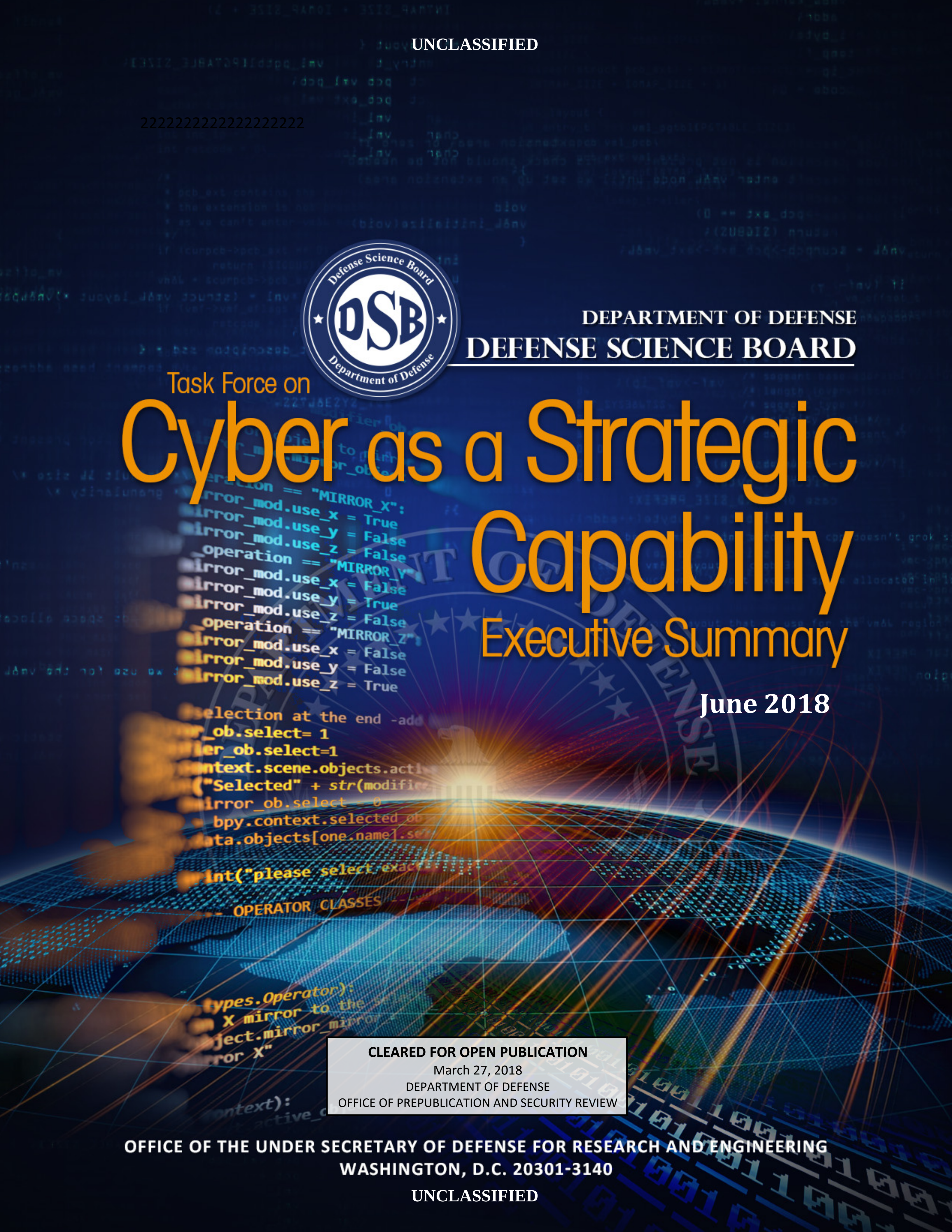
2222222222222222222



DEPARTMENT OF DEFENSE

DEFENSE SCIENCE BOARD

Task Force on Cyber as a Strategic Capability

Executive Summary

June 2018

CLEARED FOR OPEN PUBLICATION
March 27, 2018
DEPARTMENT OF DEFENSE
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING
WASHINGTON, D.C. 20301-3140

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.

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

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR THE UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Cyber as a Strategic Capability – Executive Summary

I am pleased to forward the final report executive summary of the Defense Science Board Task Force on Cyber as a Strategic Capability, co-chaired by Mr. Chris Inglis and Mr. James Gosler.

This study is one in a long line of cyber-related studies, but it is the first to specifically address how cyber capabilities can and should be used to pursue strategic objectives and protect strategic interests. The United States is currently years behind its rivals in cyberspace, both conceptually and operationally. The findings of this study illuminate the scope of the problem. The recommendations proposed in this report will, if implemented, create the necessary conditions for the Department of Defense to possess cyber as a strategic capability.

