Cybersecurity

SUMMARY

DOT&E assessments over the past fiscal year confirmed that the conclusion from previous years is still valid – DOD missions and systems remain at risk from adversarial cyber operations. Operational tests consistently discovered mission-critical vulnerabilities in acquisition programs. Assessments during Combatant Command training exercises confirmed that DOD cyber defenses are improving, but not enough to stop adversarial teams from penetrating defenses, operating undetected, and degrading missions. Tests and assessments continue to identify previously undetected vulnerabilities, and DOT&E remains committed to facilitating the remediation of these vulnerabilities and verifying that adequate solutions or mitigations are in place.

DOT&E's use of realistic, long-duration adversarial portrayal in assessments for Combatant Commands continues to show that a persistent adversary can gain significant accesses and a deep understanding of warfighter missions and plans. However, most exercises provide only limited time for realistic cyber-attacks; a short-duration (e.g., 5-day) exercise is barely long enough to confirm warfighter readiness in their basic, non-cyber-related missions. Hence, Combatant Commands usually conduct training in a relatively benign cyber environment, which is unlikely to exist for DOD. This may provide warfighters a false sense of confidence about the scope and magnitude of the cyber-attacks facing the Department.

In FY17, DOT&E cyber assessment efforts continued to focus on the ability of warfighters to execute critical missions in the expected operational environment. The demand associated with the planning and conduct of operational tests of acquisition programs remained high, as did the demand for cybersecurity assessments for Combatant Commands and Services. These demands, as well as cyber assessments of DOD weapons systems mandated by section 1647 of the FY16 National Defense Authorization Act (NDAA), resulted in a continuing shortfall for certified DOD Red Teams capable of portraying realistic threats. Operational tests and assessments associated with offensive cyber tools and processes grew, reflecting the increasing DOD interest and effort in this aspect of cyberspace operations.

Well-trained personnel are critically important for executing effective defensive and offensive cyberspace operations and for emulating cyber opposing forces. The best cyber defensive and offensive operations always included knowledgeable and skilled personnel and network users who practiced good cybersecurity. Cyber-related technology was only useful when its operators understood how to operate it effectively. When DOD fielded technology prior to adequate training of operators, as in the case of Joint Regional Security Stacks, the technology did not provide significant benefits to operators.

CYBER ASSESSMENT ACTIVITY

DOT&E continued to oversee cybersecurity OT&E for major defense acquisition programs, and to perform congressionally directed cybersecurity assessments of operational networks and systems during Combatant Command and Service training exercises. DOT&E also expanded involvement in operational assessments for offensive cyber capabilities and tools.

Based on results from operational tests and exercise assessments, DOT&E publishes reports on overarching cybersecurity topics of interest. DOT&E published two classified reports in 2017. The first report discussed special topics in cybersecurity, including defensive best practices, cross-domain solutions, capture of credentials, programmable logic controllers, and incident reporting. The second report presented findings on defensive cyberspace operations that involved a new method for evaluating how well a network can support defensive cyber operations.

Table 1 shows those acquisition programs on oversight that completed operational tests including cybersecurity, and the DOT&E-funded cybersecurity assessments of Combatant Commands and Services conducted during FY17. Table 2 shows the DOD test organizations and agencies that supported the conduct of these activities.

