UNMANNED SYSTEMS INTEGRATED ROADMAP

2017-2042

MQ-9 REAPER

RQ-4C TRITON

RQ-11 RAVEN
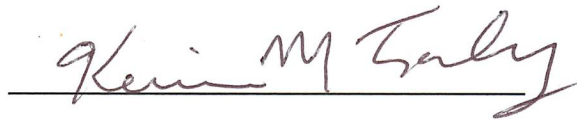
ACTUV

MQ-8C FIRESCOUT

LDUUV

This page intentionally left blank.
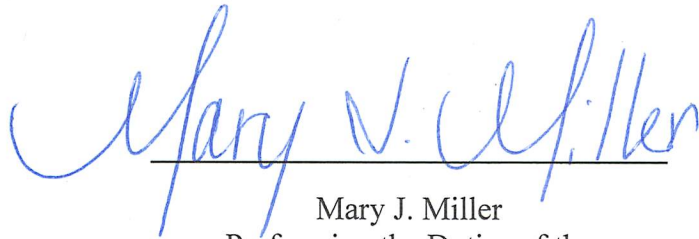
UNMANNED SYSTEMS INTEGRATED ROADMAP

FY 2017–2042

IS

APPROVED BY:

Honorable Kevin M. Fahey
Assistant Secretary of Defense
for
Acquisition

Mary J. Miller
Performing the Duties of the
Assistant Secretary of Defense
for
Research and Engineering

This page intentionally left blank.

Executive Summary

The Office of the Secretary of Defense (OSD) and the Armed Services have made extensive efforts to incorporate unmanned systems into their existing organization structures, showing the integral importance that unmanned systems considerations represent. There is still room for improved collaboration throughout the Department of Defense (DoD). Standardizing the ongoing efforts, cooperating whenever possible, and consolidating the foundational policies and technologies will enable the seamless teamwork that highlights future defense operations—whether the teams are manned, unmanned, or combined.

The progress in unmanned systems technologies has highlighted the need to transition the focus from specific domains to become domain agnostic. Advances in any domain are beneficial across all domains. Future operations will rely heavily upon multi-domain capabilities that must interface and integrate seamlessly into a Joint Force structure.

DoD, industry, and academia have advanced technologies, strategies, and standards that challenge the evolution of unmanned systems and their integration into the DoD mission. These major advancements, challenges, and trends can be consolidated into four critical themes, which address foundational areas of interest that will continue to accelerate unmanned systems into the future:

- Interoperability – Interoperability has historically been, and continues to be, a major thrust in the integration and operation of unmanned systems. Manned and unmanned systems have increasingly synergized their capabilities, focusing on the critical need to use open and common architectures. A robust interoperable foundation provides the very structure that will allow for future advances in warfighting.

- Autonomy – Advances in autonomy and robotics have the potential to revolutionize warfighting concepts as a significant force multiplier. Autonomy will greatly increase the efficiency and effectiveness of both manned and unmanned systems, providing a strategic advantage for DoD.

- Network Security– Unmanned systems operations ordinarily rely on networked connections and efficient spectrum access. Network vulnerabilities must be addressed to prevent disruption or manipulation.

- Human-Machine Collaboration – If interoperability lays the foundation, then human-machine collaboration is the ultimate objective. Teaming between human forces and machines will enable revolutionary collaboration where machines will be valued as critical teammates.

The supporting policy, requirements, and acquisition environments must continue to evolve and advance to keep pace with the rapid technical and capability advancements of all systems. To ensure our military advantage, emphasis should be placed on the evolution, availability, and employment of unmanned technology. Alignment of DoD initiatives in unmanned systems will influence the future makeup of the U.S. military.

This page intentionally left blank.

Table of Contents

List of Figures

List of Tables

1   Introduction

1.1   Purpose

DoD maintains a vision for the continued expansion of unmanned systems into the Joint Force structure, and identifies areas of interest and investment that will further expand the potential integration of unmanned systems. The intent of this document is to provide overarching strategic guidance that will align the Services' unmanned systems goals and efforts with the DoD strategic vision. This strategic guidance will focus on reducing duplicative efforts, enabling collaboration, identifying challenges, and outlining major areas where DoD and industry may collaborate to further expand the potential of unmanned systems. As DoD has embraced the use of unmanned systems across nearly every operating environment, this strategy will allow DoD to capitalize on the technology advancements and paradigm shift that unmanned systems provide.

This strategic guidance, while primarily directed toward a DoD audience, serves a diverse stakeholder community. By coalescing unmanned challenges, it will influence military department investments in unmanned innovations and be the backbone for departmental unmanned systems strategies. The strategy presents themes that will guide requirements developers, budget planners, program managers, laboratories, Warfighters, and other key DoD stakeholders. In addition, the themes provide insights that can guide the defense industry and academia, particularly independent research and development (R&D) strategies, which provide a direct benefit to DoD and other federal government agencies. This document also raises awareness of DoD's vision among key stakeholders outside of DoD, including advocacy groups and Congress.

> *DoD Unmanned Systems Vision*
>
> *DoD envisions unmanned systems seamlessly operating with manned systems to compress the warfighters' decision-making process, while reducing the risk to human life.*

DoD maintains an online interactive unmanned systems catalog to facilitate Service collaboration. This database contains DoD unmanned systems specifications and project details, and can generate comprehensive comparative data reports. The common access card-protected Unmanned Systems Information Catalog can be accessed at https://ebiz.acq.osd.mil/USIC.

In recent years, DoD has integrated unmanned systems into the Joint Force structure, Services, and DoD departments. The different organizations have all grown their respective efforts in researching, acquiring, and supporting unmanned systems across all domains, albeit in different ways according to the needs of each organization. A current snapshot of DoD organizations that are currently involved with the research, acquisition, policy, support, or operation of unmanned systems is found in Figure 1.
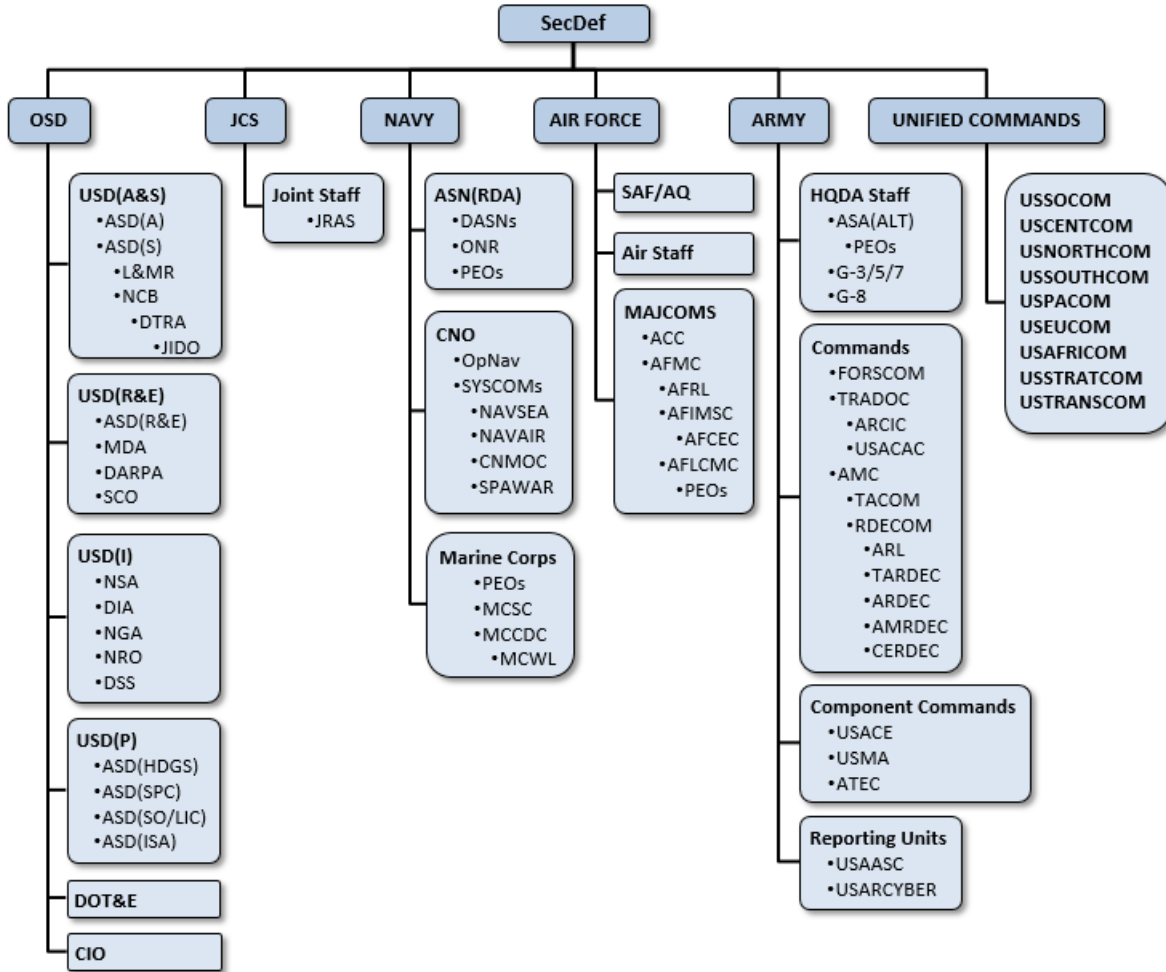
Figure 1: DoD Organizations that Involve Unmanned Systems

DoD continues to invest in Research & Development, Procurement, and Operations and Maintenance of unmanned systems across the Future Year Defense Programs. Table 1[1] summarizes fiscal year (FY) 2017 funding requested in the Base and Overseas Contingency Operations (OCO) budgets as well as the FY2017 Request for Additional Appropriations for all unmanned systems development, procurement and associated military construction (MILCON).

> *The Budget… continues to prioritize the necessary long-term investments in early-stage S&T at $12.5 billion to fund future technologies to reshape the battlespace, such as hypersonics, unmanned, and autonomous systems.*
>
> *-White House FY2017 Budget*

Table 1: DoD Unmanned Systems Funding FY2017 ($M)

2017 ($M)	Procurement	RDT&E	MILCON	TOTAL
Air Force	$955	$532	$31	$1,518
Navy	$821	$725	$113	$1,659
Army	$232	$212	$52	$496
SOCOM	$32	$45	$5	$82
DARPA	-	$292	-	$292
MDA	-	$105	-	$105
OSD	-	$93	-	$93
TOTALS	**$2,040**	**$2,004**	**$201**	**$4,245**

The Joint Services developed the 2016 Joint Concept for Robotics and Autonomous Systems (JCRAS) to describe future robotic and autonomous systems (RAS) employment, guiding comprehensive development and future acquisition initiatives across the Joint Forces (Refer to Appendix B). DoD has utilized alternative acquisition methodologies and strategies to facilitate the flexible and efficient development, procurement, and maintenance of DoD unmanned systems (Refer to Appendix C). In addition, OSD has directly supported several initiatives to develop common architectures and strategies, which the Services and industry should leverage and integrate into current and future development programs (Refer to Appendix D).

---

[1] https://www.whitehouse.gov/sites/default/files/omb/budget/fy2017/assets/budget.pdf

1.2   Themes and Enablers

DoD's strategic guidance is structured around common themes and enablers that will coalesce and advance the organizational efforts across DoD in pursuit of further expansion of military capabilities with unmanned systems technologies. An integrated product team from across DoD reviewed and analyzed over two dozen reference documents from all levels of DoD, and researched the technology trends from industry and academia to establish the common themes and enablers. (Refer to Appendix A)

The themes describe progress in advancing technologies that enable effective use of unmanned systems, and highlight potential advancements that form the basis of DoD strategy. Analysis of JCRAS, technology trends, and current initiatives resulted in the identification of a number of overarching **themes**. These themes provide the foundation needed to measure progress in technologies that advance the use and integration of unmanned systems and highlight potential improvements across the Doctrine, Organization, Training, materiel, Leadership, Personnel, Facilities + Policy (DOTmLPF-P) spectrum. Within each theme, a number of technology or policy **enablers** are identified that detail the ongoing work, or challenges, that require further effort, investment, and advancement to continue the paradigm shift that unmanned systems offer. The themes and enablers identified below are further detailed in sections 2 through 5 of this Roadmap.

The overarching themes that were identified are as follows:

- Interoperability

- Autonomy

- Secure Network

- Human-Machine Collaboration

The selection of these four themes is not meant to represent an all-encompassing view of the future of DoD unmanned systems. Over the last decade, the advancement of unmanned systems technology has exploded, and the extrapolated growth curve hints that by the time of the publication of this document, some unidentified emerging technology or issue will likely emerge to disrupt any path that a traditional strategy might lay out. Therefore, the intent is to lay a path toward an agile and flexible technology and policy foundation in which unforeseen disruptive technologies and operations can take root, and be seamlessly integrated into the current advancements and efforts across DoD. The rapid advancement in technology development requires DoD to be more agile in developing, standardizing, acquiring, deploying, lawfully operating, and maintaining the technology.

