UNITED STATES ARMY CYBER CENTER OF EXCELLENCE

STRATEGIC PLAN

SEPTEMBER 2015

U.S.ARMY

WHERE TRADITION MEETS THE FUTURE
Team Gordon
UNITED STATES ARMY
CYBER
CENTER OF EXCELLENCE | FORT GORDON

FOREWORD

Successful Unified Land Operations increasingly depend on the ability of Army and Joint Force Commanders to effectively integrate cyber, signal, electronic warfare, intelligence, information operations, and space capabilities to ensure cyberspace dominance while simultaneously denying the same advantage to adversaries.

During the past 14 years of persistent conflict, the Army has enjoyed the most robust and capable communications capabilities in its history. Communications services provided by a combination of joint, inter-organizational, multinational and commercial partners enabled effective mission command, precision fires, intelligence, surveillance, and reconnaissance (ISR), logistics and medical operations. Unfortunately, this decisive advantage is not assured. Current and future adversaries have taken notice of the advantage and dependency the U.S. places on its communications capabilities. As the U.S. quickly expanded to meet the challenges of current operations, expediency sometimes took precedence over criteria such as security, affordability, sustainability, and coalition compatibility. Threats to our information dominance include internal malign actors as well as external adversaries. Significant changes are required across the DOTLMPF to ensure that our commanders and soldiers continue to enjoy the advantage of information dominance in the future while we simultaneously deny our adversaries the capability to operate effectively in the same space.

Department of Defense Information Network Operations (DODIN OPS) are the most complex and vital operations that DoD conducts 24/7. Army and Joint Commander's simply cannot execute Mission Command, Precision Fires, ISR, Joint Logistics and other necessary warfighting capabilities without a properly architected, operated and defended network. Army performance in the cyberspace domain requires a fundamental shift in Army strategy, doctrine, force development and operational techniques. The Cyber Center of Excellence (Cyber CoE) as the integrating Headquarters plays a pivotal role in this process ICW Army Cyber Command and the Army Cyber Institute to develop and merge key doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) enabling concepts and capabilities to maximize the Army's development, use, and successful mission execution in cyberspace.

DoD's dependence on cyberspace has changed the way the Department of Defense (DoD) manages, fights, wins wars, and fundamentally impacts the responsiveness, lethality, and effectiveness of Army land operations. Cyberspace can no longer be considered exclusively a signal or intelligence mission, a boutique weapons capability, or an information operations enabler. It is a domain the Army must understand, maintain awareness of for full situational understanding, and key terrain we must control for operational success across all unified land operations (ULO). Both state and non-state adversaries have employed novel capabilities, created by combining increasingly available military and commercial technologies. The 39th Chief of Staff of the Army, GEN Milley recently wrote that "The Army currently benefits from an overmatch that enables a historically small number of Soldiers to accomplish significant operations while minimizing casualties. This advantage has a shelf life; the technologies that gave us the advantage today are increasingly available to state and non-state adversaries at dramatically lower cost than even a decade ago. As that overmatch degrades, the risk to Soldiers increases." We at the Cyber CoE assess that to win in a complex world, we must dominate the cyber domain.

The dynamic nature of the cyberspace operational environment (OE), and increasingly high operational risk posed by cyberspace actors requires the Army to act now. The Army must adapt and change the way we develop concepts and capabilities, and educate and train our cyber force to make them high value, high impact operators on the Joint battlefield. This requires innovative, agile learning mechanisms and modern facilities that place cyber technology and threats, and integration of cyber tradecraft advances and operational lessons learned on a much accelerated basis. It requires new talent management approaches to attract, screen, recruit and retain Soldiers and civilians with a high level of native cyber aptitude, and integrated approaches across cyber organizational structure, leadership training, and skills development. The velocity of the cyber evolution also mandates shorter technology refresh cycles to take advantage of market innovations, and requires continuous CoE interaction with Army and Joint stakeholder communities to shape supporting regulations, policies and the Army Operating Concept.

The following strategic plan outlines foundational Cyber CoE needs and a framework of required action. It documents our desired end-state or "ends" (vision and mission) which we believe we can achieve by 2020, and includes five lines of effort (ways) with aggressive initiatives (means) to get us there. We will overcome the many related challenges with Army leadership support, dedication of the talented Cyber CoE team, and by leveraging expertise from across the extended Joint, DoD and Intelligence Community (IC) cyber stakeholders.

Major General Stephen G. Fogarty
Commanding General

INTRODUCTION

PURPOSE & SCOPE

This document provides a strategy and framework to transform the Cyber CoE and Team Gordon (tenant organizations and community partners), develop concepts, doctrine, requirements, integrate cyberspace operations and train Soldiers and leaders. This strategy defines the Cyber CoE vision, mission, lines of effort, strategic imperatives, and objectives required to integrate capabilities across the Army to include the Army's signal, electronic warfare (EW), and military intelligence (MI) partners (see Figure 1) together with other Joint Service and Intelligence capabilities. The Cyber CoE with Army Cyber Command (ARCYBER) and the Army Cyber Institute (ACI) form the nucleus of "Team Cyber" for the Army while leveraging the Intelligence Center of Excellence (ICoE), the U.S. Army Intelligence and Security Command (INSCOM), the Network Enterprise Command (NETCOM), along with the greater Signal and Intelligence Communities to achieve dominance in the cyberspace domain. Cyber CoE activities must be coordinated and complementary with/to ARCYBER and ACI. The Cyber COE Strategy spans from the present through FY 2025 to meet emerging Joint, Interagency, and Multi-national (JIM) operational environment challenges.

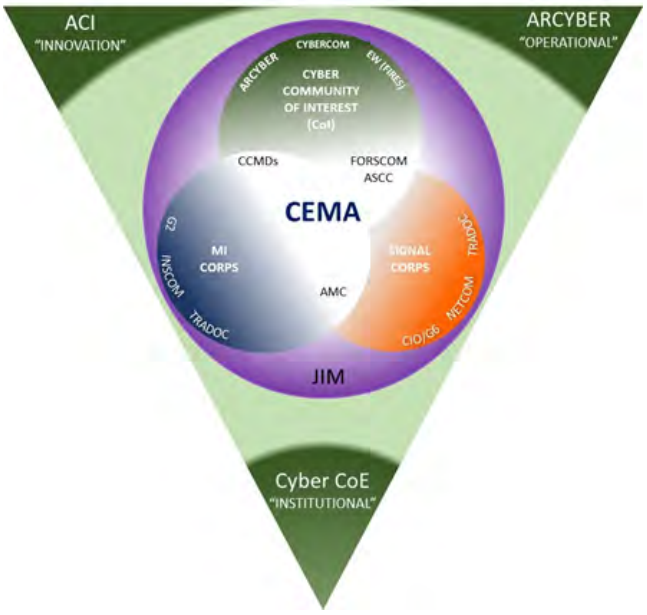


Figure 1 - Cyber Partners

STRATEGY OVERVIEW

The framework of this strategic plan documents the desired state or "Ends" (vision and mission) and includes "Ways" (lines of effort" (LOEs)) with aggressive "Means" (initiatives) to accomplish these ends. This strategy is nested with the ARCYBER Commander's Vision and Strategic Plan, the CIO/G-6 LOEs (Provide Signal Capabilities to the Force and Enhance Cybersecurity Capabilities), as well as, G-2, INSCOM and NETCOM visions. It is nested in "The Army's Operating Concept" (AOC), Army imperatives, and supports two Army Warfighting Challenges (AWFCs) -- Develop Situational Understanding; Conduct Space and Cyber Electromagnetic Activities and Maintain Communications. The Cyber CoE will collaborate with key stakeholders to prioritize enterprise-to-foxhole requirements, develop a holistic resourcing strategy and work with the acquisition community to develop materiel solutions. Stakeholder support and collaboration are key for success.

