ITEA Journal 2010; 31: 495–498

Test and Evaluation of Cyber Warfare Systems: Basic Requirements

Norman E. Johnson
SDS International, Ft. Meade, Maryland

The Department of Defense requirements process is designed for systems that will provide decades of service. Well-considered requirements are important for getting it right the first time; however, the Department of Defense does a poor job of articulating requirements for Cyber Warfare Systems that may become obsolete within months. Nevertheless, there are six Mission-Readiness Considerations that form a set of basic requirements that should be evaluated by test and evaluation to inform a mission-ready or fielding decision: safety, security, interoperability, legality, effectiveness, and suitability. Each of these considerations is discussed in detail.

Key words: wartime acquisition environment; capability overlap; obsolescence; mission-readiness; technical risk; interoperability; safety; information assurance; effectiveness; suitability; legality.

Requirements in the Department of Defense (DoD)

Requirements form the foundation for acquisition. They provide overseers with justification to fund an acquisition effort; they provide developers with design objectives; they provide testers with parameters to measure; and they provide decision makers with success criteria.

The DoD requirements process is described in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01G and the Joint Capabilities Integration and Development System (JCIDS) Manual (CJCSI 2009; JCIDS 2009). The process focuses on identifying capabilities needed to perform a mission, capabilities currently available, and the gaps between them. Once the gaps are identified, a process is initiated for closing them. This process includes examining all aspects of doctrine, organization, training, leadership, education, personnel, facilities, and policy. If changes in these areas do not satisfy the gaps, a materiel acquisition program is initiated. It is a top-down, mission-driven process that is generally very good, but it has its weaknesses.

Since it is not a bottom-up process, front line warfighters have very little input. The people who are out there getting shot at sometimes have some excellent ideas on what is really needed to prosecute a war. The process flatters itself by providing an environment to drive technological breakthroughs, but it tends to ignore independent breakthroughs that could provide undreamed of capabilities. For example, motorized tanks and machine guns were huge technological achievements that appeared on the scene not too long after the civil war, but Robert E. Lee would never have dreamed about asking for something like that. The process has many moving parts and is deliberative, ponderous, and slow. This is not a fatal problem for ships, tanks, and aircraft. Those acquisition efforts result in products that provide service for decades, so it is vitally important to set a firm foundation in well-considered requirements. They have to get it right the first time. Cyber warfare systems, on the other hand, are subject to Moore's Law and could become obsolete in a matter of months. They provide capabilities that must stay inside the enemy's decision loop timing, so a drawn-out requirements process is absolutely fatal. Even when the gaps are identified, users have difficulty articulating what is needed to fill them. If you do home handyman chores, how many times have you gone to the hardware store thinking, "I can't really describe what I want, but I'll know it when I see it."

The DoD does a poor job of articulating requirements for cyber warfare systems. This is not to cast aspersions on requirements organizations who strive mightily to do the right thing. They are simply overwhelmed by a wartime culture of urgency and the need to quickly get cutting edge technology into the field in order to stay one step ahead of a very clever and resourceful enemy. In contrast to DoD's 3170.01 process (CJCSI 2009), most "requirements processes" for cyber warfare systems are driven by technological innovations. The research and development (R&D)

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Test and Evaluation of Cyber Warfare Systems: Basic Requirements	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **SDS International,Fort Meade,MD,20755**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**4**	

teams come up with a spectacular capability, and the forward-leaning product teams rapidly produce it and get it into the field with very little testing. This approach has its weaknesses as well.

The requirements and acquisition teams breathlessly try to keep up with the necessary documentation to satisfy overseers and justify funding. This documentation is supposed to be for planning and program guidance, but in this environment it is just an irritating formality. The products that are hastily pushed into the field have very little in the way of concept of operations documentation, training, or logistics support. The designs of urgently needed products frequently do not include reliability or maintainability features. As a result, front line users may spend large amounts of valuable time away from mission duties as they learn how to use the new capability or coax it to work properly. Time saved at the front end of the process (by avoiding a rigorous requirements process) is spent in larger quantities at the back end: "pay me now or pay me more later." Some good ideas cascading out of the R&D brain trust and fielded by product teams are redundant with capabilities already in the field. A more rigorous requirements process would vet these ideas and minimize the capability overlaps. Front line users frequently get unexpected and unrequested capabilities dropped in their laps with an overly sunny briefing, if they get one at all, from the developer or Program Manager (PM). Since many of these capabilities have come straight from development, the users end up doing unstructured beta testing that takes them away from direct mission duties.

When this undeclared beta testing is complete, the users have figured out how to use the capability in a productive manner and have even become a little dependent upon it. After all, it was *supposed* to provide a better capability than the legacy systems. The new system, however, may not have all the features of the old one, so the user ends up employing both. The system gets integrated into operations without formal considerations of safety, security, interoperability, legality, effectiveness, or suitability, which brings us back to requirements. Without documented requirements, these considerations for mission readiness are hollow anyway. How can a decision maker determine if a system is safe, secure, legal, interoperable, effective, or suitable without corresponding metrics? How can he/she even determine how much risk is being assumed? These metrics, and their associated threshold and objective values, flow from well-considered requirements, which can then be measured and evaluated by a robust test and evaluation (T&E) process.