For each of the themes, the specific enablers highlight and elevate the various issues, challenges, opportunities, and ways ahead that may be present. The enablers for each theme are:

- Interoperability
    - Common/Open Architectures
    - Modularity and Parts Interchangeability

- o Compliance/Test, Evaluation, Verification and Validation
- o Data Strategies
- o Data Rights

- Autonomy
    - o Artificial Intelligence and Machine Learning
    - o Increased Efficiency and Effectiveness
    - o Trust
    - o Weaponization

- Secure Network
    - o Cyber Operations
    - o Information Assurance
    - o Electromagnetic Spectrum and Electronic Warfare

- Human-Machine Collaboration
    - o Human-Machine Interfaces
    - o Human-Machine Teaming

2   Interoperability

Future warfare will hinge on critical and efficient interactions between warfighting systems. These interactions will depend on an interoperable technological foundation that establishes and enables the data and communication networks and services across the warfighting systems enterprise. This interoperable foundation will transmit timely information between information gatherers, decision makers, planners, and warfighters.

A comprehensive approach to developing unmanned systems, guided by a common vision for joint operations, will lead to greater fiscal efficiency and operational effectiveness. This is especially important given the likelihood of increased investment in and the resulting employment of unmanned systems as the Joint Forces embrace rapidly evolving technologies. Interoperability will form the foundation of holistically integrated joint and coalition forces that fully exploit unmanned system technology. In a force with a dynamic mix of manned and unmanned systems, it is imperative that unmanned systems are able to communicate, share information, and collaborate with one another and human counterparts across systems and domains. In tomorrow's operational environment, it will be imperative that forces and systems can communicate among multiple command levels, across various units, share information and tasking, and assist mission leads as events play out on the battlefield in real time.[2] A summary of the future path for the five key enablers for interoperability is shown in Table 2.

Table 2: Comprehensive Roadmap for Interoperability

INTEROPERABILITY		2017 - - - - - - - - - 2029 - - - - - - - - - - 2042	
		NEAR-TERM	MID-TERM FAR-TERM
	Common/Open Architectures/AI Frameworks	-Standardized C2 & Reference Architectures	-Support Seamless, Agile, Autonomous Human-Machine Collaboration and inter-Machine collaboration
	Modularity & Parts Interchangeability	-Retrofit Existing Systems -Plan Modularity into New Systems	-Rapid Upgrades and Configuration Changes
	Compliance/ Verification & Validation	-New TEVV Approach -New V&V Tools & Techniques	-Highly Complex Autonomous Systems TEVV
	Data Transport Integration	-Common Data Repositories -Integrated End-to-End Delivery	-Anti-Jamming - Low Probability of Intercept/Detection
	Data Rights	-Secure Needed Data Rights -Evolve Data Rights Policy	-Maximum Mission Support Flexibility

2.1   Common/Open Architectures

Common architecture standards for command, control, and communications are critical to ensure synergy between systems and across domains, and facilitate the development of successful and achievable objectives. The objective is not one standard or service for all systems, rather, the use of common standards or services in the mission space or operating

---

[2] Joint Concept for Robotic and Autonomous Systems (JCRAS), 19 October 2016

domain. Common architectures shall include multiple common viewpoints, such as the Operational, Systems, Services and Data and Information viewpoints of the DoD Architecture Framework (DoDAF).[3] The Data and Information Viewpoints shall include common data models formulated in common languages that enable effective communications among interoperable systems and their modules. A foundation of commonality creates future opportunities for interoperability as new mission needs arise. Both requirements and materiel developers must advocate for and help create architectures for control systems and data links. Furthermore, while difficult to standardize and implement, open architectures foster innovation. Open design will allow potential control and integration of multiple platforms simultaneously, including across operational domains. Additionally, these architectures will allow for component upgrades to be interchangeable amongst platforms.[4]

2.1.1 Challenges

There are many challenges for achieving common/open architectures including, but not limited to, the Services and Combatant Commands collaborating to create a common set of requirements. Many other challenges exist such as different domains concurring on having appropriate tests of compliance for unmanned systems. A prudent course of action for DoD is to leverage and enhance commercially available technologies and seek consensus on a system of interchangeable architectures that can span multiple domains and multiple Services' requirements.

2.1.2 Way Ahead

In the near-term, the priorities of DoD and the Services will focus on the implementation of common/open architectures and DoD standards for all systems. Efforts should be made to examine all platforms, across the entire life cycle, and develop a strategic and economical plan for implementing secure common/open architectures. DoD near and midterm focus will span across the missions, domains, and Services to achieve the necessary requirements for these unmanned systems. Initial focus should be on C2 and common architectures that improve interoperability.

In the mid- and far-term, DoD will implement open architectures on all new unmanned systems platforms, then federate as a single authoritative source managed for conformance and currency.[5] The DoD-wide baseline architectures shall be established, well defined, and adaptable to all systems, with seamless interoperability between all manned and unmanned systems enabling robust and agile teaming, with the understanding that advances in autonomous systems technology will challenge our traditional C2 methodologies.

2.2 Modularity and Parts Interchangeability

Modularity and interchangeability in software, firmware and hardware parts are important for unmanned systems. These features reduce the difficulties associated with having multiple

---

[3] http://dodcio.defense.gov/Library/DoD-Architecture-Framework/
[4] Joint Concept for Robotic and Autonomous Systems (JCRAS), 19 October 2016
[5] Ibid.

systems to manage and support in the field. Modularity is also vital for unmanned systems to facilitate updating of hardware as newer missions and requirements become available. Specifically, to air systems, certified modular subsystems can streamline airworthiness certifications and realize time and cost savings.

The basis for interoperability and modularity in unmanned systems is to have common messages, or messages using common languages (e.g., Extensible Markup Language (XML) vocabularies of the National Information Exchange Model (NIEM)[6] and Web Ontology Language (OWL)) flowing between subsystems (controllers, robots, cameras, manipulator arms, sensors, etc.). This is enabled by standardizing the software and hardware interfaces, such as utilizing interoperability profiles (IOP)[7]. Unmanned Systems Interoperability Profiles (USIP)[8] help drive the implementation of approved DoD and/or joint interoperability priorities at the Service level and may even require a new Service IOP or revision to an existing IOP. The purpose of a USIP is to define profiles of standards sufficient to guarantee interoperability in support of a specific mission capability. A USIP may reference DoD standards, Intelligence Community standards, Service-specific IOPs, and commercial standards to achieve capability-based interoperability. USIP initiatives provide architectural basis and standards foundation for development of future interoperable systems.[9]

2.2.1 Challenges

DoD has not effectively emphasized modularity in past systems that have been acquired. Therefore, DoD labs are trying to retrofit parts interchangeability into legacy systems. As most of these systems have limited data rights, retrofitting introduces extreme levels of complexity into these projects. DoD has spent extensive time and energy attempting to define standard interfaces. However, current standard interfaces are not uniform across all domains and Services. Ideally several simple standards would be developed that are flexible enough to handle most, if not all, anticipated future capabilities and would streamline the implementation process.

2.2.2 Way Ahead

In the near-term, DoD will continue to focus on retrofitting parts for interchangeability and modularity into legacy systems. DoD is preparing for part interchangeability and modularity in new efforts and should ensure rapid acquisitions adhere to the standards as well. Therefore, the Department must continue to unite the Services and the programs to implement efforts of common standards across Services for changeability and modularity. The Services should utilize current common ground control stations, USIPs, software, and common interfaces to improve modularity and parts interchangeability.

In the mid- to far-term, optimized acquisition and the continued shift of functionality from hardware to software will decrease costs and enable rapid upgrades and configuration changes. Acquisition contracts shall incorporate DoD rights for reuse of software and hardware designs, as well as data rights wherever feasible. Innovative development processes (such as the

---

[6] https://www.niem.gov/.
[7] http://www.dtic.mil/ndia/2013/groundrobot/Iavecchia.pdf
[8] Unmanned Aircraft System (UAS) Memorandum 14667-07, 13 September 2007
[9] Joint Concept for Robotic and Autonomous Systems (JCRAS) Baseline Assessment Report, Version 2, Dec 2016

use of additive manufacturing), as well as designing modularity into systems, will enhance shared capabilities and safeguard against system-wide vulnerabilities.[10]

2.3   Compliance/Test, Evaluation, Verification, and Validation

The roles and capabilities of unmanned systems are being expanded in keeping with the desire to use autonomy to improve performance through increased operational speed, reduced cognitive load, and increased performance in denied environments. The test, evaluation, verification, and validation (TEVV) of these autonomous systems is a critical element in building the high assurance of autonomy. OUSD(R&E) has established a Community of Interest (COI) to address autonomy. The TEVV working group is a sub-group of the Autonomy COI. The TEVV working group published a Technology Investment Strategy in 2015 outlining strategic research goals across DoD for the next four years. The strategy contains five major goals:

1) Methods and tools assisting in requirements development and analysis

2) Evidence-based design and implementation

3) Cumulative evidence through research, development, test, and engineering (RDT&E), developmental testing (DT), and operational testing (OT)

4) Run-time behavior prediction and recovery

5) Assurance arguments for autonomous systems

Compliance/Test, Evaluation, Verification and Validation focuses on precise, structured standards and tools to automate requirements evaluation for testability, traceability, and de-confliction. Improved tools and methods to help the systems engineering community better articulate, formalize, and validate autonomous requirements are paramount to the success of systems V&V. This allows systems engineers to be assured that requirements are explicit and that assumptions are clearly defined. Equal vigor must address not only functional requirements of an autonomous system, but also equivalent models of the environment with which it will interact. This will allow for the creation of accurate and effective simulations to perform testing.

Fielding of future unmanned and autonomous capabilities will require close coordination with The Office of the Director, of Operational Testing and Evaluation (DOT&E), to ensure their realistic testing of mission-dependent capabilities, Concept of Operations (CONOPS)-related functions, scenario-dependent outcomes, and end-to-end or system-of-systems interactions or effects. Research and development programs will require a clear transition plan that encompasses modeling and simulation, developmental testing, and operational testing in realistic environments.[11]

---

[10] Ibid.

[11] Director, Operational Test and Evaluation (DOT&E) Test and Evaluation Master Plan (TEMP) Guidebook, Version 3.1, Jan 2017

2.3.1 Challenges

For the most demanding adaptive and non-deterministic systems, a new approach to traditional TEVV will be needed. For these types of highly complex autonomous systems, an alternate method leveraging a run-time architecture that can constrain the system to a set of allowable, predictable, and recoverable behaviors should be integrated early into the development process. Emergent behaviors from large-scale deployment of interacting autonomous systems poses a difficult challenge. The analysis and test burden would thereby, be shifted to a simpler, more deterministic run-time assurance mechanism. The effort for new approaches to TEVV endeavors to provide a structured argument, supported by evidence, justifying that a system is acceptably safe and secure not only through offline tests, but also through reliance on real-time monitoring, prediction, and fail-safe recovery. Within this paradigm, formal design approaches (such as those advocated in the previous goals) might provide the offline design considerations and formalisms necessary for articulating the allowable and certifiable behaviors of the advanced, uncertified system and for validating the design of a run-time constraint, as well as prediction and recovery methods.

An assurance case can be defined as a structured argument, supported by evidence, intended to justify that a system is acceptably safe and secure. A defensible argument of acceptable risk is required as part of the regulatory process, with a certificate of assurance being granted only when the regulator is satisfied by the argument presented. The previously mentioned TEVV approaches can collectively provide a body of evidence to be presented to a certification board, and ultimately the milestone decision authority, to determine an acceptable level of safety, security, performance, and risk for a specific platform. It will not be possible that any single method for V&V will be adequate for all future autonomous systems. Therefore, not only do multiple new TEVV methods need to be employed to enable the fielding of autonomous systems, but a new research area needs to be investigated to formally articulate and verify that the assurance argument itself is valid. This structured argument-based approach must be developed in coordination with and as an integral part of the Test and Evaluation Plan (TEP) and the Test and Evaluation Master Plan (TEMP), providing a claim of how the V&V activities will attempt to quantify risks and mitigation strategies to inform risk-acceptance decisions. Additionally, standard autonomy argument templates can be developed to enable the reuse of explicit arguments of risk, performance, and safety that are closely tied to autonomy requirements and TEVV best practices. The templates will provide an acceptable collection of evidence for an autonomous system.