TABLE 1. CYBERSECURITY OPERATIONAL TESTS AND ASSESSMENTS IN FY17	
PROGRAMS COMPLETING OPERATIONAL TESTS OF CYBERSECURITY	
Amphibious Assault Vehicle Survivability Upgrade	Joint Light Tactical Vehicle
AC-130J Ghostrider	Joint Regional Security Stack
Amphibious Combat Vehicle	Joint Warning and Reporting Network
Advanced Field Artillery Tactical Data System	Key Management Infrastructure
AN/SQQ-89A(V) Integrated Undersea Warfare (USW) Combat Systems Suite	LHA 6 *America*-class Amphibious Assault Ship
Ballistic Missile Defense System	Air Force Mission Planning Systems
Common Analytical Laboratory System	Next Generation Diagnostic System
Consolidated Afloat Networks and Enterprise Services	P-8A Poseidon
Chemical Demilitarization	Patriot Advanced Capability 3
Defense Agencies Initiative	Paladin/Field Artillery Ammunition Supply Vehicle (FASSV) Integrated Management
Defense Enterprise Accounting and Management System	Spider XM-7 Network Command Munition
DOD Healthcare Management System Modernization	Ship Self-Defense System
Defense Medical Information Exchange	SSN 784 *Virginia*-class Submarine
F-35 Joint Strike Fighter	Stryker Engineering Change Proposal
Ground/Air Task Oriented Radar	Warfighter Information Network – Tactical
Joint Air-to-Ground Missile	
CYBER READINESS CAMPAIGNS WITH ASSOCIATED EXERCISE	
U.S. Africa Command Judicious Response 2017	U.S. Northern Command Alaska North American Aerospace Defense Command (NORAD) Region Event
U.S. Air Force 603rd Air Operations Center Event	U.S. Pacific Command Pacific Sentry 2017
U.S. Army Reserve Command Event	U.S. Southern Command Integrated Advance 2017
U.S. European Command Austere Challenge 2017	U.S. Special Operations Command Epic Guardian 2017
U.S. European Command Steadfast Cobalt 2017	U.S. Special Operations Command Jade Helm 2017
U.S. Forces Korea Ulchi Freedom Guardian 2017	U.S. Strategic Command Global Lightning 2017

TABLE 2. CYBERSECURITY TEST COMMUNITY	
OPERATIONAL TEST AGENCIES	
Military Services	Air Force Operational Test and Evaluation Center
	Army Test and Evaluation Command
	Navy Operational Test and Evaluation Force
	Marine Corps Operational Test and Evaluation Activity
Defense Agencies	Joint Interoperability Test Command
CYBER TEAMS	
Air Force	57th Information Aggressor Squadron
	177th Information Aggressor Squadron
	92nd Cyberspace Operations Squadron
	46th Test Squadron
	18th Flight Test Squadron
	Air Force Information Operations Center
	688th Information Operations Wing
Army	1st Information Operations Command
	Threat Systems Management Office
	Army Research Laboratory, Survivability/Lethality Analysis Directorate
Navy	Navy Information Operations Command
	Space and Naval Warfare Systems Command
	Navy Operational Test and Evaluation Force
Marine Corps	Marine Corps Information Assurance Red Team
Defense Agencies	National Security Agency
	Defense Information Systems Agency Red Team

Operational Test and Evaluation with Cybersecurity

DOT&E continued to emphasize the planning and conduct of operational tests that include cybersecurity testing. DOT&E recommends cybersecurity testing for all systems that transmit, receive, or process electronic information, by direct, wireless, or removable means. These tests identify vulnerabilities that developers should fix so that secure and resilient systems are developed and fielded, enabling units or agencies equipped with the systems to complete assigned operational missions in a cyber-contested environment. In FY17, DOT&E monitored operational tests with cybersecurity phases for 30 acquisition programs, and continued efforts to enhance the operational realism of cybersecurity tests by researching techniques and tools for testing cross-domain solutions, non-Internet Protocol data buses, and programmable logic controllers.

Assessment of Offensive Cyber Capabilities

In January 2017, DOT&E issued a memorandum that highlighted concerns with the limited operational realism of tests for offensive cyber capabilities. DOT&E is working with capability developers and their testers to explore how best to integrate operationally realistic testing into the non-traditional acquisition lifecycles of these capabilities, which often involve compressed timelines. Concurrently, DOT&E is working with the Joint Technical Coordinating Group for Munitions Effectiveness to identify the data required to build predictive analysis tools for planners to predict cyber effects.

The Combatant Commands are maturing their operational processes for targeting and employing offensive cyber capabilities. U.S. Pacific Command (USPACOM) and U.S. Forces Korea (USFK) requested that DOT&E assist in assessing their cyber fires planning and execution processes during Pacific Sentry 17-2 and 17-3, as well as Ulchi Freedom Guardian 2017. DOT&E assessed the synchronization of cyber fires with component schemes of maneuver, integration of intelligence support, and support to commander objectives, and made recommendations to improve these critical procedures. DOT&E also observed, on closed ranges, the demonstration of several offensive cyber capabilities.

