Cyber Operational Architecture Training System – Cyber for All

Dr. David "Fuzzy" Wells, IPA, CMSP
USPACOM J81 / Cyber War Innovation Center
Camp H.M. Smith, HI
william.d.wells1.ctr@pacom.mil

Derek Bryan
USPACOM J81 / Ingenia Services, Inc.
Camp H.M. Smith, HI
derek.bryan.ctr@pacom.mil

ABSTRACT

Current methods for conducting cyber training are incompatible with the traditional, simulation-based training architectures used to conduct battlestaff training. As a result there is little to no interaction between the cyber domain and the traditional warfighting domains during exercises. This situation does not accurately reflect the current operational environment nor does it address the Secretary of Defense's (SECDEF) and the Chairman of the Joint Chiefs of Staff's (CJCS) directives and guidance for incorporating realistic cyberspace conditions into major Department of Defense (DoD) exercises. The Cyber Operational Architecture Training System (COATS) is a U.S. DoD Modeling & Simulation Coordination Office (M&SCO) High-Level Task (HLT) that integrates existing cyber range environments, traditional simulation architectures, operational networks, and cyber emulations to safely and securely synchronize and deliver realistic cyber effects to the entire battlestaff – cyber for all. In doing so COATS provides an integrated and contested training environment where operators plan, execute and experience realistic cyberspace operations and conditions in all domains. This paper describes the key components of the COATS architecture, including the application of network guards and the first draft of a cyber data exchange model, lessons learned from the demonstration and employment of COATS during three U.S. Forces Korea exercises, and recommendations for future cyber and traditional modeling and simulation capability research, development, test and evaluation.

ABOUT THE AUTHORS

Dr. David "Fuzzy" Wells is the Director of the U.S. Pacific Command's (USPACOM) Cyber War Innovation Center (CWIC) and the Technical Lead for COATS. A retired Air Force (AF) officer, his past assignments include: Chief Scientist for Research and Development at the Joint Warfare Analysis Center; Chief of Ops Assessment at AF Central Command's Combined Air & Space Ops Center; Chair of Ops Research Working Group, Director of Modeling & Simulation (M&S) Education and Assistant Professor of Computer Science at the U.S. Air Force Academy; AF M&S lead for U.S. Joint Forces Command's Millennium Challenge experiment while at the AF Agency for M&S; and Prime Warrior Course Director and AF lead for the Prairie Warrior exercise while at the AF Wargaming Institute. He has served as exercise designer and senior controller for battlestaff training exercises worldwide. He was the first AF officer to obtain a Ph.D. in Modeling, Virtual Environments and Simulation from the Naval Postgraduate School. He also earned the first M.S. in Modeling & Simulation from the AF Institute of Technology. He is a Certified Modeling & Simulation Professional Charter Member and a National Modeling & Simulation Coalition Plankholder.

Derek Bryan has provided direct support to the USPACOM J81 – Joint Innovation and Experimentation program since 2005. In this role he is responsible for the research, testing, and assessment of innovative solutions to USPACOM capability gaps. Mr. Bryan is currently providing project management and engineering support to the CWIC and the COATS project. Mr. Bryan has a B.S. in Computer Science from James Madison University and an M.E. in Modeling and Simulation from Old Dominion University.

Cyber Operational Architecture Training System – Cyber for All

Dr. David "Fuzzy" Wells, IPA, CMSP
USPACOM J81 / Cyber War Innovation Center
Camp H.M. Smith, HI
william.d.wells1.ctr@pacom.mil

Derek Bryan
USPACOM J81 / Ingenia Services, Inc.
Camp H.M. Smith, HI
derek.bryan.ctr@pacom.mil

OPERATIONAL PROBLEM

There is no controversy regarding the realities of cyber threats to U.S. interests at home and abroad. The DoD, in partnership with international, federal, state and local governments is tasked with defending those interests and enabling an open, secure and prosperous environment for all. The April 2015 DoD Cyber Defense Strategy guides the development of cyber capabilities necessary to organize, train, and equip U.S. military forces in these missions. This guidance calls for the development of "… an individual and collective training capability … to conduct joint training (including exercises and mission rehearsals), experimentation, certification, as well as the assessment and development of cyber capabilities and tactics, techniques, and procedures for missions that cross boundaries and networks" (Carter, 2015).