The Autonomy Community of Interest TEVV Working Group within OUASD(R&E) has identified four current challenges to autonomy TEVV and six gaps in the current V&V processes when applied to systems that have higher levels of autonomy. To remedy these current shortcomings the working group outlined five goals aimed at modernizing the TEVV of autonomous systems. These goals are intended to align DoD Research and Development programs and allow them to overcome the unique challenges posed by performing TEVV practices on advanced autonomous systems.[12]

The integration into the National Airspace System (NAS) of unmanned aircraft systems (UAS) with autonomous capabilities will be a major challenge in the TEVV of these systems.

---

[12] Technology Investment Strategy 2015-2018, DoD R&E Autonomy COI TEVV Working Group, May 2015

As UASs become more prevalent, complex, and autonomous, their integration and maintenance of Safety of Flight must be addressed through close coordination between all government stakeholders to ensure they can safely operate in the United States. Additionally, the growing use of Electromagnetic Spectrum (EMS) by commercial entities is restricting access to DoD, and this may potentially impact the TEVV of fully autonomous system, which will rely on EMS access to a greater degree than other weapons systems. Both challenges will require DoD to coordinate with other government agencies to ensure that the TEVV of UASs with autonomous capabilities can be conducted in a safe, effective, and comprehensive manner within the United States.

2.3.2   Way Ahead

The development of effective methods to record, aggregate, and reuse test and evaluation (T&E) results remains an elusive and technically challenging problem. It is important that the V&V tools and techniques used early in the process to define requirements and develop systems support the transition of autonomous systems to the DT and OT communities. DoD shall improve the transition from DT to OT to assist with defining the TEP. A more well-defined TEP will increase the focus and effectiveness of testing implementation for unmanned systems. T&E methods are required to record, aggregate, leverage, and reuse modeling and simulation (M&S) and T&E results throughout the systems engineering process, spanning requirements to model-based designs, and live virtual construction experimentation to open-range testing. These methods need to become standards that are implemented across all future programs. Additionally, statistics-based design of experiments (DOE) will need methods containing mathematical constructs capable of designing affordable test matrices for non-deterministic autonomous software.

2.4   Data Transport Integration

It is anticipated that the sensor mixes, collection rates, and amount of data produced by unmanned systems will continue to exponentially increase. This creates a data strategy challenge and provides opportunities in pre-processing, processing, and analytics to fuse the time-sensitive data to provide the Warfighter with timely decision-quality information, enabling technical advantage on the battlefield. The data strategies need to include the architecture, analytics, storage, management, and modeling components of the unmanned system, and integrate with the existing and future intelligence production centers. The data variety will create a challenge and opportunity in the employment of the strategy to manage, process, and analyze. The data strategies need to provide meaning and context to the Warfighter, transforming the overwhelming amount of data into information that the Warfighter can use to make decisions. Data variety will include on-board sensor systems, off-board sensors, and C2 data providing both situational awareness and contextual information to understand intent and provide time-sensitive decision-quality results. Government ownership of the technical baseline and aligning data to standard formats that enable collaboration across unmanned systems is advancing. Open architecture standards are enabling advanced data analytics. Commercial industry practices are driving plug and play architectures, allowing for agile operations in acquiring advanced data analytics.

Future operating environments are expected to be both contested and congested. This will create new challenges and opportunities for unmanned systems and the data strategies that they employ. With the anticipation of contested and congested environments, data processing and analytics closer to the leading edge are vitally important. Whether the unmanned system is airborne, ground based, or sea based, communication is critical to the employed data strategies. Unmanned systems must be able to operate in automatic or autonomous control affecting the employed data strategies, thereby automatically analyzing data and developing decision-level results. Unmanned systems with greater levels of autonomy would be capable of containing vast amounts of sensitive data. It will be crucial to ensure that these sensitive data sets are properly secured to ensure their safety from adversaries, should the system be comprised either through physical capture or cyberattack.

Over the past decade, usage of manned and unmanned intelligence, surveillance, and reconnaissance (ISR) capabilities proliferated exponentially to address collection requirements in support of globally dispersed operations. The Services and other DoD organizations developed and resourced capabilities to support urgent Combatant Command (CCMD) requirements using both major acquisition programs of record and quick reaction capabilities. In the absence of an overarching strategy to field these systems, the resulting data transport capabilities were Service and platform specific, with little integration across platforms. This led to significant gaps in coverage, inconsistent and often inadequate delivery of data to required consumers, and delays in meeting urgent warfighter requirements.

ISR data transport supports globally dispersed strategic, operational, and tactical consumers at the time and place and with the quantity and quality they need. Timely and assured delivery of ISR data is required to enable fused intelligence and active mission data that warfighters can act upon during globally integrated operations in support of counterterrorism, theater campaign plans, and contingency operations.

As illustrated in recent counterterrorism operations, all ISR platforms, to include our smaller tactical UAS (e.g., Scan Eagle) and ground/maritime unmanned platforms, have potential strategic and operational impacts requiring near real-time delivery of video and other sensor data to theater operations centers and rear area headquarters to support urgent targeting and force protection decisions.

2.4.1 Challenges

Establishing effective executive oversight to cut across CCMD/Service/Agency boundaries and drive joint synchronized infrastructure capabilities is critical to resolving current data transport issues. With a reliance on using rapidly changing commercial off-the-shelf capabilities to meet data transport requirements, defining interoperability standards is no longer sufficient to ensuring DoD-wide integration. Military standards and commercial standards are not bound by the same requirements. The Department's focus must shift towards building universal transport capabilities that potentially leverage multiple vendor products to support common data transport requirements. Teaming efforts that cut across CCMD/Service/Agency boundaries to build universal gateway and relay capabilities have the potential for dramatically improving mission performance while also reducing the overall cost of transport infrastructure. U.S. Special Operations Command provides a useful illustration of this. They teamed with the USAF to modify their remotely piloted aircraft (RPA) gateway in the Pacific to support manned

aircraft operating in theater. Building a new satellite gateway to support these platforms would have cost much more for the initial installation, as well as millions more for the annual operations and maintenance.

There are many challenges impeding success in advancing DoD data strategies with unmanned systems. In many cases, the government does not own the technical baseline of a system. This places ownership of the data strategies on a single contractor and impedes our ability to advance data analytics. Government ownership of the data strategy allows for innovation and informed decision making in using data strategies and analytics.

Maintaining antiquated IT equipment leads to cost growth and inferior capability. The commercial sector is often driving advancements in data strategies and open system architectures. Staying current with commercial sector data strategies is critical to being agile in advancing data analytics, controlling cost growth, and sustainment.

Trust in data analytics is often a barrier to data strategies. Manual analysis of raw data is impractical and impossible given the volume, variety, and veracity of the data. Contested environments make this even more challenging by forcing the data strategies to be more automated in support of decision making. Analysts need to be able to trust unmanned systems data analytics and strategies to process, store, fuse, analyze, and report information.

2.4.2 Way Ahead

Unmanned systems need the ability to collect and automatically process data and autonomously adjust the data strategies based on mission, environment, and situation. The platform will be required to perform these tasks onboard, in real time, and determine the mission critical information required to be transmitted to the operator. Autonomous data strategy adaptation is the ability of a system to automatically make decisions in real-time around its data processing, storage, fusion, analysis, and reporting activities, and will ensure that decision-quality information is produced. Technologies like deep neural networks and neuromorphic computing will advance to allow the strategies to learn, think and employ capabilities that adapt to situational changes. Often these strategies will need to be employed in real-time with the understanding of mission goals and constraints. The future envisions the data strategy to be agile, responsive, adaptive, and protected.

In the near-term, the Department must establish common standards for access to ISR data repositories and federated delivery capabilities. Figure 2 highlights some key transport capability blocks required to provide assured and responsive delivery of data to dispersed consumers.
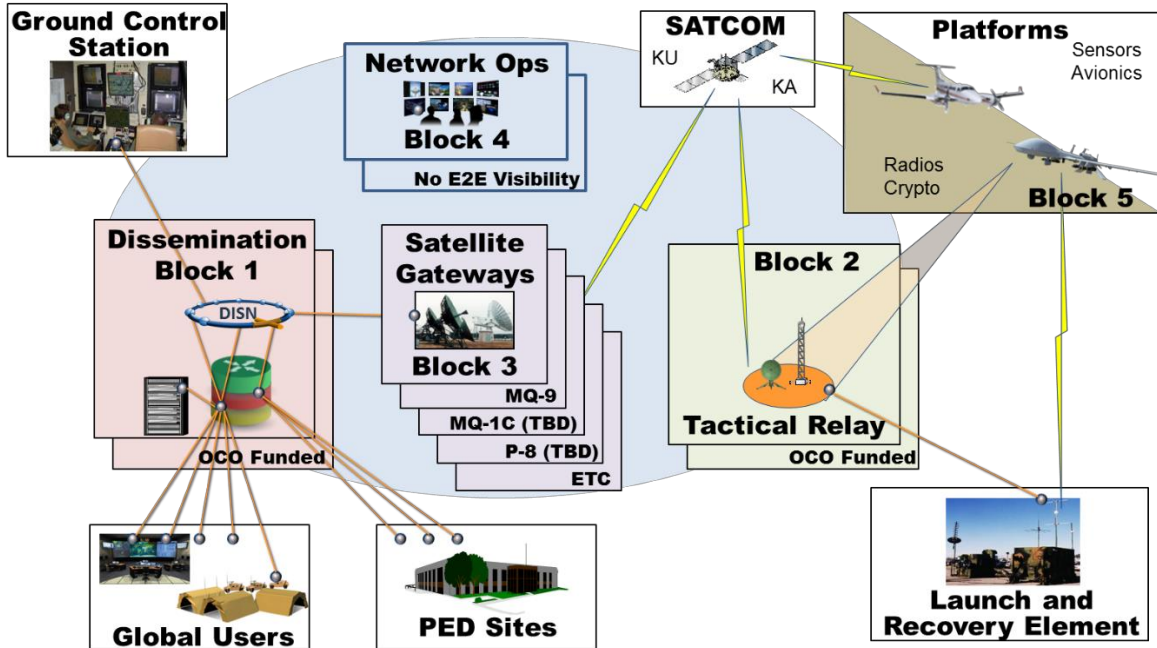
Figure 2: ISR Data Transport Capabilities

Over the next three years the Joint Information Environment (JIE) Executive Committee (EXCOM) will identify core requirements for each of these capability blocks, document them via the joint requirements process, and recommend appropriate material/non-material capability development efforts. Although developed for airborne ISR (AISR), the same blocks are applicable for all domain platforms as the transport infrastructure is platform agnostic.

- **Block 1 (Dissemination)** will build common interface points for DoD and coalition/ mission partner sensor data leveraging the DoD Information Systems Network (DISN) for global delivery. By FY21, the department will have a programmed capability to ingest and distribute sensor/video data in near real-time to limited high-resolution and multiple low-resolution consumers on US classified and coalition releasable networks.

- **Block 2 (Tactical Relay)** provides line of sight (LOS)-only sensor platform (e.g., small UAS) connectivity to the DISN for global distribution, as well as supporting beyond line of sight (BLOS) sensor platforms that have insufficient connectivity to strategic gateways with DISN access. By FY22, a defined and programmed tactical capability(s) will be readily available to support a limited number of sensor platforms.

- **Block 3 (Satellite Gateways)** builds universal gateways to support multiple platform types (e.g., manned and unmanned aircraft) and multiple sensor types (e.g., full-motion video, signals intelligence) in all CCMD areas of operation, providing connectivity within established theater contingency timelines. Wherever possible, block 3 will leverage existing DoD strategic gateways to maximize performance and minimize resources required to provide this capability. By FY23, a system of universal gateways

will be available to support global distribution of sensor data interconnected via the DISN.

- **Block 4 (Network Operations (NETOPs))** establishes common situational awareness and visibility of both space, aerial, and terrestrial network components from end to end. By FY24, the Department will integrate the current disparate NETOPs activities and establish a common operating picture for sensor data transport capabilities.

- **Block 5 (Platforms)** will focus on life-cycle upgrades to existing platforms in FY19-23, leveraging state-of-the-art multi-band satellite capabilities to access both commercial and military satellite systems, while improving survivability in an anti-access environment. By FY24, both LOS and BLOS platform radio capabilities will employ National Security Agency (NSA)-approved encryption to prevent hostile intercept/tampering and assure delivery of C2 and sensor traffic.

By the mid-2020s, the Department will address operations in less permissive environments, to include adding anti-jam and low probability of intercept/detection capabilities. These capabilities will be integrated into the end-to-end architecture, and ensure that state-of-the-art cyber defense detection and prevention systems are employed.

2.5   Data Rights

DoD procurement of proprietary systems is fiscally inefficient and restricts the fielding of common robotic platforms with customized payloads for various DoD end users. Commercial-off-the-shelf (COTS) systems that lack open hardware and software interfaces create an unfavorable business model for the acquisition of unmanned systems.

