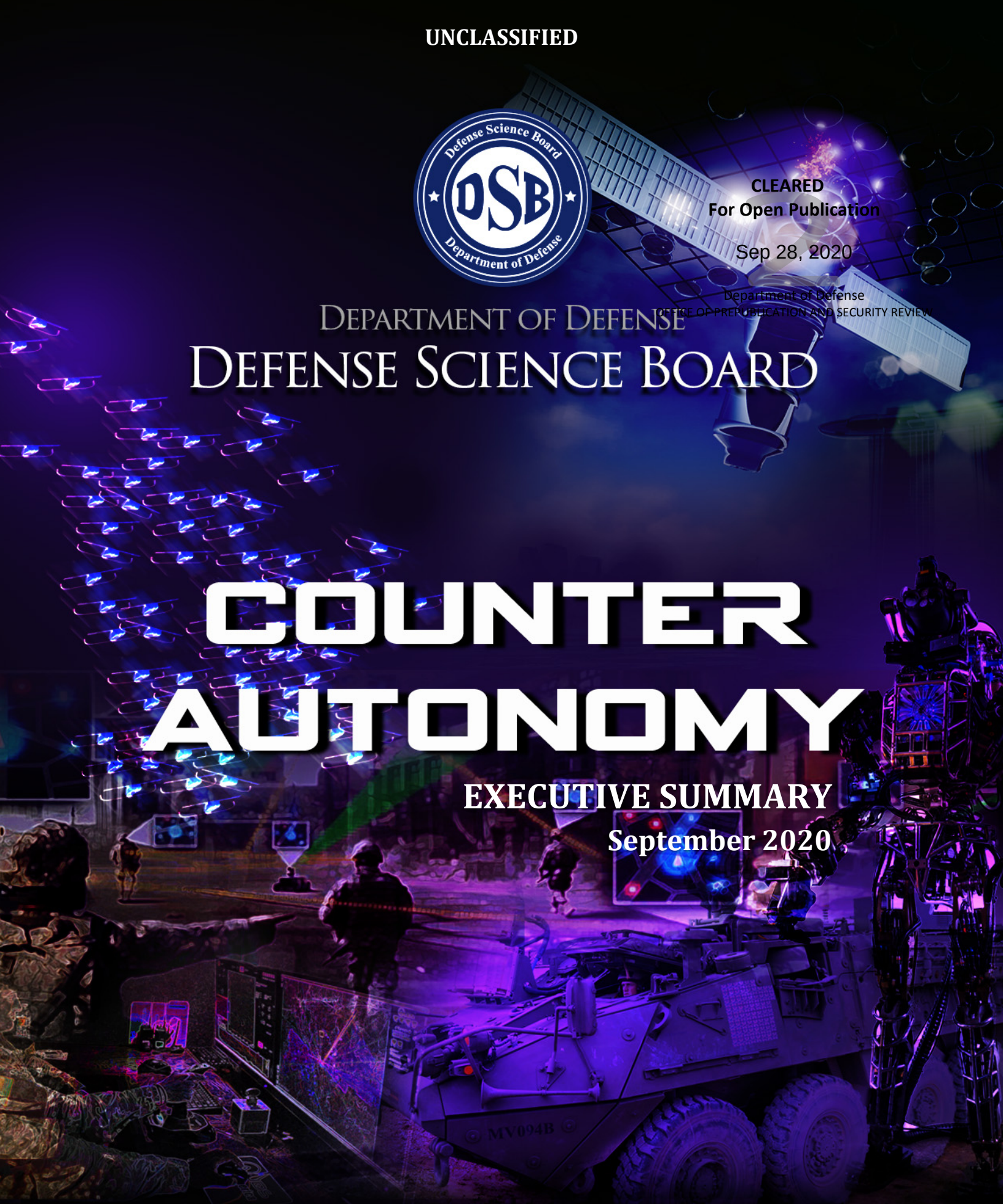
DEPARTMENT OF DEFENSE
DEFENSE SCIENCE BOARD

COUNTER AUTONOMY

EXECUTIVE SUMMARY

September 2020



OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

DEFENSE SCIENCE BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

SUBJECT: Final Report of the Defense Science Board Task Force on Counter Autonomy

I am pleased to share the final report of the Defense Science Board (DSB) Task Force on Counter Autonomy, co-chaired by Mr. James Carlini and Dr. Mark Maybury.