ASSUMPTIONS

The Cyber CoE has four key resourcing and manpower requirements generating assumptions for building capable and trained cyber forces and capability; setting conditions for effective and efficient integration of cyber forces into the operational Cyber Mission Force; transforming Fort Gordon into a modern cyber power projection platform integrating signal, EW, intelligence, and ISR capabilities with other Joint organizations.

1. Cyber CoE has the ability to leverage existing Army, Joint and USCYBERCOM cyber training and tradecraft capabilities.
2. Cyber CoE receives resource priority across the Program Objective Memorandum (POM)/Futures Years Defense Program (FYDP) to enable a rapid and comprehensive stand-up and establishment of foundational Army cyber capabilities.
3. Department of the Army approves essential Cyber CoE manpower skill changes and growth, while providing the CoE with the facilities and personnel resources required to ensure success of this critical enterprise.

4. Department of the Army implements streamlined requirements and acquisition processes that support cyberspace doctrine, organization, training, materiel, leader development and education, personnel, and facilities (DOTMLPF) capability development and associated activities.

STRATEGIC FRAMEWORK

The Cyber CoE strategic framework uses the Ends / Ways / Means methodology. Figure 2 depicts how we will transform the current as-is state of Signal, EW, and MI functions to generate integrated Cyber capability. We will achieve our Ends through execution of five prioritized LOEs. Implementation will be executed across the DOTMLPF process. The desired end state is a transformed CYBER CoE, underpinned by Team Gordon, as a modern power projection platform for DoD and Army cyberspace mission operations. The goal is to build cyber capacity and have a trained and ready Cyber Force with Joint integration.

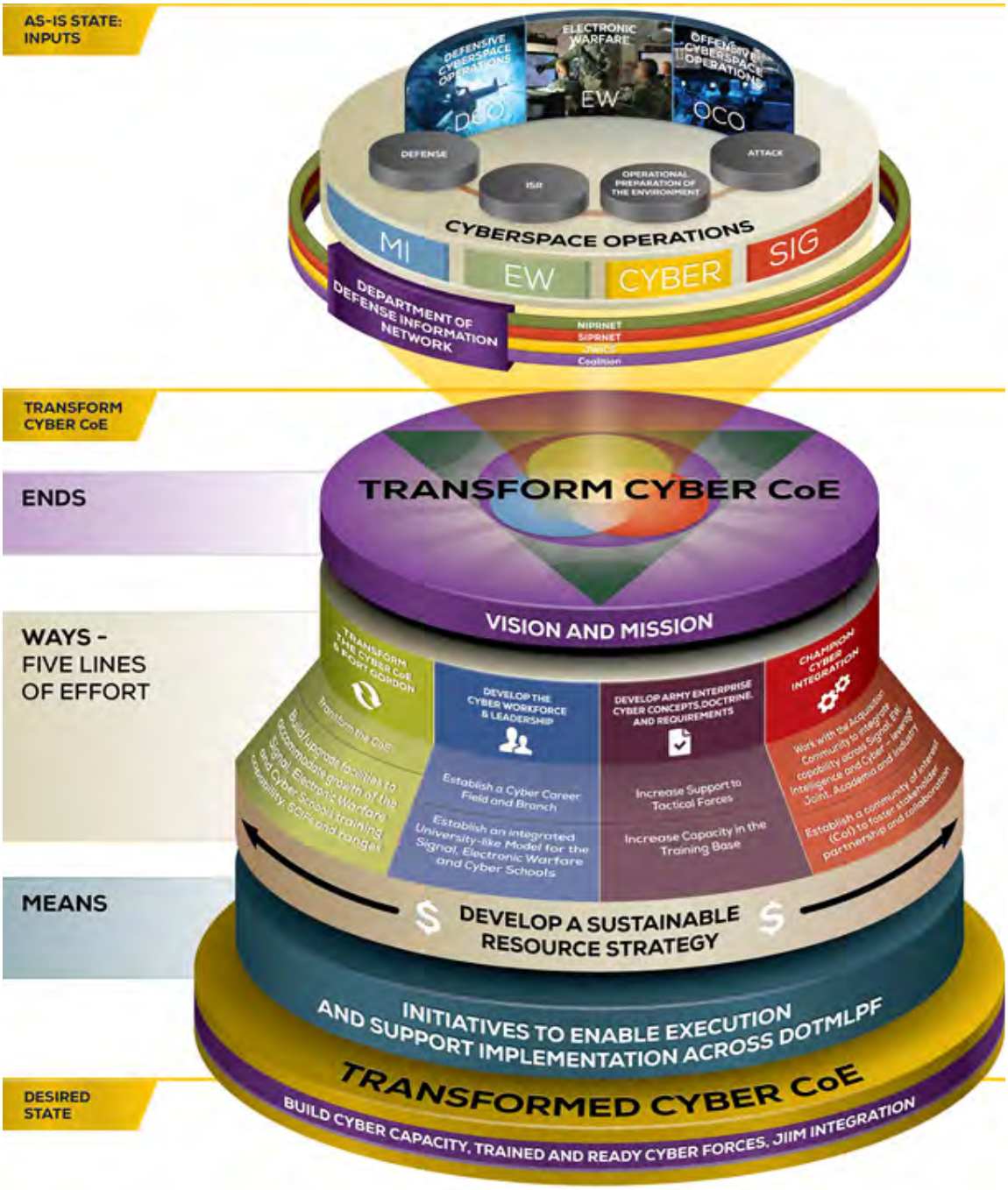


Figure 2 - Cyber CoE Strategy

VISION

The Cyber Center of Excellence (including the Signal and Cyber Schools) and Team Gordon: a highly-skilled workforce that effectively collaborates with relevant stakeholders to develop and lead integrated cyber, signal, and electronic warfare and signal solutions (capabilities) for the Army and Joint Forces.

MISSION

The United States Army Cyber Center of Excellence trains and educates highly skilled cyber, signal, and electronic warfare Soldiers and civilians and develops DOTMLPF solutions (capabilities) to conduct effective cyberspace, signal, and electronic warfare operations in the cyber domain in support of Unified Land Operations.

WAYS AND MEANS

The LOEs depicted in Figure 3 outline the major components necessary to move the Cyber CoE toward the Chief of Staff's vision for cyberspace operations outlined in (HQDA EXORD 057-14), and capture the ways in which success will be achieved and measured. The LOEs support the vision and encapsulate priorities and objectives tied to transformational steps, force structure changes, leader development, and cyber capabilities development and integration across warfight-ing functions. They leverage related efforts from across the Cyber Community of Interest (COI) (e.g., ARCYBER, ACI, CIO/G-6, G-2, U.S. Cyber Command, ICoE, NETCOM, INSCOM, etc.) and provide the basis for planning, preparing annual Program Objective Memorandum (POM) requirements, and building an enduring cyberspace operations program and platform. Together, they create a capable Army cyber force that enables the operating force in a complex and evolving environment.

