1. Maintain a secure and effective nuclear deterrent
2. Provide for military defense of the homeland
3. Defeat an adversary
4. Provide a global, stabilizing presence
5. Combat terrorism
6. Counter weapons of mass destruction
7. Deny an adversary's objectives
8. Respond to crisis and conduct limited contingency operations
9. Conduct military engagement and security cooperation
10. Conduct stability and counterinsurgency operations
11. Provide support to civil authorities
12. Conduct humanitarian assistance and disaster response (p. 11)

29. Chuck Hagel, "The Defense Innovation Initiative," memorandum for Deputy Secretary of Defense et al., Washington, DC: Secretary of Defense, November 15, 2014. Secretary Hagel describes the context of the Third Offset Strategy as:

> History is instructive on this 21st Century challenge. The U.S. changes the security landscape of the 1970s and 1980s with networked precision strike, stealth, and surveillance for conventional forces. We will identify a third offset strategy that puts the competitive advantage firmly in the hands of American power projection over the coming decades. (p. 2)

30. Carter, "Drell Lecture." Secretary Carter describes the historical context of the second offset strategy as:

> Let me step back. During the Cold War, Bill Perry drove a so called "offset strategy" that harnessed American technology to radically change warfare through precision guided munitions, network centric forces, and stealth aircraft. It came to life during the 1991 Gulf War – when the world watched, stunned, at what the American military might had achieved. But the world has since had a quarter century to figure out how to counter these capabilities.

31. Bob Work, "The Third Offset Strategy and Its Implications for Partners and Allies," speech presented at the Willard Hotel, Washington, DC, January 28, 2015, available from *defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies*, accessed August 27, 2016. Deputy Secretary of Defense Work describes how the DoD is continuing to pursue the initiative started by SECDEF Hagel:

> So to maintain our warfighting edge, we're trying to address this erosion our perceived erosion of technological superiority with the Defense Innovation Initiative and the Third Offset Strategy. Now, as Secretary Hagel said, this new initiative is an ambitious department-wide effort to identify and invest in innovative ways to sustain and advance America's military dominance for the 21st century.
>
> Now, we make significant investments in our nuclear enterprise; new space capabilities; advanced sensors, communications and munitions for power projection in contested environments; missile defense; and cyber capabilities.

32. H. Richard Yarger, "Toward a Theory of Strategy: Art Lykke and the U.S. Army War College Strategy Model," in J. Boone Bartholomees, Jr., ed., *The U.S. Army War College Guide to National Security Issues, Volume I: Theory of War and Strategy*, 4th Ed., Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, July 2010, ch. 3, p. 45.

33. Ibid., pp. 45-48.

34. "Internet Users," available from *internetlivestats.com/internet-users/*, accessed August 29, 2016. This website lists the number of Internet users in 2011 as 2,231,957,359 and in 2015 as 3,185, 996,155. It defines an Internet user as an "individual who can

access the Internet at home, via any device type and connection." Of course, many Internet users connect through a multitude of devices—computers, mobile telephones, television, automobiles, etc.—and thus may have multiple persona on the Internet. During this same timeframe, the website reports that the number of websites increased from 346,004,403 to 863,105,652. It defines a website as a "unique hostname" (a name which can be resolved, using a name server, into an IP address).

35. Yarger, p. 49.

36. *The DoD Cyber Strategy*, p. 1.

37. Ibid., p. 1.

38. Ibid., p. 7. Strategic Goal IV includes:

> To facilitate this work, the Joint Staff will work with USSTRATCOM to synchronize and integrate requirements into planning and provide recommendations to the Chairman of the Joint Chiefs of Staff on the alignment, allocation, assignment, and apportionment of Cyber Mission Forces. (p. 26)

39. U.S. Joint Staff Joint Force Development (J-7), *Cross-Domain Synergy in Joint Operations: Planner's Guide*, Washington, DC: Joint Chiefs of Staff, January 14, 2016, available from *www.dtic.mil/doctrine/concepts/joint_concepts/cross_domain_planning_guide.pdf*, accessed August 2016.

40. *The DoD Cyber Strategy*, p. 11.

41. Ibid., p. 6.

42. Ibid. The strategy describes the different CMF teams as follows:

> The Cyber Mission Force will be comprised of cyber operators organized into 133 teams, primarily aligned as follows: Cyber Protection Forces will augment traditional defensive measures and defend priority DoD networks and systems against priority threats; National Mission Forces and their associated support teams will defend the United States and its interests against cyberattacks of significant consequence;

and Combat Mission Forces and their associated support teams will support combatant commands by generating integrated cyberspace effects in support of operational plans and contingency operations. Combatant commands integrate Combat Mission Forces and Cyber Protection Teams into plans and operations and employ them in cyberspace, while the National Mission Force operates under the Commander of USCYBERCOM. Outside of this construct, teams can also be used to support other missions as required by the Department. (p. 6)

43. G. Alexander Crowther and Shaheen Ghori, "Detangling the Web: A Screenshot of U.S. Government Cyber Activity," *Joint Force Quarterly*, No. 78, 3rd Quarter 2015, pp. 75-83. The article lists the four Joint Forces Headquarters-Cyber (JFHQ-C) as:

- JFHQ-C Washington supports U.S. Special Operations Command, U.S. Pacific Command, and U.S. Southern Command.
- JFHQ-C Georgia supports U.S. Central Command, U.S. Africa Command, and U.S. Northern Command.
- JFHQ-C Texas supports U.S. European Command, USSTRATCOM, and U.S. Transportation Command.
- JFHQ-DoDIN defends DoD information networks at USCYBERCOM. (p. 81)

44. *The DoD Cyber Strategy*, p. 20.

45. Ibid., p. 29. The Principal Cyber Advisor was created in the National Defense Authorization Act of 2014.

46. *The DoD Cyber Strategy*, p. 4. Other significant mentions of the role of the President in DoD cyberspace operations include:

> While cyberattacks are assessed on a case-by-case and fact specific basis by the President and the U.S. national security team, significant consequences may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States. . . . If directed by the President or the Secretary of Defense, the U.S. military may conduct cyber operations to counter an imminent or on-going attack against the U.S. homeland or U.S. interests in cyberspace. . . . There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's

military related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. (p. 5)

The United States has articulated this declaratory policy in the 2011 United States International Strategy for Cyberspace, in the Department of Defense Cyberspace Policy Report to Congress of 2011, and through public statements by the President and the Secretary of Defense. (p. 11)

47. Ibid., pp. 5, 11.

48. Ibid., p. 30.

49. Ibid., pp. 1-12.

50. Ibid., p. 2.

51. Ibid., p. 9. The strategy states "China steals intellectual property (IP) from global businesses to benefit Chinese companies and undercut U.S. competitiveness." However, it does not provide any costs related to this theft.

52. Ibid., p. 7.

53. Michael S. Rogers, "Beyond the Build, Delivering Outcomes through Cyberspace: The Commander's Vision and Guidance for US Cyber Command," Fort Meade, MD: U.S. Cyber Command, June 3, 2015.

54. Ibid., back cover.

55. Despite the vague nature of the USCYBERCOM vision document, component commands have attempted to support its major themes. See "Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision," *Joint Force Quarterly*, No. 80, 1st Quarter 2016, pp. 86-93.

56. Figure adapted from Rogers, "Beyond the Build, Delivering Outcomes through Cyberspace," p. 11, back cover.

57. Michael S. Rogers, "Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command before the

Senate Armed Service Committee, 5 April 2016," Washington, DC: U.S. Government Printing Office.