As rapid technological advances in autonomy and artificial intelligence continue, countering adversary autonomous physical and information systems will be a critical line of effort in future military operations. The threat of adversary autonomous systems will be present in all phases of conflict and across all domains – land, sea, air, space, and cyberspace. Existing capabilities may be adequate for countering some autonomous threats, but the emerging nature of the threat will necessitate some novel tactics, techniques, and procedures as well.

With autonomy as an emerging capability for the Department, counter autonomy is even more nascent. The establishment of an organizational focal point within the Department is critical to fully realizing the nature of this threat and implementing policies and strategies to mitigate it. There are few counter autonomy and counter artificial intelligence programs throughout the Department or the U.S. Government as a whole. A senior-level advocate for counter autonomy and counter artificial intelligence should advise the Department when and if new initiatives are needed, and when counter autonomy and counter artificial intelligence considerations should be integrated into existing initiatives.

The Task Force developed a series of recommendations that, if adopted, will position the Department to successfully counter autonomous systems in future operations. I support the recommendations detailed in this report and urge the Department to adopt and implement them.

Eric D. Evans

Dr. Eric Evans
Chairman, Defense Science Board

THIS PAGE LEFT INTENTIONALLY BLANK

DEFENSE SCIENCE BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

MEMORANDUM FOR: UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Counter Autonomy

Attached is the final report of the Defense Science Board Task Force on Counter Autonomy. The Task Force was asked to conduct a strategic assessment of U.S. counter autonomy capabilities today and 30 years from now across all domains (land, sea, undersea, air, space, and cyberspace). The Task Force considered both physical and digital autonomous systems. Specific areas of focus include:

- the projected future of autonomy and artificial intelligence (AI);
- gaps in U.S. counter autonomy capabilities;
- vulnerabilities unique to autonomous systems;
- non-traditional counters to autonomous systems; and
- the current state of autonomy/AI talent across DoD.

The Task Force found a heavy focus across the whole-of-government on fielding U.S. autonomous systems with very little attention given to countering autonomous systems deployed by adversaries. One major exception is the U.S. government's many programs focused on the counter unmanned aerial system (c-UAS) mission. Although c-UAS is critical to ensuring the safety and security of U.S. forces, allies, and the homeland, the DoD must adopt a broader view of counter autonomy or it will not be prepared to effectively defeat future adversary systems.

Like the introduction of cyberspace, the growth of autonomy and AI will bring new capability to the public and private sector, but it will also introduce vulnerabilities to current and future capabilities. Therefore, the Task Force felt it necessary to not only develop recommendations aimed at counter autonomy but also counter-counter autonomy. The integrity of each component used to develop a physical or digital autonomous capability must be considered across the entire lifecycle of a system to maintain confidence in its efficacy and reliability.

The Task Force has provided a series of recommendations that, if implemented, will effectively aid the DoD and the wider U.S. government in developing a full-scope counter autonomy capability, strengthen U.S. autonomous systems, and result in a more resilient and lethal force.

Dr. Mark Maybury
Co-chair

Mr. James Carlini
Co-chair

THIS PAGE LEFT INTENTIONALLY BLANK

Executive Summary of the DSB Report on Counter Autonomy

Table of Contents

Executive Summary of the DSB Final Report on Counter Autonomy

Scope of the Study

Autonomous technology is rapidly advancing, affordable, and ubiquitous. Developments in autonomy impact the physical, cyber, and information realms across the public and private sector. U.S. competitors and adversaries are rapidly adopting and deploying autonomous systems for domestic, commercial, and military use.