STRATEGIC IMPERATIVES

The Cyber CoE's success in meeting the overarching objectives of this strategy, and realizing the stated vision, depends greatly upon three strategic imperatives.

First, the Cyber CoE must champion a change in Army culture. The effective execution of cyberspace operations requires successful integration of cyber, signal, EW, intelligence, information operations, and fires at all echelons. The requirement for most of the Signal workforce to possess a Top Secret/SCI security clearance is one of many changes the Signal Corps has to make to take to move into the future. Likewise, the Intelligence Corps must significantly change how it provides intelligence support to DODIN operations.

Next, the Cyber CoE must build a modern campus, equipped with a state-of-the-art training capability essential for the cyber, signal, and EW workforce. This new campus must be organized around the weapons system of the Cyber Force; a fully functional operational network that is TS/SCI down to unclassified. The campus must have appropriate SCIF space, other controlled access areas, a classified library for research and access to cyber ranges.

Finally, the Cyber CoE must drive convergence across the Army's networks, data, and common operating environment to fully create the knowledge required to win in the cyber domain.

PRIORITIES AND OBJECTIVES

The Cyber CoE is the U.S. Army's force modernization proponent for cyberspace operations, signal/communications networks and information services, spectrum operations, and EW. As such, it is responsible for developing the underlying concepts and refining processes for identifying, training, educating, and developing world-class, highly-skilled professionals supporting strategic, operational and tactical cyberspace, signal, and EW operations. In order to meet these proponent requirements, the LOEs have a unique set of priorities and objectives to define modernization and underpin the organization's vision and mission.

Requirements determination, resourcing, and acquisition comprise critical components of each LOE, Priority and Objective. The priorities and objectives enable Cyber CoE to focus on warfighter requirements, while ensuring business needs applicable at all levels – enterprise to foxhole – are considered. Well-defined and articulated requirements set the stage for engagement with the COI and key leadership to move identified requirements through the processes involved with resourcing and acquisition, and enable the team to respond quickly to urgent and emerging needs.

Figure 3 displays the five LOEs, the priorities by LOE, and the overarching objectives to achieve the vision and mission.

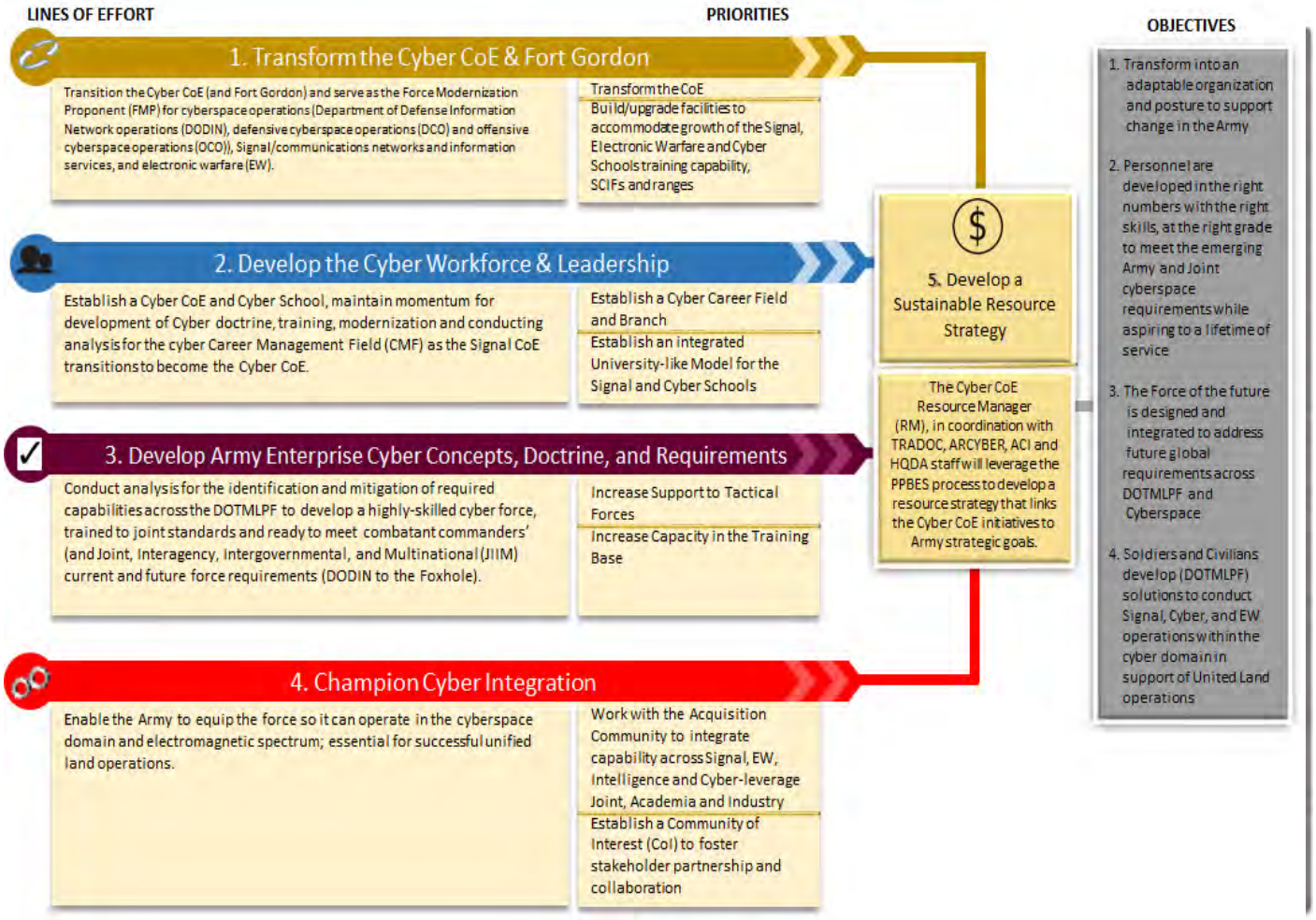


Figure 3 - Lines of Effort to Meet Overarching Objectives

The initiatives listed under the LOEs provide the means by which Cyber CoE and Team Gordon will transform to provide the capabilities and infrastructure needed to support and sustain key cyberspace functions, both operational and institutional. The initiatives focus efforts to develop Army Cyber Mission Forces, as well as leaders who understand how cyberspace operations support Unified Land Operations (ULO) and mission command. The initiatives provide a structure for doctrine development needed by the Army. They also provide a basis for understanding current cyberspace, signal, EW and electromagnetic spectrum operations, while writing concepts that describe how the Army will operate in challenging cyber, signal, and EW environments in the future.

LINES OF EFFORT (WAYS) AND INITIATIVES TO ENABLE EXECUTION (MEANS)

1. Transform the Cyber CoE & Fort Gordon

The rapid evolution of cyberspace threats and the major risks posed to ULO require immediate transformation of the Signal Center of Excellence to a modern, integrated Cyber Center of Excellence capable of training and educating the Army's future cyber work force and cyber leaders while maintaining a highly skilled and trained Signal force. Effectively implementing the Army's Cyber University is the key to success. This requires urgent financial investments in faculty and staff. Students and facilities capable of leveraging classified operational and intelligence resources are required immediately, as well as related advanced technologies needed for cyber Soldiers and civilians to effectively collaborate in support of the worldwide operating forces.

