BULLETIN

NO. 14-06

MAY-14

Brigade Combat Team Cybersecurity Operations:

Trends, Lessons Learned, and Tactics, Techniques, and Procedures
Cyber Bulletin No. 1

Lessons and Best Practices

Handling Instructions for CALL
Electronic Media and Paper Products

Center for Army Lessons Learned (CALL) authorizes official use of this CALL product for operational and institutional purposes that contribute to the overall success of U.S. government efforts.

The information contained in this product is provided for informational purposes only and is not necessarily approved U.S. Army policy or doctrine.

This product is designated for official use by U.S. government personnel and their approved contractors. It cannot be released to allies, coalition partners, or the public without the consent of CALL. This product has been furnished with the expressed understanding that it will be used for official defense-related purposes only and that it will be afforded the same degree of protection that the U.S. affords information marked "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" in accordance with U.S. Army Regulations 380-5, section 5-2. Official military personnel, civil service/government personnel, and approved contractors of the United States may paraphrase; quote; or use sentences, phrases, and paragraphs for integration into official U.S. government products or research.

However, integration of CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" information into official products or research renders them FOUO, and they must be maintained and controlled within official channels or approved contractor facilities and cannot be released to allies, coalition partners, or the public without the consent of CALL.

CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" documents may be placed on protected UNCLASSIFIED intranets within military organizations or units, provided that access is restricted through user ID and password or other authentication means to ensure that only properly accredited military, government officials, and approved contractors have access to CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" materials.

Regulations strictly forbid posting CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" documents to Army Knowledge Online or other Department of Defense (DOD) websites that do not restrict access to authorized personnel. AR-25-1, 15 Jul 2005, Army Knowledge Management and Information Technology, paragraph 6-4 n (2) (b) and DOD Web Site Administration Policy and Procedures (11 Jan 2002), Part II, paragraph 3.6.1 require appropriate mechanisms to protect sensitive information. DOD 5400.7-R, DOD Freedom of Information Act Program, September 1998, provides guidance on the release, safeguard, and unauthorized disclosure of FOUO information.

Appropriate disciplinary action may be taken against those responsible for the unauthorized release of FOUO information. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against those responsible for the release; in addition unauthorized releases by contractor personnel to unauthorized persons may warrant action relative to the contractor under the Federal Acquisition Regulation (FAR).

When no longer needed, all CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" paper products and electronic media will be shredded or destroyed using approved paper shredders or CDROM destroyers.

CENTER FOR ARMY LESSONS LEARNED

SUPPORTING THE WARFIGHTER

Brigade Combat Team Cybersecurity Operations: Trends, Lessons Learned, and Tactics, Techniques, and Procedures

Cyber Bulletin No. 1

This page intentionally left blank.

Foreword

This bulletin is the first in a series aimed at identifying and disseminating key lessons learned associated with integrating cyberspace operations and cyber electromagnetic activities (CEMA) into the Army organizational culture, operations, and procedures. Each bulletin will focus on observed trends; tactics, techniques, and procedures (TTP); and best practices Army units should leverage regarding cyberspace operations as part of unified land operations. These lessons are focused on ensuring that commanders and their units are prepared and proficient to dominate in the modern operational environment.

The lessons units have learned, while conducting training rotations, provide incredible insight into how commanders and their units can best perform at these training centers. Evaluators and operational forces at the training centers have incorporated the requirements of cyberspace operations into their expectations of unit proficiency.

To achieve dominance of cyberspace, protecting friendly networks, systems, and data is paramount. Identifying and implementing cyberspace lessons learned into TTP, doctrine, and materiel development cycles is foundational to the Army's success in the modern five-domain environment in which it will operate. Identifying and disseminating the lessons quickly to the operational force will be a key factor to success during doctrine development cycles, which will result from the rapid advancement of technology and threat-based vulnerabilities.

This page intentionally left blank.

Brigade Combat Team Cybersecurity Operations: Lessons Learned and Tactics, Techniques, and Procedures

Table of Contents

This page intentionally left blank.

Introduction

This edition of the Cyberspace Lessons Learned Bulletin focuses on cybersecurity (formerly called information assurance [IA]) lessons learned resulting from trends observed at training centers. Awareness of these lessons will aid commanders with integrating cybersecurity holistically into their units' daily operations and culture. It is published in two versions: one version at the unclassified, For Official Use Only (FOUO) level, and another version at the classified level, along with additional information, to also include a threat update and Joint Publication 3-12, which can be found at http://call.army.smil.mil.

The lessons learned presented in this bulletin generally relate to the planning, integration, coordination, and assessment of the employment of cybersecurity in unit operations. The lessons and tactics, techniques, and procedures (TTP) pertain to operational incorporation of cybersecurity, cyberspace rules of engagement, social media policy, and reporting procedures. Also highlighted are trends and lessons regarding computer network defense application of updates and patches. The bulletin concludes with two informative papers that focus on insider threats and social media concerns.

Implementation of the TTP identified in this bulletin will assist brigade combat team commanders with ensuring that comprehensive cybersecurity practices are in place within their units. Diligent application of cybersecurity will result in more hardened, survivable networks, thereby facilitating enhanced mission accomplishment.

Note: The terminology IA has recently been changed to cybersecurity. However, some use of IA persists, particularly in reference to proper names, programs, and positions. In these instances, the reader should be conscious of this terminology change. Over time, the legacy use of IA will need to be updated.

This page intentionally left blank.

Background

Armies have historically defined themselves geographically wherein the control of physical terrain has measured success. Cyberspace transcends geography and conventional borders. The majority of modern land operations will occur in areas with access to multiple levels of technology, involving populations with varying degrees of technological sophistication. Cyberspace provides America's competitors and enemies with an asymmetric, multi-dimensional aim point to strike at the core of a previously uncontested advantage in time and space across the full range of military operations.

Commanders, Soldiers, and systems must remain connected to the people, applications, services, and data that they need to accomplish their mission from anywhere in the world. Employing sound cybersecurity practices is the key to maintaining this connectivity and is attained through the application of enforceable standards, specifications, and common tactics, techniques, and procedures that are developed, in part, through studying lessons learned. The ability to protect the network through diligent cybersecurity practices is paramount to successful Army operations, enabling the operations process to effectively integrate all elements of combat power across all domains — land, air, sea, space, and cyberspace — that govern modern military actions.

Doctrinal Context

Doctrine regarding the cyberspace domain has been in development for some time. The integration and synchronization of cyberspace operations is codified in Joint Publication 3-12, *Joint Cyberspace Operations*; Army Doctrine Publication (ADP) 3-0, *Unified Land Operations*; and ADP 6-0, *Mission Command*. It is covered extensively as a holistic aspect of Field Manual 3-38, *Cyber Electromagnetic Activities (CEMA)*.

The Commander's Role in Cyberspace

Commanders are critically important to the successful conduct of cybersecurity. Command emphasis on comprehensive application of all aspects of cybersecurity will enhance unit capabilities and performance by protecting friendly networks, systems, and data. Cybersecurity also nests into other operational aspects and is paramount to the integration of CEMA into combined arms operations to seize, retain, and exploit an advantage over adversaries in the natural domains, cyberspace, and the electromagnetic spectrum, thereby facilitating overall mission success.

