Defensive Cyber Operations (DCO)

Breakout Panel

Nov. 4, 2021

Defensive Cyber Operations

Defensive Cyber Operations (DCO) rapidly delivers innovative and dominant cyberspace capabilities, as well as tailored information technology solutions for our national, joint and allied partners. We are the leader within the cyberspace domain, delivering innovative, integrated and cost-effective solutions.

Cyber Analytics & Detection (CAD)

Product Manager
Lieutenant Colonel Dakota Steedsman

Cyber Platforms & Systems (CPS)

Product Manager
Lieutenant Colonel Bradley Son

Applied Cyber Technologies (ACT)

Product Lead
Mr. Arthur Edgeson

Technology Applications Office (TAO)

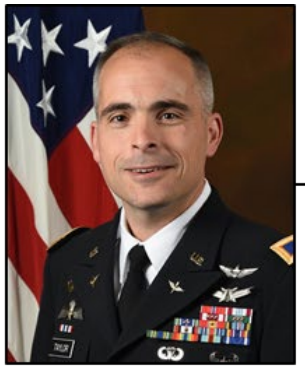
Product Lead
Mr. John Swart

Allied Information Technology (AIT)

Product Lead
Mr. Brian Bricker, Acting

Project Manager DCO
COL Mark Taylor

Defensive Cyber Operations
Leadership Changes 2021



Project Manager
Colonel Mark Taylor

Deputy Project Manager
Ms. Patricia Ocasio

Cyber Platforms & Systems (CPS)

Product Manager
Lieutenant Colonel Bradley Son

Applied Cyber Technologies (ACT)

Product Lead
Mr. Arthur Edgeson

Cyber Analytics & Detection (CAD)

Product Manager
Lieutenant Colonel Dakota Steedsman

Allied Information Technology (AIT)

Product Lead
Mr. Brian Bricker, Acting

MISSION

Rapidly deliver innovative and dominant cyberspace capability and tailored information technology solutions to national, joint, and allied partners to provide decisive, warfighting information advantage.

VISION

Be recognized as the leader within the cyberspace domain delivering innovative, integrated and cost-effective solutions.

Defensive Cyber Operations (DCO)
Who We Are

WHAT DOES DEFENSIVE CYBER OPERATIONS DO?

- Provide cyber analytics and detection for cyber threats
- Provide deployable and cloud based defensive cyber solutions
- Provide rapid prototyping capabilities for rapid acquisition
- Foreign military sales - building partner relationships
- Command, Control, Communications, Computers and Intelligence (C5I) acquisition services

TOP GOALS & PRIORITIES

To deter or defeat enemy offensive cyberspace operations.

Acquire critical capabilities allowing the Army to maneuver with agility to decisively engage the adversary in the cyberspace domain.

To support our Active Duty, Reserve Component and National Guard cyber warriors

To proactively engage with industry and our stakeholders to create positive communication engagement at all levels.

US ARMY PEO EIS
PEO Enterprise Information Systems

MISSION

Rapidly deliver innovative and dominant cyberspace capability and tailored information technology solutions to national, joint, and allied partners to provide decisive, warfighting information advantage.

WHO WE ARE

Cyber Analytics and Detection (CAD)
Analyze | Identify | Mitigate

Cyber Platforms and Systems (CPS)
Powerful | Adaptive | Responsive

Applied Cyber Technologies (ACT)
Advance | Incorporate | Maintain

Allied Information Technologies (AIT)
Assist | Build | Train

Technology Application Office (TAO)
Communicate | Control | Defend

Defensive Cyber Operations (DCO)
Operational Overview

Cyber Analytics (CA)

Big Data Platform (Gabriel Nimbus)

- Facilitates counter-reconnaissance activities, discover the presence of complex threats and vulnerabilities
- Ingest large amounts of data

DCO Mission Planning (DCOMP)

- Supports mission planning and situational awareness for Cyber Wargaming, Analyses, Training, Network Visualization
- Coordinating with Joint solution for increased efficiencies and shared capabilities

User Activity Monitoring (UAM)

- Identifies and malicious activity
- Monitors Insider Threat for SIPRNet, JWICS, SAP

Threat Emulation (TE)

- Model enemy activity for training and wargaming
- Environments are in a garrison, deployed, or mission partner setting.