The asymmetry between the United States and its rivals in the cyber domain contributes to escalation and leaves the United States increasingly vulnerable to theft, sabotage, espionage, and subversion. Remedying this strategic inadequacy must be a priority for DoD military and civilian leadership over the coming years.

I fully endorse all of the Task Force's recommendations contained in this report, and urge their careful consideration and soonest adoption.

Craig Fields
Chairman, Defense Science Board

Attachment:
As stated

THIS PAGE LEFT INTENTIONALLY BLANK

DEFENSE SCIENCE BOARD

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

MEMORANDUM FOR THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Cyber as a Strategic Capability – Executive Summary

The final report executive summary of the DSB Task Force on Cyber as a Strategic Capability is attached.

The Cyber as a Strategic Capability Task Force examined the threats and opportunities posed by the employment of cyber capabilities to pursue strategic objectives. Previous DSB studies have addressed cyber vulnerabilities to specific systems and the strengthening of deterrence against cyber attacks; however, they did not examine the strategic-level implications of information operations (IO) and information warfare (IW) pursued by U.S. adversaries, nor did they consider how the United States might benefit from using cyber capabilities to achieve strategic effects and outcomes. Over the course of the year-long study, the Task Force absorbed multiple briefings from a wide array of experts and practitioners. The findings and recommendations of the Task Force are detailed in this report.

The Task Force determined that the Department of Defense must move beyond tactical applications for cyber and realize cyber as a strategic capability. To accomplish this, the USG and DoD need to revamp cyber strategy, to ensure we are not self-limiting or focused on only tactical outcomes. The adoption of a comprehensive cyber strategy oriented towards strategic effects and outcomes is essential for changing the current culture that often slows down or halts cyber options.

Stronger defenses in both the public and private sectors will be necessary to ensure offensive options are routinely considered as part of the trade space. The DoD must view cyber offense and defense as interdependent.

Cyber operators will need more experience in actually undertaking cyber operations and greater readiness before an effective and credible strategic cyber capability is achieved. At present, cyber operators do not get the exposure they need to make them proficient at their craft. Additional training can help, but there is no substitute for actual contact in the field. Allowing cyber operators to “see action” will also help stem the brain drain from the government to the private sector as cyber operators take their training they receive from the USG and seek more lucrative opportunities elsewhere.

The DoD must integrate its cyber strategy with the rest of the USG, creating a whole-of-nation approach that will align all factions of the USG with the same strategic goals. This includes closer cooperation and integration with the private sector and the defense contractors who own a large share of critical infrastructure and perform important functions for the government.

Lastly, the current policies that guide and govern cyber operations must be revised to incentivize the development of desired skills and the execution of effective cyber actions that promote U.S. strategic objectives. The authorization practices of cyber action currently impede (or at least this is the perception among practitioners) the USG's ability to execute cyber operations in a useful timeframe or manner. The United States will need to align our policies to reflect the constant contact nature of cyberspace.

If the DoD fails to harness cyber as a strategic capability, the United States will not be able to maintain its current global posture. The U.S. homeland and the military will be left unacceptably vulnerable to adversary coercion and meddling. It is our sincere hope that the recommendations provided in this report are implemented with the seriousness of purpose that they deserve.

Mr. Chris Inglis
Co-Chair

Mr. James Gosler
Co-Chair

Table of Contents

THIS PAGE LEFT INTENTIONALLY BLANK

DSB Task Force on Cyber as a Strategic Capability
Executive Summary

During the writing of this report, Dr. James Babcock, a distinguished member of this Task Force, passed away. The members would like to dedicate this report in Jim's memory. His selfless service to our Nation spanned many decades and his contributions were of high impact. His friendship and wise counsel will be deeply missed. He was a truly great American.

Introduction

The Defense Science Board (DSB) Task Force on Cyber as a Strategic Capability was established to assess how cyber capabilities are being used by U.S. competitors and adversaries to achieve strategic effects, and provide recommendations for how the United States can develop and employ a strategic cyber capability of our own. While the United States retains significant advantages in most military domains, the United States has fallen behind its competitors in the cyber domain, both conceptually and operationally. The threat that adversary nations and non-state actors pose is not a hypothetical one – the United States has witnessed the effectiveness of strategic cyber operations, both against other countries and against the United States itself, on multiple occasions. Given the degree to which U.S. civilian and military infrastructure depend on cyber-enabled technologies, U.S. risks in the cyber domain present a serious and growing challenge to the Nation's ability to defend itself at home and advance its interests abroad.