Cybersecurity Assessment Program

DOT&E's Cybersecurity Assessment Program continued to provide resources for operational test agencies, intelligence subject matter experts, and DOD Red Teams to create and assess cyber activities and effects on operational networks and systems during Combatant Command and Service training exercises. DOT&E implemented cyber readiness campaigns that help address vulnerabilities and improve cyber defenders through a series of focused events throughout the year, that culminate in an assessment during a training exercise. The larger number of cyber-readiness campaign events provides more assessment opportunities to assist Combatant Command and Services with specific areas or items of interest.

Engagement with the Intelligence Community

DOT&E is working closely with the Intelligence Community to share independent cyber testing results and analysis of DOD networks and weapon systems. DOT&E's analysis helped inform a National Security Agency assessment and a National Intelligence Council Memorandum for the Deputy Secretary of Defense. DOT&E participated in threat intelligence briefings to the Under Secretary of Defense for Intelligence and the National Security Council as part of a combined Intelligence Community team. The collaboration between the Intelligence Community and DOT&E demonstrates the importance of testing results and how those results can be applied to better understand cyber threats against the DOD and the Nation.

There were numerous reports in FY17 of unclassified data being stolen from cleared defense contractors. DOT&E is forming a team of engineers, system designers, system operators, cyber Red Team members, Intelligence Community experts, and program representatives to characterize the risk posed by the exfiltration of critical data of a DOD system via unclassified networks. The DOD should deploy more personnel to the task force that is identifying vulnerabilities based on information stolen from cleared defense contractors, and direct defense contractors to demonstrate, via cyber Red Team exercises, that they can adequately protect DOD weapons and sensitive information.

Coordination with USD(AT&L) on Statutory Cybersecurity Assessments

In FY17, DOT&E collaborated with USD(AT&L) in planning cyber vulnerability assessments for major DOD weapons systems, as directed by section 1647 of the FY16 NDAA. DOT&E invited USD(AT&L) representatives to observe cybersecurity assessments that DOT&E's Cybersecurity Assessment Program performed with several Combatant Commands, and developed concepts and processes for how best to share assessment results and align future DOT&E activities with statutory cyber assessments. DOT&E and USD(AT&L) also agreed to collaborate on the creation of a global persistent cyber opposing force that expands upon the activities that DOT&E began with USPACOM and U.S. Northern Command (USNORTHCOM).

OBSERVATIONS AND RECOMMENDATIONS

FY17 Cyber Defense Improvements

DOD network defenses against cyber adversaries portrayed in training exercises are improving over defenses observed in prior years. Adversarial teams consistently commented on the improved network defenses due to improved patching and configurations, which resulted in the teams having greater difficulty penetrating assessed networks.

Detection rates of adversarial teams following the initial network penetration were much higher when the teams had to use unauthorized tools instead of their preferred method of using tools already in the network, such as operating system administrator tools, to conduct attacks. The probability of DOD network defenders detecting the adversarial teams improved over the 3-year period starting in FY14, and they are detecting cyber-attacks that previously went undetected.

To improve detection of adversaries in the network, the DOD should:

- Continue improving the speed and completeness of fielding patches, implementing signed patches and updates to remove the ability of an adversary to modify software without authorization. DOD cybersecurity would improve and afford adversaries fewer exploitable vulnerabilities if network defenders implemented U.S. Cyber Command's directives in a timely manner.
- Reduce access to credentials and system administrator tools that adversaries can use as attack tools.
- Expand the practice of "whitelisting" to limit data and applications to authorized users.
- Actively audit system configurations to ensure they remain secure.

Vulnerabilities Remain in DOD Network Defenses

Despite improvements in network defenses, almost every assessment and test demonstrated that DOD network defenses still contain exploitable problems that provide cyber adversaries opportunities for access to DOD networks. Some adversarial teams had longer periods to plan and execute attacks, which was more representative of the time an actual cyber adversary has. These teams often found more vulnerabilities and gained a better appreciation of the operational implications of these vulnerabilities.

Once adversarial teams gained access, they were frequently able to maneuver undetected in a network and exploit trust relationships and systems connected to the network. With these system-level accesses, adversarial teams continued to demonstrate that they can exfiltrate mission-critical information and/or create effects that degrade or prevent mission accomplishment.

Assessment teams for tests and exercises persistently find and report serious vulnerabilities, many of which involve unpatched or misconfigured devices and software. Reasons for problems in basic network hygiene include ineffective operational and administrative network procedures, poor physical security surrounding network components, and shortfalls in net-defender staffing and expertise.