In response to the rapid development and deployment of autonomous technology, the Defense Science Board's Task Force on Counter Autonomy was tasked to conduct a strategic assessment of U.S. counter autonomy capabilities today and 30 years from now across all warfighting domains (land, sea, undersea, air, space, and cyberspace). The Task Force considered both physical and digital autonomous systems while examining:

- The full spectrum of projected autonomy threats
- Current and projected counter autonomy capability gaps
- Unique autonomous system vulnerabilities
- Key system capabilities and attributes essential to counter autonomy
- Acquisition, testing, and training needs
- Doctrine and strategy needed
- Options to deter and avoid being deterred by adversary autonomy

The Task Force spent a significant amount of time determining the most effective way to scope and define critical terms such as "autonomy" and "artificial intelligence." The Task Force has defined autonomous systems to be systems (physical or digital) that can act in accordance with delegated and bounded authority. This is a broad definition, but reflects the fact that autonomous functionality is being incrementally introduced into many systems. A system that is not generally autonomous may have certain functions that are autonomous or may act autonomously within certain bounds. Regardless of whether a system is fully autonomous or only partially autonomous, wherever autonomy is introduced, there is potential to attack it.

Autonomy, artificial intelligence (AI), and machine learning (ML) are often treated as near synonyms, but in fact they are not. The distinctions between the three terms are meaningful for this report. AI is a collection of disciplines that enable some autonomous systems to sense, plan, adapt, and act based on their knowledge and understanding of the world, themselves, and the situation. AI includes the ability to automate functions such as vision, speech and language processing, robotics, planning and scheduling, navigation and collision avoidance, object tracking and targeting, and collaborative swarming, among other intelligent activities. Systems engineering and domain expertise are still critical to the overall development and operations of autonomous systems.

ML is a sub-discipline of AI that uses algorithms and statistical models (e.g., deep learning) that learn from training data, examples, experience, or from others. While ML has made tremendous

advances in the past decade, there are other AI sub-disciplines besides ML that are important to the broad field of AI and autonomous capabilities. We should not forget the broader suite of AI disciplines since the next giant leap may occur in another sub-discipline.

Counter autonomy is used in this report for the comprehensive set of capabilities and TTPs that could cause an autonomous system to fail in its intended mission. This could include the more traditional kinetic destruction of the system, but also efforts to confuse the sensors or poison data, attack via cyber methods, or even efforts to cause the human operator to lose trust in the system. Any method that reduces the effectiveness of the autonomous system can be included under counter autonomy.

Counter autonomy includes both "counter autonomy" and "counter-counter autonomy." The United States should utilize counter autonomy to defend against increasingly autonomous systems deployed by adversaries, and to ensure that U.S. autonomous systems are not vulnerable to adversary countermeasures. Simultaneously, we must ensure that our own autonomous weapons are not being degraded through adversaries' implementation of counter-counter autonomy.

Autonomy in Military Missions

The potential to benefit from increased autonomous functionality applies to most military domains, missions, and support activities. It is a foundational technology with wide and varied applications.

Many individuals first associate autonomy with weapons and weapons platforms—aircraft, missiles, unmanned aerial systems (UAS), unmanned ground systems (UGS) and unmanned underwater systems (UUS). However, autonomy can also improve cyber operations, electronic warfare, intelligence, and information operations. Any place where humans currently are involved in pattern recognition, decision making, optimizing, planning, deconfliction, and information fusing is an area where increased autonomous functionality could improve our capabilities, and lessen the cognitive load for human operators.

Furthermore, there are many areas that are not seen as traditional defense domains, but where the military depends on civil and commercial infrastructure that can also benefit from increased autonomy. Clear examples are in business operations, logistics and supply, and energy management. In some cases, autonomous functionality may completely replace humans, but in many areas it will augment humans and make them more efficient and effective.

This broad applicability means that advances in autonomy have the potential to scale nationally and globally, but it also means that new risks and issues of resiliency will be introduced into many systems. The United States needs to be mindful of this double-edged sword: protect our own systems from vulnerabilities and brittleness while we discover and prepare to exploit vulnerabilities and brittleness in adversary systems.