The DSB report on Cyber as a Strategic Capability concludes that U.S. strategic competitors and other states possess effective strategic cyber capabilities and doctrine. These may, in certain scenarios, stress U.S. ability to deter adversary cyber aggression. The study, therefore, examines the laws, governance structures, and culture that impair the United States from fully possessing strategic cyber capabilities. The United States must act quickly to enable strategic cyber as an option in the spectrum of effects. Doing so will help ensure the United States maintains its current global posture and the U.S. homeland is protected against adversary blackmail and aggression.

Scope of Study

From October 2016 to September 2017, the Task Force held monthly meetings to deliberate and receive briefings about the cyber threat landscape. Experts and practitioners from a wide array of backgrounds, including the DoD, the Intelligence Community, other U.S. government agencies, think tanks, academia, and the private sector shared their insights and information.

The breadth of knowledge and expertise shared with the Task Force throughout the study ensured that the Task Force made its findings based upon the most complete and accurate information available. Those findings, and their associated recommendations, are detailed in the Task Force's classified report. The Task Force believes that if these recommendations are acted upon, the United States will be able to leverage cyberspace to accomplish strategic objectives, defend U.S.

vital interests dependent upon digital infrastructure (i.e., cyberspace), and defend against adversary actions in cyberspace.

A classified full version of the report on Cyber as a Strategic Capability can be obtained through the DSB office.

Findings and Recommendations

The Task Force deliberations resulted in the following five overarching findings.

Finding 1: Current cyber strategy is stalled, self-limiting, and focused on tactical outcomes. The DoD must build and adopt a comprehensive cyber strategy.

Finding 2: Defense is a necessary foundation for offense. Effective offensive cyber capability depends on defensive assurance and resilience of key military and homeland systems.

Finding 3: Cyber forces, including leadership, require more experience and readiness. Sustained experience in operations is essential to readiness of U.S. cyber capability.

Finding 4: The DoD must integrate cyber into a whole-of-government approach. Cyber capabilities developed by DoD must be integrated into a whole-of-government approach, and integrated with private sector and coalition efforts to most effectively defend our collective interests.

Finding 5: Current policies often thwart cyber capability. Policy guidance is both essential and currently at odds with effective use of cyber capabilities.

Based on these findings, the Task Force has put forward the following recommendations for adoption by the DoD.

Recommendation 1:

- The Secretary of Defense direct the Commander of U.S. Cyber Command (USCYBERCOM), working with the Assistant Secretary of Defense for Homeland Defense and Global Security, to develop a comprehensive cyber strategy to be widely adopted and operationalized. This strategy will contain the following components:

  - *Tactics* that are actionable, reliable, and precise on short notice (Commander USCYBERCOM action);

  - *Strategic effects* as measured by direct and timely impact to digital systems of interest (Commander USCYBERCOM action); and

  - *Strategic outcomes* as measured in terms of the advancement of U.S. objectives (Secretary of Defense articulation through the interagency).

Recommendation 2:

- The Secretary of Defense and the Chairman of the Joint Chiefs of Staff, working with the Under Secretary of Defense for Intelligence and the Under Secretary of Defense for Policy, direct the Combatant Commanders, working with the Under Secretary of Defense for Intelligence, to compile a prioritized list of targets that can be held at risk with cyber capabilities.

Recommendation 3:

- The Secretary of Defense, through the National Security Council, working with the Department of Homeland Security's Assistant Secretary for Cybersecurity and Communications, direct the Commander USCYBERCOM lead and expand the DoD support to the protection of private sector and critical infrastructure in advance of contingency and crisis:

  - promote DoD-sponsored institutions to share unclassified/classified situational awareness information that informs DoD actions in the conduct of its authorized missions;

  - deem DoD-derived vulnerability information of private sector infrastructure shareable to the appropriate private sector entities;

  - deem DoD-derived threat information (e.g., adversarial targeting information) shareable to the appropriate cross-U.S. and private sector entities (important information should not be held close by just a few and unavailable to those who need it most); and

  - critical infrastructure providers should be offered direct monitoring services and tools by DoD assets.

Recommendation 4:

- The Secretary of Defense direct the National Security Agency to establish an independent Strategic Cyber Security Program to perform cyber red teaming on DoD critical systems and critical infrastructure. This recommendation is consistent with *Recommendation 2.2* of the DSB Task Force Report on Cyber Deterrence.

  - The Strategic Cyber Security Program analysis should include both current critical systems as well as future acquisitions before the DoD invests in/employs new capabilities.

  - The Secretary of Defense should receive quarterly updates on identified challenges, plans, and progress.

Recommendation 5:

- The Commander USCYBERCOM direct and ensure development of a portfolio of cyber military capabilities/effects, focused on adversary military targets, which:

    - includes the development of infrastructure and tools to support the Cyber Mission Forces;

    - ensures operational experience and an exquisitely skilled workforce; and

    - creates agility to respond to dynamic situations/opportunities.