Defender Expertise is Essential

Effective cyber defense requires effective cyber technology coupled with well-trained operators and defenders. Fielding new technology without the support of capable operators can reduce and even eliminate the potential benefits of that technology. A prime example of this is the fielding of Joint Regional Security Stacks (JRSSs), which are expensive, room-sized technology suites with complex integration challenges. JRSSs are intended to centralize and standardize network security into regional architectures.

The Army and Air Force started fielding JRSS in 2016 without performing the independent cybersecurity assessments that are normally required for major acquisition programs. The Defense Information Systems Agency (DISA) performed an operational assessment in September 2017, which discovered key cybersecurity deficiencies with JRSS technology, processes, and training. New JRSS program leadership intends to address these deficiencies. In the meantime, network defenders who already struggled with legacy network security problems must deal with additional JRSS-related problems.

In recent years, DOT&E has observed well-defended networks only where mature and well-configured network technology supported well-trained and experienced network defenders. The expedited fielding of immature network technology and training packages helps neither the warfighter nor the teams who strive to support the warfighter with enabling technologies.

DOT&E observations continue to highlight that human expertise is essential for effective cyber operations, including defensive cyberspace operations, offensive cyberspace operations, and cyber adversarial teams. System and network users must understand that they are both users and defenders of their mission space. Users and cyber defenders must understand the networks and systems under their purview at least as well as potential adversaries. They must be well-versed in the procedures for reporting and responding to cybersecurity incidents and conduct clear and timely communications between cyber-defense organizations.

Major training events should include periods where a threat-representative cyber adversarial team demonstrates attacks and stresses the networks, systems, and missions; the network users and defenders should demonstrate whether they can sustain critical missions in such a contested environment. Although directed by The Chairman of the Joint Chiefs of Staff in 2011, and endorsed by two subsequent Secretaries of Defense, DOT&E has not observed many demonstrations that Commands can "fight-through" a major cyber-attack and sustain their critical missions. The Combatant Commands and Services should perform frequent training that includes disruptions in order to prepare for expected cyber-attacks, and develop and document well-coordinated responses in operational playbooks.

Adversarial teams must understand adversarial capabilities and intent, but to portray an advanced adversary they must also understand DOD mission objectives and defensive capabilities. Armed with this aggregated knowledge, adversarial teams can perform representative cyber-attacks to train operators and defenders, and help identify the most likely and critical vulnerabilities for mitigation.

Hiring, training, and retaining people with cyber knowledge, awareness, and skills is both more efficient and more difficult than simply buying the latest technology. Retention of an expert cyber workforce – including operators, defenders, adversarial teams, and assessors – is essential to achieving the goals of the DOD Cyber Strategy.

Maturation of cyber skills and capabilities requires experience and knowledge from testing and training in realistic conditions. To this end, the DOD should:

- Allow disruptions caused by threat-representative cyber effects in all major exercises in order to demonstrate mission resiliency to cyber-attacks.
- Consider additional ways to retain highly skilled personnel that the DOD requires for effective cyber-defense, offense, and assessment missions.
- Ensure operators of new cyber technology receive adequate training prior to fielding the technology.
- Hold users who commit serious violations that degrade DOD cybersecurity more accountable.
- Minimize the use of and improve the monitoring of cross-domain solutions.
- Consider reducing the connection between the Non-classified Internet Protocol Router Network and the Internet for most DOD users. This could reduce the cyber-attack surface and allow defenders to focus their time and energy on attacks by more advanced adversaries.

Defender Span of Control

The concept of cyber span of control must mature to understand how many defenders can cover assigned network terrain. To-date, defenders of small headquarters networks (networks that host a few hundred users) have been more likely than defenders of large networks to succeed against a realistic cyber opposing force. Cyber Red Teams find it easy to operate undetected across large networks like the Air Force Information Network, which supports approximately 800,000 users.