Secured data rights allows for long term sustainment, modernization, and competition planning without being dependent or beholden to the owners of the data. DoD should seek to negotiate the appropriate data rights as determined by the program offices to support the entire life cycle of the system prior to entering into all unmanned systems contracts and agreements.

2.5.1   Challenges

DoD had acquired numerous legacy and COTS systems over the years to meet urgent needs/requirements. Due to the urgency to obtain these systems, the data rights and technical baselines received are often limited. Therefore, DoD is constrained in making the necessary updates to controllers and software that keep pace with the changing operational environments of these unmanned systems. Even in programs that are routine, and where DoD does its due diligence in contracting for data rights and technical baselines, they are not always granted by the contractor. To date, DoD has not been consistently successful in asserting its rights to the data necessary to perform the required work in house (updates, modifications, etc.), or in negotiating to get additional rights after the fact. These additional data rights are often prohibitively expensive, resulting in DoD contracting with the data rights owner for upgrades, modifications, or updates. This activity incurs a cost which compounds as continuous updates are required.

2.5.2   Way Ahead

In the near-term, DoD needs to consider the cost benefit of acquiring the data rights to existing systems when it is most beneficial and efficient. DoD must consider adjusting data rights policy when considering contracting price and effort. In addition, program offices must increase vigilance in obtaining and defending contracted data rights focusing on improving a capability's performance or decreasing cost. The government must develop a strategy for information ownership, by either using a framework or by determining a cost-effective approach for procuring critical data rights.

In the mid- to far-term, DoD should have well established data rights policies in place to secure the necessary critical system information to ensure maximum mission support and flexibility. Having modularity and common architectures built into a project will provide added levels of security against using company-specific proprietary systems that make updates to these systems unachievable. However, it will be important to identify and focus on the areas where the government can own the frameworks and define their inputs and outputs to facilitate future capability insertions.

3   Autonomy

U.S. military strategy in the modern era has focused on maintaining technological superiority over our adversaries. However, the ability of DoD to maintain a strategic advantage over its adversaries through developments in science and technology (S&T) is being challenged by globalization and the information revolution. Ongoing advancements in autonomy offer DoD the ability to maintain its technical superiority in a variety of areas, including unmanned systems. Due to the revolutionary potential of the technology, DoD must continue to pursue innovations in autonomy that enhance the integration of unmanned systems into the future Joint Force structure.

Autonomy is defined as the ability of an entity to independently develop and select among different courses of action to achieve goals based on the entity's knowledge and understanding of the world, itself, and the situation. Autonomous systems are governed by broad rules that allow the system to deviate from the baseline. This is in contrast to automated systems, which are governed by prescriptive rules that allow for no deviations. While early robots generally only exhibited automated capabilities, advances in artificial intelligence (AI) and machine learning (ML) technology allow systems with greater levels of autonomous capabilities to be developed.[13] The future of unmanned systems will stretch across the broad spectrum of autonomy, from remote controlled and automated systems to near fully autonomous, as needed to support the mission. A summary of the future path for the four key enablers for autonomy is shown in Table 3.

> *"We are in a period of incredible technological flux. Advances in autonomy and in artificial intelligence and autonomous control systems and advanced computing and big data, and learning machines and intuitive graphic visualization tools, metamaterials, miniaturization -- they're leading us to a time of great human-machine collaboration…"*
>
> *-Former DARPA Director (2012-2017) Arati Prabhakar*

---

[13] Defense Science Board: Summer Study on Autonomy June 2016

		2017 - - - - - - - - 2029 - - - - - - - - 2042		
		NEAR-TERM	**MID-TERM**	**FAR-TERM**
AUTONOMY	Artificial Intelligence/ Machine Learning	-Private Sector Collaboration -Cloud Technologies	-Augmented Reality -Virtual Reality	-Persistent Sensing -Highly Autonomous
	Increased Efficiency and Effectivness	-Increased Safety & Efficiency	-Unmanned Tasks, Ops -Leader-Follower	-Swarming
	Trust	-Tasking Guidance and Validation, Ethical Requirements for Human Decisions		
	Weaponization	-DoD Strategy Consensus -LAWS assessment	-Armed Wingman/Teammate (Human Decision to Engage)	

Table 3: Comprehensive Roadmap for Autonomy

3.1 Artificial Intelligence and Machine Learning

ML is a rapidly growing field within AI that has massive potential to advance unmanned systems in a variety of areas, including: C2, navigation, perception (sensor intelligence and sensor fusion), obstacle detection and avoidance, swarm behavior and tactics, and human interaction.[14] Deep learning, a promising form of artificial neural networks, can leverage the many cores of graphical processing units (GPUs), conventional CPUs and custom neuromorphic chips to learn patterns and models in data. AI and ML will allow the development of systems that are capable of learning and making high-quality decisions autonomously. This ability to learn will directly result in the development of unmanned systems with greater levels of autonomy, which will impart expanded and improved functionality. Furthermore, autonomous unmanned systems will vastly enhance battlespace awareness maximizing the utility of AI/ML-enabled decision aids that will revolutionize battlespace management and C2.[15]

3.1.1 Challenges

While significant advances are being made in AI, there are several challenges to the full adaptation of these technologies in unmanned systems. Although safety, reliability, and trust of AI-based systems remain areas of active research, AI must overcome crucial perception and trust issues to become accepted. Policy and legal restrictions (including international) must also evolve. M&S and TEVV must revolutionize to accommodate AI/ML capabilities. Unmanned systems also have unique technical requirements with regards to size, weight, and power (SWaP) restrictions. Additionally, many of the current AI data processing platforms run computations in cloud environments, which may not be suitable for unmanned systems operating in communications-denied environments. However, this challenge may be mitigated in the future

---

[14] http://www.defense.gov/News-Article-View/Article/716156/work-robot-warship-demonstrates-advances-in-autonomy-human-machine-collaboration
[15] TRADOC Pamphlet 525-3-1 USA Operating Concept 2020-2040

as industry leaders develop cloud solutions that may be embedded in unmanned systems. Improved TEVV and demonstration of ultimate human control over autonomous unmanned systems must be determined to build trust with artificial intelligence and machine learning solutions.

> *"I don't ever expect the human element to be completely absent; there will always be a command element in there. But there's more, much more, we can do. In the end, what do you want? You want actionable knowledge… and you want to get that as fast as possible."*
>
> *-Navy Rear Adm. Robert Girrier*

Data quality is another issue that must be addressed to integrate AI/ML into unmanned systems. Quality data is the foundation of automated analysis and subsequently decisions that are made in support of operations. Quality is not just impacted at the point of origin/collection, but more so when it is transformed into various interpretable forms by the system. DoD must establish and adhere to enterprise data standards, and conduct deliberate enterprise assessments of data quality. This quality data is needed to enable increased automation to support on-board tactical processing, swarm technology, time-dominant decisions, and eventually full autonomy.

3.1.2 Way Ahead

In the near-term, DoD should strengthen connections to the private sector so that as AI/ML solutions mature, DoD is able to procure the most promising solutions and use them in unmanned systems. Many AI/ML solutions rely on large, integrated cloud technologies for data storage, processing, and dissemination. As a result, DoD should seek to heavily exploit cloud technologies and allow them to be adapted for use in AI/ML solutions. To accomplish this, data collection, standardization, and sharing needs to be addressed throughout and across the services. DoD must also continue to lead the national and international discussions concerning AI perception, policy, and laws.

In the mid-term, AI/ML solutions will likely have matured in M&S, TEVV, and SWaP usage to the point where it is possible to embed them into unmanned systems. As AI/ML advances, DoD should invest in augmented reality and virtual reality interfaces that allow for enhanced interaction between unmanned systems and human operators. DoD will also need to continue to embrace and encourage industry development and sustainment of AI/ML open architectures, and enhance partnerships with industry and academia to reap the benefits. Concerns that intelligent machines may pose a danger to the human shall be addressed through improved TEVV and demonstration of ultimate human control over autonomous unmanned systems.

In the far-term, advances in deep AI will allow for the development of applications that give human operators control and persistent sensing from unmanned systems. Advances in AI and computing will enable machine systems (including unmanned systems) with human-like intelligence, both in terms of learning and decision making.

3.2 Increased Efficiency and Effectiveness

Increased autonomy will enable unmanned systems to perform a greater range of tasks, which will directly increase operational capability.[16] Greater autonomy will also remove the need for constant input from human operators. This will allow for higher-level control or supervision of multiple unmanned assets simultaneously, and will increase effectiveness by reducing the operator's cognitive load, allowing operators to make command decisions and perform other high-level tasks.[17] Machine-to-machine interactions between autonomous systems will promote efficiencies, especially in complex environments, by enabling self-organization, division of tasking, and the coordination of activities. The ability of autonomous systems to ingest, process, and analyze large complex data sets and communicate valuable data trends or correlations to humans through data visualization will have benefits for both humans and autonomous systems. This type of human-machine interaction will allow humans to make more informed and better decision as well as enhance the learning process of autonomous systems by providing them frequent system feedback. Finally, elevated levels of autonomy will increase the decision speeds of unmanned systems and allow them to perform tasks that require decision cycles faster than human reaction time, greatly increasing their operational capabilities in a variety of mission areas, such as missile defense.[18] Technological advancements that increase the efficiency and effectiveness of unmanned systems will be crucial to the development of a military of the future.

3.2.1 Challenges

The increased efficiency and effectiveness that will be realized by increased autonomy are currently limited by legal and policy constraints, trust issues, and technical challenges. Increased autonomy will allow unmanned systems to perform tasks that previously could only be performed by humans. The most contentious of these tasks will involve the use of lethal force. Technologies underpinning unmanned systems would make it possible to develop and deploy autonomous systems that could independently select and attack targets with lethal force.[19]

The deployment of unmanned systems in a greater range of operational scenarios and with greater frequency will also fundamentally change military training requirements, personnel management, and force structure. As autonomous systems become more advanced it will be critical to investigate, understand, and document their interaction with humans. Operators and commanders will need a high degree of understanding of how these systems operate and how they will respond in various operating environments and when faced with particular operational challenges. The challenges posed by human-machine teaming will be overcome by effective training of the human operators and team-members as well as the development of the machines involved to enhance understanding of common team objectives, their separate roles, and the ways in which they are co-dependent. Lessons learned during the development and operation of human-machine teams can then be applied in the subsequent development and operation of more autonomous systems, as appropriate.

---

[16] http://www.defense.gov/News-Article-View/Article/716156/work-robot-warship-demonstrates-advances-in-autonomy-human-machine-collaboration
[17] The US Army: Robotic and Autonomous Systems Strategy
[18] Defense Science Board: Summer Study on Autonomy June 2016
[19] United States Air Force RPA Vector: Vision and Enabling Concepts 2013-2038

3.2.2   Way Ahead

The expansion of capabilities in unmanned systems over the coming decades will largely be dependent on the ability to effectively team humans and autonomous systems in the force structure. In the near-term, advances need to be made that increase operational safety and efficiency, such as in-air collision avoidance and automated safety features for ground vehicles.

In the mid-term, autonomy algorithms, improved sensors, and computer processing will improve teaming of humans and machines, evolving from task level support to operational support, and will allow machines to directly assist humans in a variety of operations. For example, elevated levels of autonomy in unmanned systems will allow for leader-follower capabilities, where trailing semi-autonomous vehicles follow a designated lead vehicle in logistics convoy operations. Similarly, autonomous "robotic wingmen" may accompany piloted aircraft, crewed ground fighting vehicles, and crewed surface and underwater vessels.

Finally, in the far-term, humans will form integrated teams with nearly fully autonomous unmanned systems, capable of carrying out operations in contested environments. This could include heterogeneous swarms of UAS directly supporting soldiers on the ground through ISR or aerial strikes.

3.3   Trust

Trust is complex and multi-dimensional.[20] As a result, trust of autonomous systems must be established by the continual assessment of key indicators of behavior and function, beginning in the development stage and continuing throughout all stages of a system's life cycle. Extensive assurance helps to promote trust not only for the operator and commander, but also for designers, testers, policy and lawmakers, and the public as a whole. Furthermore, autonomous systems must exhibit run-time transparency, and be capable of explaining decisions and actions, as well as communicating goals and plans in a concise and usable format to human operators. Establishing trust with operators in this manner will ensure that human authority remains at the center of mission approval for autonomous systems and ensures effective human-machine teaming. Without an adequate level of trust between operators/commanders and autonomous unmanned systems, to function properly with a high degree of consistency, these systems will not be used in any mission set.