This page intentionally left blank.

Threat Update

Cyberspace threats are real, sophisticated, growing, and evolving. The Army must anticipate disruption attempts, plan for an adversary's potential ability to destroy friendly networks, and account for the impacts of social networks on Army operations. Our adversaries realize that if they cannot compete with our capabilities within the land, air, sea, and space domains, their efforts in the cyberspace domain could undermine our ability to operate freely to train, organize, and equip to attain the complete advantage. Adversaries are developing capabilities to use the cyberspace domain to their advantage, including capabilities to perform offensive and defensive cyberspace operations.

The full current threat update is available in the classified publication of this bulletin, located at http://call.army.smil.mil.

This page intentionally left blank.

Trends and Observations

The lessons learned and tactics, techniques, and procedures (TTP) in this bulletin stem from observed exercise trends at the Combat Training Centers (CTCs) and the Network Integration Exercise. The full briefings are available from the links provided in the *References* section of this bulletin.

The trends indicate that cybersecurity operations have not yet been holistically integrated into brigade combat team operations, culture, and commonplace situational awareness. They indicate that units lack fully-adequate levels of cybersecurity procedures and reporting requirements. Structured reporting procedures generally have not been fully incorporated into unit standing operating procedure (SOP) or practiced adequately through realistic training. The trends show that cyber electromagnetic activity (CEMA) staff elements and working groups, as enablers of cybersecurity into combined arms operations, remain to be integrated within the operations process.

Sample Observation

Employment of the full range of cybersecurity capabilities in unit operations: *The brigade combat team staff was not trained on the integration of cybersecurity into their operations. Their ability to integrate cybersecurity and cyberspace operations improved after remedial training and additional guidance by the brigade combat team commander on what he wanted from the staff.*

Not all the trends were negative. Some trends have indicated that units are making positive progress toward incorporating concerns of cybersecurity into their operations.

Positive Trends

- Some units have implemented Incident Response Plans and generally did follow them.
- Security updates were generally applied to computing systems.
- Units focused on defense of servers against remote access through password protection.
- Network server configurations were adequately “locked down,” in most cases.
- S-6 officers generally reacted appropriately to reports of suspicious emails, once reported.
- S-6 officers were successful at protecting their exchange servers, in most cases.

Needs-Improvement Trends

Many of the exercise trends have indicated areas where improvement is still needed. While these shortfall areas may not have been observed in all units, analysis of the exercise trends has identified the following five categories of concern, which are listed with their associated trends, along with examples of correlating, specific observations.

Cybersecurity Procedures

Trends indicate that cybersecurity practices and procedures were not being followed. In some cases, users opened emails from untrusted sources, suspicious attachments, and phishing attempts. In other cases, phishing email and suspicious activity were identified but not reported due to a lack of awareness and established reporting procedures.

Phishing attacks were the primary means by which cyberspace adversaries were able to penetrate and exploit the rotational training unit's network. The article "*Tactical Cyber Threats*" by Rick San Miguel in this bulletin discusses how users, who recklessly open suspicious emails, can cause extensive negative impact to friendly networks.

Sample Observation

Phishing attempt: *The brigade combat team experienced a cyber attack from a phishing attempt. The battalion S-1 was the first to identify the attack via an email and immediately contacted the battalion S-6. The battle captain was informed, and announced the attack in the tactical operations center (TOC). The TOC notified all units of the phishing attack and directed the units not to open the email. The brigade combat team succeeded in informing the TOC and issued directions to subordinate units to mitigate the impacts of the attack.*

Untrusted transportable media was not always scanned for viruses prior to placing the media into unit computer systems, leaving them at risk for acquiring a malicious code.

Some units were not performing regular vulnerability assessments, application of quarterly computing system updates, Security Technical Implementation Guides (STIGs), Information Assurance Vulnerability Alerts (IAVA), patches, or best business practices.

Sample Observation

Cybersecurity procedures: *Rotational training units fail to consistently implement STIGs, IAVA, updates, patches, and best business practices across their entire network. In many cases, their systems are not current or hardened. Typically, the trends have indicated a lack of authentication to SharePoint, unit portals not being enabled, or unrestricted access. Trends have also indicated that units lack compliance with cybersecurity procedures and processes to ensure their networks are protected. Generally, firewalls have not been properly configured, including port filtering, router access control lists, and default/password manager passwords. These conditions create a portal for the enemy to conduct cyber attacks and exploit friendly networks.*

Password techniques and strong password requirements were inadequate in some cases. Standardized and generic user passwords were in use in some units, leaving these systems vulnerable to unauthorized access. The requirement for users to authenticate when accessing SharePoint and unit data portals was not enabled by some units, leaving their internal data systems vulnerable to intrusion.

Units did not universally include the considerations of social media in their cybersecurity plans and SOPs. Inappropriate use of personal devices can easily lead to operational security (OPSEC) breaches and mission compromise.

Sample Observation

Social media OPSEC compromise: *During the first 24 hours of operations, an individual posted his location (from a photograph) and status on Facebook. Some photographs taken with smartphones provide 10-digit grids. The individual's Facebook post provided the enemy with his location and his unit's forward area refueling point, which compromised the unit. Access to social media was not controlled during deployment and led to compromising the unit's safety.*

Incident Response and Reporting

Individuals were generally unaware of how to respond to a cyberspace threat or incident, such as suspicious emails, attached files, or an introduction by unscanned media.

Sample Observation

Cybersecurity reporting: *A compact disk with malware was distributed throughout the brigade combat team. The unit employed cybersecurity procedures through virus disk scanning to detect the infected disk. There was no indication of a virus being employed from within the unit. The unit followed its communication security/cybersecurity SOP, preventing the spread of a computer virus. However, the unit did not report this incident to the division.*

Education was lacking on which threats and indicators users should watch for, and on reporting procedures once a threat was noted. Users must report suspected wrongdoing and anything out of the ordinary. Individuals were generally unaware of the requirements for reporting cyberspace threats or incidents, such as the format for reporting and to whom to report to. In some cases, units responded effectively to cyberspace threats, but failed to report the incidents, which could have been disseminated for awareness.

Sample Observation

Communications security (COMSEC) reporting: *COMSEC compromise procedures and reporting were not followed. A vehicle with radio was taken during the first 24 hours of the operation. Once reported, the unit had to get the S-6 to ensure certain questions were answered to identify the extent of the compromise (e.g., whether the radio had been zeroized, what frequency load/nets were in the radio). Reporting was slow in developing due to a lack of understanding on what questions to ask. The unit had COMSEC compromise procedures in place, but the operations cell did not ask comprehensive questions to adequately determine the extent of the compromise in order for them decide on the appropriate actions to take.*

Systems Monitoring

Units generally lacked awareness of adversarial cyber presence and activity within their networks due to inadequate emphasis on monitoring procedures, regular review of server logs to detect anomalies, and comprehensive Active Directory management.