Defensive Cyberspace Operations Tools Suite

- Software used to detect intrusion and conduct analysis
- Tools are used and developed in all 3 platforms below
- Over 100 tools several are acquired for advanced threats
- Tools continually change as new requirements emerge
- 100% of the tools are available 100% of the time

Forensics and Malware Analysis (F&MA)

- Rapidly triages cyber-incidents and performs analysis and collection of malicious data. (malware)
- After the fact assessment and resolution
- a trace to source solution and a containment solution.

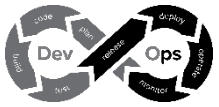
PLATFORMS AND DEVELOPMENT

Deployable DCO System (DDS)

(DEPLOYABLE)
Configurable hardware kit, can be easily fit in an aircraft overhead compartment. It is armed with the ability to tap into a network and host tools for defensive measures.

Garrison DCO Platform (GDP)

(FIXED)
Provides remote operational capabilities and a common platform. It has the ability to integrate with the Big Data Platform, Global Enterprise Fabric and cloud environments.



DCO Development Environment (DCODE)

(Innovation and Deployment)
Forge (Develop), Armories (Deploy), Development Environment (Training, Testing and Integration)

Emerging Capabilities

Threat Deception: Deceive the Enemy (Reconnaissance) and Detect Intrusions. Allows an operator to monitor the adversary's behavior

Security Automation Orchestration and Response (SOAR): Automated Internal Defense Measures for Evolving Threats

US ARMY PEO EIS
PEO Enterprise Information Systems

The employment of defensive capabilities achieve the following objectives: deter, destroy and defeat cyberspace threats; gain time; economy of force; control key terrain; protect tasked critical assets and infrastructure; and develop intelligence

CAPABILITIES NEEDED

- Network Mapping
- Counter Infiltration Tools
- Cyber Intelligence Integration
- Data Analytics – Artificial Intelligence and Machine Learning
- Security Orchestration, Automation and Response (SOAR)
- Threat Analysis
- Forensics and Malware Analysis (F&MA) – Licences, Training, Professional Services and Maintenance
- Deployable Defensive Cyberspace Operations – Modular, New Equipment Training Virtualization
- Cloud Based Garrison Defense

Cyber Platforms and Systems (CPS)

Cyber Platform & Systems (CPS) focuses on the procurement and delivery of cyber platforms and cybersecurity tools for the Armed Forces. The Cyber Platform is the foundational piece of equipment used by Cyber Soldiers. It allows them to conduct maneuvers on cyber terrain and affect Department of Defense Information Network (DODIN) defense.

Product Manager CPS
LTC Bradley Son

MISSION

Support Cyber Defenders – Rapidly Acquire and Deliver Innovative, Proven and Tested Capability – Protect the Infrastructure, Preserve Security, and Achieve Information Advantage – Support Defense Cyber Operations.

Cyber Platforms and Systems

Innovative | Integrated | Effective

TOP GOALS & PRIORITIES

- Provide operational capability to the Army Cyber Command's Cyber Protection Brigades allowing for rapid evaluation and response to unexpected and dynamic cyber threats.
- Provide the ability to rapidly triage an incident and place the impacted system back in service. A portable capability enables cyberspace defenders to quickly review information stored on deployed computers in real-time – without altering or damaging it.
- Deliver new prototype solutions allowing deployment in austere environments to defend the Department of Defense Information Network (DoDIN)

CAPABILITIES

Deployable Defensive Cyberspace Operations Systems-Modular (DDS-M)
Is a configurable hardware kit that can be easily fit in an overhead compartment of an aircraft.

Garrison Defensive Cyberspace Operations Platform (GDP)
Provides remote operational capabilities and a common platform between DCO and Department of Defense Information Network-Army (DoDIN-Army) systems.

Defensive Cyberspace Operations Tools Suite (DCO Tools Suite)
Integrates Commercial Off-the-Shelf (COTS) and open-source software (OSS) tools and products and continually leverages the user assessment approach

Forensics and Malware Analysis (FM&A)
Forensics provides the ability to rapidly triage cyber-incidents and perform forensics analysis and collection remotely or locally.