Recommendation 6:

- The Commander USCYBERCOM develop a deliberate plan and acquisition strategy that leverages existing infrastructure and identifies where new infrastructure and tools are required.

Recommendation 7:

- The Commander USCYBERCOM, with the advocacy of the Secretary of Defense within the National Security Council, develop a plan for joint training and exercises—and ultimate operations—with and alongside other U.S. organizations, operating as joint teams.

    - Operating deliberately "joint," not on an ad hoc basis, will improve effectiveness and efficiency.

Recommendation 8:

- The Secretary of Defense direct the Chiefs of Staff of the Army and the Air Force, the Chief of Naval Operations, and the Commandant of the Marine Corps to direct their personnel staffs (i.e., the "1s") to treat the cyber mission career field as a national security priority, where promotion boards understand the cyber mission as a priority and facilitate recruitment, retention, and career-long professional development in cyber expertise.

Recommendation 9:

- The Commander USCYBERCOM establish and expand professional military education opportunities, at all levels, to allow military personnel to work in cyber-related private sector positions. Offer greater commercial exchange opportunities to allow both military and civilian personnel "commercial tours" to improve skills and operational understanding.

Recommendation 10:

- The Secretary of Defense lead, through the National Security Council, the creation of a coordination and collaboration authority or entity that coordinates national cyber priorities and private-public collaboration across the spectrum of peacetime, contingency, and crisis:

  - USCYBERCOM should play a key and unique role within the proposed entity;
  - an ultimate goal must be to integrate the private sector/industry into this collaborative enterprise; and
  - UK and Israeli cyber entities can serve as models for U.S. efforts to build private-public sector collaboration, yielding mutually supporting collaboration amongst government, industry, and academia in the design, operation, and defense of U.S. critical infrastructure.

Recommendation 11:

- The Under Secretary of Defense for Policy, in coordination with the Director of National Intelligence, the Department of Homeland Security's Assistant Secretary for the Office of Cybersecurity and Communications, counterparts in the Department of Justice, the Chairman of the Joint Chiefs of Staff, and the Commander USCYBERCOM, lead the effort within the National Security Council to codify new policy and establish a new U.S. policy directive.

  - This new policy framework would replace existing Presidential Policy Directives 20 and 41 guidance and provide guidance on the use of cyber capabilities that acknowledges we are always at some level of conflict or competition in cyberspace. The framework would clearly address the DoD's role in protecting critical infrastructure (especially in those cases where military missions are dependent), identifying actions DoD may take under standing rules of engagement, and ensure decision making is streamlined and, where possible, delegated to Commander USCYBERCOM.

  - Furthermore, a new operations approval framework should be developed to incorporate the concept of a standing small cadre of National Security Council and interagency "approvers" to streamline decision making around both offensive and defensive cyber operations abroad. This cadre should utilize specific techniques to proactively gather and manage policy precedents; the current approval process is too long and bureaucratic.

Recommendation 12:

- The Secretary of Defense authorize USCYBERCOM leadership to engage early with the interagency to brainstorm proposals before options or proposals reach the Principals Committee or the Deputies Committee or the level within the interagency. Nothing is prohibiting this action from taking place now, except culture.

Recommendation 13:

- The Director of the Office of Net Assessment in the Office of the Secretary of Defense, in coordination with the Under Secretary of Defense for Policy, the Director of National Intelligence, the Chairman of the Joint Chiefs of Staff, and the Commander USCYBERCOM, establish a continuous strategic net assessment process to support U.S. campaign planning against strategic competitors, adversaries, and rogue regimes. This process should leverage the Intelligence Community, industry, and allied partner capabilities and incorporate persistent red team assessment activity for measuring our effectiveness in cyberspace.

Recommendation 14:

- The Deputy Secretary of Defense work with counterparts at the Department of Homeland Security and the Office of the Director of National Intelligence to expand the scope of the Enduring Security Framework to better promote private sector collaboration for protecting and promoting national interests in cyberspace.

  - This expanded Enduring Security Framework charter should include representatives from other critical infrastructure sectors such as energy, telecommunications, and transportation where defense and national security have clear dependencies and where threats from competitors and adversaries can be reasonably anticipated, if not already observed.

  - This expanded charter should also take into account the evolution of industry partner roles to support the synchronized U.S. campaign planning, standards development, and information sharing.