Units typically did not fully understand how to use network and system performance tools for enterprise services and network operations (NETOPS), which are used to monitor networks for intrusion signatures.

Sample Observation

Cyber intrusion detection and reporting: *The CTC cyber section was able to access a unit's network through an adjacent unit. When it tried to access the brigade combat team network, the unit stopped it. The NETOPS section was able to detect and block cyber intrusions, but did not report the incident to the division. This enabled the enemy to continue its intrusion operations through the adjacent units.*

Sample Observation

Policies and procedures for computer network defense (CND): *Rotational training units have generally been unprepared to conduct CND. Personnel have not been trained, CND deployment has been inconsistent, and CND tools (i.e., host-based security system) have not been used. Units have been unable to see themselves within the cyber domain, and have been unable to monitor/identify whether their networks are being scanned or attacked. Units' peripheral and network devices (printers, network storage, and servers) have also been unsecure due to standardized/generic user passwords.*

Systems Configuration and Management

Units did not consistently implement STIGS, IAVAs, updates, and patches across their entire networks. Units were not following procedures to secure and maintain virtual information systems and were not always required to authenticate to access their TOC network. Units are not ensuring least-privilege access by duty responsibility. Compartmentalization of access to information through user profile management was not followed by some units. Units systems contained outdated users.

Firewalls were not properly configured in some cases (port filtering, router access control lists, and default passwords). Incomplete system configuration management led to default security settings remaining on some systems. Units are not consistent changing default passwords for their network equipment. Some peripheral and network devices (printers and network storage) were consequently vulnerable to cyberspace adversaries entry into friendly networks. This trend also inhibits the effective application of defensive cyberspace operations and internal defensive measures to protect friendly networks, systems, and data through effective cyber defense planning.

Cybersecurity Planning and its Integration into Operations

The Cybersecurity Plan incorporates cybersecurity with OPSEC, physical security, and COMSEC within the context of CEMA. The Cybersecurity Plan is a key aspect for integrating cyber domain considerations into combined arms operations through CEMA and associated doctrine. This integration will enhance the overall operational effectiveness of combined arms units through a mutually-supporting focus and through common mitigation of threat factors.

CEMA doctrine calls for the establishment of integrating boards and cells within the operations development process. The trends indicate that units lack a full understanding and implementation of CEMA doctrine in the use of CEMA staff elements and working groups as integrators of combined arms. Rotational training units are not universally implementing these boards and cells. Consequently, analysis of the scope and impact of cyber threats did not always result in adequate consideration of cybersecurity matters, cyber defense planning in operations orders, or consistent integration into combined arms operations.

Sample Observation

Lead the CEMA working group: *The brigade combat team did not conduct a formal CEMA working group. The unit combined numerous working groups into the targeting working group, since the key individuals were the same. The unit conducted informal CEMA huddles between the S-2, S-3, and S-6 as key injects prompted coordination of CEMA enablers and cybersecurity, electronic warfare, cyber, lethal/nonlethal working groups, which were consolidated into one group.*

Sample Observation

Cyberspace rules of engagement: *Cyber rules of engagement were not developed to guide units on their left and right boundaries for the conduct of cyber activities. This factor directly affected the CEMA element's ability to properly plan, deconflict, and execute CEMA-related tasks. However, after additional training was provided, the brigade combat team staff planned for cyber targets that met the commander's intent. Additionally, the inclusion of operational cyberspace rules of engagement was needed.*

Sample Observation

Prioritize CEMA effects and targets. *The CEMA element had cyber as a weapons system in the targeting synchronization matrix/high priority target list. The brigade combat team's target decision board was often unsynchronized and did not achieve the brigade combat team commander's intent to enable well-informed targeting decisions. Staff performance improved during the exercises, leading to informed strike decisions by the brigade combat team commander and a Cyber Effects Request Format submission.*

This page intentionally left blank.

Lessons Learned and Tactics, Techniques, and Procedures

This section summarizes the lessons learned and tactics, techniques, and procedures (TTP) that address training center trends. The TTP have training in common, either as the focus of a TTP itself, or by training as a key means by which to implement TTP. Therefore, this section begins with a discussion of a key overarching TTP that has been developed to integrate cybersecurity training. This is followed by sections correlating with their respective trends sections. These numbered sections briefly recap the lessons learned, then focus on presenting practical and concise TTP in tabular format, with the intent of informing brigade combat team commanders on methods to overcome the trending challenges other units have faced. Generally, the TTP focus on training, technical requirements, policies, and procedures commanders can implement, while preparing for rotations at institutional training centers, and, ultimately, for optimal unit performance during combined arms operations.

TTP Cybersecurity Training

Cybersecurity training is an overarching TTP through which all of the trends can generally be addressed. Comprehensive unit cybersecurity training, including collective and individual tasks, contribute to all of the TTP in this bulletin. The Combat Training Center has developed the Unit Training Plan (a link to the plan is provided in the *Resources* section of this bulletin), which is shown in Table 1. It provides commanders with a training plan and effective training framework to help prepare their units. The plan is founded on key factors of the *Army Training Strategy* (Oct 2012), and outlines the cybersecurity functions units are expected to perform during training rotations. The training plan references specific collective tasks, individual tasks, and resources, providing commanders with a focus on how to train their units so they can become competent in cybersecurity. Additional information is available in the *Resources* section of this bulletin.

Successful cybersecurity integration requires cyber training and education to include the following:

- Increased awareness of cyber threats at all echelons and their effects on the brigade combat team.
- Identification of poor information system configuration management, vulnerability management, and cybersecurity shortfalls.
- Recognizing and responding to cybersecurity incidents.
- Exercising incident handling procedures and information system security readiness.
- Development of leadership in the cyber domain across all warfighting functions.

Awareness of the possibility of insider threats must also be considered. The article "*Internal Threats Lessons Learned*," by Russell A. Fenton, found in this bulletin, discusses the threat TTP commanders can use to counter cyber threats.

270-180 Days Out

- Conduct unit Information Awareness (IA) Self Assessment, focus on critical and failing deficiencies. https://iatraining.us.army.mil

  1: Incident handling.
  2: IA training and certification.
  3: Information Assurance Vulnerability Management (IAVM).
  4: IA program management.
  5: Public key infrastructure (PKI).
  6: Certification and accreditation.
  7: IT contingency planning.
  8: Wireless security.
  9: Portable electronic device (PED).
  10: Army web risk content management.
  11: Personal identifiable information (PII) protection.
  12: Minimum IA technical requirements.
  13: Classified systems management.
  14: Leadership IA assessment.

- Develop/implement a plan of action and milestones (POAM).

- Correct deficiencies.

180-90 Days Out

- Conduct a 1st Information Operations (IO) Staff Assisted Visit (Blue Team).

- Conduct a 1st IO Vulnerability Assessment (Red Team)(incorporate into mission command Systems Integration Training Event 3).

90-60 Days Out

- Conduct academic cyber threat/capabilities brief (ARCYBER). http://arcyber.army.smil.mil (company and above leadership)

Table 1. CTC Unit Training Plan

Cybersecurity Procedures

"We must change our culture, enforce compliance, and ensure that people are accountable for proper security procedures…Beyond required security training, we need you to make certain that all of your Soldiers, civilians, and contractors understand the threat they pose to operational security by not complying with (cybersecurity) policies and practices."