Applied Cyber Technologies (ACT)

Applied Cyber Technologies (ACT) through DCO Development Environment (DCODE), is the mechanism to bring in rapid innovation, sustainment of Defensive Cyber Systems, and Training and DEVSECOPS Environment. This capability spans three mission sets: Forge, Armory, and Mission network.

Product Lead ACT
Mr. Arthur Edgeson

MISSION

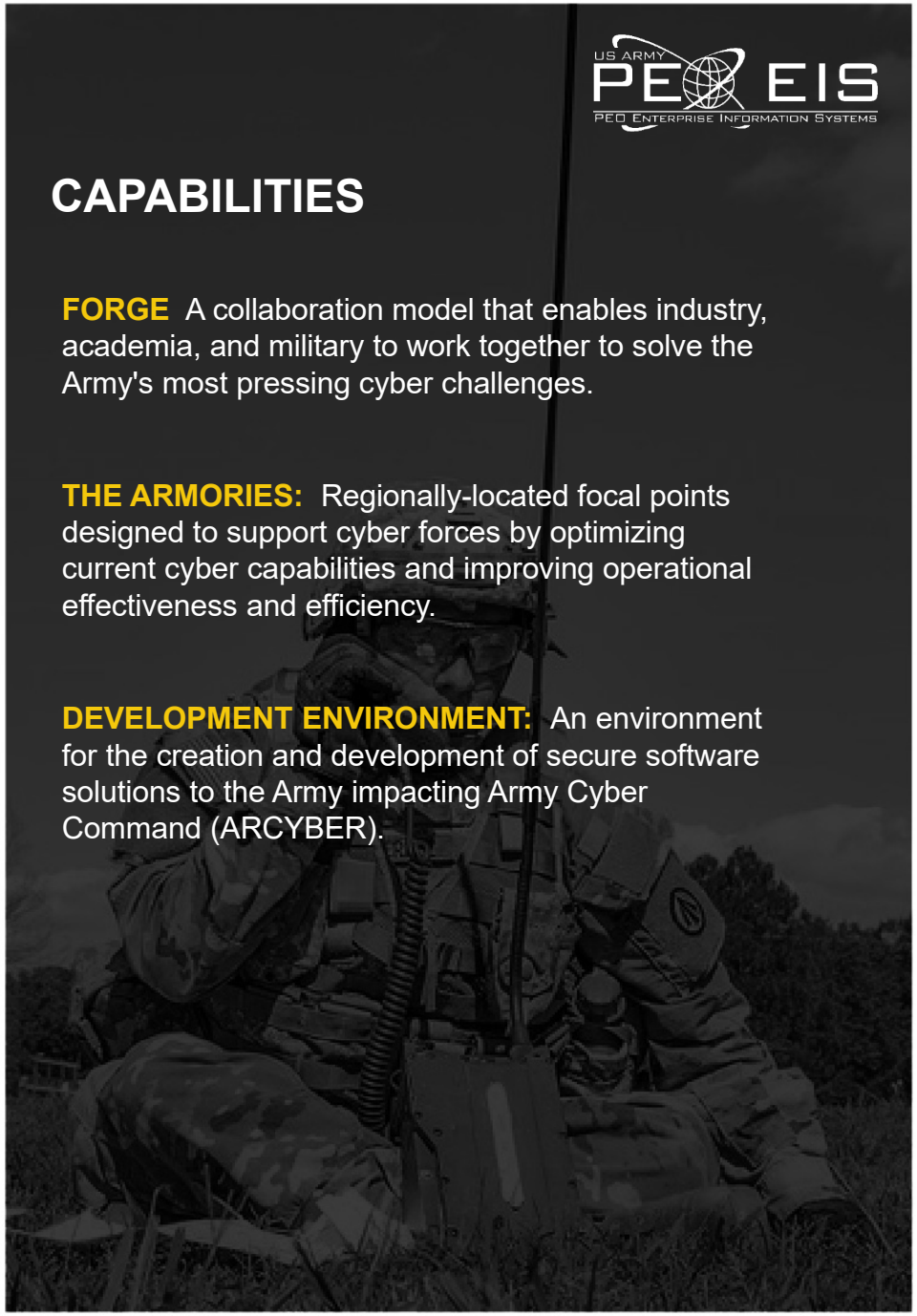
Rapidly provide the U.S. Army's cyber defenders the critical capabilities they need to meet the needs of an evolving cyber landscape.

