DEPARTMENT OF THE ARMY
UNITED STATES ARMY CYBER COMMAND/2ND ARMY
8825 BEULAH STREET
FT BELVOIR VA 22060-5246

REPLY TO
ATTENTION OF:

ARCC-CG

MEMORANDUM FOR UNITED STATES ARMY CYBER COMMAND AND SECOND ARMY

SUBJECT: U.S. Army Cyber Command and Second Army 2014 Strategy: Leading the Nation's Army in Cyberspace

1. The attached document is the United States Army Cyber Command and Second Army Strategy. It is the capstone strategic document for the Command, informed by higher level guidance and documents, that provides the Command's vision and approach to integrate all ARCYBER and Second Army activities in support of Joint and Army forces and requirements.

2. The Strategy synchronizes and integrates the efforts of the ARCYBER and Second Army staff as well as NETCOM, the Joint Force Headquarters-Cyber, 1st Information Operations Command, 780th Military Intelligence Brigade, and the Cyber Protection Brigade to fulfill our mission requirements in support of Unified Action and Unified Land Operations. Everything the headquarters and subordinate units do should be linked to the strategy and its objectives, to ensure the synchronization of efforts throughout the command.

3. This strategy supports my vision that ARCYBER and Second Army is a preeminent cyber-force that conducts decisive cyberspace operations in support of Joint and Army commands. Furthermore, it supports a concept that by 2020, ARCYBER and Second Army, with the JFHQ-C are fully operational capable and integrated at Fort Gordon, GA, collocated with NSA-G and conducting effective cyberspace operations.

4. U.S. Army Cyber Command and Second Army play a vital role in the nation's cyberspace security by ensuring freedom of action in and through cyberspace for friendly forces, and denying the same to our adversaries. To this end, the ARCYBER and Second Army Strategy: *Leading the Nation's Army in Cyberspace* serves as the guide for all ARCYBER and Second Army activities.

Thanks for the great teamwork that made this strategy possible!

Edward C. Cardon

EDWARD C. CARDON
Lieutenant General, US Army
Commanding

# United States Army Cyber Command and Second Army


# Strategy

## *Leading the Nation's Army in Cyberspace*

**18 November 2014**

# U.S. Army Cyber Command and Second Army Strategy

## *Leading the Nation's Army in Cyberspace*

## Table of Contents

# Army Cyber Command and Second Army

# Strategy

## *Leading the Nation's Army in Cyberspace*

*"America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas."* (Statement by the President on the Cybersecurity Framework, February 12, 2014, President Obama)

*"We will invest in new and expanded cyber capabilities and forces to enhance our ability to conduct cyberspace operations and support military operations worldwide, to support Combatant Commanders as they plan and execute military missions, and to counter cyberattacks against the United States."* (Quadrennial Defense Review 2014)

## Section 1: Introduction

Operations in and through cyberspace enable the Joint Force and the Army to fulfill their responsibilities in defense of the Nation. The Joint Force conducts Unified Action to achieve national objectives, and the Army contributes to this effort through Unified Land Operations. To maintain a decisive advantage, both Unified Action and Unified Land Operations depend heavily upon cyberspace capabilities for mission command, maneuver, fires and effects, intelligence, protection, sustainment and engagement. Cyberspace capabilities have continued to mature through both evolution and transformation of operations and capabilities, providing commanders with a wider range of options both singularly, or combined with other capabilities.

Headquarters, Department of the Army established United States Army Cyber Command and Second Army as the primary Army headquarters responsible for Cyberspace Operations[1] in support of Joint and Service requirements. Army Cyber Command is the Army Force Component Headquarters to United States Cyber

[1] Cyberspace Operations consists of Offensive Cyberspace Operations, Defensive Cyberspace Operations, and Department of Defense Information Networks Operations (DoDIN)(Joint Publication 3-12)

Command. Army Cyber Command established Joint Force Headquarters-Cyber to command and control cyber forces supporting Combatant Commands and select Army requirements. The Army Cyber Command Commanding General is also the Commanding General for Second Army. Second Army serves as the single point of contact for Army missions and functions related to reporting on, assessing, planning, coordinating, integrating, synchronizing, directing and conducting Army network operations. The Army Cyber Command Staff Principals serve as the Second Army Staff Principals. Together, Army Cyber Command and Second Army ensure all Army and Joint cyberspace operations are fully integrated and synchronized, and appropriate Army stakeholders fulfill all statutory responsibilities. In addition to the cyberspace missions, the Commander, Army Cyber Command conducts Information Operations missions for the Army in accordance with AR 525-20.