3.3.1   Challenges

A lack of trust by the Warfighters, and the wider public, is a major roadblock in DoD's continued development and use of autonomous unmanned systems. This lack of trust is highlighted by international efforts at the United Nations (UN) to consider policies that would prohibit the deployment of autonomous systems with lethal capabilities. Additionally, there are technological shortcomings in the current abilities of AI regarding ethical thinking that may limit the public's trust of autonomous unmanned systems developed for military capabilities. Situational ethical reasoning is currently not coherently implementable by AI in the range of scenarios that military forces may encounter. Given this limitation, it is paramount to ensure that

---

[20] "Trust in Automation" Vol. 28, Issue 1 (January/February 2013)

human authority, accountability, and the ability to maintain C2 are preserved as increasing numbers of unmanned systems become more widely deployed.

3.3.2 Way Ahead

DoD will continue to update the existing military framework of operation orders (OPORDs) and cooperative tasking to include tasking guidance and validation for unmanned systems. Additionally, analysis of military missions can identify what ethical requirements will require the input of a human decision maker. This type of thinking should be applied to the use of proposed/planned autonomous unmanned systems. An initial manned/unmanned teaming (MUM-T) campaign-of-learning could explore several elements of human-machine integration to establish foundations for trust.

Success in this area will provide commanders, policymakers, lawmakers, the public, and other applicable stakeholders with confidence in the ethical framework. Human-directed tactical tasking of unmanned systems and the overall performance of these systems can and will be shown to meet all ethical requirements for the rules of engagement (ROE) and the Law of Armed Conflict (LOAC).

3.4   Weaponization

In considering the specific use of weaponized systems, Department of Defense Directive (DoDD) 3000.09, Autonomy in Weapon Systems, signed in November 2012, established policies and assigned responsibilities to shape the development and use of autonomous functions in weapon systems, including manned and unmanned platforms. It mandates that autonomous and semi-autonomous weapon systems be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force. DoDD 3000.09 also requires that persons who authorize the use of, direct the use of, or operate autonomous and semi-autonomous weapon systems must do so with appropriate care and in accordance with the law of war, applicable treaties, weapon system safety rules, and applicable ROE. DoDD 3000.09 underwent a mandatory periodical update with administrative changes (Change 1, May 8, 2017), but a more substantive update was expected to be completed in late 2017. That substantive update, when released, is expected to involve clarifications of definitions and processes rather than a shift in the overall thrust of the policy.

DoD does not currently have an autonomous weapon system that can search for, identify, track, select, and engage targets independent of a human operator's input. These tasks currently rely heavily on a human operator using remote operation, also referred to as "tele-operation." In the future weaponization will be a crucial capability in mission sets where the unmanned system is directly supporting forces engaging in hazardous tasks.

3.4.1 Challenges

In the realms of public and international diplomacy, concerned states, non-governmental organizations (NGOs), and experts in AI have urged an immediate and intensive effort to formulate and secure an international treaty restricting the development, deployment, and use of weapon systems that can autonomously locate, select, and attack human targets. In response to

similar expressions of concern from some High Contracting Parties to the Geneva Conventions on Certain Conventional Weapons (CCW), the UN Office in Geneva hosted informal experts' meetings on lethal autonomous weapon systems (LAWS) in 2014, 2015, and 2016. The CCW established a Group of Governmental Experts (GGE) which met to discuss LAWS in a more formalized setting in 2017. A second meeting is foreseen for 27 to 31 August 2018.[21] If such restrictions on autonomous weapon systems were to come into existence, and if the U.S. were to follow it, the ban would severely limit the ability to develop and use lethal autonomous weapon systems.

3.4.2 Way Ahead

In the near-term various departmental and interagency working groups will continue to address the variety of diplomatic, policy, legal, and implementation issues relating to LAWS. To inform departmental efforts in those working groups, structure future force development efforts, and inform the update to DoDD 3000.09, the Deputy Secretary of Defense and Vice Chairman of the Joint Chiefs of Staff commissioned a 90-day assessment of LAWS and AI. Additionally, the 2018-2022 Defense Planning Guidance (DPG) included direction on autonomous weapons development and future departmental-level force planning guidance is likely to contain guidance on the topic.

In the mid- to far-term there will be rapid growth in the development of highly autonomous unmanned systems with the potential to be armed. These advances will come as AI enables increasingly complex machine response capabilities. These systems will be deployed alongside Warfighters and focus on mission tasks where there is a high probability of injury or death. Unmanned Systems with integrated AI, acting as a wingman or teammate, with lethal armament could perform the vast majority of the actions associated with target identification, tracking, threat prioritization, and post-attack assessment while tracking the position and ensuring the safety of blue-force assets –minimizing the risk to its human teammates. This level of automation will alleviate the human operator of task level activities associated with the engagement of a target, allowing the operator to focus on the identified threat and the decision to engage.

---

[21] 2018 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS). https://www.unog.ch/80256EE600585943/(httpPages)/7C335E71DFCB29D1C1258243003E8724?OpenDocument

4   Secure Network

In today's environment where many of an organization's mission-critical functions are dependent upon information technology (IT), the ability to manage this technology and to assure confidentiality, integrity, reliability, scalability, and availability of information is essential. As a result of DoD's increasing reliance on IT, the security of information systems is more of a focal point for commanders at all levels. This problem is especially apparent in unmanned systems, which by their very nature have an elevated

> *"Soon, all wars will have a cyber component. There will be traditional wars with cyber aspects. And there will be stand-alone cyber conflicts. But the future is less about massed armies and more about the combination of IT, unmanned systems and surgical special forces. In all of these areas, we are unprepared and under-investing."*
>
> *- Senators Joni Ernst (R-IA) and Ben Sasse (R-NE)*

reliance on information systems to function safely, effectively, and consistently. As unmanned systems continue to become more autonomous and integral to the overall DoD military strategy, the availability, reliability, and scalability of the network becomes increasingly critical with the addition of autonomy in the battlespace. A summary of the future path for the three key enablers for secure networks is shown in Table 4.

SECURE NETWORK		2017 - - - - - - - - - - 2029 - - - - - - - - - - 2042	
		NEAR-TERM	MID-TERM FAR-TERM
	Cyber Operations	-Defense in Depth -Vulnerability Assessment	-Transition to Cyberattack Resilience -Autonomous Cyber Defense
	Information Assurance	-Private Sector Collaboration	-Develop & Evolve IA Policies, Procedures, Techniques -Suite of IA Products/Technologies for Unmanned Systems
	Spectrum/ Electronic Warfare	-More Efficient, Flexible, Adaptable, Agile Spectrum for Sustained Operations -Hardened Robust Electronic Protection	

Table 4: Comprehensive Roadmap for Secure Networks

4.1   Cyber Operations

Across the federal government, cyber is a point of emphasis[22]. This is especially true in DoD where nearly every new advanced weapon system relies heavily on a network of information systems. Unmanned systems may be at an even greater risk of cyberattack than traditional systems, due to their autonomy and potential operations in communication and/or Global

---

[22] http://www.ernst.senate.gov/public/index.cfm/columns?ID=F039F811-2D93-48D3-96B6-FD1DC166A620

Positioning System (GPS)-denied environments. This risk is further exacerbated due to the lethal capabilities that some of these systems possess. As a result, cyber expertise and technology must be fully integrated from the onset in the development of unmanned systems architectures.[23] These systems must also be designed with flexibility and the ability to add updates as new cyberattack vectors are identified and new capabilities are incorporated.[24] For unmanned systems to effectively operate, they must maintain integrity, availability, and the confidentiality of sensitive information. If adversaries are able to exploit cyber vulnerabilities in an unmanned system to corrupt any one of these three objectives, the result could be a variety of critical failures, including loss of C2.[25]

4.1.1 Challenges

The challenge of incorporating security measures into unmanned systems is similar to that of manned systems, however there are C2 requirements which are unique to unmanned systems and expand their overall requirement for security. The added complexity of these systems and the new technologies they often employ increases the opportunity for adversaries to discover and exploit zero-day vulnerabilities, which may rapidly and severely compromise unmanned systems in new or unexpected ways. This system complexity along with the wide range of capabilities that these systems will be expected to perform will increase the number of attack surfaces for adversaries to exploit.[26]

Additionally, it will be challenging to ensure that the underlying architectures of unmanned systems consistently remain in a properly patched and configured state to eliminate any known cyber vulnerabilities. Cyber is made more challenging by the rapid advancement in the capabilities and design of unmanned systems, which makes fully testing the security of each new iteration extremely difficult. The network needs to be able to handle adding new systems without that affecting the security, availability, throughput, or reliability.

4.1.2 Way Ahead

In the near-term, DoD should move beyond boundary protection. This level of protection alone has been shown to be inadequate at protecting from the full range of cyber threats that may impact an information system. DoD should begin developing and implementing defense-in-depth for unmanned systems to combat cyber threats from the insider, supply chain, or Trojan horses latent in software. Due to unmanned systems' frequent use and reliance on sensors, a database that captures potential or known cybersecurity vulnerabilities of the various sensors should be developed. This will ensure that vulnerabilities are identified as early as possible in development and that steps to mitigate these vulnerabilities can be taken.

In the mid- to far-term, DoD should transition from a cyber defense that focuses on robustness (i.e., resisting an attack) and instead focus on resilience (i.e., recovering from an attack and/or maintaining as much mission performance as possible while operating through an attack). The resilience approach is favorable over robustness in unmanned systems, due to the complexity that autonomy brings and the requirement for these systems to operate in

---

[23] The US Army: Robotic and Autonomous Systems Strategy
[24] Defense Science Board: Summer Study on Autonomy June 2016
[25] Ibid.
[26] Ibid.

communication-denied environments, making network-centric approaches unviable. Additionally, allowing unmanned systems to defend themselves autonomously using resilience measures could allow for near-instant responses to cyberattacks.[27]

The 2015 DoD Cyber Strategy lists specific goals and objectives in detail for cyberspace missions. Advancements toward these goals and objectives will directly impact the effectiveness and availability of unmanned systems.[28]

4.2 Information Assurance

Information assurance applies to and touches on all mission sets currently identified for unmanned systems. Unmanned systems have the potential to operate and store some level of sensitive data, which will require the use of secure architectures. Mission sets that handle extremely sensitive information (such as ISR) may even require the use of elevated or additional information assurance solutions to ensure that data is kept fully intact and confidential.

4.2.1 Challenges

The largest challenge facing information assurance in unmanned systems is the lack of high assurance solutions developed specifically for unmanned systems. To remedy this problem, end-users must develop a close and trusted relationship with approving authorities, such as the NSA. These types of relationships will allow all stakeholders to ensure the effective and efficient development of high assurance solutions that are not only sufficiently secure, but also designed to perform in the unique operating environments of unmanned systems. Additionally, special considerations should be given to unmanned systems that have the ability to store sensitive information.

4.2.2 Way Ahead

Currently, there are no high assurance security solutions designed specifically for use in unmanned systems. The dual-use solutions that are currently employed result in an ineffective use of funding and an end product that is insufficiently secure. In the near-term, DoD should seek to develop and approve a trusted suite of high assurance security solutions that are designed for a specific category of unmanned systems. Additionally, DoD must continue to develop and strengthen ties with commercial companies that develop and provide information security products and services. Over the next several years these companies will likely play an ever increasingly important role in developing information assurance technologies and solutions for unmanned systems.

In the mid- to far-term, as DoD continues to develop more unmanned systems and use more network capacity to collaborate, it will be essential to develop and evolve policies, procedures, and techniques to secure all aspects of this information infrastructure. Not only will

---

[27] Defense Science Board: Summer Study on Autonomy June 2016
[28] Department of Defense, Cyber Strategy, 2015

information within the boundary need to be secured, but information that leaves the boundary must also be secured.

At this stage DoD should work to develop a suite of information assurance technologies approved specifically for use in unmanned systems within their operational environments. This will require sustainment of this suite of technologies to ensure their continued effectiveness in unmanned systems.

4.3   Electromagnetic Spectrum and Electronic Warfare

Sufficient EMS access is crucial to DoD's ability to conduct modern military operations. Unmanned systems are particularly dependent on the EMS to ensure effective and consistent communication with operators. This is highlighted in the DoD Electromagnetic Spectrum Strategy which states, "The growth in the complexity of modern military systems has similarly led to an increase in spectrum requirements. Some examples include: the increased reliance on unmanned vehicles to collect ISR information and relay communications."[29] EMS superiority during conflict is something that can no longer be guaranteed or assumed. Our adversaries continue to invest in the development of electronic warfare (EW) assets in an attempt to deny access to critical portions of the EMS. Additionally, all Services at all levels have paid insufficient attention to EW, a fact that was highlighted in 2014 by the Defense Science Board. This combination has eroded DoD's dominance in the area of EW.[30] Due to unmanned systems' heavy reliance on spectrum access and susceptibility to forms of electronic attack, unmanned systems must be hardened with robust electronic protection capabilities, and be spectrally efficient, flexible, and adaptable while operating in contested environments. If denied access to EMS, through electronic attack or lack of available spectrum bandwidth, unmanned systems may not be able to communicate with their operators, resulting in the loss of key operational capabilities.