Recommendation 15:

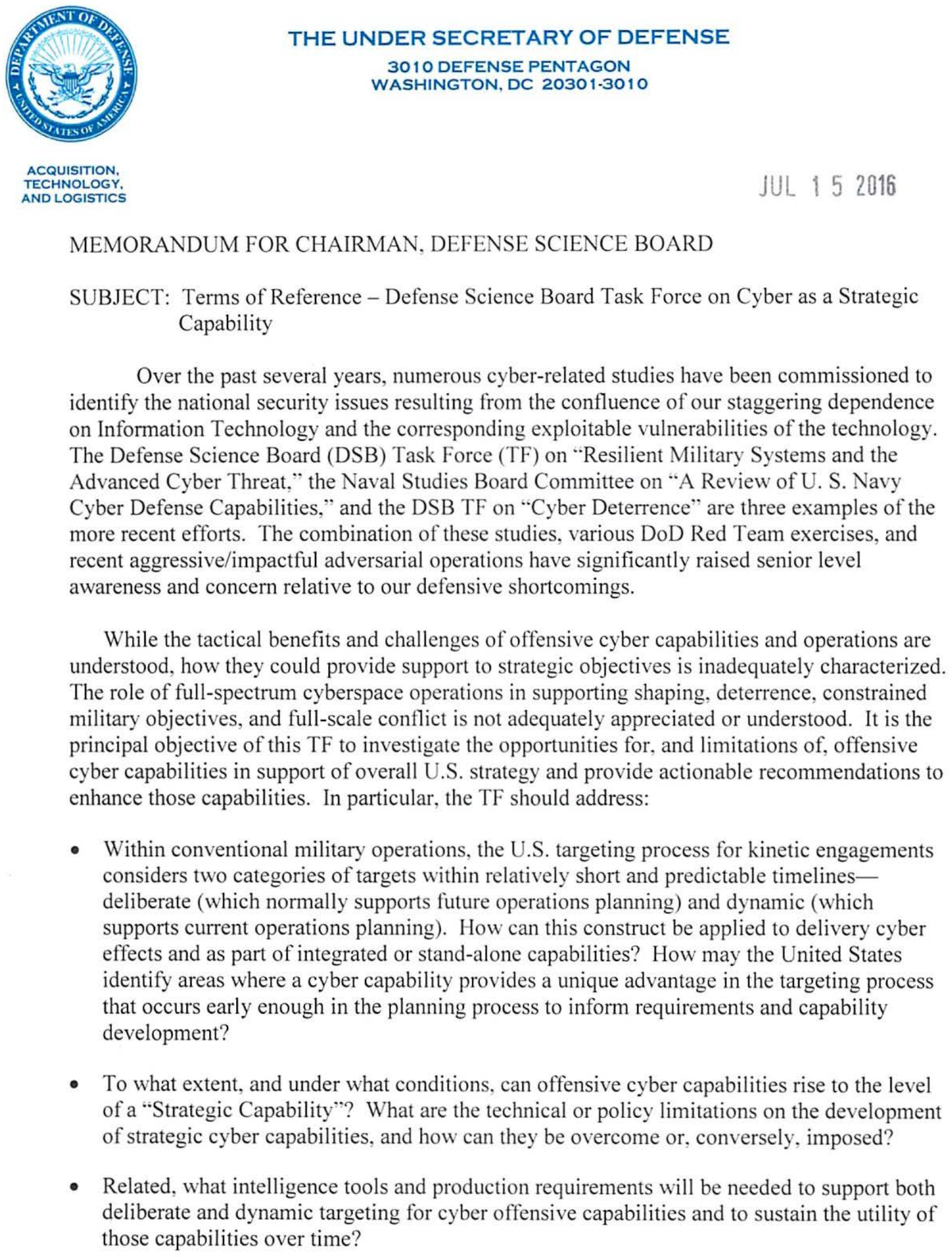
- The Secretary of Defense (Office of General Counsel), in coordination with the Under Secretary of Defense for Policy, the responsible leadership in the Department of Homeland Security, Department of Justice, the Joint Staff, and USCYBERCOM, review existing statutes governing DoD and U.S. action in cyberspace (e.g., Electronic Communications Privacy Act and Computer Fraud and Abuse Act), and update or draft replacement language to enable continuous offensive and defensive actions for protecting and promoting national interests in cyberspace.

  - Specifically, this task should include drafting legal statutes for enabling anticipatory defense, active defense, and other countermeasures in cyberspace in accordance with national and international law, and providing liability protection and other legal incentives for robust private sector participation to support national interests in cyberspace.

Recommendation 16:

- The Under Secretary of Defense for Policy, in coordination with counterparts in the Departments of State, Commerce, and Homeland Security, lead bilateral and multilateral activities to support the development and operation of an International Cyber Stability Board of like-minded nations and industry partners for the purpose of protecting cross-border critical infrastructure, creating common standards, and enabling coalition campaigning.