— Hon. John McHugh, Secretary of the Army

Units have not fully implemented and enforced the Army IA (cybersecurity) program in accordance with Army Regulation 25-2, *Information Assurance*. These shortfalls have resulted in unnecessary and avoidable operational security compromise.

To help enforce compliance with cybersecurity, the Army Chief Information Officer (CIO)/G-6 serves as the proponent for the governance process for Army cybersecurity risk management. In this capacity, the Army CIO/G-6 published the *Leader's Information Assurance/Cybersecurity Handbook* in June 2013. It provides leaders with the information and tools to address today's complex cybersecurity challenges. It contains best practices and tasks for managing these issues, which will help commanders ensure all personnel know their responsibilities and that these requirements and practices are understood, implemented, and enforced. Cybersecurity must be integrated into the cultural roots of units and must become naturally integrated into all Army operations, missions, and functions. Commanders must make certain their units adopt and institute the practices necessary to ensure the protection of information and personnel.

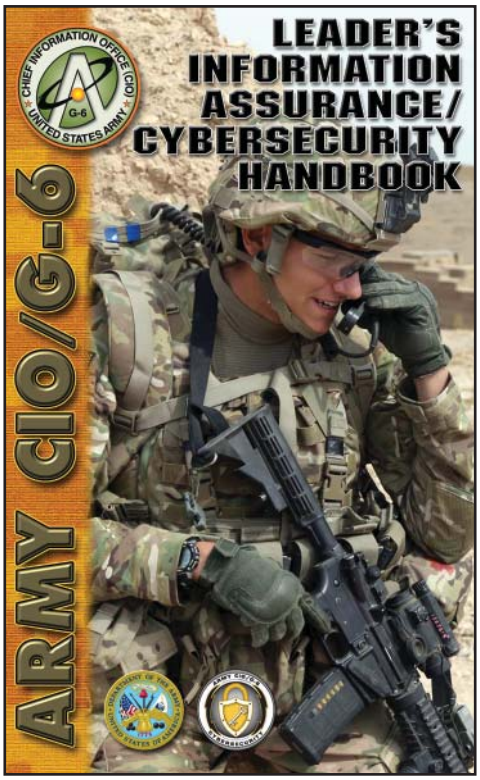

Figure 1. ***Leader's Information Assurance/Cybersecurity Handbook***

Key TTP from the handbook are summarized in Table 2. These TTP will aid the commander in instituting cybersecurity imperatives, empower the unit cybersecurity team, train unit personnel, and ensure adequate unit cybersecurity posture. A link to the *Leader's Information Assurance/ Cybersecurity Handbook* can be found in the *References* section of this bulletin.

TTP: Incorporate cybersecurity into the risk management process.

TTP: Treat cybersecurity like safety.

TTP: Link cybersecurity to readiness.

TTP: Form and empower a unit cybersecurity team that manages the unit program:

- G-6/S-6: Responsible for managing the commander's cybersecurity program .
- IA program Manager (IAPM): Senior cybersecurity advisor to the commander.
- IA Manager (IAM): Implements the program with assistance from the IASOs.
- IA Support Officer (IASO): Provides oversight, guidance, and support .

TTP: Constantly assess unit cybersecurity posture and program with regard to readiness, risk, resources, and reporting.

TTP: Use the IA Self Assessment Tool located at https://iatraining.us.army.mil to evaluate and address any weaknesses identified.

Table 2. *Leader's IA/Cybersecurity Handbook* TTP

Of particular concern is ensuring that users do not open emails from untrusted sources, suspicious attachments, and phishing attempts. These phishing attacks were the primary means by which cyberspace adversaries were able to penetrate and exploit the rotational training unit's network. The article "*Tactical Cyber Threats*" by Rick San Miguel in this bulletin discusses how users, who recklessly open suspicious emails, can cause extensive impact to friendly networks.

The key TTP and trends for commanders to address with cybersecurity in their units are summarized in Table 3. Applying these TTP, along with the practices prescribed in the Army CIO/G-6, *Leader's Information Assurance/Cybersecurity Handbook* will ensure units succeed in these aspects of Defense Cyber Operations (DCO), both in exercises and operationally.

TTP: Unit data portals, such as SharePoint, must employ authenticated access and must be actively monitored for unauthorized access.

TTP: Units must enforce strong password requirements for all individual and system authentication.

TTP: Units must ensure all transportable media is always scanned for viruses prior to placing the media into their computer systems. Commanders should address this through local policy, enforcement, training, and should ensure this procedure becomes a normal part of everyday business throughout their units.

TTP: Commanders must ensure regular vulnerability assessments and application of computing system updates.

TTP: Units should employ cyber reporting procedures into standard operating procedures (SOPs) in order to mitigate cyber attack impacts. Units should establish SOPs and checklists to ensure the unit is in compliance with IA policies. IA procedures as well as network battle drills should be integrated into operations. These procedures must be exercised regularly because prevailing observations have indicated that education of threats and reporting procedures within the tactical environment needed improvement. All users must realize the importance of reporting suspected unusual activity on the network, and should be familiar with proper reporting procedures.

Table 3. Key DCO IA/Cybersecurity TTP

Incident Response Reporting

There is a need for additional emphasis on awareness of cyberspace threat indicators and immediate response measures. The unit training program in Table 1 details the resources required to accomplish these requirements, such as self assessment tools, assistance visits, and training guidelines. The importance of reporting all suspected cyberspace threats should be formalized by local policy, and practiced and reinforced by realistic training.

Brigade combat teams should have reporting procedures in place for communications security (COMSEC) and cyber incidents. These could take the form of a cyber meaconing, interference, jamming, and intrusion reports. Units should incorporate COMSEC compromise plans into their operations and understand the critical questions that must be answered in order to determine what actions are required to mitigate the incident.

Units should also incorporate cyber reporting procedures into SOPs and battle drills and ensure that all leaders understand the importance of reporting cyber incidents in order to mitigate the impact of cyber attacks. Prevailing observations indicate that education of threats and reporting procedures within the tactical environment needed improvement, therefore, procedures must be exercised regularly. All users must realize the importance of reporting suspected unusual activity on the network and should be familiar with the proper reporting procedures.

The 25th AD has successfully implemented the following Cyber Nine Line incident report from its numerous rotations in support of the Network Integration Evaluation, detailed in Table 4; It serves as an example TTP model.

TTP: Commanders should implement standardized reporting within their units and enforce its use to report all suspected incidents. Unit SOP should also detail the procedures by which cyber incident reports are received, consolidated, assessed, acted-upon, and disseminated for situational awareness. 25th AD Cyber Nine Line Report: 1. Location/Node. 2. Date/time/group of event. 3. Attacked system name/Internet Protocol (IP) address. 4. Attacker system name/IP address. 5. Traffic direction (attacker to attacked/attacked to attacker). 6. Type of event (signature description, user description of events). 7. Number of systems affected. 8. Action taken (reported, system removed from the network, etc.). 9. Identification method (user, log management, Host Based Security System [HBSS], etc.).