4.3.1   Challenges

The dependence of unmanned systems on EMS is a vulnerability that our adversaries may seek to exploit, particularly as unmanned systems become a more important part of U.S. military operations. For example, non-kinetic attacks may be capable of disabling subsystems or interfering with spectrum access to inhibit communication. If this threat is not accounted for and unmanned systems are left vulnerable to electronic attack, these systems may be a liability if deployed against "pacing competitors" (also referred to as "near-peer adversaries").[31]

In recent years, demand for spectrum from commercial entities in the global wireless broadband industry has increased significantly. This is largely due to the increased use of wireless devices and the associated data-intensive applications that these devices operate. The trend of diminishing spectrum is likely to persist as the rise in mobile network traffic outpaces usage efficiency gains over the coming years.[32] As the amount of available spectrum decreases

---

[29] Department of Defense, Electromagnetic Spectrum Strategy, 2013
[30] Department of Defense, Electronic Warfare Strategy, 2017
[31] Ibid.
[32] Department of Defense, Electromagnetic Spectrum Strategy, 2013

due to greater demands from DoD, commercial entities, and hobbyist, DoD must develop strategies and technologies that allow it to become both efficient and flexible in its use of available spectrum for unmanned systems. Additionally, DoD has several ongoing efforts to engage the commercial market, including the Defense Innovation Unit Experimental (DIUx) and the Strategic Capabilities Office (SCO), with the goal of ensuring spectrum access for commercial and defense purposes.

4.3.2 Way Ahead

To ensure that DoD is able to effectively operate unmanned systems in an EMS-constrained environment, it must strive to make spectrum operations more efficient, flexible, adaptable, and agile. This includes being capable of maneuvering operations to less dense, denied, or exploitable parts of the EMS to enhance resilience, decrease chance of interception, and allow for sustained operations. To counter electronic attack, unmanned systems must be designed and built to be hardened with robust electronic protection capabilities. Additionally, DoD must remain informed and responsive to on-going spectrum regulatory and policy changes across the globe. This will assure that DoD is able to adapt spectrum-dependent operations to maximize efficiency and effectiveness.[33, 34]

Both the 2013 DoD Electromagnetic Spectrum Strategy and the 2017 DoD Electronic Warfare Strategy list specific goals and objectives in detail toward addressing EMS and EW issues. Advancements toward these goals and objectives will directly enhance the effectiveness and availability of unmanned systems.

---

[33] Department of Defense, Electromagnetic Spectrum Strategy, 2013
[34] Department of Defense, Electronic Warfare Strategy, 2017

5 Human-Machine Collaboration

Human-machine collaboration is essential to meeting the unmanned systems community's vision of an "integrated manned/unmanned force that strengthens the U.S as the world's preeminent land, sea, and air power."[35] Military operations of the future will require collaboration between unmanned systems and humans (i.e., airman, marine, sailor, soldier, or civilian). A summary of the future path for the three key enablers for human-machine collaboration is shown in Table 5.

Table 5: Comprehensive Roadmap for Human-Machine Collaboration

| HUMAN-MACHINE COLLABORATION | 2017 - - - - - - - - - 2029 - - - - - - - - - 2042 | | |
	NEAR-TERM	MID-TERM	FAR-TERM
Human-Machine Interfaces	-Control Multiple Systems -Human-Machine Roles/Cues	-Human-Machine Dialog -"What-If" Scenario Processing -Task Sharing Mission Mgmt	-Infer Human Intent -Deep-Learning Machines
Human-Machine Teaming	-Load Lightening -Reduce Sorties -Certain Maintenance Tasks	-Fully Integrated Robot Teammates -Reduce Warfighter Cognitive Load	
Data Strategies	-Automatically Collect & Process Data -Adjust Data Strategies Autonomously	-Deep Neural Networks -Agile, Responsive, Adaptive	

5.1 Human-Machine Interfaces

Human-machine interfaces (HMIs) are the mechanisms by which humans operate and gather information from unmanned systems. The extent to which HMIs are intuitive and efficient directly impacts mission success. HMIs have historically been domain and/or vehicle specific, resulting in the Department to have acquired multiple stand-alone non-integrated systems. Design and implementation have focused on an individual unmanned system control rather than on task or mission objectives.

"The way we will go after human-machine collaboration is allowing the machine to help humans make better decisions faster."

-The Honorable Robert O. Work

Improved HMIs are needed that facilitate the retrieval of "actionable" information, generate shared awareness of human and machine state/intent, enable flexible human-machine collaborative decision making, and facilitate coordination between heterogeneous members for teaming applications. The effectiveness of unmanned systems C2 HMIs is also dependent upon the extent to which human systems integration (HSI) methods consider the interface in the context of the total human-unmanned vehicle system, including its missions, operating environment, and support requirements.[36]

---

[35] JGRE presentation to the 2012 National Defense Industrial Association (NDIA) Ground Robotics Capabilities Conference and Exhibition, March 2012

[36] Cooke, N.J., Rowe, L.J., Bennett, W. (Eds). Remotely Piloted Aircraft: A Human Systems Integration Perspective, Wiley, October 2016.

In the future, it is desirable to have each operator control multiple unmanned systems, thus shifting the human's role from operator towards mission manager. To ensure agility, the HMIs must support a range of control options whereby the human can be either "off the loop" with no control over an autonomous system, "on the loop" supervising the unmanned systems, or "in the loop" exercising commands to control a particular vehicle's path or payload.[37,38] HMIs enabling multi-vehicle control would be able to support new capabilities such as heterogeneous unmanned systems cooperating to provide a wide area search; inspecting a target from multiple perspectives; tracking moving targets; and relaying communications to mitigate "lost link" situations. Additionally, new HMIs are necessary to support future warfare teaming concepts (e.g., swarms and "loyal tactical wingman") in terms of managing the increased available information and more complex control transfer and coordination requirements.

5.1.1 Challenges

The operation of unmanned systems is inherently challenging due to the loss of direct sensory information.[39] The operator must rely on limited control information from displays accessed during demanding, multi-tasking missions. A new challenge is shifting the design perspective for HMIs so that it employs a mission- and team-centered approach whereby the human and machine collaborate in decision making and flexibly interact to share tasking that meets dynamic mission objectives with multi-domain resources. HSI principles need to be addressed, especially human factors[40] that drive the HMI content, layout, and interaction metaphor. Organizational changes are required to promote effective designs and training for the likely operator pools. Changes will result in control approaches that are common and compatible across the Services as much as possible. The HMIs need to provide display and control functionality for specific unmanned systems types and missions. Ideally, the HMIs should have an application-agnostic look and feel as much as possible despite the variety of unmanned system control approaches (from fixed-based command centers to mobile individual Warfighters).[41] Envisioned collaborative multi-domain missions will also require cooperation across traditional program offices and updated warfare tactics, techniques, plans, and procedures. Furthermore, approaches to test and validate new designs for HMIs are required that enable researchers to systematically manipulate machine reliability and competency boundaries. Complex scenarios that include both normal and non-

While Hollywood may show us futuristic robot armies, the truth is in unmanned systems initially will be to augment our current capabilities. And so, this manned-unmanned interface is the one that will be the hallmark of this new era of warfighting. We don't plan to take the human out of the loop, but we do think it's time to redefine where the human fits into that loop.

- The Honorable Ray Mabus

---

[37] United States Air Force RPA Vector: Vision and Enabling Concepts 2013-2038, 17 Feb 2014. 86-87.
[38] Autonomous Horizons: System Autonomy in the Air force – a Path to the Future. Volume 1: Human-Autonomy Teaming. USAF Office of the Chief Scientist, AF/ST-TR-15-01, June 2015.
[39] Ibid.
[40] Uninhabited Military Vehicles (UMVs): Human Factors Issues in Augmenting the Force, RTO-TR-HFM-078, July 2007.
[41] Ibid.

routine situations (e.g., degraded communications) should also be employed. These features will help evaluate how human trust can be appropriately calibrated to the reliability and functionality of the system in various circumstances. Advancements in testing are needed to help ensure that any complexity associated with the interaction of human and machine team members does not lower operator situation awareness, slow decision making, or increase cognitive workload. Finally, HMI must support cooperative and resilient human-machine collaboration.[42]

5.1.2 Way Ahead

Future HMI must enable new levels of human-machine collaboration and combat teaming. That teaming should pair human's pattern recognition and judgment capabilities with recent machine advances in AI and autonomy. Therefore, HMI must allow strategic and tactical synchronized operations using air, ground, and maritime unmanned systems.

Near-term goals include: operator supervisory control of multiple unmanned systems; explicit cues that make autonomous behavior more transparent and support a shared mental model, trust, and teaming; HMI to dynamically establish human/autonomy roles in task completion through information grounded in the mission; improved automated decision support; and multi-modal control including voice-commands.

Mid-term goals include: mechanisms for machines to conduct predictive algorithm-in-the-loop queries to support human-autonomy dialog when compensating for control time lags and exploring mission-level consequences;[43] HMIs for the operator to interact with machine autonomy processing for more complex "what if" scenarios; improved cooperative mission management between human and machine team partners, with HMIs that support decision and task sharing/coordination; cues that critique, remind, and direct attention based on autonomic scenario/operator monitoring; HMIs for improved information dissemination and transfer of control/handoffs; and rapid resynchronization of information, knowledge, and plans between autonomous remote platforms and central C2 after periods without communications.

Long-term goals include: mechanisms for machines and autonomy to infer human intent for mission-based planning and actions; machine driven task planning and execution with human oversight and override provisions; natural language processing/understanding; HMIs that harness the affordances of advancements in computational techniques (e.g., deep-learning machines) and battlespace technologies (e.g., semi-autonomous weapons).[44,45]

5.2 Human-Machine Teaming

Human-machine teaming is the synchronized employment of soldiers, airmen, marines, sailors, and civilians, working with manned and unmanned systems to create improved lethality, survivability, and situational awareness. The goal of human-machine teaming is to produce

---

[42] Autonomous Horizons: System autonomy in the Air force – a Path to the Future. Volume 1: Human-Autonomy Teaming. USAF Office of the Chief Scientist, AF/ST-TR-15-01, June 2015.
[43] Ibid.
[44] Ibid.
[45] Martinage, R. Toward a New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability. Center for Strategic and Budgetary Assessments, 2014.

synergy and overmatch with asymmetric advantages by combining the inherent strengths of the Warfighter with manned and unmanned systems.[46]

5.2.1 Challenges

One of the major challenges associated with human-machine teaming is achieving the right balance of the appropriate team members to the missions. Optimization of the tasks as well as utilizing the current state of technology requires a delicate balance. Keeping apprised of the commercial market in conjunction with maintaining an understanding of technological advancements will help to guide DoD efforts.

5.2.2 Way Ahead

The human-machine teaming mission is focused on finding the most efficient balance between the Warfighter, manned systems, and unmanned systems. The initial plan is to build upon current possible missions to add more automation into unmanned systems, eventually allowing one operator for many systems. In the near-term, human-machine teaming will consist of tasks such as lightening the load that Warfighters carry in special ground missions, increasing the number of airborne payloads with UAS wingmen, reducing the number of human sorties required, and completing certain maintenance tasks on ships and submarines.

In the mid- and far-term, human-machine teaming will increase capabilities within DoD. Further technology advancements in advanced sensors, deep machine learning, and the ability for the operator to trust the machine will evolve the human-machine teaming dynamic. As technology advances, robots will evolve from tools into full teammates that are integrated with our soldiers, airmen, marines, and sailors. DoD will rely upon unmanned systems more and more to assist in certain tasks (not fully defined as of yet) which, in turn, will allow Warfighters to focus on tasks requiring human interactions.

---

[46] The U.S. Army Robotic and Autonomous Systems Strategy 16 May 2016.