Initiative A - Implement the University Model

The Army educational system as it exists today is not structured to provide the skills required to meet the cognitive challenges that Army leaders will face in 2025 and beyond. The U.S. Army Learning Concept for Training and Education and the Army Operating Concept describe the educational approach and the type of leader qualities (agile, adaptive, innovative) necessary to navigate in this rapidly evolving environment. To date, the Army has done little to address the issue. The TRADOC Commanding General acknowledged this shortfall in the Army's educational system when he approved the "Strategic Business Plan for the Army University" in March 2015. This plan is designed to transform the Army's schools into a University model better postured to achieve six strategic goals: agile, adaptive and innovative Soldiers, Civilians and leaders; intellectual overmatch of our potential adversaries; operational agility; enhanced Army Professional Military Education; broadened Joint Professional Military Education (JPME) I and II; and committed professionals…Soldiers for Life.
The Cyber CoE's role in meeting the intent of these Army concepts and the University construct is to transform the Signal School and establish the Cyber School in collaboration with TRADOC leadership and key stakeholders. This transformation will fulfill the CSA, TRADOC and Cyber CoE visions for a flexible, synchronized and integrated approach to an educational system that will train and educate cyber, signal and EW Soldiers and civilians.

To execute and achieve this initiative, the Cyber CoE must recruit the best cyber-savvy faculty from across industry and academia, work across TRADOC to develop the best curriculum and create processes that allow for updates to programs of instruction commensurate with the dynamic changes in the cyberspace environment. The CoE must concurrently work with key stakeholders to design, build, and maintain state-of-the-art facilities that will accommodate the training of defensive and offensive operationsacross the disciplines of cyber, signal, and EW.

Initiative B - Develop a Modern Cyber Campus

The existing Cyber CoE campus infrastructure was built between 1960-1980s with very few upgrades since that time. Of the 735 classrooms on Fort Gordon, only 8 received Classroom XXI updates (TRADOC template to upgrade classrooms) with 192 classrooms receiving limited IT upgrades. In order to train our Soldiers and civilians to conduct future cyberspace, signal, and EW operations where critical thinking, agile and adaptable leaders are required, the Army must design and build – not merely renovate - state-of-the-art facilities. The intent is to create an educational environment based on real world challenges and solutions. The campus redesign must provide an interactive Cyber center where the students and faculty alike derive relevant solutions. The campus design must facilitate collaboration with cyber, signal, and EW Soldiers and civilians, faculty and the operational community, as well as, establish effective linkage with the Intelligence COE, at the TS/SCI level, in order to fully develop the application, impact, and integration of the Intelligence Warfighting Function into cyberspace operations. The Cyber CoE will establish in this environment, the operational community with designated subject matter expertise embedded within the institutional training base. In this construct, cyber faculty can utilize the operational community to quickly adapt and modify programs of instruction to incorporate current real world joint cyber requirements and facilitate continuous development of cyber doctrine, tactics, techniques, and procedures, and integration into Army capstone documents. The result is a cyber warrior trained in real-time, real-world cyberspace operations. This enhances the Army's ability to maintain a technical edge in the cyber domain where rapid identification of cyber requirements and capability delivery, including trained operators, is critical.
The Cyber Campus modernization will include the convergence of existing communications network infrastructure from the strategic enterprise to tactical level signal systems as necessary to achieve shared cyber domain situational understanding, high synergy collaboration and effective learning. The enhanced Network Operations Center will serve as a single, integrated hub for cyber, signal, and EW capabilities across all classification levels. We will identify and leverage existing industry, academia, Joint and IC infrastructure to meet Cyber CoE University and campus mission needs.

Initiative C – Transform the Signal Experimentation Division to a Cyber Battle Lab

The design and implementation of cyber-related leader development, education, and training must evolve from traditional group training approaches to more flexible cyberspace tradecraft platforms best suited to highly intuitive, visually oriented learners. Effective solutions must leverage existing, high quality Joint and IC distance learning programs and meet dispersed, multi-component cyber, signal, and EW Soldier/Civilian needs.

This will require significant investment in Cyber Campus infrastructure as discussed above and conversion of the Signal Experimentation Division into a TRADOC designated Cyber Battle Lab (CBL) to perform live, virtu-al, and constructive experimentation and support a persistent training environment for cyber, signal, EW, and intelligence (ISR) practitioners at multiple classification levels, across both defensive and offensive mission sets. Currently under consideration as part of the TRADOC 2014 Bold Initiatives campaign is the transformation of the Signal Experimentation Division into an integrated Cyber Battle Lab (CBL) with cyber range capability that will allow the Cyber CoE to leverage classified intelligence inputs to realistically emulate/ simulate com-plex data networks, test emerging cyber capabilities and technologies to identify cyber, signal, and EW capabil-ity gaps and produce potential solutions. Additionally, establishing a battle lab collaborative simulation envi-ronment that develops and integrates cyber, signal, and EW concepts with other CoEs could possibly mitigate interoperability challenges. Our approach will assist cyberspace concept development and inform the Army Warfighting Assessment Strategy. This integrated virtual environment does not exist today at Fort Gordon and is necessary for shared Cyber Mission Force understanding of technologies, threat activities, and appropriate countermeasures development. Since CBL capabilities already exist in the Joint and IC, we will concurrently identify high synergy opportunities for partnerships with Air Force, Navy, DISA and NSA counterparts to increase effectiveness and reduce costs. We will also actively collaborate with Government and commercial science and technology (S&T) and materiel developers to leverage existing investments of relevance.

Initiative D – Establish Force Modernization Proponent

The Cyber CoE is the Army's principal official for all force modernization DOTMLPF requirements and activities related to cyber, signal and EW. Army Regulation 5-22, The Army Force Modernization Proponent System provides guidelines and functions for establishing and maintaining an effective force supporting Army warfighting requirements. As such, the Cyber CoE must develop a strategy for how cyberspace operations are implemented throughout all Army operations and organizations. These operations must be synchronized with policy, captured and documented in Army concepts and doctrine.

Initiative E – Develop Strategic Messaging Around Transforming Team Gordon

Our strategic message will clearly articulate the strategy and vision for the growth of Fort Gordon. We will establish partnerships within the local and regional communities to develop implementation plans which manage the internal and external impacts of anticipated personnel, logistics, and transportation growth, and foster an open dialogue with local/ regional leaders for community support along with the greater Army community of interest. Our messaging will support Army initiatives and strive to inform external organizations of the critical needs of Cyber CoE and Team Gordon to assist in leveraging additional resources from DoD/ Congress to support Army requirements.