58. Ibid., pp. 3, 5.

59. Ibid., pp. 13-14.

60. *DoD Cybersecurity Discipline Implementation Plan*, Washington, DC: DoD, October 2015, Amended February 2016, p. 4, available from *dodcio.defense.gov/Portals/0/Documents/Cyber/Cyber-Dis-ImpPlan.pdf*, accessed August 23, 2016. The plan is organized along four Lines of Effort:

> 1. Strong authentication—to degrade the adversaries' ability to maneuver on DoD information networks;
>
> 2. Device hardening—to reduce internal and external attack vectors into DoD information networks;
>
> 3. Reduce attack surface—to reduce external attack vectors into DoD information networks; and,
>
> 4. Alignment to cybersecurity/computer network defense service providers—to improve detection of and response to adversary activity. (p. 3)

61. Ibid., pp. 23-26.

62. Martin E. Dempsey and Ash Carter, "Department of Defense Cybersecurity Culture and Compliance Initiative," Memorandum for Secretaries of the Military Departments, Washington, DC: Office of the Secretary of Defense, September 30, 2015, available from *defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf*, accessed August 29, 2016.

63. Ibid., pp. 2-5.

64. Rogers, p. 1.

65. DoD, *Cyberspace Workforce Strategy*, Washington, DC: DoD, December 4, 2013, p. 3, available from *dodcio.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed(final).pdf*, accessed August 31, 2015. This strategy preceded the 2015 *DoD Cyber Strategy* and addresses the entire DoD

cyberspace workforce, not just the cyber mission force. Much of the policy and responsibilities related to this strategy have been codified in DoD Directive 8140.01, *Cyberspace Workforce Management*, Washington, DC: DoD Chief Information Officer, August 11, 2015.

66. *Defense Information Systems Agency Strategic Plan 2015-2020*, Fort Meade, MD: Defense Information Systems Agency, June 10, 2015, available from *www.disa.mil/~/media/Files/DISA/About/Strategic-Plan.pdf*, accessed August 23, 2016.

67. Headquarters, U.S. Army, *Army Network Campaign Plan: 2020 & Beyond*, Washington, DC: Office of the Army Chief Information Officer/G-6, February 2016, pp. 7-8, available from *ciog6.army.mil/Portals/1/Architecture/ANCP%20PRINT%206%20FEB%2015.pdf*, accessed August 31, 2016. The plan has five lines of effort:

[1] Provide Signal Capabilities to the Force

[2] Enhance Cybersecurity Capabilities

[3] Increase Network Throughput and Ensure Sufficient Computing Infrastructure

[4] Deliver IT Services to the Edge

[5] Strengthen Network Operations (pp. 12-18).

68. Department of the Navy, *Marine Corps Concept for Cyberspace Operations*, Version 2.0, Quantico, VA: Headquarters U.S. Marine Corps, October 9, 2015, p. iii, available from *marinecorpsconceptsandprograms.com/sites/default/files/concepts/pdf-uploads/MCFC%206-1%20Cyberspace%20Operations_1.pdf*, accessed August 31, 2016.

69. *U.S. Fleet Cyber Command/TENTH Fleet Strategic Plan 2015-2020*, Fort Meade, MD: U.S. Fleet Cyber Command/Tenth Fleet, May 2015, available from *www.navy.mil/strategic/FCC-C10F%20Strategic%20Plan%202015-2020.pdf*, accessed August 4, 2015. The Executive Summary includes "we lay out five pivotal, strategic goals that we will achieve in the next five years. For each of those five-year goals, we also cite specific, verifiable outcomes that

must be achieved in the next 18 months to ensure that we are on course." (p. 2) These five strategic goals are:

[1] Operate the Network as a Warfighting Platform (p. 10)

[2] Conduct Tailored Signals Intelligence (p. 14)

[3] Deliver Warfighting Effects Through Cyberspace (p. 16)

[4] Create Shared Cyber Situational Awareness (p. 18)

[5] Establish and Mature Navy's Cyber Mission Force (p. 20)

70. U.S. Air Force Chief Information Officer (CIO)/A6 Chief, *Information Dominance, Air Force Information Dominance Flight Plan: The Way Forward for Cyberspace IT in the United States Air Force*, Washington, DC: Secretary of the Air Force, May 1, 2015, available from *www.safcioa6.af.mil/shared/media/document/AFD-150610-015.PDF*, accessed August 31, 2016. This USAF plan focuses on four strategic goals:

1. Provide Airmen trusted information where they need it so they can be most effective. (p. 18)

2. Organize, train, equip, and educate Cyber-Airmen to be experts in cyberspace and the Air Force core missions to which they contribute. (p. 18)

3. Deliver freedom of action in and through cyberspace to advance Air Force core missions. (p. 19)

4. Optimize the planning, programming, budgeting and execution of cyberspace investments. (p. 19)

71. *U.S. Coast Guard Cyber Strategy*, Washington, DC: U.S. Coast Guard, June 2015, pp. 9-10, available from *uscg.mil/seniorleadership/DOCS/cyber.pdf*, accessed August 4, 2016. The USCG strategy includes supporting goals for each of its three strategic priorities:

Strategic Priority: Defending Cyberspace:

Goal 1. Identify and Harden Systems and Networks (p. 23)

Goal 2. Understand and Counter Cyber Threats (p. 24)

Goal 3. Increase Operational Resilience (p. 25)

Strategic Priority: Enabling Operations:

Goal 1: Incorporate Cyberspace Operations into Mission Planning and Execution (p. 27)

Goal 2: Deliver Cyber Capabilities to Enhance All Missions (p. 28)

Strategic Priority: Protecting Infrastructure

Goal 1. Risk Assessment—Promote Cyber Risk Awareness and Management (p. 32)

Goal 2. Prevention—Reduce Cybersecurity Vulnerabilities in the MTS (p. 33)

72. Robert Ferrell, "Network Readiness in a Complex World," presentation at the 15th Annual Army IT Day, Vienna, VA, Armed Forces Communications and Electronics Association, March 31, 2016. As part of his unclassified presentation, LTG Ferrell, Army Chief Information Officer/G6, provided an overview of the hierarchy and linkage of documents that form the Army network strategy.

73. Robert Ferrell, "The Army and the New DoD Cyber Strategy," leader blog available from *ciog6.army.mil/AboutCIO/LeaderBlog/tabid/108/EntryId/61/TheArmyandtheNewDoDCyberStrategy.aspx*, accessed August 4, 2016.

74. Headquarters, U.S. Army, *Army Network Campaign Plan: Implementation Guidance Near Term 2016-17*, Washington, DC: Office of the Army Chief Information Officer/G-6, February 2016, available from *ciog6.army.mil/Portals/1/ANCP/ANCP%20Near-term%20impl%20plan%2016-17.pdf*, accessed September 1, 2016.

75. Headquarters, U.S. Army, *Army Network Campaign Plan: Implementation Guidance Mid Term 2018-22*, Washington, DC: Office of the Army Chief Information Officer/G-6, February 2016, available from *ciog6.army.mil/Portals/1/Home/Tabs/Strategy/ANCP%20Mid-term%20Impl%20Plan%2018-22.pdf*, accessed September 1, 2016.

76. *Shaping the Army Network: 2025-2040*, Washington, DC: Office of the Army Chief Information Office/G-6, March 2016, available from *peoc3t.army.mil/c3t/docs/Shaping_the_Army_Network_2025-2040.pdf*, accessed April 5, 2016.