The majority of today's cyber training is conducted on dedicated, closed network "ranges" that provide the basic services and controls necessary to train DoD Cyber Mission Forces on their primary tasks and missions. While sufficient for this purpose, these ranges operate independently from the traditional M&S environments used to conduct battlestaff training across the spectrum of DoD operations, many of which are influenced by or rely on the cyber domain. As a result, there is a lack of integration with the cyber domain during major DoD exercises that limits the battlestaff's ability to plan, integrate, and execute integrated cyber operations. Perhaps more importantly, this limitation restricts the battlestaff's opportunities to experience and fight through degraded and denied conditions as required by the April 2014 CJCS Instruction 3500.01H entitled "Joint Training Policy for the Armed Forces of the United States" (Goldfein, 2014). Manual workarounds (e.g., "white cards") can be used by exercise controllers to inject rudimentary degraded or denied conditions into exercises, but these workarounds are typically low fidelity and have little or no relation to the ongoing cyber war within the cyber ranges or the M&S environment used to stimulate the Command, Control, Communications, Computers and Information (C4I) systems in use by the battlestaff. This situation is summarized in Figure 1 below.

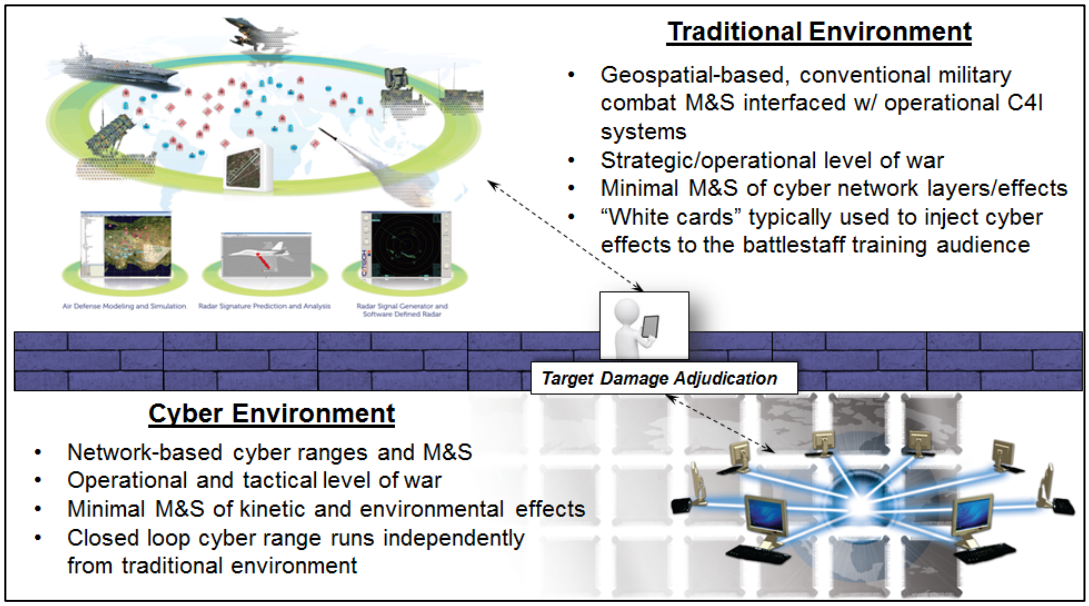

Figure 1: Current Exercise Environment

COATS DESCRIPTION

In 2014 M&SCO funded an HLT to develop an integrated training environment prototype capable of addressing the operational needs described above. COATS leverages and integrates existing cyber range environments, traditional battlestaff training architectures, operational networks, and cyber emulations to synchronize and deliver realistic cyber and traditional effects to the entire battlestaff. This integration is facilitated by the use of a network guard to protect and assure data flow between disparate networks and a new cyber Data Exchange Model (DEM) for interoperability between cyber and traditional M&S systems as depicted in Figure 2 below.

