



RESEARCH
AND ENGINEERING

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

CLEARED
For Open Publication

Nov 22, 2019

THE UNDER SECRETARY OF DEFENSE

3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

NOV 06 2019

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference - Defense Science Board Task Force on Internet of Things: Vulnerabilities and Opportunities

In the late 1960s the Department of Defense (DoD) began to acquire IT systems in earnest. As expected, these systems—both enterprise and combat systems—provided substantial new and improved capabilities. Not fully appreciated at the time, however, were attendant cyber vulnerabilities that proved not merely incidental, but inherent in the complexity of the software.

Since then DoD acquisition of such systems has both normalized and accelerated, yet the imbalance of enthusiasm for capabilities as opposed to concerns over vulnerabilities remains. DoD increasingly depends on these systems for its efficient and effective operation and its successful conduct of military operations while potential adversaries have a growing arsenal of powerful tools for cyber-attack. In sum it is unclear whether DoD is operationally better off or worse off relative to cyber threats.

Now, half a century later, DoD is beginning to acquire a second wave of systems still more capable yet equally lacking in cyber security; indeed, there is mis-appreciation that the systems, at heart, IT systems let alone appreciation of their accompanying cyber vulnerabilities. Previous generations of military hardware and ancillary devices, whether purpose-built or adaptations of commercial items, generally had restrictive information-handling and specialized interconnection capabilities. Increasingly, these constraints have given way to vastly more powerful, general purpose processing and global, common-user networks.

The term of art for their ensemble is “Internet of Things” or IoT and, broadly, is the collection of devices and networks of computing systems that contain embedded technology to communicate, sense, and interact with the external environment. The evolution of these devices will seriously impact both US and adversary military capabilities, for better and for worse. In short, increasingly more commercial, industrial and consumer devices DoD and its personnel are acquiring are basically sensor suites integrated with networked computers and surely possessing significant cyber vulnerabilities. These devices often have RF, optical, and acoustic sensors, and geo-location information that could yield lucrative intelligence. Their cyber vulnerabilities may be innate or may be introduced by an adversary using tools for cyber-attack. The ever-increasing array of globally accessible, smarter and smarter devices—both government-issue and personal, purpose-built or commercial, our and theirs—provide the canonical “Challenge and Opportunity.” DoD must exploit adversary devices for both intelligence collection and, if required, sabotage, all the while making effective use of its own device while remaining assured of confidentiality, integrity and availability.

Key questions that should be considered:

- How should the risks posed by the Department's use of IoT devices be managed?
- How should the risks of IoT devices not owned by the Department (but impacting Department capability) be managed?
- What opportunities presented by IOT devices should the Department take advantage of?

The main purpose of the Task Force on DoD and IoT is to significantly raise awareness of both DoD and the Defense Industrial Base that DoD and DoD personnel in acquiring IoT devices are purchasing IT systems with worrisome cyber vulnerabilities, and to point out the cyber defense tools and techniques that can and should be employed with IoT devices. Many of the panoply of currently available approaches to cyber defense can be applied to IoT devices – once consciousness is raised.

While the focus should be on DoD and IoT the use of IoT devices by the American people is accelerating rapidly and along with that use cyber vulnerability is concomitantly increasing. The findings and recommendations of the Task Force will have collateral benefit to the American citizenry.

A second purpose of the Task Force devolves from the observation that adversaries, both state and non-state, are also purchasing IoT devices and there are potentially lucrative non-traditional intelligence opportunities that should be vigorously explored including the required supporting technologies for analyzing these new sources of data as well any necessary changes to current policies.

Finally a third intent of the Task Force arises from the emergence of IoT-enabled urban areas. Cities face many challenges such as traffic management, law enforcement, waste management, weather impacts, and so on that are exasperated by the population density and scale of the city. Many cities are implementing IoT systems and networks to assist with traffic flow sensing and dynamic traffic management, ubiquitous video surveillance, mesh networks of environmental and weather sensors, and human population flow characterization, just to name a few. In a future urban conflict where the United States military finds itself fighting in such a city these IoT systems could pose both a threat to our forces as well as an opportunity to co-opt them and utilize them to extend our tactical situational awareness. The richly instrumented environment will include networks of surveillance cameras, sensors embedded in roads and streets, acoustic sensors for characterization and localization, and more. Threat or opportunity will depend on our forces' concept of operations in such environments.

To these ends the Task Force should report on the scope of acquisition of IoT devices by DoD; assess the state of cyber vulnerability—confidentiality, integrity and availability—and cyber defense for those devices; point out the potential vulnerabilities so introduced and the possible operational implications; and recommend what should be done in both management and technical terms to mitigate the risks while obtaining the benefits of IoT devices.

Finally, the Task Force should also consider operational concepts germane to force generation and embarkation/debarkation as well as urban combat in cities rife with IoT devices,

wherein we would greatly benefit from exploitation of the instrumentation and denying that exploitation to others.

I will sponsor the study. Dr. Ruth David and Mr. Chris Day will serve as Co-Chairs of the Study. Mr. Tom Walcott will serve as the Executive Secretary. Mr. Dan Wilmouth will serve as the Defense Science Board Secretariat representative.

The task force members are granted access to those DoD officials and data necessary for the appropriate conduct of their study. The Under Secretary of Defense for Research and Engineering will serve as the DoD decision-maker for the matter under consideration and will coordinate decision-making as appropriate with 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 P.L. 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, U.S.C. section 208, nor will it cause any member to be placed in the position of action as a procurement official.



Michael D. Griffin