6   Summary

6.1   Challenges Summary

Some of the challenges across the themes and enablers include:

- Lack of common requirements

- Need for evolved TEVV standards

- Need for more collaboration across the Services

- Lack of foresight in design flexibility and securing data rights

- SWaP restrictions

- Legal and policy constraints

- Lack of understanding human-machine interactions

- Lack of trust

- Lack of agile acquisition

- C2 complexity

- Vulnerable networks

- Difficult, cumbersome, lagging software upgrades

- Lack of high information assurance solutions

- Need for evolved spectrum strategy

- Lack of refined sensitive HMIs

- Maintaining antiquated equipment

- Affordability of future platforms and networks

6.2   Way Ahead Summary

This document attempts to lay out a foundational path to advance the supporting and warfighting capabilities of unmanned systems well into the future. A number of the specific non-technical areas of advancement include:

- Flexible agile acquisition

- Architecture requirements

- Autonomous system requirements

- Architecture/modularity design policy

- New approach to TEVV for autonomous systems

- New approach to securing data rights

- Strengthen connections to private sector advancements

- Ethical requirements for increased trust

- Weaponized autonomous system policy

- Information assurance policy, procedures, techniques

- Human-machine tactics, techniques, procedures (TTP)

6.3   Key Technologies

Some of the key technologies identified or referred to in this document include:

- Robotics advancements

- Prioritized common/open architectures

- Common data repositories

- Autonomous modeling and simulation advancements

- Machine learning advancements

- Artificial Intelligence advancements

- SWaP/miniaturization advancements

- Swarming capabilities

- Augmented Reality

- Virtual Reality

- Sensor advancements

- Collision avoidance

- Leader-follower

- GPS-denied solutions

- Cyber resilience and robustness

- Information assurance solutions

- Increased network and spectrum capacity

- Human-machine interface advancements

- Autonomous data strategy adaptation

Appendix A   FOUNDATIONAL DOCUMENTS AND REFERENCES

This document leverages previous versions and strategic guidance produced by the individual military departments and agencies and focuses on the common themes and challenges that each Armed Service faces in pursuing further expansion of military capabilities with unmanned systems technology. The following list of documents formed the foundation of this document.

EXECUTIVE/DOD LEVEL

National Security Strategy, 2015

Department of Defense Strategic Management Plan FY2012-FY2013, 2011

Quadrennial Defense Review, 2014 (DoD)

Better Buying Power 3.0, 2015 (A&S)

Joint Concept on Robotics and Autonomous Systems, 2016 (JCRAS) Defense Science Board Summer Study on Autonomy, 2015 (A&S)

DSB Summer Study on Strategic Surprise, 2015 (A&S)

The DoD Cyber Strategy, 2015 (DoD)

Technology Investment Strategy 2015-2018, DoD R&E Autonomy COI TEVV Working Group, May 2015 (R&E)

SERVICE LEVEL

THE ARMY VISION - Strategic Advantage in a Complex World, 2015 (USA)

Army Materiel Command 2014-2024 Strategic Plan, 2013 (AMC)

U.S. Army Operating Concept 2020-2040, 2014 (TRADOC)

Research, Development, and Engineering Command Strategic Plan, 2014 (RDECOM)

Army Research Laboratory Technical Strategy 2015-2035, 2014 (ARL)

Army RAS Strategy, 2017 (USA)

AUTONOMOUS HORIZONS – System Autonomy in the Air Force – A Path to the Future, Vol I, 2015 (USAF OCS)

America's Air Force: A Call to the Future, 2014 (USAF)

USAF Strategic Master Plan, 2015 (USAF)

AF Future Operating Concept, 2015 (USAF)

U.S. Air Force RPA Vector, 2014 (USAF)

Small UAS Flight Plan: 2016-2036, 2016 (USAF)

Autonomy S&T Strategy, 2013 (AFRL)

Naval S&T Strategy, 2015 (ONR)

CNO Navigation Plan 2015-2019, 2015 (CNO)

Future Naval Capabilities Guidebook, 2017 (ONR)

Appendix B   JOINT CONCEPT FOR ROBOTICS AND AUTONOMOUS SYSTEMS

The JCRAS is the joint vision for future robotic and autonomous systems (RAS) employment in 2035 to guide comprehensive development across the Joint Forces. Currently, commercial technology in diverse disciplines is developing at an accelerating rate. Advances in RAS technologies give the Joint Forces a tremendous opportunity to enhance capabilities and maintain operational advantage in an increasingly lethal and sophisticated operating environment.

Because RAS technology will significantly advance in the next two decades, this concept offers broad themes rather than an attempt to predict specific military applications. The central idea of JCRAS is to integrate RAS into joint operations across all functions by 2035 to increase the Joint Force Commander's options. The Joint Concept provides precepts as an aim point for systematic RAS development. Emerging capabilities, such as human-RAS teaming and autonomy, offer the Joint Forces potential solutions to the challenges of the future operating environment described in the Joint Operating Environment 2035.[47] As current capabilities are enhanced and new ones introduced, the Joint Forces must develop innovative concepts that allow them to combine emerging RAS technologies and existing systems to create decisive operational effects.

Advances in RAS technology over the next 20 years will produce military capabilities that can provide the Joint Forces with significant advantages in the future operating environment. Global commercial interests will drive RAS advancements, changing how the U.S, partner nations, allies, and potential adversaries employ RAS. A broad range of technologies from multiple disciplines is developing fast, resulting in advanced commercial applications such as driverless cars, advanced cancer diagnosis, and complex stock market trading. As RAS technologies are integrated into military applications, Joint Forces capabilities will expand exponentially. Some advantages include:

- **Ability to learn.** Future RAS will learn through interaction with the environment, humans, and by accessing networked resources.

- **Greater situational awareness.** Future RAS will enhance awareness by collecting, processing, and prioritizing information from advanced sensor networks, transforming data into knowledge for the Warfighter. This will enable more effective operations in a complex, congested battlespace.

- **Enable higher performance.** Unlike manned and optionally manned systems, RAS have no human physiological limitations (e.g., fatigue). This allows for extended ranges and loiter times, persistent surveillance, and novel combinations of sensors and payloads on single platforms.

---

[47]Joint Operating Environment 2035: *The Joint Force in a Contested and Disordered World*, 14 July 2016

- **Improve efficiency and effectiveness.** More capable RAS will be able to perform more joint tasks across the range of military operations, such as intra-theater airlift, mine operations, countering weapons of mass destruction, supply, and sustainment, while improving the efficiency and effectiveness of the force.

- **Provide greater flexibility.** Future RAS systems will be rapidly reconfigurable by exchanging modular hardware and/or by downloading new software that confers new capabilities. Future RAS multi-mission functionality will enable the Joint Forces to quickly adapt to meet varied or changing mission requirements.

- **Increase tempo by operating at machine speed.** RAS "think" at ever-increasing machine speeds. RAS can fuse data from networked ISR sensors, maneuver to an advantageous location, and act more quickly than adversary humans and RAS. Advanced data analytics, real-time processing, and alternate decision-making frameworks will enable commanders to decide and act faster than adversaries.

- **Provide potential to generate mass.** The current Joint Force manned inventory is based on relatively small numbers of highly capable, sophisticated, and expensive weaponry that cannot quickly be regenerated. RAS offers the opportunity to employ large quantities of inexpensive systems to generate mass.

- **Enable distributed and dispersed operations.** Adversary technologies will target U.S. forces with greater precision and range, placing legacy forces at increased risk. Using RAS for distributed and/or dispersed operations will enhance capability in the future operating environment.

Achieving the vision of the JCRAS will require a comprehensive and innovative joint effort that includes robust experimentation, war gaming, modeling and simulation (M&S), and the continuous evolution of DOTmLPF-P. Developing RAS technologies and understanding potential Joint Force employment in the near-term is critical to maintaining decisive military advantage in the future.

While RAS technology will not change the fundamental nature of war, an advantage will belong to those who best adapt technology to create effective operational approaches. To protect U.S. national interests, it is imperative to aggressively pursue and integrate future technologies in a holistic manner, engage in rigorous experimentation to create innovative operational approaches, and (while not the focus of the JCRAS) develop means to defend against adversary RAS employment.

Technology development is an essential element of JCRAS, but only as the means for Joint Warfighters to conduct operations – fundamentally human endeavors – more efficiently and effectively. The JCRAS was developed with representation from the Military Services, CCMD, Joint Staff, OSD, and multinational partners. Key members of industry and academia provided input as well. The JCRAS will be an initial foundation for developing future capabilities to ensure the Joint Force maintains its competitive advantage to operate effectively and decisively through 2035 and beyond.

Appendix C   ACQUISITION INITIATIVES

As unmanned systems have proven their worth on the battlefield, DoD has allocated an increasing percentage of its budget to developing and acquiring these systems. DoD is investigating ways to improve acquisition agility through implementation of alternative acquisition methods. The emergence of initiatives such as the DoD Third Offset Strategy, more and more unmanned systems technology will need to be inserted into operational and organizational constructs based on doctrine, training, and exercises to allow the Joint Force to operate with such technologies to achieve an advantage. Significant investments in T&E, training, and infrastructure are needed to support the expansion of unmanned systems. A key question is how the military can work with the industrial base in new ways to simplify and streamline the acquisition process to facilitate rapid development and procurement of core technologies at a speed that keeps pace with industry. With the transition from a handful of innovative experimental systems to normalized program developments, unmanned systems are influenced by many acquisition initiatives and positioned to drive new rapid prototyping and fielding initiatives.

Unmanned systems will introduce novel life cycle, maintenance, and disposal challenges. Groundbreaking unmanned systems technologies will require investments across the acquisition life cycle, from materiel solution analysis to technology development, through engineering and manufacturing development into production and deployment, and finally through operation and sustainment to disposal. Requirements for unmanned systems will have to be developed that provide confidence in systems that interact in human-machine teams, and can learn over time. Similarly, test and evaluation/validation and verification (TEVV) methods must be able to handle teaming and learning issues to facilitate assured trust in human-machine teaming.

Processes and procedures for requirements analysis, agile systems engineering, TEVV, and maintenance must evolve to incorporate these new technologies. Ontologies are needed for inter-operation, especially on human-machine interaction requirements to avoid operators and unmanned systems being developed and tested in isolation. Open systems, such as Robot Operating System (ROS) and Maritime Open Architecture Autonomy (MOAA), and open standards such as Unmanned Aircraft System (UAS) Control Segment (UCS) Architecture, Joint Architecture for Unmanned Systems (JAUS), Future Airborne Capability Environment (FACE) and NATO Standardization Agreement (STANAG) 4586, must continue to evolve and become pervasive in the acquisition of unmanned systems to ensure the interoperability required to harness potentially game changing impact. Novel TEVV methods are needed to expand the assurances of dynamic/cyber physical systems and to assure and quantify trust in manned-unmanned teaming between human and machine. Sustainment guidance for unmanned systems acquisition will benefit from system development requirements that incorporate enablers such as condition-based maintenance (CBM) and prognostic and diagnostic data collection systems.

In addition to the far-reaching efforts of Better Buying Power (BBP) 3.0 (see next section), current activities across DoD and the Services signify an emerging environment favoring successful expansion of the acquisition of unmanned systems technologies for the future fighting force. The Commercial Technologies for Maintenance Activities (CTMA) program is an Office of the Assistant Secretary of Defense for Logistics and Materiel Readiness (OASD(L&MR)) partnership between industry, academia, and government that fosters and funds

collaborative sustainment technology.   The CBM+ Action Group, led by OASD(L&MR), promotes autonomous sustainment capabilities and policies across DoD weapon systems. The Air Force Research Lab (AFRL) is engaged in formal modeling of requirements through the verification and validation (V&V) of the Complex and Autonomous Systems program. The Army G-8 is working to establish prototyping efforts to permit program managers to develop technologies based upon approved Initial Capabilities Documents (ICDs). OUSD(R&E) is formulating a time-phased investment strategy and modernization plan for testing autonomy driven by a formal study of test capability gaps, resources and methodologies within the major range and test facilities base and support facilities. The Test and Resource Management Center (TRMC) is seeking to develop test technologies for autonomous and unmanned systems technologies through a Broad Agency Announcement (BAA). This list of activities represents only a cross-section of efforts to innovate acquisition to keep pace with emerging unmanned systems technology.

Better Buying Power

BBP is the implementation of best practices to strengthen DoD's buying power, improve industry productivity, and provide an affordable, value-added military capability to the Warfighter. BBP encompasses a set of fundamental acquisition principles to achieve greater efficiencies through affordability, cost control, elimination of unproductive processes and bureaucracy, and promotion of competition. BBP initiatives also incentivize productivity and innovation in industry and government, and improve tradecraft in the acquisition of services.