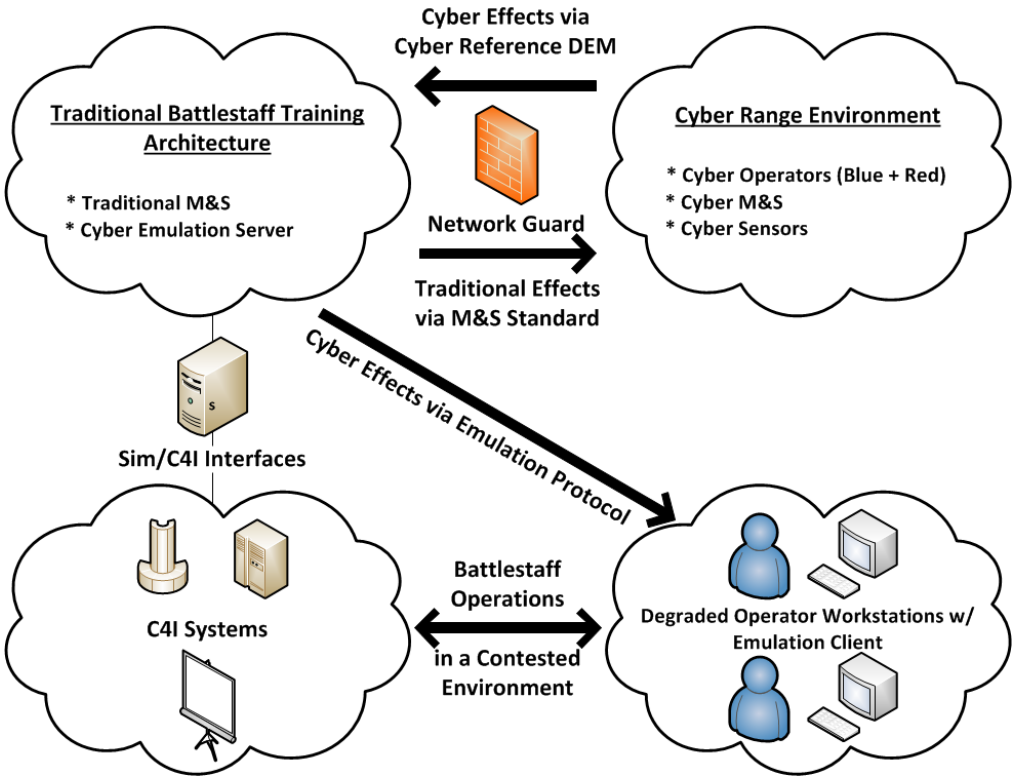

Figure 2: COATS High-Level Operational Concept Graphic

The critical components of the COATS architecture are the following:

- Cyber Range Environment – The cyber range environment is a collection of Live, Virtual and Constructive (LVC) cyber M&S tools and sensors used to create a realistic representation of critical networks, nodes, systems and message traffic correlated with the overall exercise scenario and forces. For COATS, the cyber range environment is responsible for sensing cyber effects (not attacks) of interest, translating cyber effects into the cyber DEM, and passing over a protected network to the traditional battlestaff training architecture. Message traffic must pass through a network guard prior to receipt by the traditional battlestaff training architecture. A combination of open source, Government-Off-The-Shelf, Commercial-Off-The-Shelf and custom tools are used to create the cyber range environment such as Nagios, iperf, the Joint Network Simulation (JNETS) component of the USAF's Air and Space Constructive Environment Information Operations Suite (ACE-IOS), and EXata. The cyber range is also responsible for receiving traditional effects of interest (e.g., kinetic and Electronic Warfare [EW] effects) from the traditional battlestaff training architecture and simulating those effects on the corresponding cyber range networks, nodes, systems and message traffic. Example effects include performance degradation, configuration changes and system failure. The USAF 90th Information Operations Squadron (IOS) currently provides the COATS cyber range environment.

