

CLEARED
For Open Publication

Aug 02, 2024

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Future Cyber Warfighting Capabilities

of the
Department of Defense

Executive Summary

May 2024



DEFENSE SCIENCE BOARD

UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.



DEFENSE SCIENCE
BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

**MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH AND
ENGINEERING**

SUBJECT: Defense Science Board (DSB) Report on Future Cyber Warfighting Capabilities of the Department of Defense

I am pleased to forward the final report of the DSB Task Force on *Future Cyber Warfighting Capabilities of the Department of Defense*.

The United States faces increasingly sophisticated and numerous threats from peer and near-peer adversaries in cyberspace. The Joint Cyber Warfighting Architecture (JCWA)—a platform made up of programs, tools, and sensors—was developed to help the Department integrate and synchronize its cyber capabilities against such threats.

Over the course of the study, the Task Force examined the effectiveness of the JCWA and its components, and subsequently identified what further capabilities are needed to achieve analytic superiority in the cyber environment. The recommendations included in this report provide actionable concepts on strengthening and managing the JCWA, attracting talent, and ensuring our analytic superiority in and through cyberspace, so that USCYBERCOM can more promptly address the ever-changing cyber threats our nation currently faces.

On behalf of the DSB, I fully endorse all the study's recommendations and urge their careful consideration and adoption.

A handwritten signature in black ink, reading "Eric D. Evans".

Dr. Eric D. Evans
Chair, Defense Science Board

THIS PAGE LEFT INTENTIONALLY BLANK



DEFENSE SCIENCE
BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

MEMORANDUM FOR THE CHAIR, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Future Cyber Warfighting Capabilities of the Department of Defense (DoD)

Attached is the final report of the congressionally directed DSB Task Force on *Future Cyber Warfighting Capabilities of the Department of Defense*. Section 1655 of the FY 2020 *National Defense Authorization Act* (P.L. 116-92) tasked the DSB to provide a technical evaluation of the Joint Cyber Warfighting Architecture (JCWA), with extra attention paid to the Unified Platform, Joint Cyber Command and Control, and the Persistent Cyber Training Environment. Additionally, Congress requested a technical evaluation of the tool development and acquisition programs of the DoD and an evaluation of operational planning and targeting by U.S. Cyber Command (USCYBERCOM).

In order to engage with, and ultimately surpass, strategic competitors and adversaries operating in cyberspace across the competition-conflict spectrum, USCYBERCOM must achieve and sustain analytic superiority: the ability to collect and ingest data, build robust performance models and analytics, and leverage these to achieve operational ends while exploiting or denying an adversary's ability to do the same. This requires a resilient, fully integrated architecture that is interoperable across the entire cyber force, to include key mission partners, and can rapidly adopt innovative changes and flexibly respond to mission requirements at all levels of competition, crisis, and conflict. While the JCWA of today represents a strong initial effort at addressing these needs, a JCWA NextGen is required to enable USCYBERCOM to better meet future cyberspace demands.

The Task Force received briefings from members of USCYBERCOM, including those involved in the development of JCWA and the Unified Platform, the Military Service Cyber Components, defense and intelligence agencies, and academic and industry partners. The Task Force also spoke with acquisition and program management professionals and found that DoD talent acquisition and retention pathways, as well as the Department's traditional acquisition processes, are optimized for conventional force development and are therefore far less effective at staffing, acquiring, and sustaining a complex cyber-heavy program like JCWA.

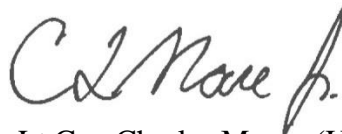
The Task Force provided eight key findings and corresponding recommendations to re-engineer JCWA and provide for its future development through new organizational structures, updated research and engineering strategies, cultural shifts within the cyber mission force, and more targeted recruitment of qualified personnel.

While implementing these recommendations will require changes in existing DoD and USCYBERCOM structures and processes, the resulting organization, policies, and frameworks

will allow JCWA NextGen to deliver all-domain, integrated effects at the speed of cyber and within the time frames combatant commanders and national leadership are operating in today. This revised approach to achieving and maintaining analytic superiority over our strategic competitors requires bold changes now to ensure the United States succeeds in deterring and providing superiority over current and future national security challenges.