Appendix A: Terms of Reference



THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY,
AND LOGISTICS

JUL 15 2016

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Task Force on Cyber as a Strategic Capability

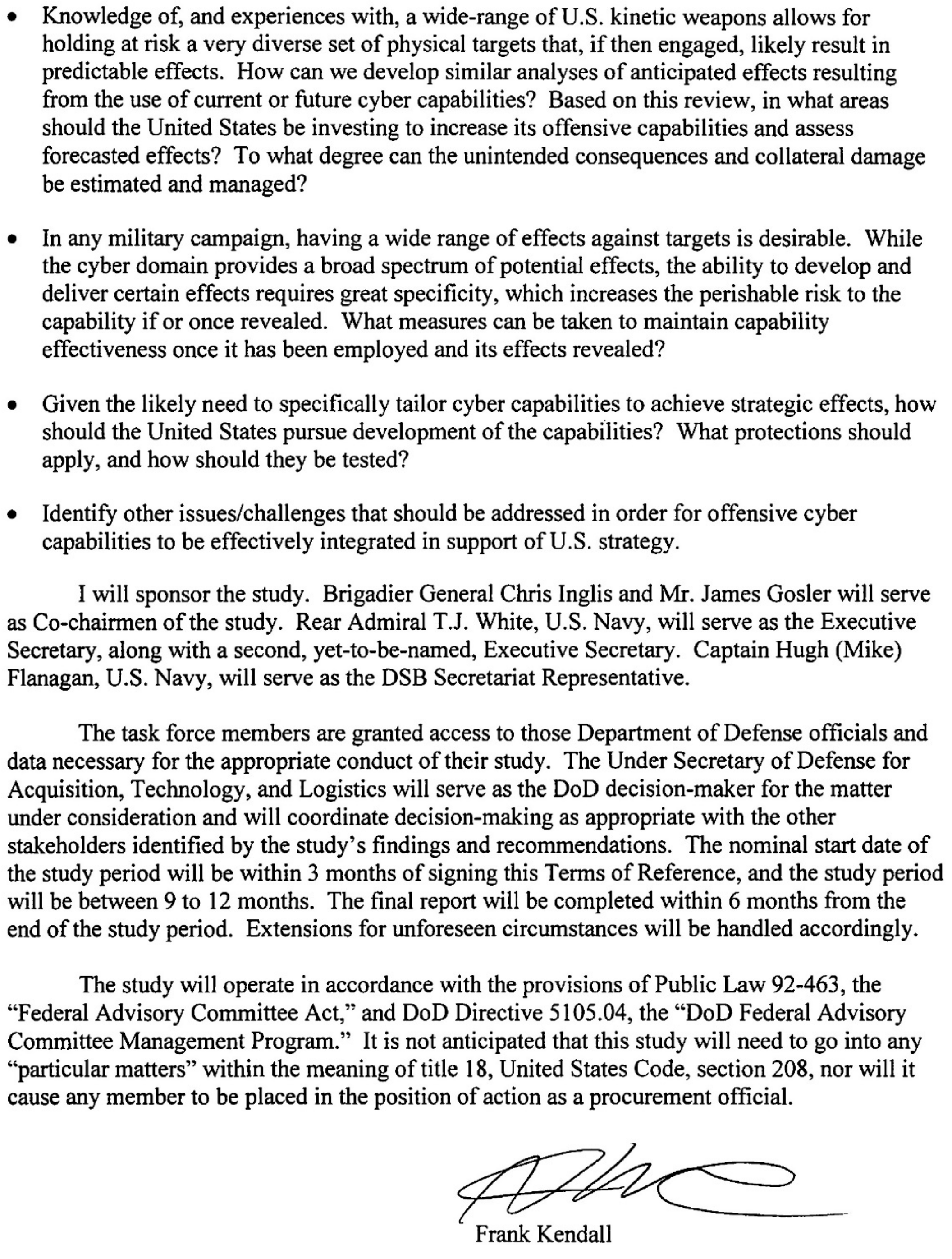
Over the past several years, numerous cyber-related studies have been commissioned to identify the national security issues resulting from the confluence of our staggering dependence on Information Technology and the corresponding exploitable vulnerabilities of the technology. The Defense Science Board (DSB) Task Force (TF) on "Resilient Military Systems and the Advanced Cyber Threat," the Naval Studies Board Committee on "A Review of U. S. Navy Cyber Defense Capabilities," and the DSB TF on "Cyber Deterrence" are three examples of the more recent efforts. The combination of these studies, various DoD Red Team exercises, and recent aggressive/impactful adversarial operations have significantly raised senior level awareness and concern relative to our defensive shortcomings.