- Cyber DEM – The cyber DEM is a draft standard developed by COATS partners that organizes and defines a series of data types that represent cyber effects of interest. The cyber DEM is necessary because there is no existing standard or method for sharing cyber M&S data within the DoD. Currently implemented as an eXtensible Markup Language schema, the cyber DEM can be easily applied to a DoD M&S standard such as the Distributed Interactive Simulation, High-Level Architecture, or the Test and Training Enabling Architecture. (Morse, Drake, Wells, Bryan, 2014)
- Network Guard – An accredited network guard is required between the cyber range environment and the traditional battlestaff training architecture to assure and protect the applicable networks and systems. The network guard implements a restrictive ruleset that ensures that only approved messages, in the proper format, are securely passed from the expected sender to the expected receiver and vice versa. The network guard does not change or validate the classification level of the data. The U.S. Navy's Radiant Mercury (RM) device, in tandem with the USAF's ACE-IOS "JIOR Broker" application, collectively acts as the network guard for COATS.
- Traditional Battlestaff Training Architecture – The traditional battlestaff training architecture is a collection of traditional (e.g., kinetic, EW, intelligence, etc.) M&S networks, protocols and software applications used to simulate key battlespace events and stimulate C4I systems and processes in use by the training audience. For COATS, the USAF's ACE-IOS system is responsible for sensing traditional effects of interest (e.g., kinetic damage to a communications capability) and passing to the cyber range environment through the network guard. The traditional battlestaff training architecture is also responsible for receiving and correlating cyber effects of interest (e.g., network performance degradation, system failure) from the cyber range environment and degrading the applicable simulated system capabilities and/or passing the effect to the cyber emulation to degrade the corresponding training audience network-based service or workstation.
- Cyber Emulation – The cyber emulation is an accredited tool for emulating network and host cyber effects on training audience workstations that have been sensed from within the cyber range environment. The cyber emulation does not affect the underlying network, nor does it damage the affected workstation. For COATS, the Network Effects Emulation System (NE2S) Master Control Station (MCS) is responsible for receiving cyber effects from the traditional battlestaff training architecture (ACE-IOS) and initiating the corresponding emulated cyber effect on the applicable training audience workstation. Using a remotely-accessible web interface, the NE2S MCS provides situational awareness and positive command and control of emulated cyber effects. An NE2S client application is installed on each workstation to be affected that must establish and maintain secure communications with the NE2S MCS in order for effects to be initiated. Effects can be instantaneously started, stopped or adjusted from the MCS for an individual workstation, a group of workstations, or all workstations. If secure communications are not established or maintained, existing effects will timeout, no new effects will be initiated, and all affected workstations will be restored to previous (unaffected) conditions.

As depicted in Figure 2 above, COATS does not interface with or affect existing simulation-to-C4I interfaces used to stimulate the operational networks and systems in use by the training audience. COATS interfaces with M&S tools within simulation federations via the cyber DEM and affects operational workstations via the cyber emulation.

COATS USFK Deployment

The COATS architecture and associated technologies were deployed across the Continental U.S., Hawaii, and the Republic of Korea to support FY14/FY15 demonstration and training events with U.S. Forces Korea (USFK) and 7th Air Force (7 AF) during exercises Ulchi Freedom Guardian (UFG) 2014, Key Resolve 2015 and UFG 2015. The cyber range environment was provided by the USAF 90th IOS and used the Joint Information Operations Range (JIOR) and the network guard (RM plus ACE-IOS JIOR Broker) to share data over the Korea Battle Simulation Center (KBSC) Training and Exercise Network (KTEN) with ACE-IOS. ACE-IOS at the Korea Air Simulation Center (KASC) communicates with other M&S tools within the Joint Training Transformation Initiative + Korea (JTTI+K) federation (e.g., the Distributed Information Operations Constructive Environment) over KTEN as well as through a firewall to the NE2S MCS on the Combined Enterprise Regional Information Exchange System-Korea (CENTRIXS-K) network. The NE2S client software is deployed at USFK 7 AF to provide a contested training environment for the battlestaffs. An alternative Wide-Area Network connection was established between Nellis Air Force Base and the KBSC by tunneling through the Joint Training Enterprise Network (JTEN) and will remain in place until the installation and accreditation of the USFK network guard has been verified. A graphical depiction of this architecture is provided in Figure 3 below.