Our Army needs expert, high quality cyber leaders who can fully leverage cyberspace capabilities in support of ULO. A modern learning environment that enables holistic understanding of the cyber OE, and high quality training and development across multiple disciplines (e.g. cryptography, machine learning, data mining) and technologies are key to generating cyber capacity for the joint operating force. The Cyber CoE, with its unique ability to directly leverage Team Gordon, is the Army's single, integrated platform for achieving that end. To position the Army's cyber forces for future joint and national demands, the Cyber CoE must successfully accomplish four key initiatives:

Initiative A: Educate, Train and Certify the Cyber Force

Establish shared cyber operational environment situational understanding across the CoE learning population as a necessary pre-requisite for cyber skills and operational tradecraft learning. Develop standards, training objectives, and curricula across the full range of cyberspace individual training for career management field (CMF) 17 as well as Military Occupational Specialties 25D, 255S, FA 26, and Career Field (CF) 17 series specialties. Certify Army cyber Soldiers and leaders to meet Army and Joint standards for offensive, defensive and network operations. Leverage cyber learning resources within the Joint community and other Services. Participate in force modernization and cyberspace research to support training certification maintenance and modification in close partnership with NSA, DISA, and ARCYBER.

Initiative B: Educate Army Leaders

Leaders at all levels will be educated in cyberspace capabilities, policy, effects and how to integrate those capabilities into military operations. Develop standards and content for effective cyber leader training to qualify cyberspace Officers, Warrant Officers and Noncommissioned Officers for key Army and Joint cyberspace operational roles. Integrate relevant cyberspace training into Army Leader Development, to include curriculum for Basic Officer Leader Course (BOLC), Captain's Career Course, Command and General Staff School, Army War College, Mission Command Training Program (MCTP), and US Army Sergeants Major Academy (USASMA). Coordinate with ARCYBER and USCYBERCOM to ensure use of Joint cyber terminology and concepts. Work with the Army Cyber Institute to develop technical and cyberspace curriculum/products to educate future cyberspace leaders. Provide enhanced enterprise cybersecurity awareness training to ensure safe use of technology across the Army. Leverage Joint schools, training with industry and academia as appropriate for training and educating both military and civilian leaders.

Initiative C: Establish the Branch Proponent for CF 17

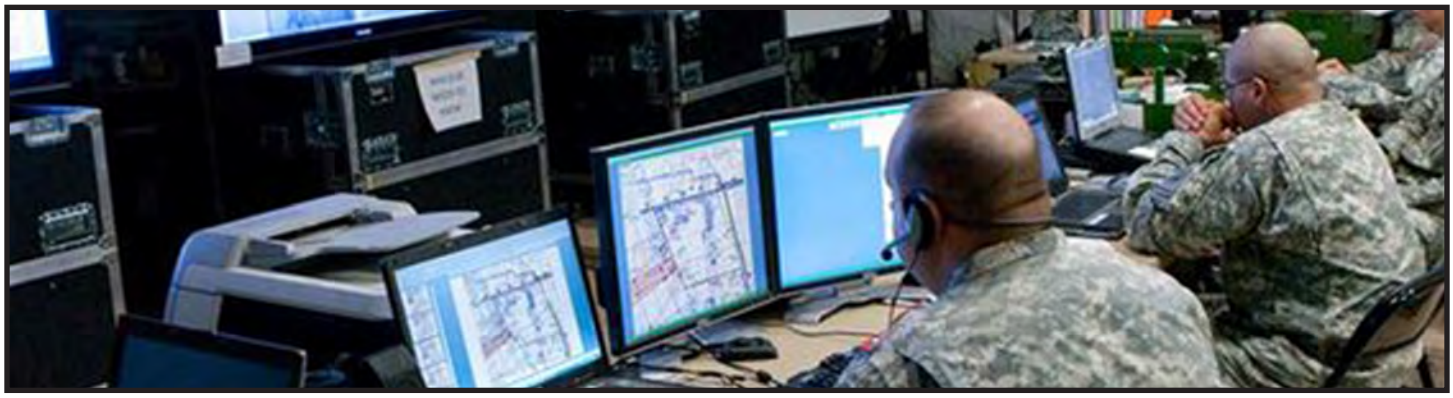
One of the key functions of FMP, as discussed in LOE 1, is Branch Proponent. The Cyber CoE is responsible for the execution of training, leader development, education and personnel actions for cyber, signal, and EW. While the branch proponents for signal and EW have matured over time in this capacity, the Cyber CoE must develop the recruiting standards for the CF 17, establish leader development processes, and establish the criteria for promotions and retention. The Army requires baseline cyberspace understanding to accomplish related acquisition, technology development, legal, and other enabling missions. The Cyber CoE must develop the standards for "general purpose user" cyber training for use by all schools and centers in order to ensure all Soldiers have a basic understanding of the cyber threat and associated defensive measures.

Initiative D: Advocate and Enable Cyberspace Operations in Collective Training and Exercises

Support the development of cyber training/exercise requirements for Army and Joint Staff collective exercises, war games, table top exercises, and limited objectives experiments. Assist in the development of specific Army and Joint cyber exercises to measure individual and staff cyberspace competence. Develop cyberspace scenarios and objectives for non-cyberspace exercises, such as Mission Readiness Exercises (MRX), Mission Command Training Programs (MCTP), and Combat Training Centers (CTC). Work to ensure that cyber component Soldiers and civilians have access to dedicated cyberspace simulations and 'live fire' range facilities, which closely replicate the complex, dynamic cyberspace OE, in order to achieve and sustain a high level of operational cyber readiness. Serve as the Army's primary advocate for advanced cyberspace modeling and simulation capabilities to enable effective learning, tool and concept development and cyber mission rehearsals.

Initiative E: Signal Workforce Realignment

Using the U.S. Army Operating Concept and the CIO/G6's Army Network Campaign Plan, the Signal School is taking major efforts to shape our regiment in order to meet the challenges of 2020 and beyond. Network convergence, emerging technologies, and the changing landscape of our joint operational environment has created the need to adapt the way the Army staffs, trains, and develops our signal enlisted force. The Cyber CoE must create a Signal Regiment structure that is poised to excel in the midst of these changes. The current Signal Regiment Enlisted MOS structure of 17 specialties is projected to be reduced to 10 by FY19 which satisfies the needs of the future Army. As part of this review, the roles of the warrant officer and officer will also be realigned.



3. Develop Army Enterprise Cyber Concepts, Doctrine, and Requirements

The Army is developing multiple DOTMLPF solutions and several capability/requirements documents to address critical operational gaps described in two recent Capabilities Based Assessments; all in the midst of building the Army's portion of the Joint Cyber Mission Force, establishing a Joint Force HQ-Cyber, and transforming the Signal CoE to a Cyber CoE. Crucial to the success of these collective efforts is stakeholder synchronization and a common vision and/or end state that does not exist today. The "Army Cyber Materiel Development Strategy 2014-2048," dated Feb 2015 (signed by ASA(ALT)) established a framework that identifies and defines four Army cyberspace mission areas to support national to tactical ULO: cyberspace control; cyberspace force enhancement; cyberspace support and cyberspace force application, however, specific CONOPS for each of these mission areas are not yet developed and available to the warfighting force.force application, however, specific CONOPS for each of these mission areas are not yet developed and available to the warfighting force.