While the tactical benefits and challenges of offensive cyber capabilities and operations are understood, how they could provide support to strategic objectives is inadequately characterized. The role of full-spectrum cyberspace operations in supporting shaping, deterrence, constrained military objectives, and full-scale conflict is not adequately appreciated or understood. It is the principal objective of this TF to investigate the opportunities for, and limitations of, offensive cyber capabilities in support of overall U.S. strategy and provide actionable recommendations to enhance those capabilities. In particular, the TF should address:

- Within conventional military operations, the U.S. targeting process for kinetic engagements considers two categories of targets within relatively short and predictable timelines—deliberate (which normally supports future operations planning) and dynamic (which supports current operations planning). How can this construct be applied to delivery cyber effects and as part of integrated or stand-alone capabilities? How may the United States identify areas where a cyber capability provides a unique advantage in the targeting process that occurs early enough in the planning process to inform requirements and capability development?

- To what extent, and under what conditions, can offensive cyber capabilities rise to the level of a "Strategic Capability"? What are the technical or policy limitations on the development of strategic cyber capabilities, and how can they be overcome or, conversely, imposed?

- Related, what intelligence tools and production requirements will be needed to support both deliberate and dynamic targeting for cyber offensive capabilities and to sustain the utility of those capabilities over time?



- Knowledge of, and experiences with, a wide-range of U.S. kinetic weapons allows for holding at risk a very diverse set of physical targets that, if then engaged, likely result in predictable effects. How can we develop similar analyses of anticipated effects resulting from the use of current or future cyber capabilities? Based on this review, in what areas should the United States be investing to increase its offensive capabilities and assess forecasted effects? To what degree can the unintended consequences and collateral damage be estimated and managed?

- In any military campaign, having a wide range of effects against targets is desirable. While the cyber domain provides a broad spectrum of potential effects, the ability to develop and deliver certain effects requires great specificity, which increases the perishable risk to the capability if or once revealed. What measures can be taken to maintain capability effectiveness once it has been employed and its effects revealed?

- Given the likely need to specifically tailor cyber capabilities to achieve strategic effects, how should the United States pursue development of the capabilities? What protections should apply, and how should they be tested?

- Identify other issues/challenges that should be addressed in order for offensive cyber capabilities to be effectively integrated in support of U.S. strategy.

I will sponsor the study. Brigadier General Chris Inglis and Mr. James Gosler will serve as Co-chairmen of the study. Rear Admiral T.J. White, U.S. Navy, will serve as the Executive Secretary, along with a second, yet-to-be-named, Executive Secretary. Captain Hugh (Mike) Flanagan, U.S. Navy, will serve as the DSB Secretariat Representative.

The task force members are granted access to those Department of Defense officials and data necessary for the appropriate conduct of their study. The Under Secretary of Defense for Acquisition, Technology, and Logistics will serve as the DoD decision-maker for the matter under consideration and will coordinate decision-making as appropriate with the other stakeholders identified by the study's findings and recommendations. The nominal start date of the study period will be within 3 months of signing this Terms of Reference, and the study period will be between 9 to 12 months. The final report will be completed within 6 months from the end of the study period. Extensions for unforeseen circumstances will be handled accordingly.

The study will operate in accordance with the provisions of Public Law 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.04, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this study will need to go into any "particular matters" within the meaning of title 18, United States Code, section 208, nor will it cause any member to be placed in the position of action as a procurement official.

Frank Kendall

Appendix B: Task Force Membership

Chairs

Mr. Chris Inglis
U.S. Naval Academy

Mr. James Gosler
JHU Applied Physics Laboratory

Members

Dr. James Babcock
Federal Data Systems

Mr. Robert Butler
Cyber Strategies, LLC

Dr. Donald Duncan
JHU Applied Physics Laboratory

Mr. Daniel Ennis
UMD Global Cyber Initiative

Dr. Joe Keogh
Booz Allen Hamilton

Dr. John Manferdelli
Google

Dr. Joseph Markowitz
Private Consultant

Hon. Judith Miller
Private Consultant

Mr. Robert Nesbit
Private Consultant

LtGen John Sattler, USMC (Ret.)
Private Consultant

Ms. Teresa Shea
In-Q-Tel

Dr. Thomas S. Walcott
USCYBERCOM

Ms. Leigh Warner
Private Consultant

Mr. Glenn “Rick” Wilson
Private Consultant

Maj Gen Brett Williams, USAF (Ret.)
IronNet Cybersecurity, Inc.

Government Advisors

Ms. Katherine Charlet
OUSD(P)

Mr. Mark Elliott
OUSD(I)

Mr. Robert Joyce
National Security Council

Mr. Eric Parker
OUSD(I)

Mr. Shawn Turskey
USCYBERCOM

Executive Secretaries

RADM T.J. White, USN
USCYBERCOM

Col Eduardo Monarez, USAF
USCYBERCOM

Defense Science Board Secretariat

Dr. Craig Fields
DSB Chairman

Mr. Edward Gliot
DSB Executive Director

Dr. Eric Evans
DSB Vice Chairman

CAPT Jeff Nowak
U.S. Navy

Study Support

Ms. Brenda Poole
SAIC

Ms. Juliet Fielding
SAIC

Appendix C: Briefings Received

05–06 October 2016 Meeting

OSD Policy Perspective
Ms. Katherine Charlet, OUSD Policy

Perspective on USCYBERCOM Capabilities and Modalities
Dr. Stephen Orr IV, U.S. Naval Academy