Mr. Bob Giesler
Co-chair



Lt Gen Charles Moore (USAF, Ret)
Co-chair

DSB Report on Future Cyber Warfighting Capabilities of the Department of Defense—Executive Summary

Table of Contents

Executive Summary 1

Appendix A: Terms of ReferenceA-1

Appendix B: DSB Membership B-1

Appendix C: Task Force Membership C-1

Appendix D: Briefings Received D-1

THIS PAGE LEFT INTENTIONALLY BLANK

DSB Report on Future Cyber Warfighting Capabilities of the Department of Defense

Executive Summary

The Defense Science Board (DSB) was directed to establish the Task Force on *Future Cyber Warfighting Capabilities of the Department of Defense*. Section 1655 of the *Fiscal Year 2020 National Defense Authorization Act* (P.L. 116-92) tasked the DSB to provide a technical evaluation of the Joint Cyber Warfighting Architecture (JCWA), with extra attention paid to the Unified Platform, Joint Cyber Command and Control, and the Persistent Cyber Training Environment. Additionally, Congress requested a technical evaluation of the tool development and acquisition programs of the DoD and an evaluation of operational planning and targeting by U.S. Cyber Command (USCYBERCOM).

USCYBERCOM is expected to deliver outcomes in competition, crisis, and armed conflict against the most formidable adversaries of the United States, and to do so with speed, scale, agility, and precision. Without a cohesive architecture and suite of capabilities, however, USCYBERCOM, cyber operational forces, Military Service cyber components, and the Nation incur unacceptable risk to the cyber mission. The JCWA is USCYBERCOM's suite of warfighting capabilities. While it has made incremental improvements since its inception, it is not a resilient, agile, future-facing warfighting architecture. Its limited capabilities are insufficient to support USCYBERCOM assigned missions.

As improvements in automation, artificial intelligence (AI), and big data transform the current technology landscape, those with better data and analytic infrastructures will have advantages across all warfighting domains—land, air, sea, space, and cyberspace. To outpace the People's Republic of China and sustain strategic and operational advantage across the competition-conflict spectrum, USCYBERCOM must achieve and sustain analytic superiority: the ability to collect and ingest data, build robust performance models and analytics, and leverage these to achieve operational ends while exploiting or denying an adversary's ability to do the same.

Today, the DoD cannot innovate and field new cyber and related capabilities in a timely manner. JCWA came from a DoD ecosystem that is falling ever farther behind as cyber technology and capabilities continue to change. The current federated approach of JCWA, with its disparate solutions and policies for storing and managing defensive and offensive cyberspace data across siloed systems, has not and cannot deliver analytic superiority. Additionally, talent acquisition and retention as currently practiced in DoD is a major limiting factor, and acquisition processes optimized for conventional force development are unable to move at cyber-relevant speed. Even if talent and conventional acquisition processes were configured to support JCWA, the lack of prioritization and stabilization of strategic and operational-level targets undermines the strategic promise of JCWA. Overcoming these limitations is essential for JCWA to deliver all-domain integrated effects that are synchronized in timing and tempo, as required by combatant commanders and national leadership. DoD and USCYBERCOM must drive bold, not incremental, changes today so that the Nation succeeds over the next decade.

THIS PAGE LEFT INTENTIONALLY BLANK

Appendix A: Terms of Reference



RESEARCH
AND ENGINEERING

THE UNDER SECRETARY OF DEFENSE

3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

21 Jan 2021

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Task Force on Future Cyber Warfighting Capabilities of the Department of Defense

Section 1655 of the National Defense Authorization Act for Fiscal Year (FY) 2020 (Public Law 116-92) requires the Secretary of Defense direct the Defense Science Board (DSB) to conduct a study on future cyber warfighting capabilities. I am tasking the DSB, through the establishment of the Task Force on Future Cyber Warfighting Capabilities of the Department of Defense, to undertake this study.

The Joint Cyber Warfighting Architecture (JCWA) was developed to integrate the collective strengths of Department of Defense cyberspace capabilities to build the 21st century statecraft necessary to understand, contest, and impose high costs on an adversary that is rapidly evolving. JCWA provides the organizing architectural framework for this integration – defining, synchronizing, and deconflicting the holistic set of cyberspace resources to function as a cohesive whole rather than disparate parts. Each of the major functional areas of the JCWA will be tightly integrated and automated to allow United States Cyber Command (USCYBERCOM) to rapidly shift the entire Cyberspace Enterprise in a coordinated and consistent manner to maneuver at the scale and scope of Combatant Command objectives.