Table 4. 25th AD Cyber Nine Line Report

Systems Monitoring

Units are having difficulty with developing capabilities to detect adversarial activity within friendly networks. Commanders can ensure their networks and systems are monitored for intrusion signatures through application of system performance tools and monitored for abnormal activity. The cybersecurity team should be trained, empowered through policy and SOPs, and resourced with the tools and time to conduct routine and thorough network monitoring. These TTP are summarized in Table 5.

TTP: Emplace and enforce local policy and monitoring procedures, regular review of server logs to detect anomalies, and comprehensive Active Directory management. **TTP**: Ensure the unit cybersecurity team is proficient with network and system performance tools for enterprise services and network operations in order to monitor their networks for intrusion signatures. **TTP**: Ensure the unit cybersecurity team is resourced with the time and authority to perform adequate system monitoring.

Table 5. System Monitoring TTP

Systems Configuration and Management

Units' networks, systems, and data are vulnerable due to incomplete systems configuration, and non-comprehensive access management policy/procedures to adequately protect access to data. Table 6 summarizes the key TTP commanders can use to ensure these vulnerabilities are addressed.

TTP: Emplace policy and procedures to ensure Security Technical Implementation Guides (STIGS) and Information Assurance Vulnerability Alerts (IAVAs) are applied on time to all devices and require commander's status reporting to ensure compliance.

TTP: Ensure procedures for securing and maintaining virtual information systems are followed and checked, including managing personnel access to systems and data:

- Require password authentication for access to all internal data management utilities.
- Compartmentalize access to information through user profile management and least-privilege access, as determined by duty responsibility.
- Integrate profile management into outprocessing procedures to ensure the profiles of old users are removed promptly.

TTP: Ensure the proper configuration of firewall port filtering and router access control lists.

TTP: Ensure default security settings and passwords are removed or changed in all computing devices, including peripheral equipment.

Table 6. Systems Configuration and Management TTP

Cybersecurity Planning and its Integration into Operations

The Cybersecurity Plan is a key aspect to integrating cyber domain considerations into combined arms operations through cyber electromagnetic activities (CEMA) and associated doctrine. This integration will enhance the overall operational effectiveness of combined arms units through a mutually-supporting focus and common mitigation of threat factors. Units have not fully established the use of CEMA staff elements and working groups as integrators of combined arms. Table 7 details key TTP as a guide for commanders for implementing this integration of cybersecurity planning in their operations.

TTP: Develop a cyber defense plan that meets tenets of IA, operational security, physical security, cybersecurity, and CEMA, which support the achievements of organizational objectives in the land and cyber (Land/Cyber) warfighting domains within authorities, regulations, policies, and procedures:

- Review applicable documents, regulations, and policies.
- Analyze current/future cyber threat intelligence and capabilities.
- Analyze organization cybersecurity plans and assess current posture.
- Identify gaps between current policies and procedures, current posture, and DCO requirements.
- Develop methods, instructions, guidance, and SOPs to mitigate defined cybersecurity gaps and counter cyberspace threats to include:
    - Identification of cyberspace mission systems and classification of cyberspace key terrain.
    - Analysis and mitigation of vulnerability assessments.
    - Threat assessment analysis and dissemination plans.
    - Defense prioritization based on CKT and mission assurance.
    - Cyber reconnaissance plan.
    - Network and systems monitoring plan.
    - Coordinate cyber incident response/incident handling plan.
    - Threat activity recovery plan.

Table 7. Cybersecurity Plan TTP

The Cybersecurity Plan considers the cyberspace threat, and network and information requirements into the operational plan. It's imperative that the plan enables the unit to better monitor its networks, the threat, and the cyber terrain in a holistic and operational view. The plan improves the organization's cyber defense posture by considering the impact of breaches in physical, network, and data security on the operational environment. The plan decreases network vulnerabilities and better prepares the unit to conduct operations in a significant cyber threat environment.

Internal Threats Lessons Learned

Russell A. Fenton
GSNA Telecommunications Specialist
U.S. Army Cyber Center of Excellence
TCM Global Network Enterprise (Cyberspace Cell)

One of the greatest threats for the nation and the U.S. Army today in cyberspace does not stem from nation states, terrorist groups, or criminal organizations, but from the inside. The insider threat is difficult to detect and prevent. Malicious activity by Soldiers, civilians, and contractors with legitimate access to networks, information systems, and data represents a growing problem in our digital world. While many motivational factors can drive an insider to exfiltrate data or conduct an action on the network that denies, disrupts, degrades, or manipulates the availability of network resources, recent high profile cases have consisted of those who are disgruntled or passionately believe their actions are justified for a noble cause. No matter what the motivation, the results stemming from these types of events impact mission assurance, morale, and the mindsets of individuals across the nation and international community. The following scenario is based on a true story and highlights how a lack of commander and leader action can empower an insider threat. Moreover, it draws attention to the fact that information cannot be assured by just implementing technical measures on the network.

John Smith was born in New York in 1993 and moved to Texas with his mother as a young boy when his parents divorced, subsequently settling in a small town located in the panhandle. During his years of middle school and high school, John was a straight "A" student but consistently demonstrated periods of behavioral problems and angry outbursts that solidified his reputation as a troublemaker. Nonetheless, John graduated from high school in 2011, and afterwards, worked a few odd and end jobs. His lack of long-term career prospects in his town convinced him to join the Army. Because of the large signing bonus, John enlisted as a wheeled vehicle mechanic (91B).

While John (now PVT Smith) had no issues during basic training, his history of behavior issues caught up with him in advanced individual training (AIT). He flew into a fit of rage during a confrontation with another Soldier that resulted in Smith striking the Soldier with a wrench, but not causing physical harm. PVT Smith was given a summarized Article 15 with reduction in pay; yet, he was allowed to continue the remaining 10 weeks of AIT without incident. The Article 15 was not included in Smith's records as he left his training unit headed to his assignment at Fort Hood, Texas.

Upon arrival at Fort Hood, PVT Smith was assigned to headquarters and headquarters company, Brigade Special Troops Battalion, 25th Armored Division. For the first six months, Smith seemed to be the model Soldier. He was promoted to private enlisted two during this time and he was making a name for himself as a great mechanic. Moreover, PV2 Smith had been using his off time to become proficient in database applications and spreadsheets. This just happened to come up in discussion between PV2 Smith and his company commander after physical training one morning. Smith brought in his personal laptop one day to show his commander, who was so impressed that he had PV2 Smith moved to the orderly room to assist in developing some personnel and property tracking databases. Not long after his transition to the orderly room, PV2 Smith was promoted to private first class.

Once again, Smith's chronic behavior issues reared their head. Due to the current manning, the unit did not have a sergeant or even a specialist to run the orderly room, so PFC Sarah Johnson was placed in charge. This did not sit well with Smith who did not like taking orders from someone his same rank. PFC Johnson did complain to the platoon sergeant on several occasions, with counseling statements generated each time. During the last counseling session, Smith confided in his platoon sergeant that he had bouts of depression for which he wanted to see a chaplain. Days after, 25th Armored Division received the order to deploy to Afghanistan within 90 days.