In 2015, BBP 3.0 core initiatives focused on: ensuring program affordability, mandating "should cost" savings opportunities, incentives to industry, an emphasis on competition, reducing bureaucracy, improving acquisition of contracted services, and building professionalism. BBP 3.0 provides focus on the concern that the nation's technological superiority is at risk. R&D efforts supporting the acquisition cycle span S&T, component development, technology demonstration, early prototyping, full-scale development, and technology insertion into field products for the Warfighter. The R&D base is vast, spanning government labs, academia, non-profit research institutions, defense industry, and increasingly, the non-defense commercial sector and international entities. BBP 3.0 initiatives are designed to improve the professionalism of the acquisition workforce to enhance the ability of DoD to identify and vast sources of innovation and technology effectively.[48]

Other Transaction Agreements

Other Transaction Agreements (OTA) are playing an important role in the future of DoD acquisition, especially in an area of rapidly changing technology such as Unmanned Systems. In accordance with provisions of 10 USC 2371b, Section 815 of the 2016 National Defense Authorization Act (NDAA), Public Law 114-92, DoD is provided authority to enter into transactions other than contracts, grants, or cooperative agreements for prototype projects. Under this authority, DoD can make awards for prototype projects that are directly relevant to enhancing the mission effectiveness of military personnel and the supporting platforms, systems, components, or materials proposed to be acquired or developed by DoD, or the improvement of platforms, systems, components, or materials in use by the armed forces. Within the inherent

[48] bbp.dau.mil

flexibility of the Section 815 authority, the government, industry, and academia are enabled to form a partnership quickly and effectively to provide innovative technology solutions to the Warfighter. The Section 815 OTA statute allows these projects to go from prototype to production, in some instances, based on the competitive nature of OTAs and their projects, thus allowing a new avenue from the traditional Federal Acquisition Regulation (FAR)-based contracting. This new prototype-to-production language represents a "game changer" for unmanned systems, providing a mechanism that has the potential to adapt the program to the current state of technology.[49]

Defense Innovation Unit Experimental

DIUx began in 2015. With outposts in California's "Silicon Valley," Boston, MA, and Austin, TX, DIUx serves as a bridge between those in the military executing some of the nation's toughest security challenges and companies operating at the cutting edge of technology. DIUx represents an experimental approach by DoD seeking new paths to identify, contract, and prototype novel innovations through sources not traditionally available to DoD. The ultimate goal of DIUx is to accelerate technology into the hands of the Warfighters.

Seeking innovative approaches to accelerate acquisition, DIUx leverages OTAs granted by Congress. DIUx established the new Commercial Solutions Opening (CSO), a contracting mechanism that enables DIUx to do business with companies that traditionally are not engaged with DoD. The CSO mirrors the commercial contracting practices these companies normally use, enabling DIUx to work with companies to design projects together, and negotiate payment milestones, terms and conditions, and intellectual property rights within 60 days. The services can leverage DIUx and OTA's to investigate capabilities that have the potential to solve technical challenges, using agile acquisition approaches that promote innovation.

---

[49] DoD Other Transactions Guide for Prototype Projects, January 2017

Appendix D   OSD INITIATIVES

OSD has supported initiatives defining common language/messaging architectures for Unmanned Air and Ground systems and a common secure communication architecture. The following initiatives provide a framework that can assist the services and industry on future development efforts:

Small Unmanned Systems Autonomy Architecture: The small unmanned system autonomy architecture, commonly referred to as "Government off-the-shelf (GOTS) GUTS" establishes a hardware and software baseline for small unmanned systems. The architecture provides a common and interoperable small UAS that can be designed to meet service requirements.

Joint Architecture for Unmanned Systems (JAUS): The JAUS (previously Joint Architecture for Unmanned Ground Systems) messaging architecture enables communication with and control of unmanned systems across the entire unmanned system domain. JAUS provides a common language enabling internal and external command, control, and communications of unmanned systems.

UAS Control Segment (UCS) Architecture: The UCS Architecture is a Service Oriented Architecture (SOA) based on a common data model, service interface descriptions are expressed in UML model (and other formats), and its platform-independent specification can be transformed by users into platform-specific implementations. The UCS Architecture is extensible and describes a multitude of application software services to support current capabilities of the DoD unmanned systems portfolio.

Joint Communications Architecture for Unmanned Systems (JCAUS): The objective of the JCAUS program is to create a flexible communication framework for unmanned systems that improves interoperability, security, and industry competition for the DoD acquisition programs. JCAUS is based on modular open system architecture principals, and enforces open standards at key interfaces to meet program objectives throughout the life cycles of the communication systems. JCAUS provides built-in flexibility that grants the Services the ability to create communication systems specific to their missions, without sacrificing constrains relevant to cross-program interoperability and/or industry competition.

UAS Ground Control Station Human-Machine Interface Development and Standardization Guide: The UAS Ground Control Station Human-Machine Interface Development and Standardization Guide provides UAS acquisition professionals, and specifically human factors engineers, a means to foster human-machine interface standardization in the design and development of UAS operating ground control stations across the Services. The premise behind the creation and development of this Guide is to reduce UAS acquisition and life-cycle costs by promoting strategies that increase design and development commonality and increase reuse of proven technologies and methodologies across the Services.

Open Business Model (OBM): The OBM for Unmanned Aircraft Ground Control Stations provides acquisition professionals within the UAS community the knowledge and a framework to enable business decisions that will result in cost effective acquisitions for the Government.

The OBM offers a reasoned approach by which traditional stove-piped UAS acquisitions can be broken apart and made open to allow all for greater participation and competition by industry. The OBM is an approach for doing business in a transparent way that leverages the collaborative innovation of participants from across the enterprise, thereby permitting shared risk, increased competition, maximized asset reuse, and reduced total ownership costs.

Appendix E   ABBREVIATIONS

Acronym	Definition
ACC	Air Combat Command
AFCEC	Air Force Civil Engineer Center
AFIMSC	Air Force Installation and Mission Support Center
AFLCMC	Air Force Life Cycle Management Center
AFMC	Air Force Materiel Command
AFRL	Air Force Research Laboratory
AI	Artificial Intelligence
AISR	Airborne Intelligence, Surveillance, and Reconnaissance
AMC	Army Materiel Command
AMRDEC	Army Aviation and Missile Research Development and Engineering Center
ARL	Army Research Laboratory
ARCIC	Army Capabilities Integration Center
ARDEC	Army Armament Research, Development and Engineering Center
ASA(ALT)	Assistant Secretary of the Army for Acquisition, Logistics and Technology
ASD(A)	Assistant Secretary of Defense for Acquisition
ASD(HDGS)	Assistant Secretary of Defense for Homeland Defense & Global Security
ASD(ISA)	Assistant Secretary of Defense for International Security Affairs
ASD(L&MR)	Assistant Secretary of Defense for Logistics and Materiel Readiness
ASD(NCB)	Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs
ASD(SO/LIC)	Assistant Secretary of Defense for Special Operations and Low Intensity Conflict
ASD(SPC)	Assistant Secretary of Defense for Strategy, Plans, and Capabilities
ASN(RDA)	Assistant Secretary of the Navy for Research, Development and Acquisition
ATEC	Army Test and Evaluation Command
BAA	Broad Agency Announcement
BBP	Better Buying Power
BLOS	Beyond Line of Sight
C2	Command and Control
CBM	Condition-Based Maintenance
CCMD	Combatant Command
CCW	Certain Conventional Weapons
CERDEC	Army Communications-Electronics Research, Development and Engineering Center
CIO	DoD Chief Information Officer
CNMOC	Commander, Naval Meteorology and Oceanography Command
CNO	Chief of Naval Operations
COI	Community of Interest
CONOPS	Concept of Operations
COTS	Commercial-Off-The-Shelf
CSO	Commercial Solutions Opening
CTMA	Commercial Technologies for Maintenance Activities
DARPA	Defense Advanced Research Projects Agency

Acronym	Definition
DASD	Deputy Assistant Secretary of Defense
DASN	Deputy Assistant Secretary of the Navy
DIA	Defense Intelligence Agency
DISN	DoD Information Systems Network
DIUx	Defense Innovation Unit Experimental
DoDAF	DoD Architecture Framework
DoD	Department of Defense
DoDD	Department of Defense Directive
DOE	Design of Experiments
DOT&E	Director, Operational Test and Evaluation
DOTmLPF-P	Doctrine, Organization, Training, materiel, Leadership, Personnel, Facilities + Policy
DPG	Defense Planning Guide
DSS	Defense Security Service
DT	Development Testing
DTRA	Defense Threat Reduction Agency
EMS	Electromagnetic Spectrum
EW	Electronic Warfare
EXCOM	Executive Committee
FACE	Future Airborne Capability Environment
FAR	Federal Acquisition Regulation
FORSCOM	Army Forces Command
FY	Fiscal Year
GGE	Group of Governmental Experts
GPS	Global Positioning System
GPU	Graphical Processing Unit
HMI	Human-Machine Interface
HQDA	Headquarters, Department of the Army
HSI	Human Systems Integration
ICD	Initial Capabilities Document
IOP	Interoperability Profile
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
JAUS	Joint Architecture for Unmanned Systems
JCAUS	Joint Communications Architecture for Unmanned Systems
JCRAS	Joint Concept for Robotic and Autonomous Systems
JGRE	Joint Ground Robotics Enterprise
JIDO	Joint Improvised-Threat Defeat Organization
JIE	Joint Information Environment
JRAS	Joint Staff Robotic and Autonomous Systems
LAWS	Lethal Autonomous Weapon System
LOAC	Law of Armed Conflict
LOS	Line of Sight
M&S	Modeling and Simulation
MAJCOM	Air Force Major Command

Acronym	Definition
MCCDC	Marine Corps Combat Development Command
MCSC	Marine Corps Systems Command
MCWL	Marine Corps Warfighting Laboratory
MDA	Missile Defense Agency
ML	Machine Learning
MOAA	Maritime Open Architecture Autonomy
MUM-T	Manned/Unmanned-Teaming
NATO	North Atlantic Treaty Organization
NAVAIR	Naval Air Systems Command
NAVSEA	Naval Sea Systems Command
NETOPs	Network Operations
NGA	National Geospatial-Intelligence Agency
NGO	Non-Governmental Organization
NIEM	National Information Exchange Model
NRO	National Reconnaissance Office
NSA	National Security Agency
OASD(A)	Office of the Assistant Secretary of Defense for Acquisition
OASD(L&MR)	Office of the Assistant Secretary of Defense for Logistics and Materiel Readiness
OASD(R&E)	Office of the Assistant Secretary of Defense for Research and Engineering
OUSD(R&E)	Office of the Under Secretary of Defense for Research and Engineering
OBM	Open Business Model
OCO	Overseas Contingency Operations
ONR	Office of Naval Research
OPNAV	Chief of Naval Operations
OPORDS	Operation Orders
OSD	Office of the Secretary of Defense
OTA	Other Transaction Agreements
OWL	Web Ontology Language
PED	Processing, Exploitation and Dissemination
PEO	Program Executive Officer
R&D	Research and Development
R&E	Research and Engineering
RAS	Robotic and Autonomous System
RDECOM	Army Research, Development, and Engineering Command
RDT&E	Research, Development, Test, and Evaluation
ROE	Rules of Engagement
ROS	Robot Operating System
RPA	Remotely Piloted Aircraft
S&T	Science and Technology
SAF/AQ	Assistant Secretary of the Air Force for Acquisition
SATCOM	Satellite Communications
SCO	DoD Strategic Capabilities Office
SOA	Service Oriented Architecture
SPAWAR	Space and Naval Warfare Systems Command

Acronym	Definition
STANAG	Standardization Agreement (NATO)
SWaP	Size, Weight, and Power
SYSCOM	Navy Systems Command
T&E	Test and Evaluation
TACOM	Army Tank-Automotive and Armaments Command Life Cycle Management Command
TARDEC	Army Tank Automotive Research, Development and Engineering Center
TEMP	Test and Evaluation Master Plan
TEP	Test and Evaluation Plan
TEVV	Test and Evaluation/Validation and Verification
TRADOC	Army Training and Doctrine Command
TTP	Tactics, Techniques, and Procedures
UAS	Unmanned Aircraft System
UCS	UAS Control Segment
UMV	Uninhabited Military Vehicle
UN	United Nations
USAASC	United States Army Acquisition Support Center
USACAC	U.S. Army Combined Arms Center
USACE	U.S. Army Corps of Engineers
USAF	U.S. Air Force
USAFRICOM	U.S. African Command
USARCYBER	U.S. Army Cyber Command
USC	U.S. Code
USCENTCOM	U.S. Central Command
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(R&E)	Under Secretary of Defense for Research and Engineering
USEUCOM	U.S. European Command
USIP	Unmanned System Interoperability Profile
USMA	United States Military Academy
USNORTHCOM	U.S. Northern Command
USPACOM	U.S. Pacific Command
USSOCOM	U.S. Special Operations Command
USSOUTHCOM	U.S. Southern Command
USSTRATCOM	U.S. Strategic Command
USTRANSCOM	U.S. Transportation Command
V&V	Verification and Validation
XML	Extensible Markup Language

This page intentionally left blank.

MANNED AIRCRAFT

RQ-7 SHADOW

HEXACOPTER SWARM

GROUND CONTROL STATION

LEADER-FOLLOWER

Statement A. Approved for public release: distribution unlimited.