77. Ibid., pp. 32-34. For more details in the mission command network, see *The Mission Command Network: Vision & Narrative*, Fort Leavenworth, KS: Combined Arms Center, October 1, 2015, available from *usacac.army.mil/sites/default/files/documents/mccoe/MissionCommandNetworkNarrative1Oct15.pdf*, accessed September 1, 2016. This documents define mission command network as:

> The "Mission Command Network (MC Network)" is integrated mission command and LandWarNet capabilities, which enable commanders, leaders & soldiers to exercise mission command (the philosophy) and integrate all warfighting functions and Unified Action enablers (the warfighting function). It is an inherent component of the Joint Information Environment. The MC Network allows commanders to develop and maintain situational understanding, maneuver across domains and locations, and conduct joint combined arms operations to accomplish the mission. (p. 3)

78. *Army Cloud Computing Strategy*, Version 1.1, Washington, DC: Office of the Army Chief Information Office/G-6, March 2015, available from *ciog6.army.mil/Portals/1/AboutCIO/Mission/Strategy/20150424_Army_Cloud_Computing_Strategy.pdf*, accessed August 31, 2016. The document's Executive Summary states its purpose:

> The Army Cloud Computing Strategy establishes and communicates the Army's vision and strategy for delivering cloud-enabled network capabilities to improve mission and business effectiveness, increase operational information technology (IT) efficiencies and protect Army data and infrastructure. The Army Cloud Computing Strategy extends the baseline and concepts defined in the various federal, DoD, and Army policies and documents and is nested with the Army Network Campaign Plan. (p. 1)

79. *Army Data Strategy*, Version 1.0, Washington, DC: Office of the Army Chief Information Office/G-6, February 2016, available from *ciog6.army.mil/Portals/1/AboutCIO/Mission/*

*Strategy/20160303_Army_Data_Strategy_2016.pdf*, accessed August 31, 2016. The document's Executive Summary states its purpose:

> The Army Data Strategy describes the Army's vision and goals for establishing a solid foundation for sharing data, information and IT services across the Army – extending into the Joint Information Environment. The Army Data Strategy builds upon the Department of Defense (DoD) Net-Centric Data Strategy baseline of making data visible, accessible, understandable, trusted and interoperable. As part of these efforts, the Chief Information Officer/G-6 has partnered with the Assistant Secretary of the Army (Acquisition, Logistics and Technology) to implement the Common Operating Environment. (p. 7)

80. *U.S. Army Cyber Center of Excellence Strategic Plan*, Fort Gordon, GA: U.S. Army Cyber Center of Excellence, September 2015, available from *cybercoe.army.mil/images/CyberCoE%20Documents/strategic_plan_2015_revision4_9_14_2015.pdf*, accessed October 22, 2015. The purpose of scope of this plan includes:

> This strategy defines the Cyber CoE vision, mission, lines of effort, strategic imperatives, and objectives required to integrate capabilities across the Army to include the Army's signal, electronic warfare (EW), and military intelligence (MI) partners (see Figure 1) together with other Joint Service and Intelligence capabilities. The Cyber CoE with Army Cyber Command (ARCYBER) and the Army Cyber Institute (ACI) form the nucleus of "Team Cyber" for the Army while leveraging the Intelligence Center of Excellence (ICoE), the U.S. Army Intelligence and Security Command (INSCOM), the Network Enterprise Command (NETCOM), along with the greater Signal and Intelligence Communities to achieve dominance in the cyberspace domain. Cyber CoE activities must be coordinated and complementary with/to ARCYBER and ACI. The Cyber COE Strategy spans from the present through FY [fiscal year] 2025 to meet emerging Joint, Interagency, and Multi-national (JIM) operational environment challenges. (p. 3)

81. *The DoD Cyber Strategy*, p. 3.

82. "Foreign Policy Cybersecurity," White House official website, available from *https://obamawhitehouse.archives.gov/node/233081*, accessed August 30, 2017.

83. *The DoD Cyber Strategy*, p. iii.

84. "Foreign Policy Cybersecurity" White House official website. The priority numbers listed in Table 6 reflect the same order of presentation on the White House website.

85. Shaun Donovan, Beth F. Colbert, and Tony Scott, Executive Office of the President, "Federal Cybersecurity Workforce Strategy," M-16-15, Memorandum for Heads of Executive Departments and Agencies, Washington, DC: Office of Management and Budget, July 12, 2016, p. 10, available from *obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf*, accessed September 1, 2016.

86. Barack Obama, Executive Order 13718 of February 9, 2016, "Commission on Enhancing National Cybersecurity," *Federal Register*, Vol. 81, No. 29, February 12, 2016, p. 7441, available from *gpo.gov/fdsys/pkg/FR-2016-02-12/pdf/2016-03038.pdf*, accessed September 1, 2016.

87. Shaun Donovan and Tony Scott, "Cyber Strategy and Implementation Plan (CSIP) for the Federal Civilian Government," N-16-04, Memorandum for Heads of Executive Departments and Agencies, Washington, DC: Office of Management and Budget, October 30, 2015, available from *https://www.hsdl.org/?view&did=788143*, accessed August 30, 2017.

88. Barack Obama, Executive Order 13691 of February 12, 2015, "Promoting Private Sector Cybersecurity Information Sharing," *Federal Register*, Vol. 80, No. 34, February 20, 2015, p. 9349, available from *gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf*, accessed September 1, 2016.

89. Barack Obama, Executive Order 13636 of February 12, 2013, "Improving Critical Infrastructure Cybersecurity," *Federal Register*, Vol. 78, No. 33, February 19, 2013, pp. 117399-11740, available from *gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf*, accessed September 1, 2016.

90. Barack Obama, "Presidential Policy Directive—United States Cyber Incident Coordination," PPD-41, Washington, DC: The White House, July 26, 2016, available from *https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident*, accessed August 30, 2017.

91. Barack Obama, Executive Order 13694 of April 2, 2015, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," *Federal Register*, Vol. 80, No. 63, April 2, 2015, pp. 18077, available from *gpo.gov/fdsys/pkg/FR-2015-04-02/pdf/2015-07788.pdf*, accessed September 1, 2016.

92. Barack Obama, Executive Order 13687 of January 2, 2015, "Imposing Additional Sanctions With Respect To North Korea," *Federal Register*, Vol. 80, No. 3, January 6, 2015, pp. 819, available from *gpo.gov/fdsys/pkg/FR-2015-01-06/pdf/2015-00058.pdf*, accessed September 1, 2016.

93. Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington, DC: The White House, May 2011, p. 14.

94. Rita Tehan, "Cybersecurity: Legislation, Hearings, and Executive Branch Documents," *Congressional Research Service (CRS) Report R43317*, Washington, DC: Congressional Research Service, July 8, 2016, p. i.

95. Ibid., pp. 1-3.

96. "Fact Sheet: Cybersecurity National Action Plan," Washington, DC: The White House, February 9, 2016, available from *https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan*, accessed August 30, 2017. The four major parts of the CNAP are:

- Establish the "Commission on Enhancing National Cybersecurity.
- Modernize government IT and transform how the Government manages cybersecurity through the proposal of a $3.1 billion Information Technology Modernization Fund.
- Empower Americans to secure their online accounts by moving beyond just passwords and adding an extra layer of security.

- Invest over $19 billion for cybersecurity as part of the President's Fiscal Year (FY) 2017 Budget.

97. Ibid.

98. *2015 DoD Cyber Strategy*, p. 10.

99. "Fact Sheet: Highlights of National Defense Authorization Act for Fiscal Year 2016," Washington, DC: U.S. House of Representatives, September 29, 2015, pp. 6-7, available from *rules.house.gov/sites/republicans.rules.house.gov/files/114/PDF/114-CRHR1735-SxS.pdf*, accessed August 29, 2016. The NDAA included significant efforts to improve DoD cyberspace operations:

> The Conferees agreed to a number of provisions to create, expand or clarify authorities to support the Department's ability to man, train and equip cyber forces, and operate cyber forces at the speeds necessary to function in the cyber domain. These include:
>
> Creation of a new cyber personnel hiring authority for U.S. Cyber Command and the cyber commands of the military department;
>
> Limited cyber acquisition authority for U.S. Cyber Command;
>
> Codification of cyber liability protections for certain covered contractors;
>
> Designation of an entity responsible for the acquisition of certain critical cyber capabilities;
>
> An assessment of the capabilities of Cyber Command to defend the U.S. from cyber-attacks;
>
> A plan for biennial exercises for responding to cyber-attacks; and,
>
> Evaluation and remediation of cyber vulnerabilities of major weapons systems. (p. 7)

100. "Consolidated DoD FY17 Budget Fact Sheet," DoD website, available from *defense.gov/Portals/1/features/2016/0216_budget/*

*docs/2-4-16_Consolidated_DoD_FY17_Budget_Fact_Sheet.pdf*, accessed August 23, 2016.