Applied Cyber Technologies

Advance | Incorporate | Maintain

TOP GOALS & PRIORITIES

- Provide operational capability to the Army Cyber Command's Cyber Protection Brigades allowing for rapid evaluation and response to unexpected and dynamic cyber threats.
- Provide the ability to rapidly triage an incident and place the impacted system back in service. A portable capability enables cyberspace defenders to quickly review information stored on deployed computers in real-time – without altering or damaging it.
- Deliver new prototype solutions allowing deployment in austere environments to defend the Department of Defense Information Network (DoDIN)



CAPABILITIES

FORGE A collaboration model that enables industry, academia, and military to work together to solve the Army's most pressing cyber challenges.

THE ARMORIES: Regionally-located focal points designed to support cyber forces by optimizing current cyber capabilities and improving operational effectiveness and efficiency.

DEVELOPMENT ENVIRONMENT: An environment for the creation and development of secure software solutions to the Army impacting Army Cyber Command (ARCYBER).

Cyber Analytics and Detection

Cyber Analytics and Detection (CAD) provides essential capabilities required to protect against, search and discover, mitigate and engage, and eradicate advanced cyberspace threats and vulnerabilities.

Product Manager
LTC Dakota Steedsman

MISSION

Deliver tailored, innovative, and dominant cyberspace capabilities to discover vulnerabilities and deter advanced cyber threats defending the Army's networks in support of joint all-domain operations

Cyber Analytics and Detection

Analyze | Identify | Mitigate

TOP GOALS & PRIORITIES

- To broaden cyberspace analytic capability to allow for the comprehensive collection, analysis, and visualization of data stemming from all tiers of the Army's network enterprise.
- Develop new cybersecurity capabilities through development and integration of defensive cybersecurity solutions
- Identify threat trends, behavior patterns, and tactics, techniques, and procedures associated with relevant portions of the designated network

CAPABILITIES

Defensive Cyber Operations Mission Planning (DCOMP)
Integrates cybersecurity requirements, intel, & vulnerability analyses with the outputs of mission analysis to determine probable attack vectors and produce a set of relevant internal defense measures, triggers, and decision points.

Cyber Analytics (CA)
Offers interfaces and visualizations accessible by cyberspace defenders at all levels to facilitate counter-reconnaissance activities meant to discover the presence of advanced or sophisticated cyber threats and vulnerabilities.

User Activity Monitoring (UAM)
A scalable solution that proactively identifies internal risks associated with the theft or misuse of critical and assists with the establishment of the Army's Insider Threat (InT) Program.

Threat Emulation
Allows the Cyber Community to conduct threat emulation in a garrison, deployed, or mission partner environment on information systems, net-enabled warfighting platforms, and critical infrastructure by closely resembling adversarial capabilities.

Allied Information Technology

Allied Information Technology (AIT) builds and fosters relationships with partner nations and allies, ensuring Foreign Military Sales (FMS) cases are written in a holistic and strategic way so that partners across the globe are not only receiving the system capabilities they need, and also obtain opportunities to expand skill sets through additional training, advice and assistance to optimize system readiness and improve battle staff operations.

Product Lead
Mr. Brian Bricker

MISSION

Enhance U.S. and Partner Nation security and interoperability by delivering non-standard Command, Control, Communications, Computers, Cyber and Intelligence (C5I) capabilities under the auspices of Defense Security Cooperation and Assistance programs, primarily using the Foreign Military Sales (FMS) process

.