Section 2: Environment

This strategy accounts for the current operating environment described in the *U.S. Army Operating Concept: Win in a Complex World 2020-2040*, and looks out to 2020 to anticipate future changes. The threat will continue to grow in width and depth, vulnerabilities will increase across the lifetime of systems and platforms, the complexity will increase as more capabilities are networked together, and the adversaries' barriers to entry for cyberspace operations will continue to decrease. The complicated and complex nature of the information and operating environment, innovations in information technologies, the continuing development of operational concepts in and through cyberspace, and the competition for talented cyberspace professionals create both opportunities and challenges. This domain requires constant improvement, adaptation and innovation at the speed of operations for both the operating and information environments.

Section 3: Purpose

Given a highly dynamic and complex operating environment, the Army Cyber Command and Second Army Strategy, *Leading the Nation's Army in Cyberspace*, integrates all of the Army Cyber Command and Second Army activities and operations. The strategy includes all Active and Reserve Component Army Cyberspace and Information Operations forces for a Total Army approach to Cyberspace Operations and Information Operations that support the Army's ability to Prevent, Shape, and Win. This strategy not only guides what we must do, but also who we must become. Defining our values and fostering an innovative culture are foundational elements of this Strategy.

Everything the headquarters and subordinate units do should be linked to the strategy to ensure the synchronization of efforts throughout the command for the next five years.

Section 4: Strategic Approach

*Mission, Vision, Values, Objectives, Priorities and Method*

Mission. United States Army Cyber Command and Second Army directs and conducts cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace, and to deny the same to our adversaries.

Commander's Vision and Desired State 2020

Commander's Vision. A preeminent cyber-force that conducts decisive cyberspace operations in support of Joint and Army commands.

Desired State 2020. In 2020, Headquarters Army Cyber Command and Second Army, and Joint Force Headquarter-Cyber, are at full operational capability and integrated at Fort Gordon, Georgia, collocated with National Security Agency-Georgia and conducting cyberspace operations. Defensive Cyberspace Operations, Offensive Cyberspace Operations, and Department of Defense Information Network operations are planned, coordinated, integrated and synchronized to defend Army networks, to support Army Service Component Commands and to support designated Combatant Commands. Organizations conducting cyberspace operations are properly aligned through Army and Joint processes for command and control. The Joint Information Environment and Army network modernization is fully implemented and contributing to the defense of Army Networks. United States Army Network Enterprise Technology Command is an operational headquarters that is the lead for conducting Department of Defense Information Network cyberspace operations for the Total Army, and other missions as directed, through Army Cyber Command and Second Army. The Cyber Mission Force build is complete, and the Army is further organized with cyber capabilities to support Corps level and below. The Army has world-class cyberspace planners at echelon. Structures and processes are in place for the integration of enablers with a focus on the integration of Information Operations, Electronic Warfare and space capabilities. Army Cyber Command and Second Army have a unique and special relationship with the United States Army Cyber Center of Excellence and with the Army Cyber Institute. Army Cyber Command and Second Army, as an organization, embraces innovation and continuous experimentation, and has established mechanisms, to gain and maintain the initiative in this dynamic environment. Army Cyber Command and Second Army are partnered with select government, industry, academia, and partners and Allies to create a collaborative network to best meet mission requirements.

In 2020, cyber is institutionalized within all Army processes. There is an Army advocate on the HQDA Staff. The Army has policies that help recruit, develop, manage, and retain the talent for its professional, innovative, imaginative, and collaborative workforce. The Army has institutionalized individual and collective cyber training at

echelon with a persistent training environment. Army Cyber Command and Second Army have an established resourcing strategy within the Planning Programming Budgeting System. Finally, the Army has created a resourcing, capabilities and acquisition process and strategy to meet the full range of cyber requirements.

Army Cyber Command and Second Army Values. In addition to the Army values, Army Cyber Command and Second Army embrace a core set of values for organizations and people that display Character, are Trusted and Professional, Innovative and Imaginative, and Collaborative. These values not only help define who we are, but also who we want to be.

Objectives. The following three objectives are enduring and they provide the purpose for Army Cyber Command and Second Army activities. These three objectives must be accomplished for mission success.

- The Army has trained and ready Army cyber forces with cyberspace capabilities to Prevent, Shape, and Win.
- Army Cyber Command supports Combatant and Army Commands with and through Cyberspace Operations to enable mission accomplishment.
- Army networks are secure, reliable, and postured to conduct or support operations in all domains.

Priorities. The following priorities focus the command's efforts and must inform the development of the Campaign Plan.

(1) Operationalize Cyberspace Operations to Support Combatant and Army Commands at Echelon.

(2) Pursue a more Defensible Network.

(3) Organize, Man, Train and Equip Ready Cyber Forces.