DOT&E has observed a number of cases of successful network defense during exercises and operational tests. These successful defenses occurred in small networks, including those at Combatant Command headquarters. These small networks typically had at least one defender for every few hundred user accounts, enabling defenders to monitor network and user activity, and to apply cybersecurity best practices effectively. DOD should continue to implement the following best practices:

- Operators and defenders have expert knowledge of their missions and networks, are familiar with normal operations and can recognize anomalies, have current playbooks for rapid and effective response actions to counter detected attacks, and do not have to defend more cyber terrain than their resources can support.
- Network authorities implement effective password policies and practices that address password storage, reuse, and complexity to reduce opportunities for adversaries to masquerade as legitimate users.
- Defenders implement up-to-date configurations and timely patching of systems to remove known paths for access and exploitation.

- Network authorities implement authentication for use of externally accessible websites or place such websites in special network zones to minimize attack paths to better protect sensitive information.
- Network authorities implement segmented networks and matching of user privileges and services with operational needs. This reduces adversary access to restricted software and information, and forces adversaries to use more detectable tools and techniques.

The size and scope of cyberspace precludes defending everything, requiring operators and defenders to implement the concept of cyber key terrain. Cyber key terrain is the subset of information, networks, and devices within cyberspace upon which critical missions depend. Organizations must consider how sharing information with other organizations and networks outside of their direct control affects security, such as when sharing information in the joint and coalition environments. DOT&E observed instances where judicious selection and monitoring of cyber key terrain enabled defenders to focus their defensive efforts and prevent cyber adversarial teams from degrading critical missions.

Evolving Requirements for Cyber Tests and Assessments

It is good news that the DOD's cyber defenses are improving, especially in smaller networks, but it also highlights that the DOD must improve the cyber adversarial teams to realistically portray advanced cyber adversaries and continue driving cybersecurity improvements. Operational Test Agencies and DOD Red Teams must become capable of portraying cyber adversaries in accordance with known doctrine, tactics, and capabilities in both offensive and defensive operations.

Technical capability needs include:

- Non-Internet Protocol data transmission systems. The Services are developing tools and test capabilities for some non-Internet Protocol components, but some operational tests in FY17 had limitations related to needed tools and expertise.
- Supervisory control and data acquisition systems. Testing protocols are needed for components such as programmable logic controllers.
- Multiple spectrum cyber threats. More tools and expertise is needed to conduct cybersecurity tests using radio frequency, acoustic, and radar data.

The Service cyber Red Teams do not have the capacity to fully meet the demands for tests, assessments, and training exercises. This has resulted in an increasing number of operational test-related conflicts and delays. The Cyber Protection Teams (CPTs) include an element to assist in portraying a threat, but these elements do not possess the National Security Agency certification or skills required of a DOD Red Team operating on DOD networks. The DOD should provide resources to expand capacity and capabilities of DOD cyber Red Teams for more representative threat portrayal in exercise assessments and operational tests.

Cyber Protection Team Observations

CPTs encountered operational challenges in deploying and integrating with local defenders to defend networks assessed in large-scale training exercises.

- Some CPTs were understaffed and members had minimal operational experience with tools and operations.
- Some CPTs did not have the knowledge and experience on the intended networks to rapidly integrate with and supplement existing defenders.
- Some CPTs spent a disproportionate amount of time on local administrative requirements that reduced their dwell time working on the intended networks.

In a few cases, DOT&E observed network authorities attempting to offset these CPT shortfalls, for example:

- U.S. African Command (USAFRICOM) established an out-of-band connection between their headquarters enclave and their assigned CPTs at Fort Gordon, Georgia. This connection allows those teams to operate continuously on the USAFRICOM enclave, resulting in better network familiarity and mission support.
- The U.S. Navy plans to deploy teams of cyber defenders with major combatant ships, equipping them with a standard toolkit to rapidly detect abnormal activity on shipboard networks and capture data for analysis, forensics, and remediation.
- The U.S. Air Force plans to develop specialized cyber defenders to support specific operational mission areas.

DOT&E will continue to observe and record observations from the operational employment of the CPTs in assessed Combatant Command training exercises.

Confidence in Offensive Cyber Capabilities

Maturing the processes for planning and employing cyber fires is essential for cyber fires to become a more effective option for commanders. The synchronization and coordination of cyber fires with kinetic and non-kinetic effects continued to improve, with Combatant Commands exploring how to modify existing operational processes to match the operational characteristics of cyber fires. Assessments of operational processes during training exercises identified challenges from mismatches in terminology, differences in expectations for operational timelines for cyber and other fires, and delays associated with the level of approval and authorities required to employ offensive cyber capabilities.

