Fighting Tomorrow's Fight Today:

Joint All Domain Operational Testing of Next Generation Technology

By

Captain Robyn N. Taylor (USAF)

Air University Advanced Research Group – Joint All Domain Command and Control

07 August 2020

The conclusions and opinions expressed in this research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, Department of Defense, or The Air University

eSchool of Graduate PME

Maxwell AFB, Alabama

ABSTRACT

As we forge what Joint All Domain Operations will look like from an Air Force and Joint perspective, we need to understand the ways services can better communicate, integrate weapon capabilities, and conduct ops at blistering speed to keep our adversaries off balance. The critical component to how we, as a service, will doctrinally fight to win wars in 2030 and beyond is directly linked to what affords us more time and interoperability. As the need to upgrade technology persists, there will be a requirement for combined operational test and evaluation criteria and a method to present technological test results to the joint force from the decision makers on Capitol Hill down to the tactical teams on the ground. A repository of all developmental and operational testing performed within the Department of Defense, that is both protected from adversaries and accessible between branches and organizations, will offer significant returns and prevent delays due to repeated efforts caused by lack of information.

INTRODUCTION

Time is by far the most significant element of success in current and future wars. The more time you have to gather information, or the less time it takes to engage an enemy, become significant advantages in both traditional and irregular warfare. However, we cannot create more time nor can we regain time that has passed. What we can do is shorten the processes involved in creating shared understanding. With the advancements in technology, the Department of Defense (DoD) is working to upgrade systems and devices to more modern equipment and shorten the acquisitions process for continually doing so. Although the overall intent is captured, a key aspect of this scenario needs attention. As it currently stands, there is a legal requirement for testing software and hardware before use in the DoD, but nothing forces the information to be shared, nor to perform any testing as a joint team. Weapons systems such as the MQ-9 and F-35 are utilized by multiple service branches, but the lessons learned in updating each are isolated to the organization performing the testing, causing duplicated efforts. The fix action for this growing problem is to first establish a joint operational test and evaluation standard and process for our network connected equipment, and second to provide a repository for all results associated with our weapon systems and munitions.

RELEVANCE

To understand this issue better and the impact of resolving it, I sought out a variety of sources on the plans for Joint All Domain Operations (JADO) and needs identified by the cyber communities. I interviewed cyberspace experts in the Air Force and US Central Command, along with reviewing a RAND study on the Reflections of Future Warfare, joint publications, a DoD Acquisition of Information Technology Instruction, and a commentary published by the Center for Strategic and International Studies on Making the Most of the Air Force's Investment in Joint All Domain Command and Control (JADC2). It is abundantly clear there is widespread interest in shortening the acquisitions process for technology, creating a data aggregate between the services, and improving defense of our assets in and through the cyberspace domain. However, that data is limited to operational information. The missing piece is a process which makes certain the new products being plugged into our cyber infrastructure are able to do what the military needs and any unforeseen issues or benefits arising from further use are able to be captured then rapidly understood and implemented across the whole of the joint force. That information will enable both short and long term improvements as the processes shift toward data driven acquisitions.[1]

TIME AND INTEROPERABILITY

Joint developmental and operational testing is critical as the value of time and the significance of interoperability cannot be overstated, and establishing a means to provide and access results of joint and other forms of technological testing will provide the United States with both. As it is explained in Joint Publication 3-0, Joint Operations, pages III-11 to III-14, “in one sense, decisions are the most important products of the C2 function, because they guide the force toward objectives and mission accomplishment.”[2] Things like compatibility of systems shared terminology enable all personnel and all equipment required to work together to accomplish an objective the ability to "speak the same language" while still safeguarding vital information from adversaries. The Joint Publication 1, Doctrine for the Armed Forces of the United States, chapter 1 states that “‘Joint’ connotes activities in which elements of two or more Military Departments participate. Joint matters relate to the integrated employment of US military forces in joint operations, including matters relating to: national military strategy (NMS), deliberate and crisis action planning, command and control (C2) of joint operations, and unified action with Department of Defense and interagency partners.”[3] It further explains “the capacity of the Armed Forces of the United States to operate as a cohesive joint team is a key advantage in any operational environment. Unity of effort facilitates decisive unified action focused on national objective and leads to common solutions to national security challenges.” The ability to translate information across multiple platforms and organizations laterally, up, and down various chains of command rapidly affords authorities the ability to make urgent decisions and allows subordinates the ability to implement swift execution of those orders. This in turn allows for better communication between services and other agencies, integration of multi-force weapon capability, and ultimately the ability to conduct operations ahead of adversaries.

