



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAY 19 2011

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board (DSB) Task Force on Resilient Military Systems

You are hereby directed to establish a Task Force to assess issues affecting the resiliency of military systems that rely on information and communication technology (ICT), including through consideration of the following for mission operational systems:

- Identify measures and techniques under development in the ICT space to quantify system vulnerability and the effectiveness of defense measures;
- Dissect the concept of operations (CONOPS) of various potential cyber attacks and describe the opportunities in the system to develop diagnostics relating to detecting and understanding the attack;
- Apply the diagnostics to 2-3 different mission threads to understand the differences in risk among different types of architecture components (e.g., hardware, software, network, and human risks);
- Study tool/modeling opportunities to predict/measure system vulnerabilities.
- Assess techniques/processes to identify the applicability of human suitability and reliability (e.g., the Personnel Reliability Program);
- Define meaningful measures and metrics to evaluate and monitor the level of system resiliency. Survey metrics developed to characterize resilience in other domains (e.g., insurance, financial systems, and security systems); and
- Identify tactics, procedures and design techniques that could improve system resiliency. In addition, identify research opportunities and estimate the level of investment to achieve results consistent with DoD needs.

Innovative use of modern ICT (e.g., networks, software and microelectronics) in military systems plays a key and vital role in making the U.S. military second to none. However, the effectiveness of these military systems is extremely dependent upon the information assurance provided by its ICT underpinnings and on the personnel who operate and maintain the systems. An unintended consequence of the reliance on ICT to sustain superior U.S. capability is that our adversaries can erode or eliminate our advantage by targeting and exploitation at both the system and component level.

Several factors complicate the ability to maintain our advantage. A short, but certainly not comprehensive, list would identify the complex technology involved, the slowness to understand the problem, and the difficulty to develop effective metrics.



OSD 04475-11



Based in part on the complexity of modern software and microelectronic systems, very small and difficult-to-detect defects or subversive modifications introduced at some point in the life cycle of the systems create debilitating effects. As an example, although remote software system upgrades (remote provisioning) provide great flexibility and efficiency, they also introduce a very attractive vector for an enemy to compromise a system. The same complexity amplifies the human factor – whether malicious or innocent. Insertion of an infected flash drive produced the most significant breach of U.S. systems to date; while the intentional downloading of thousands of classified documents to “music”-labeled CDs generated its own set of problems. As a result of the great and growing complexity of DoD systems, cyber resiliency is an extremely broad and difficult attribute to guarantee.

DoD and military officials have long understood our advantage in the utilization of these technologies in military systems. Unfortunately, DoD officials have been slow to develop sufficient understanding of the mission assurance implications of adversary capability to operationally exploit these systems. Although the contest is simple to characterize, it is an extremely complex matter and a difficult one in which to achieve confidence in the desired outcome. To continue to take advantage of modern technology to increase our military effectiveness, we must possess sufficient confidence that these systems are not compromised to such a degree that we lose the benefit. In addition, we want to work actively to decrease the confidence of our adversaries that their clandestine operations targeting our systems are effective enough to eliminate our advantage.

An important step toward designing, implementing, and maintaining more resilient systems is to understand how to measure the resiliency of those systems relative to various cyber attacks and adversaries. Establishing useful measures and metrics is a first step toward quantifying and developing systematic methods and standards to improve both real resiliency and confidence in our process. These tools would allow organizations to apply scarce resources (people and dollars) more effectively in all phases (research, acquisition, and maintenance) of the life cycle of these systems to improve our confidence in the resiliency of these capabilities, and to enhance the ability of those systems to perform as expected in a hostile environment.

Prior efforts to develop useful measures and metrics have largely failed due to the difficulty of the subject. There is no guarantee that this effort will fare better. However, if fully adequate and robust metrics are not developed, the Task Force will describe the weaknesses of the proposed metrics and describe an iterative process to obtain improved metrics over time.

Administration support and funding will be provided by the Under Secretary of Defense for Acquisition, Technology, and Logistics. Additional support will be provided by the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, the Director, Operational Test and Evaluation (DOT&E), the Vice Chairman of the Joint Chiefs of Staff, and the Commander, U.S. Cyber Command. All Task Force members, consultants, and supporting personnel will be appointed or designated in accordance with DoD Instruction (DoDI) 5105.04, “Department of Defense Federal Advisory Committee Management Program.”

The Task Force will be established and operated in accordance with the provisions of the "Federal Advisory Committee Act" (5 U.S. Code Appendix, as amended), DoDI 5105.04, the DSB Charter, and all applicable laws, policies, and regulations. It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of section 208 of title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.

A handwritten signature in black ink, appearing to read "W. C. Lyne". The signature is written in a cursive style with a long horizontal stroke at the end.