Over the past 10 years, our adversaries have defined the space we are operating in, conducting actions that have largely been uncontested – stealing our intellectual property, leveraging stolen Personally Identifiable Information of American citizens, and attempting to interfere in our Democratic processes. Our responses were reactive, focused on shoring up defenses against exploitation while the adversaries had already moved on to far more impactful, disruptive, and destructive actions.

Persistent engagement must be the Nation's foundational approach to taking on near-peer adversaries. We must bring the cyber fight to the adversary by impacting their actions, imposing costs for those activities, and sending a message that we will contest their attempts to disrupt and destroy our national security and democracy. Taking on near-peer adversaries, and ultimately getting ahead of them, requires USCYBERCOM to bring to bear all cyberspace resources at any time in a cooperative engagement. All opportunities afforded by integrated offensive, defensive, and Department of Defense Information Network operations must be leveraged to learn about the adversary, assess risk, and decide on a coordinated response approach. When fully fielded by the end of FY 2024, the JCWA will enable USCYBERCOM to orchestrate planning and execution at the pace of cyber by automatically shifting and turning resources as an interoperable system of systems. This study will focus on the following areas as outlined in Section 1655 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116-92):

CLEARED
For Open Publication

Feb 18, 2021

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

- A technical evaluation of the Joint Cyber Warfighting Architecture of the Department, especially the Unified Platform, Joint Cyber Command and Control, and Persistent Cyber Training Environment, including with respect to the following:
 1. The suitability of the requirements and, as relevant, the delivered capability of such architecture to modern cyber warfighting.
 2. Such requirements or capabilities as may be absent or underemphasized in such architecture.
 3. The speed of development and acquisition as compared to mission need.
 4. Identification of potential duplication of efforts among the programs and concepts evaluated.
 5. The coherence of such architecture with the National Mission Teams and Combat Mission Teams of the Cyber Mission Force, as constituted and organized on the day before the date of the enactment of this Act.
 6. The coherence of such architecture with the Cyber Protection Teams of the Cyber Mission Force and the cybersecurity service providers of the Department, as constituted and organized on the day before the date of the enactment of this Act.
 7. The coherence of such architecture with the concepts of persistent engagement and defending forward as incorporated in the 2018 Department of Defense Cyber Strategy, including with respect to operational concepts such as consistent spy-on-spy engagement, securing adversary operating pictures, and preemptively feeding indicators and warning to defensive operators.

- A technical evaluation of the tool development and acquisition programs of the Department, including with respect to the following:
 1. The suitability of planned tool suite and cyber armory constructs of the USCYBERCOM to modern cyber warfighting.
 2. The speed of development and acquisition as compared to mission need.
 3. The resourcing and effectiveness of the internal tool development of the USCYBERCOM as compared to the tool development of the National Security Agency.
 4. The resourcing and effectiveness of the internal tool development of the USCYBERCOM as compared to its acquisition.
 5. The coherence of such programs with the concepts of persistent engagement and defending forward as incorporated in the 2018 Department of Defense Cyber Strategy, including with respect to operational concepts such as consistent spy-on-spy engagement, securing adversary operating pictures, and preemptively feeding indicators and warning to defensive operators.

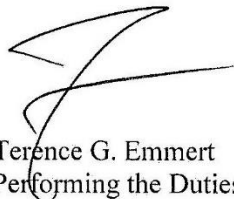
- An evaluation of the operational planning and targeting of the USCYBERCOM, including support for regional combatant commands, and suitability for modern cyber warfighting.

- Development of such recommendations as the Board may have for legislative or administrative action relating to the future cyber warfighting capabilities of the Department.

The DSB Study’s findings, observations, and recommendations will be presented to the full DSB for its thorough, open discussion and deliberation at a properly noticed and public meeting subject to Government In Sunshine Act requirements. The Under Secretary of Defense for Research and Engineering (USD(R&E)) will serve as the Department of Defense decision-maker for the matter under consideration and will, as such, take into consideration other stakeholders identified by the study’s findings and recommendations. The nominal start date of the study period will be within 30 days of the initial appointment of its members, and Section 1655 of the National Defense Authorization Act requires a report be submitted no later than November 1, 2021. In no event, will the duration of the study exceed 24 months from the start date.