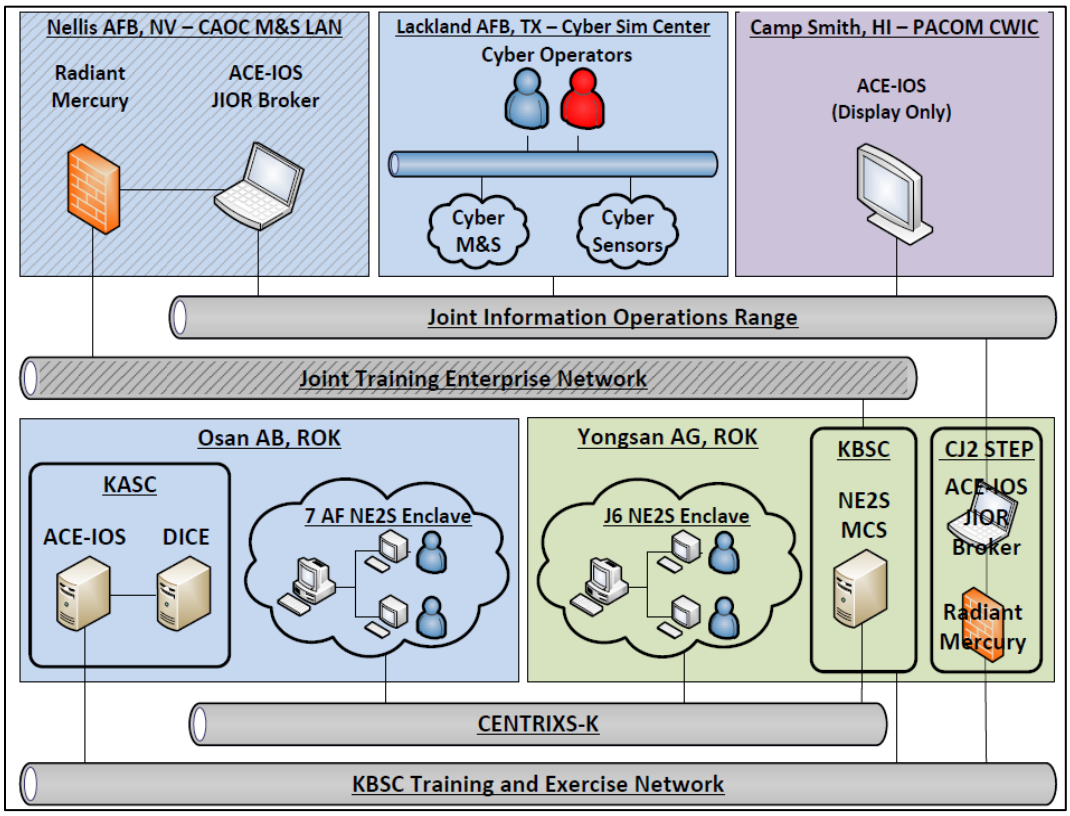

Figure 3: COATS USFK Deployment

The COATS USFK deployment supports four generic vignettes that can be tailored and integrated into the exercise scenario and Master Scenario Event List (MSEL) as required. The four vignettes are:

- Computer Network Attack (CNA) – Live red CNA against virtual blue systems to demonstrate virtual host degradation effects on live operator workstations. See Figure 4 below for additional details.
- Physical Node Attack – Constructive red kinetic attack on a constructive blue communications facility to demonstrate C2 disruption effects on live operator workstations.
- Distributed Denial of Service – Live red CNA on virtual blue systems to demonstrate virtual full-motion video degradation effects on live operator workstations.
- Threat Network Degradation – Live blue CNA on virtual red networks to demonstrate constructive system degradation on constructive red systems.

