DEPUTY UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

RESEARCH
AND ENGINEERING

December 6, 2024

MEMORANDUM FOR CHAIR, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Study on Maintaining a Cyberspace Warfighting Advantage

Over the past decade, our nation and the Department of Defense (DoD) have faced challenges dealing with rapid changes in technology, geopolitics, the cyberspace operational environment, and the complexities of international economic competition, and will continue to experience these challenges in the years ahead. Recognizing cyberspace as a domain of competition and conflict, as well as a mission enabler, the United States must sustain, strengthen, and protect our military capabilities to provide strategic deterrence, to preserve and assure our military advantages, and to ensure our adversaries cannot threaten the peace and stability of the United States or our international allies and partners.

The Department of Defense Information Network (DoDIN) comprises the totality of networks, technologies, and capabilities which collectively enable key departmental objectives and national interests. All major functions of the DoD crucially depend on the availability and integrity of the DoDIN and its data to enable and sustain missions. Technological advances have necessitated an infusion of capabilities that are susceptible to cyber manipulation into every facet of DoD equipment, processes, and doctrine. Once declared an operational domain, cyberspace became a battlespace with an assigned commander, signaling a major shift in how the DoD intends to treat cyber moving forward.

Like any other battlespace, the cyber battlespace must be understood, coordinated, synchronized, and controlled to maintain U.S. advantage. Similarly, military norms established in other warfighting domains should be adapted to cyberspace to enable consistency across the joint force while minimizing constraints.

The Defense Science Board (DSB), working through its Permanent Subcommittee on Strategic Options ("the Permanent Subcommittee"), is directed to conduct a study on maintaining a cyber warfighting advantage. The study should examine all facets of battlespace management (e.g., policy and doctrine, technology and capabilities, command relationships, force composition and management, common operational picture for domain awareness and real time maneuver warfare) to enable cyber battlespace advantage. Through this process, the study should:

- Consider policy and material options to enable the cybersecurity data standards, censoring, and defense of DoD weapon systems;

- Review the current command and control (C2) framework as it pertains to securing, operating, and defending the cyber battlespace, including the DoDIN, while identifying areas to reduce the attack surface and improve/modernize/enhance operational

effectiveness for current and future steady-state, crisis, and conflict. Review how changes in cyber protection conditions (CPCON) may impact the mission of other Combatant Commands during steady-state, crisis, and conflict.

- Identify and examine opportunities for optimization of authorities within doctrine, regulations, policies, and federal statutes regarding the roles and responsibilities in cyberspace operations, including the implications for elevating the DoDIN to a sub-unified Command among the DoD, intelligence community (IC), and federal partners.

    - Identify authorities and architectures to enable DoD to leverage capabilities from public, private, and allies and partners to enhance cyberspace operations in a defensive environment.

    - Highlight authorities and architecture opportunities to leverage and integrate commercially available emerging technologies (i.e., artificial intelligence, high performance computing, data standards and analytics, and automation) and implications for what the future of cyberspace terrain (future operational environment) will look like based on incorporation of the new technologies by the United States and its adversaries.

- Consider options for DoD to impose more costs on the adversary through secure, operate and defend measures (e.g., identifying authorities, key cyber data and defensive standards, normalization, aggregation, and transport for broad DoDIN application).

- Examine and consider bold and/or novel measures to increase the Department's redundancy, resiliency, and survivability, in peacetime and conflict (or transition), across all classification levels.

- Explore the benefit of developing and applying high-level performance measures, such as key performance parameters, to quantify operational readiness of cyberspace systems (e.g., desired operational effectiveness of the DoDIN).

- Explore the potential impact of the presence of foreign companies in the United States on the performance of the cyber warfighting domain across the spectrum of conflict.

- Examine the architecture of the DoDIN to explore alternatives to enhance effectiveness in the cyber warfighting domain.

The Permanent Subcommittee 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, unless the meeting must be closed in accordance with one or more of the exemptions found in subsection 552b(c) of title 5, United States Code (U.S.C.). The DSB will provide its findings and recommendations to Under Secretary of Defense for Research and Engineering (USD(R&E)) as the Sponsor of the DSB. The nominal start date of the study period for this terms of reference (ToR) will be within 30 days of when this ToR is signed. In no event will the duration of the study exceed 12 months from the first meeting to development, deliberation, and adoption of the final briefing/report.

In support of this ToR and the work conducted in response to it, the DSB and the Permanent Subcommittee have my full support to meet with Department leaders. The DSB staff, on behalf of the DSB and the Permanent Subcommittee, may request the Office of the Secretary of Defense and DoD Component Heads to timely furnish any requested information, assistance, or access to personnel to the DSB or the Permanent Subcommittee. All requests shall be consistent with applicable laws; applicable security classifications; DoD Instruction 5105.04, "Department of Defense Federal Advisory Committee Management Program"; and this ToR. As special government employee members of a DoD federal advisory committee, the members of the DSB and the Permanent Subcommittee will not be given any access to DoD networks, to include DoD email systems.

Material provided to the DSB and the Permanent Subcommittee becomes a permanent part of the DSB's records. All data/information provided is subject to public inspection unless the originating Component office properly marks the data/information with the appropriate classification and Freedom of Information Act exemption categories before the data/information is released to the DSB and the Permanent Subcommittee. The DSB has physical storage capability and electronic storage and communications capability on both unclassified and classified networks to support receipt of material up to the TS/SCI level.

The DSB and the Permanent Subcommittee will operate in conformity with and pursuant to the DSB charter, chapter 10 of title 5, U.S.C.; subsection 552b(c) of title 5, U.S.C.; and other applicable federal statutes, regulations, and policy. Individual DSB and Permanent Subcommittee members and the Permanent Subcommittee as a whole do not have the authority to make decisions or provide recommendations on behalf of the DSB nor report directly to any Federal representative. The members of the Permanent Subcommittee and the DSB are subject to certain Federal ethics laws, including section 208 of title 18, U.S.C., governing conflicts of interest, and the Standards of Ethical Conduct regulations in 5 Code of Federal Regulations, Part 2635.

HONEY.DAVID.A.1044947591 Digitally signed by HONEY.DAVID.A.1044947591 Date: 2024.12.06 14:25:07 -05'00'

David A. Honey, PhD