> **Addressing Cyber Threats.** In response to increased threats, we will spend $6.7 billion strengthening cyber defenses and increasing options available in case of a cyber-attack. The Budget:
>
> Executes *The DoD Cyber Strategy* to defend DoD networks and systems, defend the United States and its interests against cyber-attacks of significant consequence, and provide integrated cyber capabilities to support military operations.
>
> Supports the Cyber Mission Force, continuing to provide personnel to create 133 fully operational teams by the end of FY 2018, investing in innovative approaches to provide a virtual environment for cyber personnel to train, and equipping the force with necessary tools and platforms.
>
> Develops offensive cyber capabilities to support military operations and provide response and deterrence options to leadership. (p. 5)

101. Ibid., p. 5.

102. Jeffrey Caton, *Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, and Response Implications*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, September 2013, pp. 52-53.

103. Obama, PPD-41.

104. Ibid., para. II of this document contains the following definitions:

> **A. Cyber incident**. An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

> **B. Significant cyber incident.** A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

105. *The DoD Cyber Strategy*, p. 5. Significant cyberattacks are decribed as:

> While cyberattacks are assessed on a case-by-case and fact specific basis by the President and the U.S. national security team, significant consequences may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States. (p. 5)

106. Obama, PPD-41.

107. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, *Cyber Incident Handling Program*, Washington, DC: Joint Chiefs of Staff, July 10, 2012.

108. Ibid., pp. A-5 and F-6.

109. Ibid., p. B-A-4.

110. "Annex for Presidential Policy Directive—United States Cyber Incident Coordination," Washington, DC: The White House, July 26, 2016, available from *obamawhitehouse.archives.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident*, accessed September 2, 2016.

111. PPD-41 Annex.

112. Ibid.

113. Ibid.

114. "DoD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents," Report GAO-16-332, Washington, DC: U.S. Government Accountability Office, April 2016, p. 12, available from *gao.gov/assets/680/676322.pdf*, accessed September 6, 2016.

115. Ibid., p. 26.

116. Barack Obama, "Presidential Policy Directive—Critical Infrastructure Security and Resilience," PPD-21, Washington, DC: The White House, February 12, 2013, available from *https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil*, accessed August 30, 2017.

117. Ibid. PPD-21 describes information sharing as follows:

> A secure, functioning, and resilient critical infrastructure requires the efficient exchange of information, including intelligence, between all levels of governments and critical infrastructure owners and operators. This must facilitate the timely exchange of threat and vulnerability information as well as information that allows for the development of a situational awareness capability during incidents. The goal is to enable efficient information exchange through the identification of requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternate capabilities should there be a disruption in the primary systems.
>
> Greater information sharing within the government and with the private sector can and must be done while respecting privacy and civil liberties. Federal departments and agencies shall ensure that all existing privacy principles, policies, and procedures are implemented consistent with applicable law and policy and shall include senior agency officials for privacy in their efforts to govern and oversee information sharing properly.

118. Obama, Executive Order 13691 of February 12, 2015.

119. "Fact Sheet: Cyber Threat Intelligence Integration Center," Washington, DC: The White House, February 25, 2015, available from *https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center*, accessed September 6, 2016. The CTIIC relationship to existing cybersecurity information fusion centers is described as:

> The CTIIC will not be an operational center. It will not collect intelligence manage incident response efforts, direct

> investigations, or replace other functions currently performed by existing departments, agencies, or government cyber centers. Instead, the CTIIC will support the NCCIC in its network defense and incident response mission; the NCIJTF in its mission to coordinate, integrate, and share information related to domestic cyber threat investigations; and U.S. Cyber Command in its mission to defend the nation from significant attacks in cyberspace. The CTIIC will provide these entities, as well as other departments and agencies, with intelligence needed to carry out their cybersecurity missions.

120. Ibid.

121. "Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015," Washington, DC: The Office of the Director of National Intelligence, and the Departments of Homeland Security, Defense, and Justice, February 16, 2016, available from *us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_(103).pdf*, accessed August 5, 2016.

122. "About ISACs," National Council of ISACs official website, available from *isaccouncil.org/*, accessed September 6, 2016. The website describes the original of ISACs as:

> The concept of ISACs was introduced and promulgated pursuant to Presidential Decision Directive-63 (PDD-63), signed May 22, 1998, after which the federal government asked each critical infrastructure sector to establish sector-specific organizations to share information about threats and vulnerabilities. Some ISACs formed as early as 1999, and most have been in existence for at least ten years.

123. "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015," Washington, DC: DHS and DoJ, available from *us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_(Sec%20105(a)).pdf*, accessed August 5, 2016.

124. "Automated Indicator Sharing (AIS)," factsheet, Washington, DC: DHS, available from *us-cert.gov/ais*, accessed August 5, 2016.

125. Lisa O. Monaco, "Administration Efforts on Cybersecurity: The Year in Review and looking Forward to 2016," Washington, DC: The White House, February 2, 2016, available from *https://obamawhitehouse.archives.gov/blog/2016/02/02/administration-efforts-cybersecurity-year-review-and-looking-forward-2016*, accessed August 30, 2017.

126. "RD: TSO: DAMO," Technology Security Office official website, Office of the Assistant Secretary of Defense for Research & Engineering, available from *acq.osd.mil/rd/tech_security/damo/*, accessed August 19, 2016.

127. "Opportunities Exist for DoD to Share Cybersecurity Resources with Small Businesses," Report GAO-15-777, Washington, DC: U.S. Government Accountability Office, September 2015, p. 22, available from *gao.gov/assets/680/672724.pdf*, accessed September 7, 2016. The DIB Cyber Security/Information Assurance Program:

> Provides members with more than 117,000 unclassified threat indicators, including technical signatures that identify potentially malicious actors. Defense Industrial Base Cyber Security/Information Assurance also includes a classified explanation for each threat indicator. Additionally, Defense Industrial Base Cyber Security/Information Assurance members receive regular updates on new threats, and receive additional assistance as needed from DoD Chief Information Officer based on information collected by DoD. Defense Industrial Base Cyber Security/Information Assurance also provides an environment for threat information sharing among members through regular threat information updates and actions as needed from the DoD Chief Information Officer based on information provided by Defense Industrial Base Cyber Security/Information Assurance members.

128. Ibid., pp. 13, 25. The report's conclusions include:

> While DoD OSBP [Office of Small Business Programs] officials have recognized the importance of educating defense small businesses about cybersecurity, they have not identified and disseminated cybersecurity resources through their outreach and education efforts to businesses because they have been focused on other priorities, such as developing a training curriculum for DoD professionals

who work with small businesses. By identifying and disseminating information about existing cybersecurity resources to defense small businesses, these businesses may be made more aware of cybersecurity practices and cyber threats, thereby potentially assisting them in protecting their networks against cyber exploits. (p. 13)

129. "Defense Innovation Unit Experimental," official website, available from *diux.mil*, accessed September 8, 2016. The website lists the DIUx mission as:

> The U.S. Department of Defense relies on innovation to maintain our nation's ability to deter, and if need be, prevail in conflict.
>
> With outposts in the heart of Silicon Valley and Boston, Defense Innovation Unit Experimental (DIUx) serves as a bridge between those in the U.S. military executing on some of our nation's toughest security challenges and companies operating at the cutting edge of technology.
>
> As our name implies, DIUx is just that: an "experiment." We continuously iterate on how best to identify, contract, and prototype novel innovations through sources traditionally not available to the Department of Defense, with the ultimate goal of accelerating technology into the hands of the men and women in uniform.