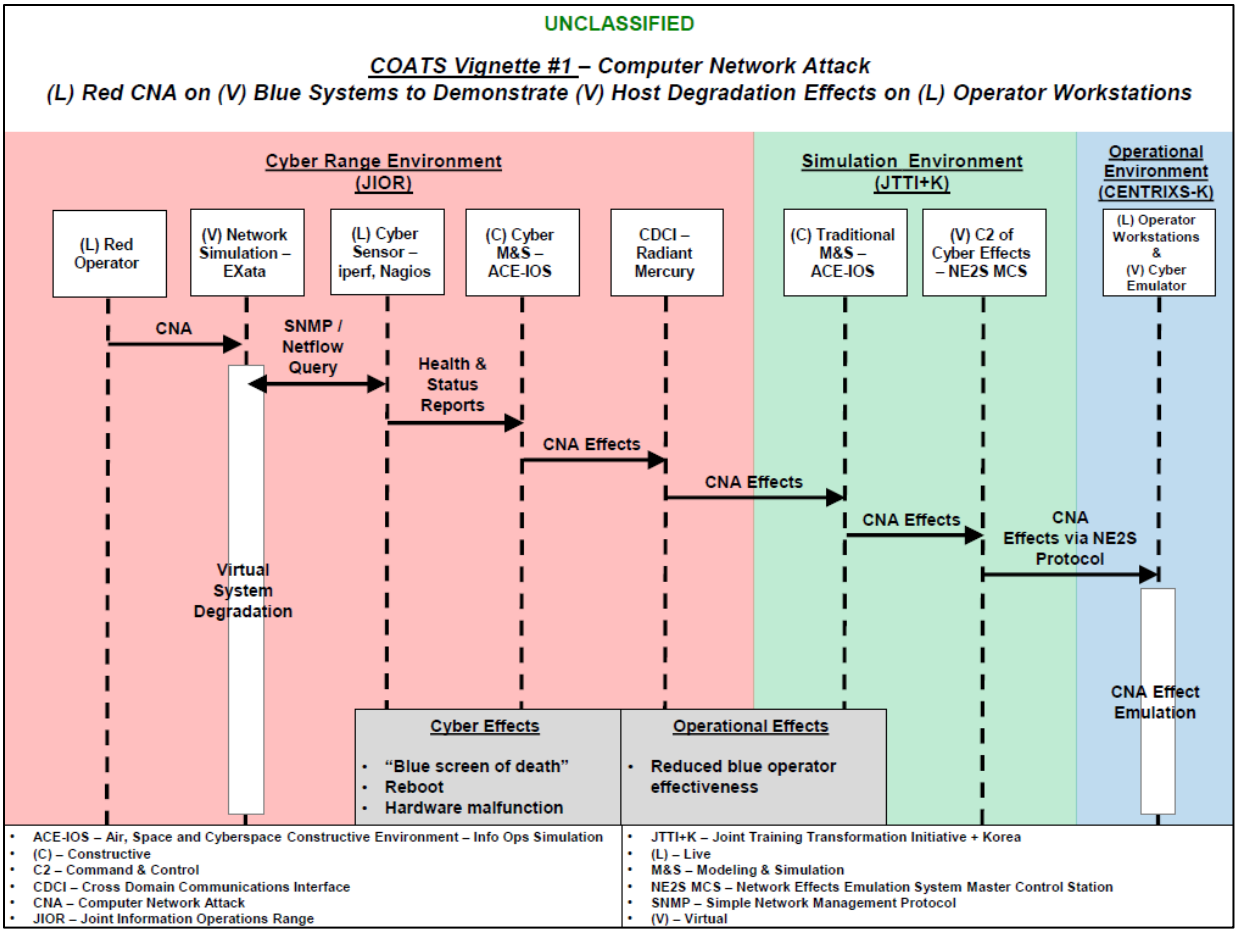

Figure 4: COATS CNA Vignette

LESSONS LEARNED

Key lessons learned from the planning, implementation, deployment and operation of COATS capabilities for two USFK large-scale battlestaff exercises are detailed in the following sections.

Planning

Planning for integrated cyber operations during a major exercise was the most significant and resource intensive challenge we experienced. Socialization and coordination of COATS activities was required across multiple organizations and throughout all levels of each organization (senior leader to action officer to technical support contractor). Past experiences with cyber training and exercises and a lack of understanding of the current state of the art often led to concerns about COATS and its potentially negative impact on the broader exercise objectives and training audience performance. As a result, an incremental approach was implemented that included multiple demonstration and test events to increase the battlestaff's level of familiarity and comfort with the technologies. Once the technologies were verified and approved, the details and procedures for how to integrate and command and control degraded cyberspace conditions in a battlestaff exercise were immature or non-existent. Exercise planning products and exercise control procedures had to be updated to include measures and controls for implementing and monitoring degraded cyberspace conditions and had to be integrated and synchronized with the overall exercise objectives, scenario, and MSELs.