Initiative A: Establish Foundational Doctrine for Army Cyberspace Operations That Is Consistent With Joint Doctrinal Tenets

Doctrine provides fundamental principles which guide military actions in support of operational objectives, drives how Army forces are organized and equipped, and serves as the basis for all Soldier and leader training and education (TR 71-20-3). Field Manual (FM) 3-12 "Cyberspace Operations" will serve as the foundational framework for cyberspace planning, integration and execution. It is intended to supersede FM 3-38, "Cyber Electromagnetic Activities," which introduced commanders to cyber terminology and use of allocated staff but failed to address operational principles or outline Army cyberspace operations concepts. As cyberspace operations are inhserently joint in nature, it is essential that FM 3-12 and all subsequent doctrinal manuals be consistent with "The U.S. Army Operating Concept," Joint and intelligence community cyberspace principles, standards and common practice to ensure 'interoperability from birth'.

Initiative B: Develop Army Cyberspace Concepts of Operation

To supplement FM 3-12, Cyber CoE will, in coordination with ARCYBER, assist in the development of Army CONOPS (aligned to the mission areas referenced above) which present a holistic, integrated picture and a useful visualization of how cyberspace operations are conducted in support of ULO. As the cyberspace OE is so highly dynamic, these CONOPs will provide a framework which can be rapidly updated for experimentation, gaming, and incorporation into training and follow-on doctrine, as appropriate. This will aid in validation of relevant Army cyber developmental initiatives and early curtailment of those initiatives/capabilities which no longer meet projected needs.

Initiative C: Develop/Leverage Methodologies That Bring Cyberspace Capabilities to the Force in an Agile, Expeditious manner

Holistic, current understanding of the cyberspace OE, mission set, and required capabilities is necessary for wise investment of scarce resources to develop and field high impact cyber capabilities. The continuous, rapid evolution of cyber innovation drives equally rapid obsolescence of cyber capabilities acquired through traditional development and acquisition processes. The IT Box process was developed to expedite the Joint Capabilities Integration and the Development System with deliberate requirements/acquisition processes through document flexibility and a degree of delegated oversight. The IT Box process, however, does not solve the core issue pertaining to funding for agile development. The deliberate acquisition process, even when leveraging IT Box efficiencies, does not keep pace with cyberspace technology development rates -- the result is often funding that comes too late for solutions that are no longer "value added" to the Cyber Mission Force. To mitigate current/future impediments to responsive, synchronized, and integrated cyber requirements and acquisition processes, Cyber CoE will coordinate with key stakeholders to implement the streamlined requirements generation and acquisition recommendations/objectives captured in the "Army Cyber Materiel Development Strategy" and the "DoDI 5000.02, Operation of the Defense Acquisition System," dated January 7, 2015.

The Cyber CoE must set the conditions to effectively develop cyber capabilities supporting JIM operations. This requires significant synchronization and integration of cyber requirements, funding, acquisition, and governance activities. The DOTMLPF process is our method to manage this Army change. The specific challenge is to synchronize the activities of numerous capability managers developing cyber capabilities across the enterprise in accordance with different authorities - Titles 10, 32, 40/44, and 50. The Cyber CoE is the integrator of requirements across the enterprise. A result of this integration will be a classified cyber operations sharing environment to support the enterprise as noted in Figure 4.

Initiative A: Drive Integrated Capabilities

To fully integrate cyberspace operational capabilities, current policy, doctrine, and title authorities must be clearly defined and understood for DODIN operations, defensive cyberspace operations, and offensive cyberspace operations activities. The Cyber CoE is positioned to lead the development of integrated capabilities required across the enterprise to increase efficiencies (e.g. big data analytics, unified cloud data, etc.) lower costs, and provide sound return on investment. Cyber CoE, as a central integrator, can drive the requirement to converge stove-piped systems, communications, and architectures while meshing with the Joint Information Environment and the Unified Platform being established by U.S. Cyber Command. Cyber CoE will champion state-of-the-art facilities, knowledge management tools, and learning aids that enable awareness, training, and education; systems and applications that support requirements determination, staffing, and production; and joint-capable training ranges which provide key resources necessary for Cyber Mission Forces to achieve and sustain a high level of readiness. Figure 4 depicts an example of the Cyber CoE vision within the Warfighter Mission Area (WMA). The Command Post (CP) evolution leads to a shared/integrated environment – leveraging the power of the enterprise (Enterprise Information Environment Mission Area (EIEMA) in support of Business Mission Area (BMA), WMA, and Defense Intelligence Mission Area (DIMA).

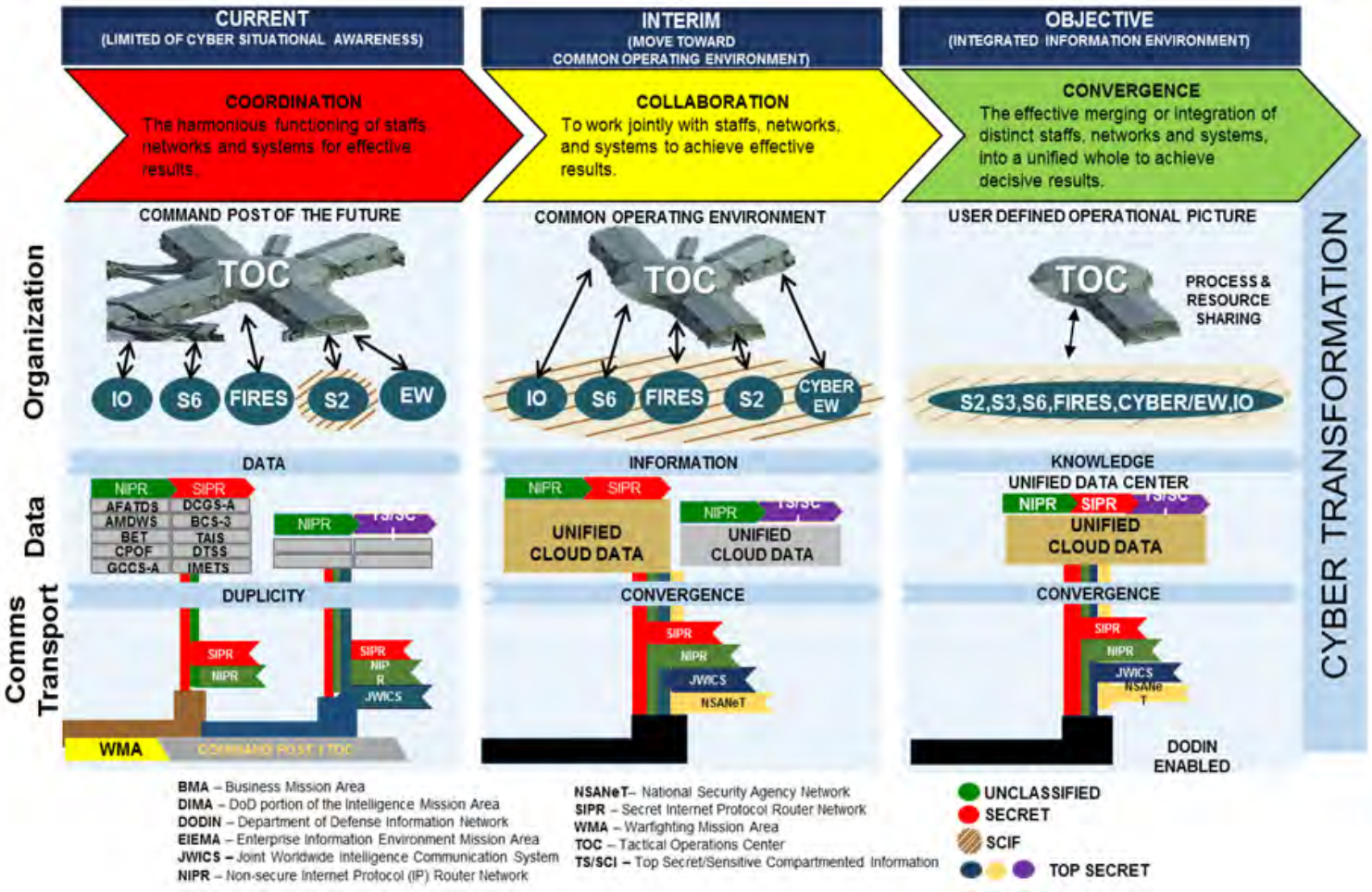


Figure 4 – Example of Convergence to enable Mission Command & Enterprise Capabilities