During the 90 days, PFC Smith's behavior became more and more erratic. He was increasingly agitated by situations, he was frequently late to formation and work, and the sessions with the chaplain indicated PFC Smith was dealing with several psychological matters. All this led to PFC Smith's platoon sergeant recommending that he not deploy. However, in a unit already dealing with manning issues, every person counted. Besides, even though PFC Smith had behavioral issues, his work in the orderly room was outstanding.

The 25th Armored Division deployed to a base northeast of Kandahar Air Base in 2012. All activities on the network were conducted via the Secure Internet Protocol Router Network and each entity within the brigade special troops battalion was given a specific folder on the shared drive to store information related to the unit and operations. Even though the battalion S-6 had set permissions on the drive in accordance with the unit's knowledge management plan, the battalion executive officer told the S-6 to remove any restrictions because required information was stored across several folders and individuals were having problems accessing it. The executive officer stated, "Individuals needing access could change on the fly, so just open it up." Although the S-6 advised against it, he did what he was told.

It wasn't long afterwards that the S-6 started to discover unauthorized files (movies and music), redundant files, files with personal identifiable information (PII) beyond that which the unit was required to track (e.g., medical information), and basically virtual chaos on the file server. He informed his battalion commander and executive officer of the issue and explained how, in many cases, Army and International Security Assistance Force policies were being violated. He was told to just clean it up. The violations continued to occur, but each time the battalion S-6 informed the commander and executive officer, he was directed to do the same thing — just clean it up.

As the deployment went on, PFC Smith became more disgruntled. He was still answering to PFC Johnson and wanted to move back to the maintenance shop where he could at least take orders from a sergeant. His bouts with depression had not been resolved before the unit deployed, and to add fuel to the fire, PFC Smith began to question the United States' involvement in Afghanistan. He even told some of his fellow Soldiers of his concerns, which were relayed to the platoon sergeant. Yet, these actions were discounted as PFC Smith trying to get his way. These internal struggles culminated in PFC Smith attacking PFC Johnson during the deployment's halfway point. This time, Smith was given a company-grade Article 15 and demoted to PV2. But because he was good at his job in supporting company operations, he was not transferred back to working as a mechanic. Additionally, his clearance was not suspended and network access was not revoked because there was no policy mandating the suspension of network access for those receiving non-judicial punishment. PV2 Smith was placed on duty during the night hours though, in order to limit his interaction with PFC Johnson.

Around this time, the division G-6, located at Kandahar Air Base, was supposed to conduct an inspection of the brigade combat team and brigade special troops battalion's networks. On the date scheduled, the route to the base of the 25th Armored Division was closed due to insurgent activity. Unfortunately, this inspection visit was never rescheduled because of the G-6's tight timetable across the entirety of the division, which needed to be completed within the next three months before preparations for redeployment.

One night while on duty, PV2 Smith convinced the system administrator, who was a buddy of his, to give him privileges to load software on one of the unit's computers, saying he wanted to load a few games and an application to view movies and to listen to music, as well as another application that would be used to better meet the commander and first sergeant's suspenses. This allowed Smith to load a crawling program that he used to search for sensitive data related to U.S. operations in theater, along with PII to be exploited as a means to commit identity theft, especially against those who Smith felt did him wrong. The crawling program worked in the background out of sight from anyone else who might use the system.

When PV2 Smith returned to his next shift, he discovered that the program collected a myriad of files, which he subsequently printed off. Because PV2 Smith basically worked alone, no one noticed the mountains of documents spewing from the printer. Although the security guard at the entrance of the secured facility inquired about Smith's carry bag looking considerably heavier when his shift was over compared to when he came on duty, the guard never checked the bag and Smith brushed it off by saying he had left some books in the office that he wanted to take back to his room and read. Once Smith returned to his containerized housing unit, he sorted through the documents, took pictures of those he found of interest, uploaded the ones that pertained to U.S. operations to a Facebook account under a fake name, and sent others with PII to a contact he found on Craigslist that agreed to pay Smith $20 for each identity that could be harvested. It wasn't long until the postings of classified documents on Facebook made headlines and unit Soldiers were notified via family members back home that fraudulent accounts were being opened in their names. The resulting investigation identified PV2 Smith as the culprit. One could only imagine the effects his actions had on Soldier morale, individual's careers, the unit, the Army, and the nation.

It may be surprising that very little of this scenario has anything to do with technical measures implemented on the network to achieve cybersecurity. Hindsight is always 20/20, but it is obvious Smith had a history that if reviewed in total, should have been used as an indicator of how trustworthy Smith would be around sensitive data. Combined with his diagnosed depression and recent disciplinary action, the justification existed to pull Smith's access to the network. He was only allowed to stay because he was good at his job. Moreover, the battalion commander and executive officer were culpable by not enforcing policy designed to limit access to information based on a need-to-know basis, as well as allowing a lax cybersecurity environment to exist. While the absence of an inspection from higher more than likely would not have resolved the leadership issues, the inspection would have captured enough faults to make higher leadership aware of leadership problems. The use of social engineering by Smith against the system administrator was key in facilitating Smith's efficient discovery of information; and once again, the granting of elevated privileges to an individual who should not have them was a violation of policy likely caused by the laissez-faire attitude to security across the battalion. Lastly, physical security measures could have been used to stop Smith from taking the sensitive information from the facility. However, the guard may not have known the policy and/or was not directed to check all bags entering or leaving the building. In the end, commanders and leaders do not need to be technical experts to play a vital role in defending the confidentiality, integrity, and

availability of information. All that is required is that they do not ignore telltale signs of those who put information at risk; they empower cybersecurity and security professionals to meet or exceed the standard; and in the end, they challenge others to do the same, while ensuring there are repercussions for intentionally violating policy.

Tactical Cyber Threats

Rick San Miguel
Cyber Lessons Learned Coordinator
U.S. Army Cyber Center of Excellence

> *"On today's battlefields, computers play a major role, controlling targeting systems, relaying critical intelligence information, and managing logistics. And, like civilian counterparts, defense computers are susceptible to computer network attacks. Cyber War provides numerous examples. For example, it includes a vivid description of a September 2007 operation, where Israeli cyber warriors reportedly "blinded" Syrian anti-aircraft installations, allowing Israeli planes to bomb a suspected nuclear weapons manufacturing facility (Syrian computers were hacked and reprogrammed to display an empty sky). Analysts across the globe are well aware that any future large-scale conflict will include cyber warfare as part of a combined arms effort."*
>
> — Richard A Clarke, *Cyber War*

Communications equipment (voice or data) systems are designed to encrypt and decrypt transmissions. They use different frequencies and algorithms to communicate, but regardless of the encryption or decryption methods used, the human factor has always been the weakest link. Training is conducted to instruct others on how to identify an insider threat and uses examples of users stealing information and exploiting networks for personal gain. Often overlooked is the user who carelessly disregards regulations and policies, putting his system and networks at risk, forgetting to change default passwords, and opening emails and links that are suspicious. Posting personal information on social media sites such as Facebook, Twitter, and Rally Point makes it easier for an adversary to target individuals by sending emails with malicious attachments or a link to a compromised website.