130. "Fact Sheet: Administration Cybersecurity Efforts 2015," Washington, DC: The White House, July 9, 2015, available from *https://obamawhitehouse.archives.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015*, accessed August 30, 2017.

131. Monaco, "Administration Efforts on Cybersecurity."

132. *Department of State International Cyberspace Policy Strategy*, Public Law 114-113, Division N, Title IV, Section 402, Washington, DC: U.S. Department of State, March 2016, p. 1.

133. *The DoD Cyber Strategy*, p. 10. The three key parts of deterrence are listed as response, denial, and resilience. (p. 11)

134. *Department of State International Cyberspace Policy Strategy*, p. 20.

135. Ibid., p. 20. Deterrence by denial and cost imposition are described as:

> The United States believes deterrence in cyberspace is best accomplished through a combination of "deterrence by denial"—reducing the incentive of potential adversaries to use cyber capabilities against the United States by persuading them that the United States can deny their objectives – and "deterrence through cost imposition" – threatening or carrying out actions to inflict penalties and costs against adversaries that conduct malicious cyber activity against the United States. It is important to note there is no one-size-fits-all approach to deterring or responding to cyber threats. Rather, the individual characteristics of a particular threat determine the tools that would most appropriately be used. (p. 20)

136. Ibid., p. 20. Methods of achieving deterrence by denial include:

> 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 (NCCIC) 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)

137. Ibid., p. 22. The DoS strategy includes an excellent and concise summary of the DoD cyber missions and force:

> The Department of Defense continues to build its cyber capabilities and strengthen its cyber defense and deterrence posture. As part of this effort, the Department of Defense is building its Cyber Mission Force of 133 teams to be fully operational by the end of 2018. The Cyber Mission Force, which already is employing capabilities, will defend Department of Defense networks, defend the Nation against cyberattacks of significant consequence, and generate integrated cyberspace effects in support of operational plans and contingency operations. (p. 22)

138. *The DoD Cyber Strategy*, p. 3.

139. *Department of State International Cyberspace Policy Strategy*, p. 3.

140. Ibid., p. 12. Details of U.S. cyber diplomacy include:

> There are three key elements to this framework: (1) global affirmation of the applicability of international law to state behavior in cyberspace; (2) the development of international consensus on additional norms and principles of responsible state behavior in cyberspace that apply during peacetime; and (3) the development and implementation of practical CBMs, which can help ensure stability in cyberspace by reducing the risk of misperception and escalation.
>
> We have forged a growing international consensus on this framework, and will continue to promote a broad consensus on international cyber stability wherever possible. Expanding and building on this consensus is a core diplomatic priority for the United States. To that end, the Department of State and the Administration have raised and will continue raising these issues at a high level in key bilateral and multilateral engagements with countries around the globe. (pp. 12-13)

141. Ibid., p. 3.

142. Caton, pp. 15-24.

143. "Internet Users."

144. *Department of State International Cyberspace Policy Strategy*, p. 19.

145. Ibid., p. 19.

146. "Fact Sheet: Framework for the U.S.-India Cyber Relationship," Washington DC, The White House, June 7, 2016, available from *https://obamawhitehouse.archives.gov/the-press-office/2016/06/07/fact-sheet-framework-us-india-cyber-relationship*, accessed August 5, 2016. Thirteen specific shared principles for the relationship were listed; they included:

> A commitment to promote international security and stability in cyberspace through a framework that recognizes the applicability of international law, in particular the UN Charter, to state conduct in cyberspace and the promotion of voluntary norms of responsible state behavior in cyberspace.
>
> A desire to cooperate in strengthening the security and resilience of critical information infrastructure.

147. *The DoD Cyber Strategy*, p. 9. For more details on these potential adversary nations, see Ilan Berman, ed., *Strategic Primer Volume 2: Cybersecurity: Current capabilities and emerging threats*, Washington DC: American Foreign Policy Council, Spring 2016.

148. Ibid., p. 28.

149. Ibid. For more details on recent Russian activity in cyberspace, see Keir Giles, *Russia's 'New' tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, London, England: Chatham House, The Royal Institute of International Affairs, March 2016.

150. *Department of State International Cyberspace Policy Strategy*, p. 17.

151. 2015 Report to Congress of the U.S.-China Economic and Security Review Commission, 114th Cong., 1st Sess., Washington, DC: U.S. Government Printing Office, November 2015, p. 218, available from *uscc.gov/Annual_Reports/2015-annual-report-congress*, accessed August 20, 2016.

152. *Department of State International Cyberspace Policy Strategy*, p. 18.

153. Ibid., p. 17.

# APPENDIX I:

# SUMMARY OF PRIMARY MISSIONS, STRATEGIC GOALS, AND IMPLEMENTATION OBJECTIVES FROM THE DOD CYBER STRATEGY (APRIL 2015)[1]

| Primary Missions in Cyberspace |
|---|
| • First, DoD must defend its own networks, systems, and information.<br>• For its second mission, DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence.<br>• Third, if directed by the President or the Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans. |
| Strategic Goal I:<br>Build and maintain ready forces and capabilities to conduct cyberspace operations. |
| • Build the cyber workforce.<br>  o Maintain a persistent training environment.<br>  o Build viable career paths.<br>  o Draw on the National Guard and Reserve.<br>  o Improve civilian recruitment and retention.<br>  o Develop and implement exchange programs with the private sector.<br>  o Support the National Initiative for Cyberspace Education.<br>• Build technical capabilities for cyber operations.*<br>  o Develop the Unified Platform.<br>  o Accelerate research and development.*<br>• Validate and continually refine an adaptive command and control mechanism for cyber operations.<br>• Establish an enterprise-wide cyber modeling and simulation capability.<br>• Assess Cyber Mission Force capability.*<br>  o Propose, collect, analyze, and report a set of appropriate metrics. |

Strategic Goal II:
Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions.

- Build the Joint Information Environment (JIE) single security architecture.*
  - Enable a robust network defense.
  - Develop a framework for developing and integrating new defensive techniques.
- Assess and ensure the effectiveness of the Joint Headquarters for DoD information network (DoDIN) operations.
- Mitigate known vulnerabilities.*
- Assess DoD's cyber defense forces.
- Improve the effectiveness of the current DoD Computer Network Defense Service Provider (CNDSP) construct in defending and protecting DoD networks.
- Plan for network defense and resilience.*
  - Integrate cyber into mission assurance assessments.
  - Assess Cyber Protection Team (CPT) capabilities.
  - Improve weapons systems cybersecurity.
  - Build and exercise continuity plans.
- Red team DoD's network defenses.
- Mitigate the risk of insider threats.
  - Extend beyond information technology and include matters of personnel and reliability.
- Exercise to provide Defense Support of Civil Authorities.
  - Include DHS and FBI in DoD annual exercise program.
- Define and refine the National Guard's role in supporting law enforcement, Homeland Defense, and Defense Support of Civil Authorities missions.
- Improve accountability and responsibility for the protection of data across DoD and the DIB.
  - Continue to assess DFARS rules and NIST standards.
  - Continue to expand companies' participation in threat information sharing programs.
  - Defense Security Service expand education and training programs for DoD personnel and DIB contractors.
  - Review the sufficiency of current classification guidance.
- Strengthen DoD's procurement and acquisition cybersecurity standards.
- Build collaboration between the acquisition, intelligence, counterintelligence, law enforcement, and operations communities to prevent, mitigate, and respond to data loss.
  - DoD CIO and USD(AT&L) assess and update specific information system security controls that underpin the DFARS.
- Use DoD counterintelligence capabilities to defend against intrusions.
  - Specify how DoD's counterintelligence agencies will collaborate with the broader U.S. intelligence and law enforcement communities.
  - DoD work with companies to develop alert capabilities and build layered defenses.*
  - DoD collaborate with Services' Damage Assessment Management Offices to better inform decisions to maintain, modify, or cancel penetrated programs.
- Support whole-of-government policies and capabilities to counter intellectual property theft.