In FY17, DOT&E performed a preliminary review of ongoing Service testing for offensive cyber capabilities, and identified some inconsistencies with OT&E methods and varying degrees of operational realism. DOT&E also noted that most testing performed by the Services does not include an opposing force or human element responsible for defending or maintaining the target of the offensive capability. Adversaries, through their responses, affect the scope and duration of cyber effects on systems they control; Services should include this element when testing capabilities for critical missions. The DOD should conduct appropriate operational testing of critical offensive cyber capabilities to provide confidence in intended effects. DOT&E will continue to oversee operational testing of offensive capabilities and assess related processes to provide a complete operational perspective on the efficacy of cyber fires.

Persistent Cyber Operations

Threat-representative cyber activity is essential for operational tests, operational assessments, and realistic training. Although most test and training events are of relatively short duration (1 to 2 weeks), real-world adversaries have a much longer window to acquire access and prepare for potential cyber-attacks. Persistent Cyber Operations (PCO) authorities afford DOD-certified Red Teams the ability to perform longer-duration planning and network-access development that is more representative of an advanced, persistent cyber threat. In FY17, DOT&E continued engagement with U.S. Cyber Command to establish global standing ground rules to simplify and enable PCO elements to portray the threats needed for operationally realistic tests and training.

Assessments supported by PCO elements with U.S. Strategic Command, USPACOM, and USNORTHCOM in FY17 demonstrated the feasibility and value of having PCO to enable representative training and assessment events. PCO assessments also demonstrated the means to identify vulnerabilities that would otherwise have gone undetected, thereby increasing both the security of networks and warfighter preparation for cyber warfare. Standing ground rules will provide the foundation for expanding the presence and benefits of the PCO across the DOD. The DOD should implement authorities for global persistent cyber opposing force operations to be replicated on DOD networks.

Challenges for Coalition Operations in Cyberspace

The DOD expects to fight side-by-side with coalition partners in many scenarios, in many theaters. In scenarios where a cyber adversary is present, coalition operations may be degraded by the restrictions that preclude sharing knowledge of cyber-attacks, status of networks, and any information that involves a vulnerability on a U.S. network. These restrictions reduce the utility of coalition training and leave the U.S. and coalition partners ill-prepared to operate effectively in combined environments that are contested by a cyber adversary. Coalition networks often do not receive the same network defense support as other DOD networks, even though they are owned and operated by the DOD. The DOD should revise cyber classification guidance to enable effective cyber-related collaboration, training, and assessment with coalition partners.

DOT&E is helping prototype cyber-range environments that may help with coalition training. These environments could also assist in the demonstration of the effects of vulnerabilities and best practices, thereby improving the cybersecurity of coalition networks. The following section discusses these efforts in more detail.

Cyber Ranges and Executive Agents

For the last several years, DOT&E has advocated for a cyber range structure that supports both test and training requirements. Because of the similarity of functions in test and training, a common architecture across these ranges is needed to provide efficiency and flexibility to address the increasing demand for cyber range resources, and to effectively respond to rapidly evolving and increasingly sophisticated cyber threats.

The FY15 NDAA directed the DOD to establish an Executive Agent (EA) for cyber training ranges and an EA for cyber testing ranges, and required their collaboration to achieve a common architecture. In FY16, the DOD established the Army as the EA for training ranges and the Test Resources Management Center (TRMC) as the EA for test ranges. In the FY17 budget, the DOD allocated funds separately for a Persistent Cyber Training Environment (PCTE) and for cyber test ranges. More than two-thirds of the approximately $750 Million allocated for cyber ranges falls within the PCTE program element, which underscores the importance for dual-use capabilities.

DOT&E has engaged with the PCTE program to advocate for the acquisition of effective and suitable range capabilities, to collaborate in the development of a test and evaluation approach, and to encourage dual use across test and training ranges. DOT&E is also interacting with both EAs to promote clear understanding of requirements, common architectures, and standards.