The key is training, training, training. Training must be enforced and implemented to ensure individuals are aware of regulations, policies, and standing operating procedures (SOPs) so they can assist in mitigating security violations. The cyber threat is real and evolving, and is becoming more sophisticated. It is imperative that we recognize and understand how cyber threats can affect the security of networks and a warfighting commander's ability to send bullets downrange.

The Cyber Center of Excellence (CCoE) Lessons Learned (LL) team visited several units throughout the last quarter during unit umbrella weeks, and at post combat lessons learned and training centers. The traits that each unit had in common was cyber, cybersecurity, and computer network defense violations, which are becoming a common trend throughout the Army. These violations are not caused by equipment or software malfunctions, but by user-initiated faults. The following observations are based on actual collections done by the CCoE LL team.

- Access was gained because users did not apply cybersecurity training (phishing email). Poor cybersecurity practices resulted in rotational training unit systems becoming infected by a Trojan virus from an email attachment. During this attack, more than 950 user names were acquired to assist in phishing campaigns. In addition, further access was allowed to operational documents via the infected website, as well as data exfiltration of all key operational data. The unit did not have a published cybersecurity/network operations SOP.

- The adversary accessed the network by sending phishing emails. Several of the emails were subsequently opened, allowing the enemy to gain access to the systems and network. The web interface of several networked printers was accessed and the names of users were extracted from the printer logs. The enemy was also able to access the Tactical Operations Center Intercommunications System server and monitor and disrupt radio communications because authentication measures were not in place. Access was also gained to a network server and passwords were set to block access, delete, and reconfigure settings. The unit did not have SOPs that provided cybersecurity guidelines and reporting procedures.

- Unit failure to follow Defense Information Systems Agency Security Technical Implementation Guides and Army Best Business Practices when implementing cybersecurity practices allowed the adversary to gain domain administrator privileges to the network. Default passwords, configurations, and failure to enforce and require users to "change password on first login" and choosing the setting "password never expires" gave the adversary access to the network. This allowed access to all the unit's mission command systems. Units are under a misconception that cyber attacks do not stop the warfighter's ability to put bullets downrange; however, the level of access the enemy gained allowed it to affect all logistical and tactical operations, if it so desired.

- The brigade combat team encountered multiple cyber attacks on the network due to the enemy launching calculated phishing attacks on brigade combat team personnel. The attacks targeted specific personnel identified through multiple sources, such as Stars and Stripes, Facebook, and Rally Point. The information gained from these sources gave the enemy enough information to compose an email that unit personnel found interesting. Once this email was opened, the enemy gained another avenue of access to the network. During these attacks, 17 percent of the personnel accessed the phishing email, but only 6 percent reported the incident. The unit did not have a published cybersecurity/network operations SOP.

- On Day One of the training exercise, critical access was gained due to users not applying their cybersecurity awareness training. Access to servers and network equipment was easily gained due to units using common or default passwords. Direct targeting of signal personnel and equipment enabled operations security violations. The unit did not have a published cybersecurity/network operations SOP.

- The cyber opposing force was able to gain access to all critical servers; this permitted free range on roughly 95 percent of the systems on the network. Attack vectors remained available following known network intrusions, allowing opportunities for additional cyber attacks and continued data exfiltration. Roughly 95 percent of the rotational training unit portal was exposed.

The trend on the observations listed is a the lack of cybersecurity awareness training, no SOPs in place to identify or report intrusions, and failure to recognize the threat of cyber warfare. What procedures do we have in place to minimize intrusion efforts? Cyber warfare is real; it is everyone's responsibility to ensure the network is secure. Ultimately, it is up to YOU, the user, to safeguard data, protect security, and implement cyber/security best practices.

For more information, visit the Cyber Center of Excellence Lessons Learned website at https://lwn.army.mil/web/slls/home.

For more information on cyber threats or to share your lessons and best practices, visit https://www.us.army.smil.mil/suite/grouppage/7609.

This page intentionally left blank.

References

Joint Readiness Training Center Cybersecurity Training Briefing

The briefing link below outlines the cyberspace competencies expected at Combat Training Centers (CTCs), identifies trends from their evaluations of units within these areas, and specifies a recommended training plan for units to prepare for CTC rotations. The briefing provides information on the CTC cyber training strategy. It places responsibility for cyber training on the unit commanders and the user community. It presents a successful approach to CTC cyber training, which is divided into two parts: home station training and collective cyber training events conducted at the CTCs. These training evolutions validate the rotational unit's home station training and establishment of systems and processes to operate and defend the network. It emphasizes that home station training should be focused on improving cybersecurity functions that are intertwined with related standards in operations security, communications security, transmission security, and information security. This training should focus on the requirements of Army Regulation 25-2, *Information Assurance*. The briefing also identifies cyber trends from units' experiences at the Joint Readiness Training Center (JRTC), which indicate that the following trends and vulnerabilities existed among rotational training units.

Source: "*JRTC Cybersecurity Training Briefing*," LTC Steven Beamount, JRTC
https://www.jllis.mil/index.cfm?disp=cdrview.cfm&doit=view&cdrid=82379

National Training Center (NTC) Cyber After Action Review (AAR) and Operational Forces (OPFOR) Observations

The briefings linked to below summarize the cyber electromagnetic activities (CEMA) assessments of units and Cyber OPFOR observations during NTC rotations. The Information Operations (IO) Command collected observations and developed trends from rotational training units at the NTC. The briefing provides AAR comments, observations, and areas that need improvement/sustainment from units' rotations at the NTC. It provides some of the challenges units experienced and identified as training requirements. The second briefing discusses recent observations from the Cyber OPFOR at the NTC. Together, these briefings have identified trends, both positive and in areas needing improvement.

Source 1: "*National Training Center (NTC) Cyber After Action Review (AAR) and Trends Briefing*," LTC Hales, IO Command
https://www.jllis.mil/index.cfm?disp=cdrview.cfm&doit=view&cdrid=82392

Source 2: "*Observations from the Cyber OPFOR at the NTC*," MAJ Andrew J. Jaskolski, Instrumentation and Information Systems Operations Group, NTC
https://www.jllis.mil/index.cfm?disp=cdrview.cfm&doit=view&cdrid=82390

Network Integration Evaluation (NIE) CEMA Demonstration Report

The NIE 13.1 report, found at the link below, results from U.S. Army Cyber Command (ARCYBER), Cyber Center of Excellence, and Mission Command Center of Excellence after conducting a CEMA demonstration from 28 October to 16 November 2012 as part of Network Integration Exercise 13.1. The purpose for the CEMA demonstration was to provide an opportunity to test the concept of cyber coordination, integration, and planning at tactical echelons. This provided an opportunity to evaluate CEMA integration within mission command of tactical operations. This CEMA concept accomplished two primary functions: integrate and synchronize cyber electromagnetic capabilities and activities to achieve desired conditions in cyberspace and the electromagnetic spectrum, and to integrate cyber electromagnetic capabilities and activities into combined arms operations.