Implementation

The implementation of COATS at USFK required the integration of existing cyber range environments, cyber and traditional M&S tools, and cyber emulations across disparate cyber, training and operational networks. This integration required the development of the cyber DEM, modifications to existing traditional M&S tools to become "cyber aware," and the use of the COATS network guard (RM and ACE-IOS JIOR Broker) to enable secure data flow between cyber ranges and simulation networks. Functionality and data flow were verified prior to each event as part of a Comprehensive Integration Test. The current implementation supports up to four generic vignettes that can be tailored and integrated into the overall exercise scenario and MSELs. Additional vignettes for different mission areas (e.g., Integrated Air and Missile Defense) are possible but would likely require additional modifications to traditional M&S tools to receive and realistically respond to the cyber effects represented within the cyber DEM. The risks and costs associated with the technical implementation of COATS at USFK were relatively low due to the reuse of existing capabilities and the straightforward integration strategy.

Deployment

The deployment of COATS technologies at USFK was most impacted by Information Assurance (IA) policies and procedures. Existing certification and accreditation products had to be reviewed or expanded before local authorities would approve installation and operation; approval via reciprocity was not an option. IA requirements for the simulation network (owned and administered by the KBSC) were different from those on the operational network (owned and administered by 8th Army's 1st Signal Brigade).

Operation

The operation of COATS technologies was straightforward and was aided by the personnel and associated roles and responsibilities detailed in Table 1:

Table 1: COATS Manning Plan

Role	Responsibilities	Qualifications	Location
Cyber Subject Matter Expert (SME)	• Monitor the execution and training audience response to all cyber MSELs, including COATS • Report results to the exercise control group • Report related issues to the COATS SME	Needs to be aware of COATS but does not need to be a COATS SME	Exercise control group / Cyber working group
COATS SME	• In coordination with the Cyber SME, monitor the execution of COATS-supported MSELs • Report COATS technical issues to the Cyber SME • In coordination with the COATS technician, monitor the status of COATS technologies	Must be a COATS SME; must understand exercise control group TTPs	Exercise control group / Cyber working group
COATS Technician	• Monitor and report the status of COATS technologies to the COATS SME • When requested by the COATS SME, troubleshoot and resolve technical issues	Must be a COATS technical SME	Various
NE2S Operator	• As requested by the Cyber SME, execute and monitor COATS-supported MSELs • Report technical issues to the COATS technician	Should be a trained, trusted agent from the supported command	Anywhere on operational network
ACE-IOS Operator	• As requested by the Cyber SME, execute and monitor COATS-supported MSELs • Report technical issues to the COATS technician	Must be an ACE-IOS SME; could be an additional duty for an existing position	Simulation center (e.g., KASC)

RECOMMENDATIONS

The following recommendations are provided to assist current and future COATS sponsors, capability developers, users and maintainers with the successful development and employment of COATS and related capabilities.

Doctrine / Leadership / Policy

Joint Commanders must understand and direct their staffs to respond to existing SECDEF and CJCS requirements and guidance for incorporating realistic cyberspace conditions into exercises. "Military campaign plans must fully incorporate the ability to operate in a degraded cyber environment; military forces must exercise and be able to conduct military campaigns in a degraded cyber environment where access to networks and data is uncertain." (Carter 2015) "Without realistic cyber effects, the training audience may have a false sense of security that their missions were not subject to degradation, and the operators and network defenders miss the opportunity to detect and respond to realistic cyber attacks" (Gilmore, 2015).

Leaders must understand and accept the risks associated with degraded/denied cyberspace conditions in exercises and encourage their peers and subordinates to incrementally improve the quality and quantity of cyber play. Accordingly, organizations should not be criticized for negative performance impacts as a result of conducting operations in a contested training environment. The SECDEF provides this guidance on the topic:

"During the Cold War, forces prepared to operate in an environment where access to communications could be interrupted by the adversary's advanced capabilities, to include the potential use of an electromagnetic pulse that could disrupt satellite and other global communications capabilities. Commanders conducted periodic exercises that required their teams to operate without access to communications systems. Through years of practice and exercise, a culture of resilience took root in the military and units were ready and prepared to operate in contested environments.