NSA Tailored Access Operations (TAO) Discussion
Mr. Robert Joyce, National Security Agency

USCYBERCOM Perspective and Discussion
RADM T.J. White, USN, USCYBERCOM

30 Nov–01 Dec 2016 Meeting

Operational Strategy
Dr. Richard Harknett, USCYBERCOM and National Security Agency

Joint Intelligence Operations Center, USCYBERCOM
CAPT Mike Studeman, USN, USCYBERCOM

Operation GLOWINGSYMPHONY
Brig Gen Tim Haugh, USAF; CAPT Steve Donald, USN, Joint Task Force Ares

A Member's Perspective
Mr. Robert Butler, Cyber Strategies, LLC

Joint Staff
Col Dean Clothier, USAF; CAPT Jeff Bernhard, USN, Joint Staff J-39

Current Policy and Legal Perspectives Panel Discussion
Hon. Judith Miller, Private Consultant; Ms. Katherine Charlet, OUSD Policy; Dr. Walter Sharp, DoD

14–15 December 2016 Meeting

History of Special Activities
ADM William Studeman, USN (Ret.)

Discussion
Rob Schrier, Subject Matter Expert

OSD(P) Perspective on Strategic Cyber Operations
Mr. Charles Swett, OSD(P)

FBI Perspective
Ms. Vanessa Bopp, FBI; Mr. Colby Daughtry, FBI

USD(I) Perspective
Mr. Mark Elliott, OUSD(I)

17–18 January 2017 Meeting

Cyber-Enabled IO Campaign Planning
COL David Lamm, National Defense University

IC Perspectives
Dr. Tom Donahue, Cyber Threat Intelligence Integration Center

Best Practices in Protection
Mr. Tony Sager, CISecurity; Mr. Curtis Dukes, CISecurity

State Department Perspective
Amb. Dan Fried, Department of State

OUSD(AT&L) Perspective
Mr. Adam Nucci, OUSD(AT&L)

21–22 February 2017 Meeting

Global Cyberspace Operations Synchronization (GCOS)
COL Stephen Letcher, USA, USCYBERCOM

UK Perspectives and Insights
Ms. Sally Ward, GCHQ

USCYBERCOM Excursion – Cyber Innovation Lab
Col Mike Burke, USAF, Cyber National Mission Force

USPACOM Perspective
USPACOM J3 and J6

USSTRATCOM Perspective
Mr. Richard Bibey, USSTRATCOM

IC Perspectives on Strategic Cyber Issues
Mr. Vinh Nguyen, ODNI

Australian Perspective
Mr. Mike Williams

04–05 April 2017 Meeting

Industry Perspective
Mr. Dmitri Alperovitch, Crowdstrike

USCYBERCOM – CIO Perspective
Mr. G. Dennis Bartko, USCYBERCOM Capabilities Development Group

The Future of Cyber Autonomy
Dr. David Brumley, Carnegie Mellon University

IC Perspective
Mr. Glenn Gaffney, Central Intelligence Agency

Current Administration’s Perspectives on Cyber
Mr. Joshua Steinman, National Security Council

24–25 May 2017 Meeting

State Department Perspective
Mr. Chris Painter, Department of State

Industry Perspective
Mr. John Watters, FireEye

Industry Perspective
Mr. Matt Devost, FusionX

Industry Perspective
Mr. J. Michael Daniel, Cyber Threat Alliance

Industry Perspective
Dr. Michael Sulmeyer, Harvard University

White House Perspective
Mr. Robert Joyce, National Security Council

12–13 July 2017 Meeting

DHS Perspective
Mr. Thomas McDermott, Deputy Assistant Secretary for Cyber Policy

Global Engagement Center (GEC) Discussion
Mr. Daniel Kimmage, GEC

Department of Commerce Perspective
Mr. Adam Sedgewick, Department of Commerce

mirror object to mirror
mirror_mod.mirror_object
operation == "MIRROR_X":
mirror_mod.use_x = True
mirror_mod.use_y = False
mirror_mod.use_z = False
_operation == "MIRROR_Y"
mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
_operation == "MIRROR_Z"
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
selection at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.acti
("Selected" + str(modifie
irror_ob.select = 0
bpy.context.selected_ob
ata.objects[one.name].se
int("please select exac
OPERATOR CLASSES
types.Operator):
X mirror to the
ject.mirror_mirror
ror X"
ontext):
tive_object
DEPARTMENT OF DEFENSE

DEPARTMENT OF DEFENSE