Allied Information Technology

Assist | Build | Train

TOP GOALS & PRIORITIES

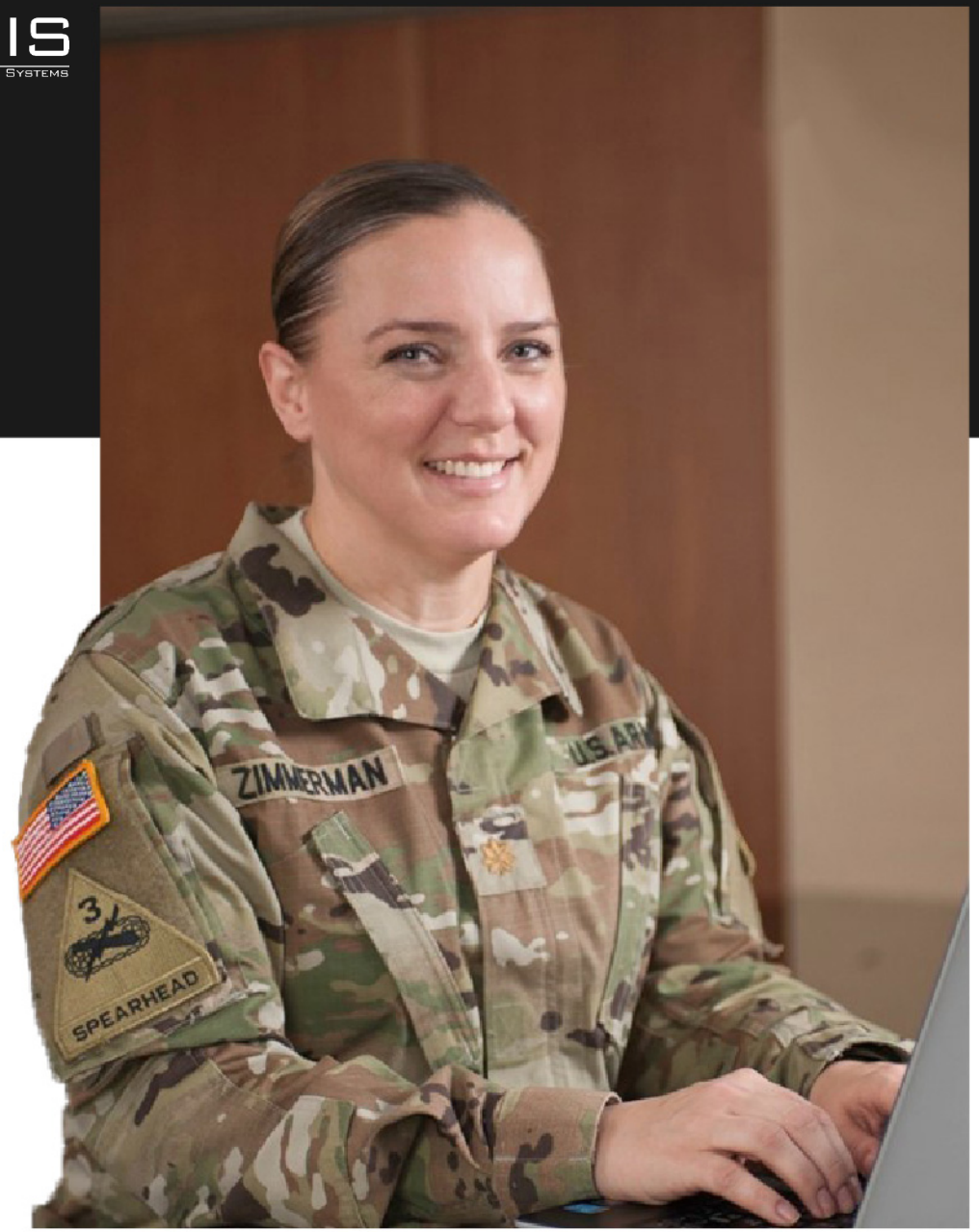
- Expand partnership with U.S. Special Operations Command and their associated subordinate commands to consistently and positively affect funding levels and the resources required to rapidly improve Allied Special Operations Forces' C5I capabilities at the speed of relevance.
- Strengthen and evolve our alliances and partnerships with geographical combatant commands and other counterparts through targeted and tailorable deliveries of secure capabilities in the C5I domain.
- Modernize Operations and Intelligence centers globally to align with NATO standards, increase security, and enhance operational capabilities.

For procurement opportunities:

https://www.eis.army.mil/opportunities

These Slides

https://www.eis.army.mil/newsroom/publications



MEET WITH US

theforge.force.com/peoeis/s/

CONNECT WITH US

eis.army.mil/mission-areas/act

Company/ArmyDCO

Usarmy.Belvoir.act.forge@mail.mil