| |
|---|
| Strategic Goal III:<br>Be prepared to defend the U.S. Homeland and U.S. vital interests from disruptive cyberattacks of significant consequence. |
| • Continue to develop intelligence and warning capabilities to anticipate threats.*<br>• Develop and exercise capabilities to defend the nation.<br>  o Build partnerships to defend the nation.*<br>  o Conduct an annual comprehensive review of DoD's defend the nation capabilities.<br>• Develop innovative approaches to defending U.S. critical infrastructure.<br>• Develop automated information sharing tools.*<br>• Assess DoD's cyber deterrence posture and strategy.*<br>  o USSTRATCOM must determine whether DoD is building the capabilities required for attributing and deterring key threats and recommend specific actions that DoD can take to improve its cyber deterrence posture. |
| Strategic Goal IV:<br>Build and maintain viable cyber options and plan to use those options to control escalation and to shape the conflict environment at all stages. |
| • Integrate cyber options into plans.<br>  o Accelerate the integration of cyber requirements into plans. |
| Strategic Goal V:<br>Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability. |
| • Build partner capability in key regions.*<br>  o Support the hardening and resiliency of Middle Eastern allies' and partners' networks and systems.<br>  o Support the hardening and resiliency of Northeast Asian allies' networks and systems.<br>  o Build new strategic partnerships in the Asia-Pacific region.<br>  o Work with key NATO allies to mitigate cyber risks to DoD and U.S. national interests.<br>  o DoD will remain flexible and agile as it builds alliances and partnerships to best respond to shifts in the strategic environment.<br>• Develop solutions to counter the proliferation of destructive malware.<br>• Work with capable international partners to plan and train for cyber operations.<br>• Strengthen the United States cyber dialogue with China to enhance strategic stability. |
| * Objective was included in the DoD Fact Sheet. |

## ENDNOTES – APPENDIX I

1. Source: *The DoD Cyber Strategy*, Washington, DC: U.S. Department of Defense, April, 2015, pp. 17-28; Strategic goals and main objectives are listed verbatim; some of the supporting sub-objectives are abridged.

# APPENDIX II:

# SUMMARY OF PHOTOGRAPHIC IMAGES AND THEIR CAPTIONS FROM THE DOD CYBER STRATEGY (APRIL 2015)[1]

| Page | Caption | Related Primary Missions & Strategic Goals | Other Themes |
|---|---|---|---|
| 1 | I. Introduction (Unsourced photograph demarcates the strategy's first section. It depicts Secretary Carter at a USCYBERCOM Podium with the DoD and USCYBERCOM seals in the background. ) | N/A | Support from SecDef |
| 2 | The Red Flag 14-1 Cyber Protection Team works on cyber defense procedures inside the Combined Air and Space Operations Center-Nellis, Nellis, NV. The CPT's primary goal is to find and thwart potential space, cyberspace, and missile threats against U.S. and allied forces. (U.S. Air Force photo by Senior Airman Brett Clashman) | PM 3<br>ST II | • Joint Operations<br>• Exercise & Training<br>• Air Force Operations |
| 3 | Mr. Joe Sciabica and Maj. Gen. J. Kevin McLaughlin sign an Air Force Civil Engineer Center-Air Forces Cyber collaboration agreement. The initiative is designed to enhance the security of industrial control systems that support critical Air Force infrastructures around the world. (U.S. Air Force photo by Shannon Carabajal) | PM 1<br>SG II | • Critical infrastructure protection<br>• Air Force Operations |

| | | | |
|---|---|---|---|
| 5 | Navy Petty Officer 1st Class Joel Melendez, Naval Network Warfare Command information systems analysis, Air Force Staff Sgt. Rogerick Montgomery, U.S. Cyber Command network analysis, and Army Staff Sgt. Jacob Harding, 780th Military Intelligence Brigade cyber systems analysis, at an exercise during Cyber Flag 13-1 at Nellis Air Force Base, NV. (U.S. Air Force photo by Senior Airman Matthew Lancaster) | PM 3<br>SG II | • Joint Operations<br>• Exercise & Training |
| 7 | U.S. Strategic Command serves as the Defense Department's global synchronizer for capabilities that affect every combatant command. Here the sun sets over some of the assets that provide capabilities at Forward Operating Base Sharana in Afghanistan's Paktika province. (U.S. Army photo by Spc. Raymond Schaeffer) | PM 3<br>SG I, IV, V | • Joint Expeditionary Operations |
| 9 | II. Strategic Context (Unsourced photograph demarcates the strategy's second section. It depicts the USAF 624th Operations Center located at Joint Base San Antonio Lackland, Texas. The center "receives orders and tasks from the United States Cyber Command, and works with 24th Air Force subordinate units to perform a wide range of cyber missions in support of Air Force and Joint Force commanders." (source: 624th OC Fact Sheet/April 2016) | PM 1, 3<br>SG I, II | • Air Force Operations |

| | | | |
|---|---|---|---|
| 11 | Airman 1st Class Nate Hammond adjusts the frequency of a Roll-On Beyond Line of Sight Enhancement, or ROBE, data link system at the Transit Center at Manas, Kyrgyzstan. A ROBE connects manpower assets on the ground to other ground or airborne units. (U.S. Air Force photo/Senior Airman Brett Clashman) | PM 1, 3<br>SG I, II, V | • Joint Operations |
| 13 | III. Strategic Goals (Unsourced photograph demarcates the strategy's third section. It depicts a female USAF lieutenant and a male USAF staff sergeant on duty in an unidentified operations center.) | PM 1, 3<br>SG I, III | • Air Force Operations |
| 14 | Cyber Flag 14-1 participants analyze an exercise scenario in the Red Flag building at Nellis Air Force Base, NV. Cyber Flag focuses on exercising USCYBERCOM's mission of operating and defending DoD networks across the full spectrum of operations against a realistic adversary in a virtual environment. (U.S. Air Force photo by Airman 1st Class Christopher Tam) | PM 1<br>S II | • Joint Operations<br>• Exercise & Training<br>• Air Force Operations |
| 17 | IV. Implementation Objectives (Unsourced photograph demarcates the strategy's fourth section. It depicts an unknown civilian addressing a small audience of Army military and civilians.) | N/A | N/A |

| | | | |
|---|---|---|---|
| 19 | Air Force Tech Sgt. Kevin Garner and Air Force Senior Airman David Solnok, cyber transport technicians assigned to the 354th Communications Squadron, hook cables in to the new Air Force Network router system at Eielson Air Force Base, AK. (U.S. Air Force photo by Staff Sgt. Christopher Boitz) | PM 1, 3<br>SG, I, II | • Air Force Operations |
| 21 | Soldiers monitor networks in the Cyber Mission Unit Operations Center at the Army's Cyber Center of Excellence, Fort Gordon, GA. (Photo by Michael L. Lewis) | PM 1, 3<br>SG I, II | • Army Operations |
| 22 | Members of the Ohio National Guard Computer Network Defense Team conduct cyber defense operations during exercise Cyber Shield 2015 at Camp Atterbury, IN. (Ohio National Guard photo by Staff Sgt. George Davis) | PM 1, 3<br>SG I, II | • Total Force<br>• National Guard Operations |
| 25 | The Defense Advanced Research Projects Agency (DARPA) Plan X program is a foundational cyber warfare program that is developing platforms for the Defense Department. DARPA uses advanced touch-table displays to use finger gestures and motions to advance the state of the art in cyber operations. (Photo courtesy of DARPA) | PM 3<br>SG I | • Technology |

| | | | |
|---|---|---|---|
| 27 | U.S. Navy Seaman Katelynn L. Ehrs discusses network and communication training with Royal Thai Navy sailors during a Cooperation Afloat Readiness and Training military operations symposium in Sattahip, Thailand, in 2010. (Photo by Petty Officer 2nd Class David A. Brandenburg, U.S. Navy.) | PM 3<br>SG I, IV | • International Operations<br>• Navy Operations |
| 29 | V. Managing the Strategy (Unsourced photograph demarcates the strategy's fifth section. It depicts an unknown operations center). | N/A | N/A |
| 30 | Sailors conduct an exercise at Fleet Cyber Command's headquarters in the Frank B. Rowlett Building, Fort George G. Meade, MD. This exercise features members of Fleet Cyber Command's Joint Force Headquarters-Cyber (JFHQ-C). | PM 1, 3<br>SG I, II | • Joint Operations<br>• Navy Operations |
| 33 | Conclusion (Unsourced photograph demarcates the strategy's final section. It depicts an unknown individual staring at an unknown screen). | N/A | N/A |