In FY17, assisted by DOT&E funding and liaison, the Joint Staff J6 provided a representative command-and-control range environment and hosted tests and training for USPACOM and the Australian Defence Force during Talisman Saber 17. Hosted by USPACOM's Cyber War Innovation Center and the 613th Air Operations Center, the event constructed a distributed classified mission rehearsal platform for the Combined Air Operations Center and Joint Operations Center. This event helped meet key objectives for U.S. and Australian cyber defense teams and Red Teams to build relationships, conduct combined operations, hone technical skills, and exchange and build new tactics, techniques, and procedures. Teams participating in this exercise found the integration with joint and coalition forces to be invaluable.

Following an exercise assessment with USFK and South Korean forces, USFK leadership requested help in executing training and assessments with their coalition partner. DOT&E is working with USFK to develop a preliminary cyber-range environment where U.S. and South Korean forces may be able to train as a coalition force on matters of critical importance to operations in the cyber domain.

EFFECTIVE DEFENDER PRACTICES

The DOD's cyber defenses are improving. In FY15 and continuing through FY17, DOD cyber Red Teams in training exercises had more difficulty accessing and exploiting networks. Defenders must have good situational awareness of the network, and activity within the network, to properly react to an adversary and provide a successful defense. The following is a summary of best defender practices, which correlate to DOT&E observations of defenders successfully reacting to DOD cyber Red Teams.

Unity of Effort for Operations, Intelligence, and Cybersecurity

As in other warfare domains, successful cyber operations require unity of effort and integration across functional elements. Reactive defenses were most successful when commanders made cybersecurity and cyber operations a focus and priority similar to other operational domains, and when they were organized to coordinate both offensive and defensive activities, including cyber. Commands where cybersecurity was a high-interest item, and where Joint Cyber Centers have been established, were more successful countering activities by DOD Red Teams.

Successful reactive defenses used knowledge of operations and intelligence to prioritize areas of the network for enhanced monitoring based on strategic intelligence analysis regarding threat intent. DOT&E observed several cases where resources were prioritized to defend cyber key terrain and provide cyber defenders information to concentrate their efforts and tools to detect malicious activity.

Successful reactive defenses also integrated external resources to enhance local defenders. For example, augmenting local defenders with CPTs allowed more timely review of sensor alerts and logs to identify and investigate suspicious or malicious activities. CPTs have been effective network defense players where they have been well-trained or given opportunities to learn and operate on the networks they defend.

Span of Control

As discussed above, a fixed number of network defenders can only successfully defend a limited set of network assets; automated tools and sensors can only extend that reach so much. DOT&E observations confirm that local defenders typically experience more success with smaller and well-defined networks than with larger and more open networks. This observation is relevant to the Joint Information Environment, which the DOD is implementing and which may expand the span of control for network defenders beyond what is practical.

Experience and Proficiency

Networks defended by experienced personnel with proven proficiency more consistently hindered and challenged the DOD Red Teams. Network defenders must sort through data provided by sensors and detection devices to identify malicious actions from normal activity. DOT&E is increasingly observing proprietary tools developed by defenders (often best described as "skilled hobbyists") who create tools, build on their performance, and integrate them into their standard procedures.

It is critical to hire and retain skilled cyber personnel. Military personnel on timelimited duty rotations often lack the opportunity to acquire adequate cyber experience, or leave the DOD after achieving that experience. DOT&E observed that selective hiring and continuity of civilian and contractor personnel allowed local defenders to develop familiarity with the networks defended, recognize normal modes of operation, and better plan for abnormal activities.

DOT&E observed that some successful network defenders were able to identify indicators and warnings for likely threats. This enhanced their understanding of adversary tactics, techniques, and procedures to include how the sensors and network logs will record and report such activity. In some cases, defenders developed software scripts and signatures to detect and alert on suspicious indicators.

Commensurate Authorities

The cybersecurity defense structure within the DOD is built around three tiers of authorities and responsibilities, although the specific duties of each tier differ from location to location. Organizations demonstrating successful reactive defenses often deviated from the formal doctrine. In some locations, cybersecurity sensors provide data only to the non-local or regional tiers. However, local defenders tended to experience success when they had direct access to sensor feeds such as the Host-Based Security System on their networks to enable improved situational awareness at the tactical level. CPTs report that when their span of view of network sensors is widened, their ability to predict and anticipate anomalous activity improves. Organizations that maintain relationships with acquisition program offices for fielded systems in their area of responsibility can work directly with materiel suppliers to solve problems. Finally, local defenders having authority to implement selected response actions with minimal external coordination can lead to improved speed of defense.