We may not be able to achieve well-considered requirements in the short turn-around times inherent with cyber systems, but it turns out that the six mission-readiness considerations mentioned above are associated with professional communities that maintain standards of acceptability that can be applied to cyber system development programs. With no formal requirements, PMs, developers, testers, and decision makers could anchor themselves to the associated communities to successfully deploy a quick-reaction cyber warfare system capability.

Safety

This is always the first concern, but with software-intensive systems, it is usually not a major concern. Department of Defense Instruction (DoDI) 5000.02 (DODI 2008) indicates that a Programmatic Environmental Safety and Health Evaluation (PESHE) is required by statute (Title 42 U.S.C. 4321). PMs and other acquisition officials are required to identify, consider, manage, and comply with environmental, safety, and occupational health issues early in the acquisition process. A PESHE, conducted by an appropriate safety organization, provides an estimate of the safety risks of a newly developed or developing capability. This in turn provides the necessary insight for a decision maker to weigh risks and benefits associated with a particular capability. This effort is not a test (the T part of T&E), but it is definitely an evaluation (the E part of T&E).

Security

This is another word for information assurance (IA), which is defined in the glossary of CJCSI 3170.01G as

> *"information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."*

IA ensures controls are in place to avoid, detect, reduce, and/or recover from a realized threat.

Before a developer can connect a system to a network to move forward with developmental testing, they must obtain an authorization from the designated approving authority (DAA) for the system to be accessed. For most DoD systems, the DAA is the Defense Information Systems Agency (DISA). Before DISA approves a newly developed product, it must undergo certification and accreditation (C&A) testing as described in DoDI 8510.01, Defense Information Assurance Certification and Accreditation Process (DODI 2007). This process embraces the idea of IA controls, as defined in DoDD 8500.1 and DoDI

8500.2 (DODD 2002, DODI 2003), as the primary set of security requirements for all cyber warfare systems. The IA controls are determined based on the system's Mission Assurance Category Confidentiality Level. An authorization from the appropriate DAA gives an acquisition decision maker the necessary confidence in the IA of a newly developed system to support continued progress.

Interoperability

Interoperability is defined in the glossary of CJCSI 3170.01F as

> *"the ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Information technology and National Security Systems interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchanged information as required for mission accomplishment."*

The metric for interoperability is the Net-Ready Key Performance Parameter (NR-KPP) standards, which comprise the following elements:

- solutions architecture compliant with the DoD Architecture Framework;
- compliance with net-centric data and services strategies;
- compliance with applicable Global Information Grid Technical Guidance;
- compliance with DoD IA requirements, as discussed above; and
- compliance with supportability requirements.

The NR-KPP is a requirement for any capability that touches the Global Information Grid. That includes just about every DoD cyber warfare system capability. Interoperability testing involves testing to evaluate the ability of a system to exchange information with other systems or components and to use information that has been exchanged, without harm. The strategy for testing interoperability should be included in the T&E Master Plan and must comply with CJCSI 6212.01E (CJCSI 2008).

The PM must coordinate with the Joint Interoperability Test Command (JITC) to obtain an Interoperability Certification. As a practical matter, JITC will normally leverage other tests to accomplish this step. When the evaluation is complete, JITC provides an Interoperability Certification. This certification is good for a maximum of 4 years. However, if there is a major change to the system it will have to be recertified earlier.

If there is an urgent operational requirement to field a system or capability but the required documentation to evaluate interoperability is not yet available, an Interim Certificate to Operate (ICTO) may be obtained. The ICTO is issued by the Military Communications-Electronics Board Interoperability Test Panel and provides the authority to field new systems or capabilities for a limited time (up to 1 year), with a limited number of platforms to support developmental efforts, demonstrations, exercises, or other operational use. During this time it is expected that the PM will work with JITC to ultimately obtain an Interoperability Certification.

Legality

The Office of General Council reviews new capabilities for compliance with legal restrictions. This is not a T&E function, but it is an evaluation and an important risk area for decision makers to consider before making a mission-ready decision.

Effectiveness and suitability

Operational effectiveness is defined in the glossary of CJCSI 3170.01G as the "measure of the overall ability to accomplish a mission when used by representative personnel in the environment planned or expected for operational employment of the system considering organization, doctrine, supportability, survivability, vulnerability, and threat" (CJCSI 2009). It is a measure of how well a capability prosecutes the mission for which it was designed. Developmental T&E (DT&E) evaluates and characterizes the performance of a new capability, but that doesn't mean it evaluates how well the capability can perform the mission. For example, a BMW automobile is a beautifully engineered piece of equipment and performs wonderfully; but if the mission is to haul rocks, it falls decidedly short. The purpose of operational T&E (OT&E) is to point that out through an effectiveness evaluation.