## ENDNOTES – APPENDIX II

1. *The DoD Cyber Strategy*, Washington, DC: U.S. Department of Defense, April, 2015.

# APPENDIX III:

# SUMMARY OF CYBERSPACE-RELATED EXCERPTS FROM THE NATIONAL MILITARY STRATEGY (JUNE 2015), THE NATIONAL SECURITY STRATEGY (FEBRUARY 2015), AND THE QUADRENNIAL DEFENSE REVIEW (MARCH 2014)[1]

| *The National Military Strategy of the United States of America 2015:* *The United States Military's Contribution to National Security* **June 2015** |
|---|
| • North Korea also has **conducted cyber attacks**, including causing major damage to a U.S. corporation. (p. 2) |
| • Of particular concern are the proliferation of ballistic missiles, precision strike technologies, unmanned systems, space and **cyber** capabilities, and weapons of mass destruction (WMD)—technologies designed to counter U.S. military advantages and curtail access to the global commons. (p. 3) |
| • They [violent extremist organizations] use improvised explosive devices (IED), suicide vests, and **tailored cyber tools** to spread terror while seeking ever more sophisticated capabilities, including WMD. (p. 4) |
| • These homeland defense partnerships are complemented by **growing investments in the cyber realm** designed to protect vital networks and infrastructure. (p. 7) |
| • Such efforts [strengthening our global network of allies and partners] are essential to maintaining regional peace and building capabilities to provide for missile defense, **cyber** security, maritime security, and disaster relief. (p. 9) |
| • Thus we are striving to interdict attack preparations abroad, defend against limited ballistic missile attacks, and protect cyber systems and physical infrastructure. Key homeland defense capabilities include resilient space-based and terrestrial indications and warning systems; an integrated intelligence collection, analysis, and dissemination architecture; a Ground-Based Interceptor force; a Cyber Mission Force; and, ready ground, air and naval forces. (p. 11) |
| • The results of these initiatives—particularly the enhanced connectivity and cybersecurity provided by the JIE [Joint Information Environment]—will provide the foundation for future interoperability. (p. 16) |
| • Important investments to counter A2/AD [anti-access/area denial], space, **cyber,** and hybrid threats include: space and terrestrial-based indications and warning systems, integrated and resilient ISR [intelligence, surveillance, and reconnaissance] platforms, strategic lift, long-range precision strike weapons, missile defense technologies, undersea systems, remotely operated vehicles and technologies, special operations forces, and the **Cyber Mission Force**, among others. (p. 16) |

| *National Security Strategy*<br>**February 2015** |
|---|
| • Escalating challenges to cybersecurity, aggression by Russia, the accelerating impacts of climate change, and the outbreak of infectious diseases all give rise to anxieties about global security. (p. i)<br>• We are shaping global standards for cybersecurity and building international capacity to disrupt and investigate cyber threats. (p. ii)<br>• The danger of disruptive and even destructive cyber-attack is growing, and the risk of another global economic slowdown remains. (p. 1)<br>• We are fortifying our critical infrastructure against all hazards, especially cyber espionage and attack. (p. 3)<br>• It also creates shared vulnerabilities, as interconnected systems and sectors are susceptible to the threats of climate change, malicious cyber activity, pandemic diseases, and transnational terrorism and crime.(p. 4)<br>• Collective action is needed to assure access to the shared spaces—cyber, space, air, and oceans—where the dangerous behaviors of some threaten us all. (p. 7)<br>• Our military will remain ready to deter and defeat threats to the homeland, including against missile, cyber, and terrorist attacks, while mitigating the effects of potential attacks and natural disasters. (p. 7)<br>• We will protect our investment in foundational capabilities like the nuclear deterrent, and we will grow our investment in crucial capabilities like cyber; space; and intelligence, surveillance, and reconnaissance. (p. 8)<br>• We are working with the owners and operators of our Nation's critical cyber and physical infrastructure across every sector—financial, energy, transportation, health, information technology, and more—to decrease vulnerabilities and increase resilience. (p. 9)<br>• The world is connected by shared spaces—cyber, space, air, and oceans—that enable the free flow of people, goods, services, and ideas. (p. 12) |

| *National Security Strategy*<br>**February 2015 (cont.)** |
|---|
| • Cybersecurity<br><br>As the birthplace of the Internet, the United States has a special responsibility to lead a networked world. Prosperity and security increasingly depend on an open, interoperable, secure, and reliable Internet. Our economy, safety, and health are linked through a networked infrastructure that is targeted by malicious government, criminal, and individual actors who try to avoid attribution. Drawing on the voluntary cybersecurity framework, we are securing federal networks and working with the private sector, civil society, and other stakeholders to strengthen the security and resilience of U.S. critical infrastructure. We will continue to work with the Congress to pursue a legislative framework that ensures high standards. We will defend ourselves, consistent with U.S. and international law, against cyber attacks and impose costs on malicious cyber actors, including through prosecution of illegal cyber activity. We will assist other countries to develop laws that enable strong action against threats that originate from their infrastructure. Globally, cybersecurity requires that long-standing norms of international behavior—to include protection of intellectual property, online freedom, and respect for civilian infrastructure—be upheld and the Internet be managed as a shared responsibility between states and the private sector with civil society and Internet users as key stakeholders. (pp. 12-13)<br><br>• On cybersecurity, we will take necessary actions to protect our businesses and defend our networks against cyber-theft of trade secrets for commercial gain whether by private actors or the Chinese government. (p. 24) |
| *Quadrennial Defense Review* **2014**<br>**March 2014** |
| • Meanwhile, modern warfare is evolving rapidly, leading to increasingly contested battlespace in the air, sea, and space domains—as well as cyberspace—in which our forces enjoyed dominance in our most recent conflicts. (p. III)<br><br>• The Joint Force must also be prepared to battle increasingly sophisticated adversaries who could employ advanced warfighting capabilities while simultaneously attempting to deny U.S. forces the advantages they currently enjoy in space and cyberspace. (p. VII)<br><br>• The Department is taking steps to ensure that progress continues in areas most critical to meeting future challenges such as full-spectrum cyberspace capabilities and where the potential for game-changing breakthroughs appears most promising. (p. VII)<br><br>• Cyber. We will invest in new and expanded cyber capabilities and forces to enhance our ability to conduct cyberspace operations and support military operations worldwide, to support Combatant Commanders as they plan and execute military missions, and to counter cyberattacks against the United States. (p. X)<br><br>• In the coming years, countries such as China will continue seeking to counter U.S. strengths using anti-access and area-denial (A2/AD) approaches and by employing other new cyber and space control technologies. (p. 6) |