Despite the growing prevalence of autonomy in military missions, the Task Force struggled to find programs across the DoD and whole-of-government with a counter autonomy focus. The Task Force found a heavy focus across the whole-of-government on fielding U.S. autonomous systems with very little attention given to countering autonomous systems deployed by adversaries. One major exception is the U.S. government's many programs focused on the counter unmanned aerial system (c-UAS) mission. Although c-UAS is critical to ensuring the safety and security of U.S. forces, allies, and the homeland, the DoD must adopt a broader view of counter autonomy.

Recommendations

Recommendation 1: Leadership

A. USD(R&E) create a single senior focal point for counter autonomy separate from autonomy leadership but of equal authority to ensure independent thinking

B. USD(R&E) champion a DoD-wide autonomy/counter autonomy community modeled on the existing low observable/counter low observable (LO/CLO) community

Recommendation 2: Capability and Operational Development

C. Military Departments (Secretaries) charter the following in order to develop robust fielded counter autonomy capabilities

- Assess, fund, and deploy modifications needed to existing conventional capabilities
- Create a robust OPFOR that mimics adversary autonomy
- Establish multi-domain CA Red Teams
- Develop CA requirements, concepts, and TTPs/CONOPS

D. Direct Service labs and DARPA to create CA R&D

Recommendation 3: Intelligence

Sensitive content – N/A

Recommendation 4: Assurance

A. USD(A&S) establish and enforce AI-enabled autonomous system resilience guidelines to mitigate AI-specific vulnerabilities

B. DT&E/OT&E establish testing and evaluation guidance for development, fielding and sustainment to assure resilience of AI-enabled autonomous systems against counter autonomy attack over lifecycle

Recommendation 5: Policy

OUSD(P) develop policy to provide appropriate defense of U.S. autonomous weapon systems, support autonomy exports, and ensure safety and security of imports

Recommendation 6: Talent

OSD and Military Departments significantly expand autonomy/AI talent through aggressive recruiting, hiring, career path, and retention actions:

- Upskill talent with AI skills through incentives and innovative methods such as free or affordable online training (e.g., edX, Coursera, Udacity)
- Military Departments establish, promote, and incentivize autonomy/AI career paths for civilian and military personnel
    - Service Academies, including Air Force Institute of Technology and Naval Postgraduate School, include counter autonomy in curriculum and research
- Expand the use of innovative staffing (e.g., IPA, HQE, SMART), and build a national talent pipeline at the graduate level with focused DoD funding
- Fully leverage Section 1107(c) Direct Hiring Authority and request Congress authorize the limitation be raised from 5 percent to 10 percent of the workforce

Defense Counterintelligence and Security Agency (DCSA) accelerate clearance adjudication for candidates with critical skills (AI/ML, robotics, cyber, etc.)

Appendix A: Task Force Terms of Reference

RESEARCH
AND ENGINEERING

THE UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

JUN 1 8 2018

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference - Defense Science Board Task Force on Counter Autonomy

Advances in Artificial Intelligence and global technology proliferation are driving the rapid evolution and global adoption of autonomy, which is creating economic, social, and military disruption. The ability of future U.S. forces to advantageously harness autonomy in both physical and information systems will be essential to address capability and capacity asymmetries. As with past disruptive military technology epochs, a focused and coherent approach to addressing both offensive and defense is critical. This is particularly true with autonomy since the ethical and legal barriers to the full use of autonomous systems are likely to be much lower for future U.S. adversaries. As such, the Defense Science Board (DSB) is tasked with conducting a strategic assessment of U.S. counter-autonomy capabilities in the near (today) and far term (out to 2030).

The Task Force should consider counter-autonomy efforts in the domains of land, sea, undersea, air, space, and cyberspace. The Task Force should focus on countering autonomous physical systems in addition to autonomous operations in the information domain. Key questions to be addressed by the Task Force include:

- Threat: What is the full spectrum of projected autonomy threats? This should include a review of both military and commercial roadmaps for autonomous systems and technologies. It must also consider future warfighting innovations that fully leverage autonomy. How do we learn about adversary intentions and capabilities, and deny the same, especially when software is constantly learning and adapting and possibly denying and deceiving?