Initiative B: Increase Support to the Enterprise

Cyber CoE will lead efforts to develop Army cyber capabilities across DOTMLPF and work with a broad community of stakeholders across the warfighting functions to fulfill the vision of having cyberspace operations capabilities from the enterprise to the tactical edge. This effort will entail integrating cyber doctrine, concepts, tools, and planning capabilities, as well as ensuring the appropriate training and education is flexible and adaptable to meet increasingly complex challenges as threats to Army operations evolve.

Initiative C: Establish an Active, Fully Coherent Cyber Community of Interest (COI)

Cyber CoE and Team Gordon will achieve synergy of effort among both operational and institutional stakeholders by enhancing senior-leader concurrence through multiple forums, such as senior leader forums and multi-branch working groups. We will ensure success by working across the COI and integrate JIM perspectives. Figure 5 is a preview of the stakeholders we must work with immediately to garner support and positively impact the Cyber CoE and Team Gordon community.

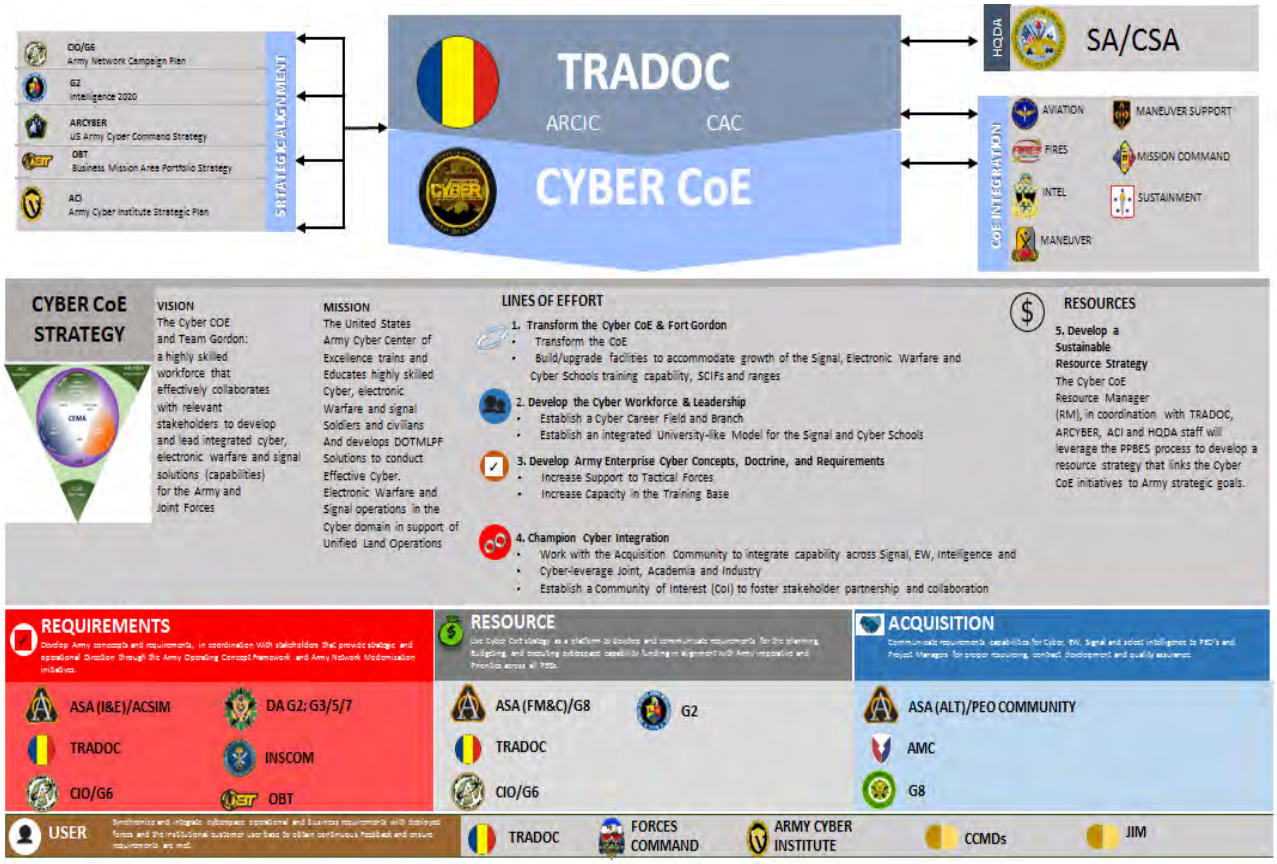


Figure 5 – Cyber CoE Stakeholder Community & Relationships

A critical component of the Cyber CoE Strategic Plan is a sustainable resource strategy to build trained cyber forces and capability. Each of the first four LOEs will be accounted for in this construct. This strategy will set the conditions for effective and efficient integration of cyber forces into the operational force and transform Fort Gordon into a modern, cyber power projection platform.

The resource strategy must nest with the Army's FY18-22 program, and capitalize on year of execution opportunities to achieve the priorities set forth in the HQDA EXORD 057-14. The Cyber CoE Resource Manager (RM), in coordination with TRADOC, ARCYBER, ACI and HQDA staff will leverage the PPBES process to develop a resource strategy that link the Cyber CoE initiatives to Army strategic goals.

This resource strategy will have three (3) major components – Operational, Training, and Infrastructure. The Cyber CoE G8 will develop a plan across the POM planning window (April – November) to communicate with the Program Evaluation Group (PEG) integrators from TRADOC HQ, CIO/G-6, and ARCYBER to ensure requirements are aligned properly and not duplicated. The Cyber CoE must have equities within all PEGs.

Initiative A: Leverage the Army Planning, Programming, Budgeting, and Execution System (PPBES) Processes

The Army's PPBES process is a constant. The Cyber CoE will account for this constant to ensure resource requirements are synchronized, submitted and visible in multiple PPBES forums such as the PEGs for validation. In concert with the key stakeholders noted above, Cyber CoE will coordinate through TRADOC with the HQDA Resource Integration Group (RIG) to prioritize CoE requirements and cyber enterprise capabilities. In addition, the CoE must aggressively target the mid-year and year end forums for year of execution resource funding.

Initiative B: Influence Key Resourcing Processes

Cyber CoE is developing cyber capabilities and adapting its infrastructure to meet the needs of the Army and cannot consider the plan complete until it is fully resourced. Cyber CoE LOEs must be nested within TRADOC, ARCYBER, CIO/G-6, and DA G2 strategic plans supporting the Army Campaign Plan.