| *Quadrennial Defense Review* **2014**<br><br>**March 2014 (cont.)** |
|---|
| • The United States has come to depend on cyberspace to communicate in new ways, to make and store wealth, to deliver essential services, and to perform national security functions. The importance of cyberspace to the American way of life—and to the Nation's security—makes cyberspace an attractive target for those seeking to challenge our security and economic order. Cyberspace will continue to feature increasing opportunities but also constant conflict and competition—with vulnerabilities continually being created with changes in hardware, software, network configurations, and patterns of human use. Cyber threats come from a diverse range of countries, organizations, and individuals whose activities are posing increasingly significant risks to U.S. national interests. Some threats seek to undercut the Department's near- and long-term military effectiveness by gaining unauthorized access to Department of Defense and industry networks and infrastructure on a routine basis. Further, potential adversaries are actively probing critical infrastructure throughout the United States and in partner countries, which could inflict significant damage to the global economy and create or exacerbate instability in the security environment. (p. 7)<br><br>• As the frequency and complexity of cyber threats grow, we will continue to place high priority on cyber defense and cyber capabilities. The Department of Defense will deter, and when approved by the President and directed by the Secretary of Defense, will disrupt and deny adversary cyberspace operations that threaten U.S. interests. To do so, we must be able to defend the integrity of our own networks, protect our key systems and networks, conduct effective cyber operations overseas when directed, and defend the Nation from an imminent, destructive cyberattack on vital U.S. interests. U.S. forces will abide by applicable laws, policies, and regulations that protect the privacy and civil liberties of U.S. persons. Further, the Department will operate consistent with the policy principles and legal frameworks associated with the law of war. (pp. 14-15)<br><br>• Deterring and defeating cyber threats requires a strong, multi-stakeholder coalition that enables the lawful application of the authorities, responsibilities, and capabilities resident across the U.S. Government, industry, and international allies and partners. We support the Federal Government cybersecurity team and will continue working with the Department of Homeland Security (DHS) to improve critical infrastructure cybersecurity, and with DHS and the Federal Bureau of Investigation to support law enforcement activities. The Department of Defense remains committed to working with industry and international partners as well, sharing threat information and capabilities to protect and defend U.S. critical infrastructure, including in our role as the sector-specific agency for the defense industrial base. We will ensure that international alliances and partnerships remain relevant to challenges in the threat environment by helping these partners improve their own cyber defense capabilities and mitigate shared cyber threats through mutual action. (p. 15) |

| *Quadrennial Defense Review* **2014**<br>**March 2014 (cont.)** |
|---|
| • Through both our alliances and partnerships, we are focused on enhancing our partners' capacity to address growing regional challenges in areas such as missile defense, cyber security, space resilience, maritime security, and disaster relief. (p. 17)<br>• Joint Forces will be prepared to battle increasingly sophisticated adversaries who could employ advanced warfighting capabilities while simultaneously attempting to deny U.S. forces the advantages they currently enjoy in space and cyberspace. (p. 19)<br>• Maintaining our ability to project power will also require exploiting, extending, and gaining advantages in cyber and space control technologies, as well as in unmanned systems and stand-off weapons. (p. 20)<br>• The Air Force brings capabilities critical to national security in the air, in space, and in cyberspace and will continue to improve performance in each. (p. 28)<br>• Cyber. The Department of Defense will continue to invest in new and expanded cyber capabilities, building on significant progress made in recent years in recruiting, training, and retaining cyber personnel. A centerpiece of our efforts is the development of the Department of Defense Cyber Mission Force. The Force includes Cyber Protection Forces that operate and defend the Department's networks and support military operations worldwide, Combat Mission Forces that support Combatant Commanders as they plan and execute military missions, and National Mission Forces that counter cyberattacks against the United States. The Cyber Mission Force will be manned by 2016. In addition to personnel, the Department is investing in state-of-the-art tools and infrastructure to conduct its missions. To defend its own networks, the Department is also migrating its information systems to a common, Defense-wide network infrastructure known as the Joint Information Environment (JIE). This JIE is critical to developing a more defensible network architecture and to improving network operations. The Department also will continue working with other U.S. departments and agencies, as well as with allies and partners abroad, to build their own cyber defense capabilities and mitigate shared cyber risks. (p. 33)<br>• Through both our alliances and partnerships, we are focused on enhancing our partners' capacity to address growing regional challenges in areas such as missile defense, cyber security, space resilience, maritime security, and disaster relief. (p. 17)<br>• Joint Forces will be prepared to battle increasingly sophisticated adversaries who could employ advanced warfighting capabilities while simultaneously attempting to deny U.S. forces the advantages they currently enjoy in space and cyberspace. (p. 19)<br>• Maintaining our ability to project power will also require exploiting, extending, and gaining advantages in cyber and space control technologies, as well as in unmanned systems and stand-off weapons. (p. 20)<br>• The Air Force brings capabilities critical to national security in the air, in space, and in cyberspace and will continue to improve performance in each. (p. 28) |

| *Quadrennial Defense Review* **2014**<br>**March 2014 (cont.)** |
|---|
| • Cyber. The Department of Defense will continue to invest in new and expanded cyber capabilities, building on significant progress made in recent years in recruiting, training, and retaining cyber personnel. A centerpiece of our efforts is the development of the Department of Defense Cyber Mission Force. The Force includes Cyber Protection Forces that operate and defend the Department's networks and support military operations worldwide, Combat Mission Forces that support Combatant Commanders as they plan and execute military missions, and National Mission Forces that counter cyberattacks against the United States. The Cyber Mission Force will be manned by 2016. In addition to personnel, the Department is investing in state-of-the-art tools and infrastructure to conduct its missions. To defend its own networks, the Department is also migrating its information systems to a common, Defense-wide network infrastructure known as the Joint Information Environment (JIE). This JIE is critical to developing a more defensible network architecture and to improving network operations. The Department also will continue working with other U.S. departments and agencies, as well as with allies and partners abroad, to build their own cyber defense capabilities and mitigate shared cyber risks. (p. 33) |
| • Cyber Mission Forces:<br>13 National Mission Teams (NMTs) with 8 National Support Teams (NSTs)<br>27 Combat Mission Teams (CMTs) with 17 Combat Support Teams (CSTs)<br>18 National Cyber Protection Teams (CPTs)<br>24 Service CPTs<br>26 Combatant Command and DOD Information Network CPTs (p. 41) |
| • From FY 2001 through FY 2012, the Department saw a steady increase in its civilian workforce, especially in emerging areas such as intelligence, cyber, and acquisition—areas where civilians are increasingly operators. (p. 47) |
| • Critical modernization programs would also be broken under sequestration-level cuts, creating deficiencies in the technological capability of our forces despite the requirement that they be able to respond to a wide array of threats, including substantial A2/AD and cyberspace challenges, as well as threats posed by adversaries employing innovative combinations of modern weaponry and asymmetric tactics. (pp. 55-56) |
| • The QDR prioritizes investments that support our interests and missions, with particular attention to space, cyber, situational awareness and intelligence capabilities, stand-off strike platforms and weapons, technology to counter cruise and ballistic missiles, and preservation of our superiority undersea. (p. 61) |
| • While a U.S. military response to aggression most often begins in the air or maritime domains—and in the future could begin with confrontations in the cyber and space domains—they typically include and end with some commitment of forces in the land domain. (p. 61) |

## ENDNOTES – APPENDIX III

1. 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; Barack Obama, *National Security Strategy*, Washington, DC: The White House, February 2015; Department of Defense (DoD), *Quadrennial Defense Review 2014*, Washington, DC: U.S. Government Printing Office, March 4, 2014.

**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**
**Mr. Jeffrey L. Caton**

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

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

*****

**Composition**
**Mrs. Jennifer E. Nevil**

FOR THIS AND OTHER PUBLICATIONS, VISIT US AT
**armywarcollege.edu**

ISBN 1-58487-773-1

9 781584 877738 90000 >

This Publication

SSI Website

USAWC Website