UPGRADING TECHNOLOGY

To state that upgrading our electronic devices across the entirety of the Department of Defense is a time-consuming, massive undertaking, and an enormous challenge is an understatement. While each branch of service has varying ages of their technologies, they are all still using “old tech”. By that what is meant is technology that is beyond end-of-life, no longer supported or updated by the originating creators, which commercially is considered obsolete. There is a natural human tendency to stick to what we know because it’s comfortable for us; the unknown carries risk and uncertainty. Much of what we have and use is antiquated or rapidly becoming so. Unfortunately, for

years the military has been forced to make do with equipment from previous generations thanks to downsizing the force after Operation Desert Storm and budget cuts across the last three decades.[4] Cue the phrase "if it ain't broke, don't fix it". But just because our equipment may not be broken does not mean we aren't behind. We are losing domain superiority in cyberspace caused by this gap in technology. The Air Force has false sense of security since their equipment is considered newer by comparison to other branches' technological equipment. However, it still falls well behind the commercial off the shelf (COTS) technologies the corporate world uses daily. Take for example the missiles community of the Air Force who recently in 2019 converted from using eight-inch floppy disks from the 1970s.[5] Like the floppy disks, much of what the US military has and uses is antiquated or rapidly becoming so. The US forces need to get better at using off the shelf technologies and updating the procedures and policies to COTS technology so they can be updated faster than a traditional acquisition cycle[6]. Upgrades not only improve functionality and security at the basic point of use, these investments improve the entire fabric of our kinetic and nonkinetic missions. For instance, we know dedicated adversaries will look for single points of failure and vulnerabilities to disrupt our missions. With antiquated technology in place, we make their job easier, thereby jeopardizing the missions these systems support.[7]

REDUNDANCY PREVENTION

As we upgrade our technology, we are required to test it prior to implementation. In order to prevent redundant efforts, there is a major need for unified testing processes across different but similar platforms. Redundancy prevention will save more time and money than continuing the current methods requiring recovery actions after the fact. Thus far, we have been in a reactive state in order to consider ourselves a joint force. So how do we become proactive? National Defense Strategy needs the cyber perspective built in. US Cyber Comman has its role but is too detached from the other branches information network management and acquisitions processes. While they could potentially integrate with the services more, culture starts at the top. How personnel in the military understand cyber can be improved with a top-down approach. Establishing law brings about doctrine and policy, which affects the culture and values. The future environment is all domain, globally integrated operations transcending combatant command boundaries. The DoD and the Air Force at large is championing that platform trying to link multiple data from sensors into a common distributed shooters network, a common data structure. Effective implementation of that plan will require operational testing of common solutions for DoD applications.

There is difficulty in the existing structure defining what important up to date technology passes to become universal implementation because there is not a unified standard. Developmental testing is a requirement for fielding the use of technology. In simple terms, pull the trigger. If it works development stops and it moves on to operational testing. It is here that the situation becomes more challenging. Frequently, product won't work but the military has already purchased it. In this instance, it passes developmental testing but fails operational testing, it is our problem and we own it, not the creators.[8] When we accept the responsibility for operational testing, it happens within each service independently. For example, testing is occurring across different branches for software updates to the MQ-9 and F-35 aircraft. Multiple branches use those, but no one talks to each other when upgrading the equipment, which in turn causes duplicated efforts and possibly missed problems or even successes simply because the lessons learned are not communicated to other parties within the DoD with the same or similar technologies. The lack of joint operational testing leads to isolated instances of lessons learned for software and hardware associated with weapons systems and munitions. These efforts by multiple branches simultaneously could be cut down or possibly eliminated with a joint standard and shared knowledge of the updates and their effects on the systems.

SENSOR TO SHOOTER AND STANDARDIZATION

In addition to establishing a common operational test and evaluation criteria for our networked weapon systems and munitions, ongoing information sharing of results and needs is required for that common application to be used across multiple services with the same capability. In order for us to decide, update, and integrate faster, we need a common baseline in order to be synergistic across the DoD, which is the goal of the new Multi Domain Operations Center. We must protect our data and systems. This gets overlooked in the conversation as we tend to think weapon system and result. We need a paradigm shift in how we operate and the interconnectedness of everything. Think of the Internet of Things where everything is connected which means everything is at risk. Our systems need to be engineered to talk to each other. Interoperability is vital to achieve the objective of linking sensors to shooters faster. We need to provide a way for tactical units tap into the testing process and results. Everyone from a squadron in garrison to fire team in the field should be able to access near real time information to maintain secure and up to date electronics technology.[9] Communicating in the battle space requires interoperable systems that allow communications. Operation Eagle Claw is a well known example where communicating and interoperability failed miserably. If we are to operate in the joint domain, we must be able to talk and to do that, we

must be able to use what others have learned instead of forcing every branch and organization to go through similar individualized problem solving.[10] These concepts of security and connectivity as outlined in the RAND study on the Reflections of Future Warfare, are paramount to successful implementation of JADC2.[1] In the words of the 21st Chief of Staff of the Air Force, General Goldfein, "If we get JADC2 right, we get the next-generation air dominance right."[11]