Source: "*Network Integration Evaluation 13.1 Cyber Electromagnetic Activities (CEMA), 29 Oct-16 Nov 2012*," CW4 Paul Morrow and Mr. Wade Melton, ARCYBER
https://www.jllis.mil/index.cfm?disp=cdrview.cfm&doit=view&cdrid=82380

Army Chief Information Officer/G-6 *"Leader's Information Assurance/Cybersecurity Handbook (2013)"*

This handbook is designed to provide leaders with the information and tools to address today's complex cybersecurity challenges. It is also a quick reference for managing cyber security issues, which will help ensure that all personnel know their responsibilities for the daily practices that will protect information and information technology capabilities.
https://www.jllis.mil/index.cfm?disp=cdrview.cfm&doit=view&cdrid=82388

Template for the Development of a Cyberspace Defense Plan (2013)

STANDARD: Develops an approved cyber defense plan that meets tenets of information assurance, operational security (OPSEC), physical security, cybersecurity, and CEMA, which supports the achievements of organizational objectives in the land and cyber (Land/Cyber) warfighting domains within authorities, regulations, policies, and procedures.
https://www.jllis.mil/index.cfm?disp=cdrview.cfm&doit=view&cdrid=82389

Doctrinal References

Joint Publication (JP) 3-12, *Joint Cyberspace Opertaions*, 5 February 2013, is classified SECRET and only resides on the Secret Internet Protocol Router Network (SIPRNET) Joint Doctrine Education and Training Electronic Information System (JDEIS). It was initiated based on the National Military Strategy for Cyberspace Operations Implementation Plan, which directed U.S. Strategic Command to assess joint doctrine in support of operations in cyberspace and the five National Military Strategy Cyberspace Operations ends. JP 3-12 addresses the uniqueness of military operations in cyberspace, clarifies cyberspace operations-related command and operational interrelationships, and incorporates operational lessons learned. The link to JP-12 can be found in the classified release of this Cyberspace Lessons Learned Bulletin, located at http://call.army.smil.mil.

Army Doctrine Publication (ADP) 3-0, *Unified Land Operations*, emphasizes that cyberspace operations and the commander's situational understanding of cyberspace goes beyond the provision of establishing and maintaining basic network and telecommunications services. The operational and technical functional capabilities of signal, intelligence, electronic warfare, spectrum management operations (SMO), space, and knowledge management, and their effects on the human aspect of conflict and the requirement for a unified effort, all having institutional and far-reaching ramifications across the full spectrum of a commander's operations. ADP 3-0 can be found online at http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adp3_0.pdf.

Field Manual (FM) 3-38, *Cyber Electromagnetic Activities (CEMA)*, presents the integration and synchronization of CEMA as a new concept. The Army codified the concept of CEMA in ADP 3-0 and ADP 6-0, *Mission Command*. The Mission Command warfighting function now includes four primary staff tasks: conduct the operations process (plan, prepare, execute, assess), conduct knowledge management and information management, conduct inform and influence activities, and conduct CEMA. CEMA consist of cyberspace operations, electronic warfare, and SMO. FM 3-38 can be found online at http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf.

Army Regulation (AR) 25-2, *Information Assurance*, provides information assurance policy, mandates, roles, responsibilities, and procedures for implementing the Army Information Assurance Program, consistent with today's technological advancements for achieving acceptable levels of security in engineering, implementation, operation, and maintenance for information systems connecting to, or crossing any U.S. Army managed network. AR 25-2 can be found online at https://armypubs.us.army.mil/epubs/pdf/r25_2.pdf.

The Cyberspace Order of Battle

The following are the U.S. Army organizations that conduct Department of Defense Information Network Operations, Defense Cyber Operations (DCO), and Offensive Cyber Operations (OCO) to support and defend our portion of the cyberspace domain, LandWarNet.

U.S. Army Cyber Command (ARCYBER)

ARCYBER is the Army's operational commander for operating, maintaining, and defending the network.

ARCYBER plans, coordinates, integrates, synchronizes, directs, and conducts network operations and defense of all Army networks; when directed, ARCYBER conducts cyberspace operations in support of unified land operations to ensure U.S./allied freedom of action in cyberspace and works to deny the same to the adversaries.

ARCYBER capitalizes on existing Army cyber resources and improves operational readiness by bringing Army cyber resources under a single command. The Network Enterprise Technology Command/9th Signal Command and 1st Information Operations (IO) Command (Land) are subordinate units to ARCYBER.
http://www.arcyber.army.mil/

The Network Enterprise Technology Command (NETCOM)

The 9th Signal Command (Army), as a major subordinate command to ARCYBER, operates, maintains, and defends the Network Enterprise to enable information superiority and to ensure that forces have freedom of access to the network in all phases of operations.
http://www.army.mil/info/organization/unitsandcommands/commandstructure/netcom/

U.S. Army Intelligence and Security Command (INSCOM)

INSCOM is an Army major command that conducts intelligence, security, and information operations for military commanders and national decision makers. INSCOM/780th Military Intelligence Brigade is under the operational control of ARCYBER to conduct Defensive Cyberspace Operations and Offensive Cyberspace Operations.
http://www.inscom.army.mil/

The 1st IO Command

The 1st IO Command, as a major subordinate command to ARCYBER, provides support to Army commands for the planning and execution of IO.
http://www.1stiocmd.army.mil/

Additionally, IO Command provides courses focused on IO and cyberspace operations available to Army commands (both resident attendees at Fort Belvoir, Va., and deployable military training teams [MTTs]):

- **Information Operations Capabilities, Application, and Planning Course (IOCAP)**. This course provides an in-depth look at each of the core and supporting elements of IO, IO related activities, and subject areas and disciplines pertinent to IO including the military decisionmaking process, intelligence support to IO, targeting, and others.

- **IO Fundamentals Course via MTT Only** to units or organizations needing familiarization with the fundamentals of Army IO.

- **Army Cyberspace Operations Planners Course (ACOPC)**. Prepares leaders to integrate, synchronize, and coordinate the employment of cyberspace intelligence, surveillance and reconnaissance, cyberspace attack, cyberspace operational preparation of the environment, and cyberspace defense activities into cyberspace concepts of support for military operations.

- **Electronic Warfare Integration Course (EWIC)**. This course provides students with the ability and knowledge to integrate, synchronize, and coordinate electronic warfare planning and execution with full spectrum IO.

- **Executive Cyberspace Operations Planner's Seminar (ECOPS)**. An 8-hour seminar that provides a strategic/operational level introduction to cyberspace and cyberspace operations planning.

For detailed information on how to request theses courses, see:
http://www.1stiocmd.army.mil/Home/iotraining

This page intentionally left blank.

Center for Army Lessons Learned
10 Meade Avenue, Building 50
Fort Leavenworth, KS 66027-1350

www.leavenworth.army.mil

US UNCLASSIFIED
FOR OFFICIAL USE ONLY

US Army
Combined
Arms Center
"Intellectual Center of the Army"