(4) Deliver a Strong Cyber Narrative.

Method. The centerpiece of our method is campaign planning that includes synchronized supporting plans and activities to enable us to accomplish the mission. We will have plans, policies and activities that organize the command, and build the required capabilities and capacity to achieve our objectives. This framework will be iterative and dynamic vice static. Finally, we will resource all of our efforts adequately, and provide mechanisms for us to evaluate and adjust our approach as required. Within an "ends, ways, means" construct, these plans, in conjunction with the priorities, constitute the "ways" of this strategy, while the objectives are our "ends". The "means" within this construct are our forces, staffs and resources.

Section 5. Strategy Implementation, Management Assessment and Risk

Strategy Implementation and Planning Requirements. Strategy implementation begins with the Campaign Plan. The Campaign Plan gives direction to unify and synchronize our efforts and links ends, ways, and means to the Strategy. It provides guidance for development of supporting plans by delineating authorities, responsibilities and establishing guidelines for resource allocation, and instituting procedures for strategy and risk management and command assessment.

Operationalizing Cyberspace and supporting Army and Joint force requirements are addressed in planning efforts such as *Support to Combatant Commands, Support to Army Service Component Commands, Information Operations, Corps and Below,* and *Joint Force Headquarters-Cyber Operations.* Our efforts for a more defensible network are incorporated in plans like *Department of Defense Information Network Operations* and *Network Modernization.* Our organizational, man, train, equip, and posture requirements are covered in efforts such as *Rationalization/Optimization, United States Army Network Enterprise Technology Command Integration, Cyber Mission Forces, Reserve Component Integration* and *Posture/Move to Gordon.* A *Strategic Communications* plan addresses the requirement to deliver a strong cyber message and narrative. Finally, the *Assessment* and *Resourcing* plans support the maintenance of all the efforts and activities.

This list of plans and planning efforts is by no means all-inclusive. The Campaign Plan addresses the current and anticipated planning efforts, and is updated and adjusted as required to ensure mission success.

Our success relies heavily upon cooperation and coordination with Headquarters, Department of the Army, Army Commands, United States Cyber Command, Joint and Department of Defense partners, as well as interagency cooperation and coordination. We must be adept at partnering with military, governmental, civilian and academic stakeholders in cyberspace. This synchronization requires a perspective that goes beyond the use of traditional forces and resources as we conduct more effective operations in cyberspace.

Strategy Management. The Campaign Plan provides a comprehensive Strategy management and resource process. This process synchronizes operations and activities through the development of supporting plans consistent with the commander's intent and priorities. It provides mechanisms to adjust plans and activities to keep pace with the operational environment, to provide appropriate feedback to the commander, and to identify methods and frequency of formal reviews, assessments, guidance updates. Finally, the management process requires subordinate units and directorates to quantify resource requirements and shortfalls that inform the budgeting and programming request process.

Strategy Assessment. The Campaign Plan directs a continuous and comprehensive assessment process. The assessment process begins with mission analysis during supporting plan development when the commander and staff develop desired outcomes and the tasks to achieve them. Metrics for outcomes and tasks must be established in order to measure progress toward achieving key objectives. The staff and commanders adjust plans, tasks, resources, operations and activities based on assessments to ensure objectives are met. The strategy and command assessment process draws upon the individual assessment of plans to provide the commander, on a regular/periodic basis (quarterly, bi-annually, etc), a report of how well the command is achieving its goals and objectives, and where adjustments to the strategy and supporting plans are warranted. Although this assessment report to the commander is periodic, the process is continuous and directly tied to the commander's decisions throughout planning, preparation and execution of Army Cyber Command's strategy.

Risk. The Campaign Plan addresses balancing risk to mission command. Army Cyber Command and Second Army must be able to balance increasing threats and increasing mission sets against resources. The growth in technology and missions outpace our current and projected resources and our plans and operations must address ways to mitigate the increasing risks.

Section 6. Conclusion

United States Army Cyber Command and Second Army, in concert with Army, Joint, Department of Defense, and interagency partners and cyberspace stakeholders, play a vital role in the Nation's cyberspace security by ensuring freedom of action in and through cyberspace for friendly forces, and denying the same to our adversaries. To this end, the Army Cyber Command and Second Army Strategy: *Leading the Nation's Army in Cyberspace* serves as the guide for all Army Cyber Command and Second Army activities. It is a dynamic strategy for a dynamic environment. The strategy provides overall planning guidance that underscores the importance of building and defending a more defensible network, organizing for a more efficient command, and conducting effective cyberspace operations in support of Army and Joint Forces that maximize the benefits of cyberspace while managing the risks.