



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