- Counter-Autonomy Gaps: What are the current and projected U.S. capability gaps for countering these threats? Is the United States on a path to close any existing gaps, stay ahead of the projected threat, and take full advantage of identified autonomous system vulnerabilities? What is the global state of counter-autonomy systems and technology and how will this evolve through 2030?

- Unique Autonomous System Vulnerabilities: What are the unique vulnerabilities associated with autonomous systems that the United States could exploit to create a lasting warfighting advantage? The full life cycle of an autonomous system should be considered, including research, development, testing, logistics, operations, and maintenance. The full span of autonomous system functions should be considered. Finally, all weapon system dependencies associated with the application of autonomy should be considered.

- Capability Needs and Investments: What key system capabilities and attributes are essential to ensure counter-autonomy from and through land, sea, undersea, air, space, and cyberspace to defend physical, virtual and human assets from autonomous systems across a range of environments and scenarios? What key counter-autonomy systems and technologies ought to be developed?

- Acquisition, Testing, and Training: Do we require new or modified methods to articulate, acquire, experiment, test, train, and evaluate counter-autonomy capabilities? How can speed of invention, innovation, acquisition, and employment of new and evolutionary capabilities be achieved to create and sustain an advantage over time?

- Doctrine/Force Strategy: What innovative Concept of Operations will yield the greatest counter-autonomy benefits? What are the barriers to adoption of effective counter-autonomy solutions and how can they be overcome?

- Deterrence: What are the most attractive options to deter and avoid being deterred by adversary autonomy?

I will sponsor the study. Mr. James Carlini and Dr. Mark Maybury will serve as the co-Chairmen of this study. RADM White will serve as the Executive Secretary. Mr. David Moreau will serve as the DSB Secretariat representative.

The Task Force members are granted access to those Department of Defense (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 three 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, "Federal Advisory Committee Act," and DoD Instruction 5105.04, "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.

Michael D. Griffin

Appendix B: Task Force Membership

Chairs

Mr. James Carlini
Leidos

Dr. Mark Maybury
Stanley, Black & Decker, Inc.

Members

Dr. Amy Alving
Private Consultant

Dr. Ruth David
Private Consultant

Dr. Kenneth Ford
Institute for Human and Machine Cognition

Mr. James Gosler
Johns Hopkins University, Applied Physics Laboratory

Mr. Ashley Llorens
Johns Hopkins University, Applied Physics Laboratory

Dr. Joe Markowitz
Private Consultant

Dr. Robin Murphy
Raytheon, Texas A&M University

Dr. Paul Nielsen
Software Engineering Institute

Mr. James Shields
Private Consultant

Mr. Lee Venturino
First Principles, Inc.

Government Advisors

Dr. John Everett
DARPA

Dr. Steven Rogers
USAF AFRL

Dr. Robert Sadowski
USA DEVCOM

Dr. Greg Zacharias
OSD(OT&E)

Dr. Dai Hyun Kim
Office of the Under Secretary of Defense for Research and Engineering

DSB Secretariat Representative

Mr. David Moreau

Defense Science Board Secretariat

Mr. Kevin Doxey
Executive Director

Study Support

Ms. Brenda Poole
SAIC

Ms. Juliet Fielding
SAIC

Appendix C: Acronyms and Abbreviated Terms

AI	*Artificial intelligence*
CA	*Counter autonomy*
CONOPS	*Concept of operations*
DCSA	*Defense Counterintelligence and Security Agency*
DoD	*Department of Defense*
DT&E	*Developmental test and evaluation*
HQE	*Highly qualified expert (appointing authority)*
IPA	*Intergovernmental Personnel Act*
LO/CLO	*Low observable/Counter low observable*
ML	*Machine learning*
OPFOR	*Opposing force*
OT&E	*Operational test and evaluation*
R&D	*Research and development*
SMART	*Specific, measurable, achievable, relevant, and time-bound*
TTPs	*Tactics, techniques, and procedures*
UAS	*Unmanned aerial system*
UGS	*Unmanned ground system*
USD(A&S)	*Under Secretary of Defense for Acquisition and Sustainment*
USD(P)	*Under Secretary of Defense for Policy*
UUS	*Unmanned underwater system*