The Cyber CoE staff will work collaboratively with key stakeholders to ensure the Center's initiatives are captured within TRADOC's input to The Army Plan (TAP). The Cyber CoE must adopt an interactive engagement policy of working with the key stakeholders in order to maintain a sure foothold on the resources required to maintain its initiatives. The Cyber CoE will assist the TRADOC G3/5/7 to shape the Army Strategic Planning Guidance (ASPG) and the Army Planning Priorities Guidance (APPG). The ASPG details the Army's vision, direction, and strategic objectives. The APPG prioritizes Army capabilities to support the realization of Army strategic imperatives and to facilitate resource allocation during programming and budgeting. Next, the Cyber CoE must coordinate through TRADOC with Army Program Analysis and Evaluation (HQ G-8/PAE) to ensure its initiatives are captured in the Army Program Guidance Memorandum (APGM). The APGM provides prioritization for the six PEGs. The Cyber CoE, in collaboration with key stakeholders, will provide input to the Army Campaign Plan (ACP). Finally, the Cyber CoE must closely monitor the development of the Total Army Analysis (TAA) processes which validate/produce the operating force and the Research Development and Acquisition (RDA) Plan. The RDA Plan is a 1-n prioritized list of all RDA program packages (Management Decision Packages (MDEPs)) for the POM. Cyber CoE's engaged monitoring of the TAA and RDA Plan ensures that resource requirements remain viable and continuous.

RISK

The Cyber CoE will play a key role as the cyber domain becomes more prominent in combat operations and national security. Because our adversaries will continue to invest in technology to evade or counter Army capabilities, sufficient investment must be made now to grow our cyber workforce, modernize our infrastructure to train and educate agile, adaptive leaders and develop DOTMLPF solutions to meet these challenges.

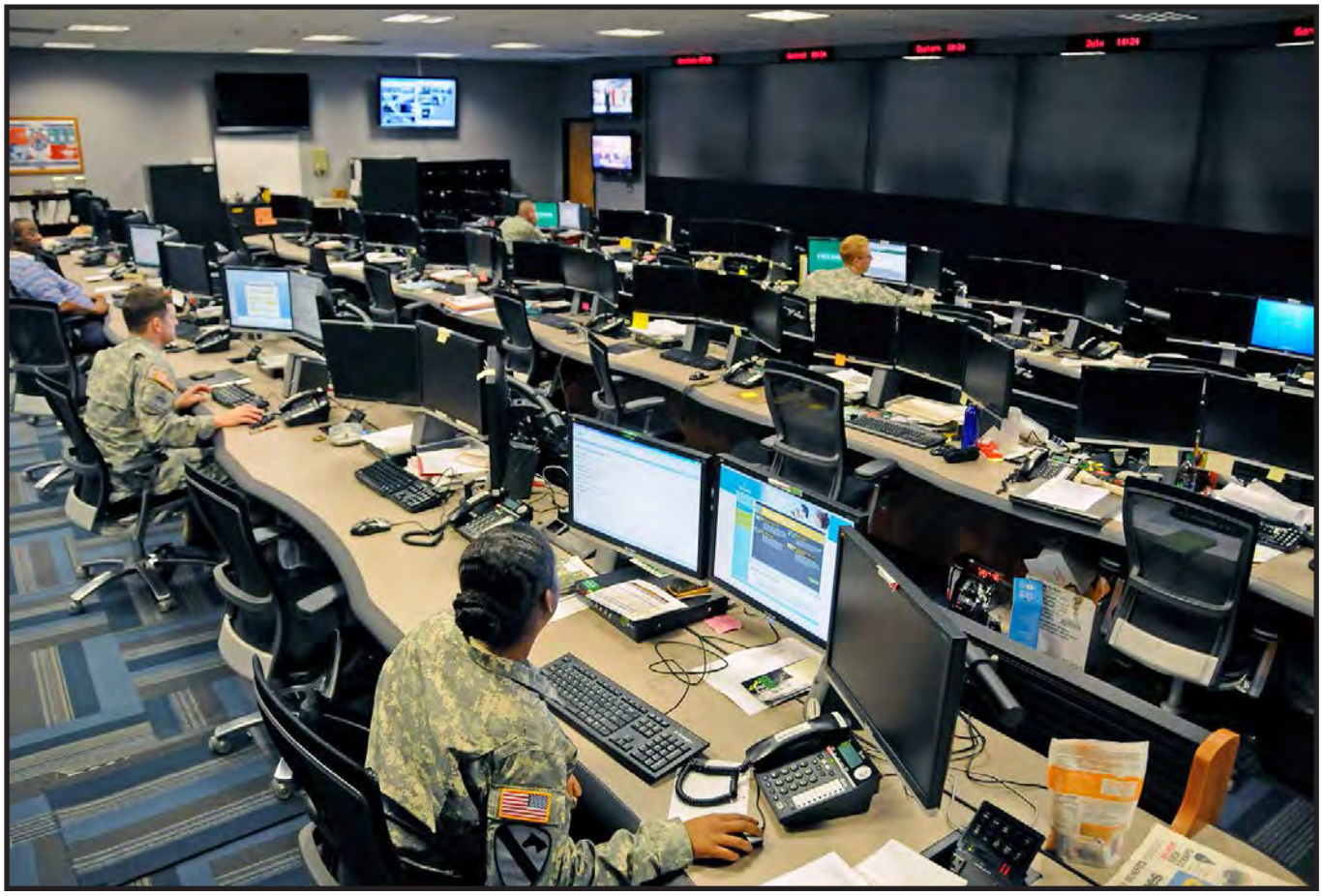
Fundamental to this strategy's success are adequate resources. The Cyber CoE faces risk in people, facilities and funding across all of its LOEs. People with the right training and skills to meet the Army's Cyber workforce requirements, modernized facilities to train and educate a "value added" cyber workforce and the funding to transform the Signal Center into a world class Cyber Center of Excellence.

To mitigate these risks, the Army must adapt to achieve high levels of readiness while also investing in future force modernization across all components (Active, Guard, Reserve). The Army must retain sufficient institutional Army capabilities to expand the force via the Cyber CoE. Improved interoperability with Joint, Interorganizational and multinational teams "provides additional methods to mitigate this risk by improving synergy across all domains and fully realizing the potential of joint combined arms maneuver." It is critical that the Cyber CoE collaborate with key stakeholders to identify and secure sufficient resources now that will support the conduct of effective cyberspace operations for ULO.

Summary

The Cyber CoE vision is clear – Integrate cyber, signal, EW, and intelligence capabilities to build operationally relevant cyber capacity and capability, train Soldiers and civilians, develop enterprise requirements which support the warfighter, and transform Fort Gordon. Adequate resourcing from the Army will be needed to achieve this vision. Our LOE's comprise essential work that must be accomplished in the next five years. Next Step – Develop a time-phased implementation plan to realize our vision by 2020. The end result is a transformed Fort Gordon and Cyber CoE as the premier cyberspace platform across the DoD and Joint communities.


TILLERY




WHERE TRADITION
Team Gordon
UNITED STATES ARMY
CYBER
CENTER OF EXCELLENCE · FORT GORDON
MEETS THE FUTURE