The study members are granted access to those Department of Defense officials and data necessary for the appropriate conduct of their studies. As such, the Office of the Secretary of Defense and Component Heads are requested to cooperate and promptly facilitate requests by DSB staff regarding access to relevant personnel and information deemed necessary, as directed by paragraphs 5.1.8. and 5.3.4. of Department of Defense Instruction 5105.04, “Department of Defense Federal Advisory Committee Management Program,” and in conformance with applicable security classifications.

The DSB and the DSB Study will operate in accordance with the provisions of the Federal Advisory Committee Act, the Government in the Sunshine Act, and other applicable federal statutes, regulations, and policy.” Individual DSB and DSB Study members do not have the authority to make decisions or recommendations on behalf of the DSB nor report directly to any Federal representative. The members of the task group and the Board are subject to certain Federal ethics laws, including 18 U.S. Code §208, governing conflicts of interest, and the Standards of Ethical Conduct regulations in 5 C.F.R., Part 2635).



Terence G. Emmert
Performing the Duties of the
Under Secretary of Defense
for Research and Engineering

Appendix B: DSB Membership

Dr. Eric Evans, Chair	Dr. John Manfredelli
Mr. Michael Appelbaum	Dr. Katherine McGrady
Dr. Jennifer Bernhard	Dr. James Miller
Dr. Alison Brown	Dr. DJ Patil
Dr. Kimberly Budil	Dr. Gary Polansky
Mr. James Carlini	Dr. Sanjay Raman
Dr. Tomás Díaz de la Rubia	Dr. David Relman
Mr. Fred Dixon	Gen Paul Selva, USAF (ret.)
Adm William Fallon, USN (ret.)	Dr. Nashlie Sephus
Ms. Laetitia de Cayeux	Dr. Reshma Shetty
Mr. Robert Giesler	Dr. Alfred Spector
Dr. Johney Green	Dr. Vincent Tang
Dr. Robert Grossman	Dr. Dorota Temple
Dr. Daniel Hastings	Dr. Jan Tighe
Dr. Ayanna Howard	Dr. Bradford Tousley
Dr. Evelyn Hu	Dr. David Van Wie
Hon. Shirley Ann Jackson	Ms. Mandy Vaughn
Dr. Ashanti Johnson	Dr. Dinesh Verma
Dr. Paul Kaminski	Dr. Steven Walker
Dr. Ann Karagozian	Dr. Robert Wisnieff

Appendix C: Task Force Membership

Task Force Co-Chairs

Mr. Bob Giesler
Lt Gen Charles Moore (USAF, ret)

Task Force Members

Mr. Bob Butler
Mr. Chris Day
Dr. Donald Duncan
Mr. Glenn Gaffney
Dr. Bob Grossman
Ms. Priscilla Guthrie
Ms. Melissa Hathaway
Mr. Sam Kinch
Mr. Richard Ledgett
Dr. John Manfredelli
Dr. James Miller
Hon. Arthur Money
Mr. David Ross
Mr. Mark Russell
VADM TJ White (USN, ret)
Dr. Bob Wisnieff

Executive Secretary

Ms. Holly Baroody, USCYBERCOM

Government Advisors

Mr. Ian Crone (DARPA)
RDML Steve Donald (U.S. Fleet Cyber Command)
Dr. Emily Goldman (USCYBERCOM)
Lt Col Ben Heruska (USAF)
Mr. Carl Martin (HAF A2/6)
Dr. Chris Mineo (USCYBERCOM)
Mr. Mark “Al” Mollenkopf (USA)
Mr. Vinh Nguyen (NSA)
Lt Col John Priestly (USAF)
Mr. Steven Rehn (USA)
COL Ben Ring (USA)
Dr. Craig Snyder (NSA)
Ms. Katherine Sutton (USCYBERCOM)
Mr. Arthur Tellis (CAPE)

DSB Secretariat

Ms. Elizabeth Kowalski, DSB Designated Federal Officer (DFO)
Mr. Kevin Doxey, DSB DFO (*former*)