Operational suitability is defined in the glossary of CJCSI 3170.01G as "the degree to which a system can be placed and sustained satisfactorily in field use with consideration given to availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, environmental, safety and occupational health, human factors, habitability, manpower, logistics, supportability, logistics supportability, natural environment effects and impacts, documentation, and training requirements" (CJCSI 2009). Suitability is almost interchangeable with supportability or sustainability. It includes all the "-ilities" and is especially concerned with reliability and maintainabil-

ity. It complements an OT&E effectiveness evaluation by assessing the infrastructure and processes that support operational use and that facilitate the capability's effectiveness over its entire life cycle. As with the other five considerations, the decision maker must evaluate the risks associated with a capability's suitability before making a mission-ready decision.

Evaluation of effectiveness and suitability is heavily dependent upon stated operational requirements such as system availability, user interface, and data volume and velocity needs. The independent Operational Test Agency (OTA) responsible for the effectiveness and suitability evaluation develops critical operational issues (COIs) based upon stated requirements. From the COIs flow the measures of effectiveness and measures of suitability, and, at the next level of detail, the measures of performance. Using this information, the OTA develops operational scenarios to gather the necessary data for evaluation. COIs are usually based upon formal requirements, but these are frequently lacking in this wartime culture of urgency saturated with technological innovations. Nevertheless, the OTA can develop COIs based upon developer intentions, perceptions of user expectations and needs, and threat environment. These COIs would not carry the same weight of authority as COIs built upon formal requirements, but they would nevertheless facilitate an evaluation of operational effectiveness and suitability. At the very least it would provide an independent assessment of system capabilities and limitations to inform a mission-ready decision, and to minimize off-mission time for the front line users as they integrate the new capability into their normal processes. When contemplating a mission-ready decision, the decision maker must review the capabilities and limitations, as presented in OT&E reports, and assess the risks associated with releasing it at a particular point in time.

Conclusion

Developmental test and evaluation is a PM tool to uncover, understand, and mitigate technical risk. Site acceptance test and evaluation is a Site Commander tool to ensure that a new cyber warfare system being installed at the site is compatible and will aid the mission, or at least not hinder it. Between these two types of testing in chronology is OT&E. OT&E is a milestone decision authority tool to ensure newly developed cyber warfare systems are effective and suitable before they are employed for mission operations. The OT&E is the last chance to ensure that risks associated with safety, security, interoperability, legality, effectiveness, and suitability are characterized well enough for the decision maker to properly balance the net risks against the net benefits to make a well-informed mission-ready decision in a hectic, urgency-driven, wartime environment replete with technological opportunities, but short on formal requirements. ❑

NORMAN JOHNSON is currently employed by SDS International as a senior advisor for Operational Test and Evaluation (OT&E) for the National Security Agency, Ft. Meade, Maryland. He began his career in T&E in 1986 when he attended the U.S. Air Force Test Pilot School at Edwards Air Force Base (AFB), California. He was a project test pilot on the B-1B development program and later moved to Chief Test Pilot on the Joint STARS development program. During Operation Desert Storm he logged 250 hours of combat flight time in command of the experimental prototype E-8A reconnaissance aircraft. He was director of T&E at the Air Force's Electronic Systems Center, Hanscom AFB, Massachusetts, and spent 5 years at the Pentagon in the Developmental T&E section of the Office of the USD(AT&L). From that office he took his Air Force retirement as a Colonel in 2004. Mr. Johnson has a bachelor of science degree in aerospace physics from the University of Colorado, Boulder; a master's degree in aviation management from Embry-Riddle Aeronautical University, Daytona Beach, Florida; and a master of science in national security strategy from the National Defense University, Washington, D.C. E-mail: nejohnson@cox.net

References

CJCSI 3170.01G. Joint Capabilities Integration and Development System, 1 Mar 09.

CJCSI 6212.01E. Interoperability and Supportability of IT and NSS Systems, 15 Dec 08.

DODD 4630.5. Policy for Interoperability and Supportability of IT and NSS, 5 May 04.

DODD 5000.1. Defense Acquisition System, 12 May 03.

DODD 8100.1. Global Information Grid Overarching Policy, 19 Sep 02.

DODD 8500.1. DOD Information Assurance, 24 Oct 02.

DODI 4630.8. Procedures for Interoperability and Supportability of IT and NSS, 30 Jun 04.

DODI 5000.02. Operation of the Defense Acquisition System, 2 Dec 08.

DODI 8500.2. IA Implementation, 6 Feb 03.

DODI 8510.01. DOD Information Assurance Certification and Accreditation Process (DIACAP), 28 Nov 07.

DODI 8580.1. IA in the Defense Acquisition System, 9 Jul 04.

Joint Capabilities Integration and Development System Manual, 1 Mar 09.