CONCLUSION

While much of the planning for the future of warfighting is taking data integration and joint interoperability into consideration, it currently lacks the central hub for developmental and operational testing outcomes on information technology. As the OODA loop accelerates from bringing these technologies on, for further study, we should ask how do we keep the data secure and connected?[6] The Center for Strategic and International Studies commentary article makes these two issues clear, "DoD struggles with joint acquisition because the military services' divergent incentives prioritize individual autonomy over collaboration…To field the ABMS architecture, the Air Force needs to levy interface standards on sensors and shooters—many of which are funded and built by the other military services."[12] Hence, joint operational testing of software and hardware and the ability to share and update those results will improve JADC2 and help us win wars in 2030 and beyond. The reality is that this problem is coming our way whether we are ready for it or not.

BIBLIOGRAPHY

1. Maucione, Scott; Serbu, Jared, "Among DoD Leadership, Eyes Are Now Wide Open to Value of Telework", Federal News Network, 20 July 2020, https://federalnewsnetwork.com/dod-reporters-notebook-jared-serbu/2020/07/among-dod-leadership-eyes-are-now-wide-open-to-value-of-telework/.

2. Department of Defense, "Joint Publication 3-0: Joint Operations", Washington DC: Department of Defense, 2017, pp. III-11 to III-14.

3. Department of Defense, "Joint Publication 1, Doctrine for the Armed Forces of the United States", Washington DC: Department of Defense, 2013, chapter 1.

4. RAND Corporation, "Reflections on the Future of Warfare and Implications for Personnel Policies of the U.S. Department of Defense", 2019.

5. Zak Doffman, "US Military to replace 1970s Floppy Disks Controlling Nuclear Missiles," Forbes, 19 October, 2019, https://www.forbes.com/sites/zakdoffman/2019/10/19/us-military-to-replace-1970s-floppy-disks-controlling-nuclear-missiles/

6. Lt Col Becky Russo, C-17 pilot and previous commander, 691st Cyberspace Operations Squadron, to the author, email, subject: Proposed Revision of the Policy of the Army and Navy Relating to Aircraft, 12 April 2020.

7. Col Billy Pope, executive, Office of Chief of Air Service, to the author, email, subject: Air Force Missions, 04 August 2020.

8. Capt Christian Sledge (J6 Branch Chief, CENTCOM Forward Headquarters, Al Udeid AB, Doha, Qatar), interview by the author, 03 August 2020.

9. Lt Col Christopher Chin (Weapons officer and Commander, 363 Intel Support Squadron, JBLE-Langley AFB, Hampton, VA), interview by the author, 03 August 2020.

10. Ret. Col Cary Amburn, previous Deputy Director of Cyberspace and Information Dominance for Air Combat Command, to the author, email, subject: 2030 Wars, 03 August 2020.

11. National Defense Magazine, "Q&A with Air Force Chief of Staff Gen. David Goldfein," interview with Gen. David Goldfein, Time, 04 August 2020, https://www.nationaldefensemagazine.org/articles/2020/8/4/qa-with-air-force-chief-of-staff-gen-david-goldfein?utm_source=Sailthru&utm_medium=email&utm_campaign=MIL%20EBB%208.5.20&utm_term=Editorial%20-%20Military%20-%20Early%20Bird%20Brief.

12. Morgan Dwyer, "Making the Most of the Air Force's Investment in Joint All Domain Command and Control," Center for Strategic and International Studies, 06 March 2020, https://www.csis.org/analysis/making-most-air-forces-investment-joint-all-domain-command-and-control.

13. Capt Natalie Howie (Cyber and Intel officer, 603d Air Operations Center, Ramstein AB, Ramstein, Germany), interview by the author, 29 July 2020.

14. DOD Instruction (DODI) 5000.82, Acquisition of Information Technology (IT), 21 April, 2020, 5, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500082p.pdf.

15. Maj Christopher Chin, "Preparing Cyberspace Forces for Warfare in the Information Age," Over the Horizon Multi-Domain Operations and Strategy, (January 2019), https://othjournal.com/2019/01/31/preparing-cyberspace-forces-for-warfare-in-the-information-age/.