SAIC Support Staff

Ms. Allison Holbert
Ms. Kathryn Hein

Appendix D: Briefings Received

Meeting 1 (22-23 Feb 2023)

USCYBERCOM Introduction	DoD Cyber Strategy 2023
USCYBERCOM J3	DASD for Cyber Policy
Evolution of Threat	Authorities Laydown
Cyber National Mission Force (CNMF)	USCYBERCOM
Campaigning to Set the Theater	
Sixteenth Air Force (Air Forces Cyber)	

Meeting 2 (15-16 Mar 2023)

<i>USCYBERCOM Briefings:</i>	
Acquisitions Overview (with OUSD(A&S))	Campaign Against PRC Aggression: Cyber +
Enhanced Budget Control	Space
China Threat Brief	CNMF
Campaign Plan	JTF-ARES
Cyber Combat Power against China	Information Operations

Meeting 3 (11-12 Apr 2023)

<i>USCYBERCOM J9 Briefings:</i>	
JCWA Overview	
Unified Platform (UP) Joint Cyber Command and Control (JCC2) Overview Briefing	
Joint Common Access Platform (JCAP)	

Meeting 4 (9-10 May 2023)

<i>NSA Briefings:</i>	
Next-Gen Cyber Threat Intelligence	
AI Analytics in CNE Operations	
NSA Next Generation Mission Platform	
Combat Support Modernization Overview	
NSA Data Architecture, Standards, and ICAM	

Meeting 5 (14-15 June 2023)

Counterintelligence Threats <i>USCYBERCOM</i>	Security and Defense Strategies – NCDOC <i>U.S. Navy</i>
The Secure, Operate and Defend the DODIN Mission Area within context of Full Spectrum Cyberspace Operations <i>JFHQ-DODIN</i>	New CYBERCOM J9 Director/CAE Introduction and Perspective <i>USCYBERCOM J9</i>
Security and Defense Strategies – RCC <i>U.S. Army</i>	The Air Force Information Network Security Operations Center (AFIN-SOC), 33 Cyber Operations Squadron <i>U.S. Air Force</i>

Meeting 6 (19-20 July 2023)

Rapid Cyber Development Network (RCDN) Portfolio <i>U.S. Army, Program Executive Office for Intelligence, Electronic Warfare and Sensors, RCDN Team</i>	Constellation <i>DARPA</i>
Joint Cyber Weapons (JCW) – Tool Development <i>USCYBERCOM</i>	Project JANUS <i>DARPA</i>
DARPA – Cyber Operations <i>DARPA</i>	Strategic Capabilities Office (SCO) – Cyber Portfolio Update <i>SCO</i>
	Persistent Cyber Training Environment – 2023 and Beyond <i>USCYBERCOM</i>

Meeting 7 (22-23 Aug 2023)

StarLink Overview <i>SPACEX</i>	LLMs and Cyber Security <i>OpenAI</i>
Threat Actor Usage of Artificial Intelligence <i>Microsoft Threat Intelligence Center (MSTIC)</i>	Findability, Accessibility, Interoperability, and Reusability (FAIR) Data at Scale <i>Advanced Research Projects Agency for Health (ARPA-H)</i>
Intrusion-Tolerant Networks <i>Distributed Systems and Networks (DSN) Lab, John Hopkins University (JHU)</i>	Generative AI and Security <i>Amazon Web Services (AWS)</i>

Meeting 8 (19-20 Sept 2023)

DoD Chief Information Officer (CIO)
Perspective
DoD CIO

5-Year AI/ML USCYBERCOM Roadmap
*USCYBERCOM, Massachusetts Institute of
Technology – Lincoln Laboratory (MIT-LL)*

Updates on AI
TF Advisor

Deputy Commander Perspective
USCYBERCOM

Meeting 9 (18-19 Oct 2023)

UK Workforce Strategy
United Kingdom Delegation

Perspective from USCYBERCOM on Cyber
Priorities, Challenges, and Concerns
USCYBERCOM

INDOPACOM – Cyber Priorities, Challenges,
and Concerns
USINDOPACOM

Use of the National Guard in Cyber Operations
National Guard, USCYBERCOM

THIS PAGE LEFT INTENTIONALLY BLANK