Since the end of the Cold War, however, a younger generation has grown increasingly more accustomed to an environment of connectivity. The generation of military men and women that grew up since the end of the Cold War have had near constant access to information and communications, and the information revolution has led to a more agile and globally adaptive force. In the face of an escalating cyber threat, the lessons of the previous generations must now be passed down. The Defense Department must be able to carry out its missions to defend the country. Organizations must exercise and learn to operate without the tools that have become such a vital part of their daily lives and operations." (Carter 2015)

Training

Exercise program strategies, plans and products must be updated to increase the quality and quantity of cyber play in accordance with an organization's concept and operational plans. Examples include exercise concepts, training objectives, scenarios, MSELs, exercise control group organization and procedures, and after action review/lessons learned procedures. An incremental approach is recommended to increase the leaders' and the staff's level of familiarity and comfort with any new technologies, processes and procedures. Consider conducting a small-scale table-top exercise or similar construct to practice key process and procedure changes prior to implementation.

Material

Additional material research, development, test and evaluation is necessary to expand and mature the current COATS technologies to better address the required mission areas and improve the level of interaction, resolution, and command and control of the integrated training environment as follows:

- Cyber Effects Resolution – The ability for cyber sensors, models and effects to interact with specific applications, services, ports and protocols.
- Virtual Network Generation – The ability to rapidly scan, generate, correlate and share network, system, and application deployment and configuration data between cyber ranges, traditional simulation architectures, and cyber emulators.
- Network Defender Training – The ability for network defenders to protect, detect, react and restore network operations based on feedback from and interaction with COATS sensors, models and effects.
- Threat Networks – The ability for COATS sensors, models and effects to realistically represent and degrade opposing force systems and networks.

- Cyber Range Command and Control – The ability to integrate and synchronize the management of cyber range environments with traditional simulation architectures (e.g., start/stop/pause/resume, checkpoint/restore, database synchronization, etc.).
- Cyber DEM – The ability to support additional missions sets (e.g., IAMD) and to be easily applied to existing DoD M&S standards.

SUMMARY

This paper introduced the COATS architecture and how it can be used to meet SECDEF and CJCS requirements for incorporating realistic cyberspace conditions into battlestaff training and exercises. The paper also discusses lessons learned from the employment of COATS during three USFK exercises and recommendations for future development and employment. Ideally COATS would be combined with other types of cyber training solutions (e.g., scenario injects and red teams) to provide a multi-resolution approach to integrated cyber training such as we see with the combination of LVC technologies used for traditional military operations training. It will take time for leaders and their staffs to become familiar and comfortable with cyber training capabilities such as COATS and it will take time for exercise programs to fully integrate cyber training objectives, processes and procedures into their existing products. COATS offers a near-term, verified method to synchronize and deliver realistic cyber effects to the entire battlestaff – cyber for all.

ACKNOWLEDGEMENTS

USPACOM would like to thank the following COATS sponsors, performers, and supporters for their dedication and expertise:

- Office of the Undersecretary of Defense, Acquisition, Technology and Logistics – Dr. Steven King and staff
- M&SCO – Mr. Jesse Citizen and staff
- The Office of the Director, Operational Test and Evaluation
- Joint Staff J7
- USFK KBSC, Joint Cyber Center, J635
- 7 AF KASC, A3, A6, 607 Air and Space Operations Center
- USAF 90th IOS
- USAF 453 Electronic Warfare Squadron
- Naval Air Warfare Center Training Systems Division
- Johns Hopkins University Applied Physics Laboratory

REFERENCES

Carter, A. (2015). The DoD Cyber Strategy. Page 17.
Gilmore, M. (2015). Director, Operational Test and Evaluation FY 2014 Annual Report. Page 331.
Goldfein, D., (2014). CJCSI 3500.01H Joint Training Policy for the Armed Forces of the United States. Page D-7.
Morse, K., & Drake, D., & Wells, D., & Bryan, D. (2014). Realizing the Cyber Operational Architecture Training System (COATS) Through Standards. 2014 Fall Simulation Interoperability Workshop. Page 7.