Army Cyber Command Strategic Plan

Session: 2
Track: Army Cyber Command

COL Thomas Goss
Army Cyber Command / 2nd Army
Army Cyber Command plans, coordinates, integrates, synchronizes, directs, and conducts network operations and defense of all Army networks; when directed, conducts cyberspace operations in support of full spectrum operations to ensure U.S./Allied freedom of action in cyberspace, and to deny the same to our adversaries

• Serve as Cyber Proponent
• Coordinate IO
ARMY CYBER VISION 2020:

⭐ A Professional team of elite, trusted, precise, disciplined warriors defending Army networks, providing dominant full-spectrum effects in and through cyberspace, enabling Mission Command and ensuring a decisive global advantage...SECOND TO NONE!
Army Cyber Forces in 2020

★ Integrated Full-Spectrum Cyber Capabilities
  • Army Cyber warriors are integrated in cyber organizations and unit staffs
  • Full spectrum cyber operations are routine and pervasive
  • Within, through, and from one Army Enterprise network

★ Achieve Cyber Domain Operational Freedom
  • Full-spectrum operations in order to seize, retain, and exploit the initiative
  • Seek the same level of freedom to operate that Army forces achieve in the Land domain

★ Ensure Mission Command
  • Mission Command is enabled by cyberspace capabilities
  • Cyberspace Operations and Mission Command are inherently linked
Army 2020 Strategy: In order to defend and advance our national interests, the US Army Force must balance resources and risk among four priority objectives:

- **Prevail** in today’s wars
- **Prevent** and deter conflict
- **Prepare** to defeat adversaries and succeed in a wide range of contingencies
- **Preserve** and enhance the All-Volunteer Force

To implement this strategy, it is imperative to develop cooperative joint and Army efforts to assess space and cyberspace architectures, vulnerabilities, and solutions.

These objectives reflect a strategic approach that can evolve and adapt in response to a changing security environment.
**Prevail.** In today’s conflicts and the conflicts in 2020, as in the past, America must ensure the success of its forces in the field. This requires:

- Future Army forces conducting CAM / WAS have the ability to operate in a **degraded network environment** and still enable mission command and deliver cyberspace effects commanders require
- Army Cyber Forces with **Active Defense, Information Operations, and full spectrum cyberspace capabilities** supported by cyber-based intelligence and a shared cyberspace situational awareness
- A **globally responsive streamlined cyberspace C2** that achieves Unity of Effort while supporting Deployed Commanders with access to the cyberspace enterprise and full spectrum capabilities
- **Improved cyberspace defense in depth**, resiliency of networks, surety of data and communication, and full spectrum capabilities allow Army Forces to have freedom to operate and confidence in its cyberspace operations
- Achieving and sustaining success in cyberspace operations requires development of a **sufficient number of cyber professionals** trained and certified to operate across the **full spectrum of cyberspace capabilities**
**Prevent.** Preventing the rise of threats to U.S. interests requires the integrated use of diplomacy, development, and defense to help build the capacity of partners to maintain and promote stability. This requires:

- Future Army forces apply an expanded understanding of combined arms that includes leveraging the cyberspace domain as well as incorporating **cyberspace Intelligence Preparation of the Environment and shared situational awareness** of cyberspace threats and what is happening on networks (at machine speed)
- **Cyberspace operations to be integrated into Theater Campaign Planning and Theater Security Cooperation** as a mechanism to build partner capacity and coordinate Partner cyberspace operations and deterrence activities
- New operational concepts, such as **active defense operations**, enhance effectiveness by enabling more rapid actions and more comprehensive actions to protect Army networks, critical infrastructure, information, and resources
- Cyberspace operations requires **JIIM integration** (joint, interagency, intergovernmental, and multinational)
- An investment in new capabilities and technologies to design networks for **better situational awareness, information assurance, and compliance**
Prepare. If deterrence fails and adversaries challenge our interests with the threat or use of force, the United States must be prepared to respond in support of U.S. national interests. This requires:

- Deployable, scalable, and agile Army cyberspace formations which have trained in live, virtual, and constructive cyberspace training areas against a “World-Class” cyber opposing force (OPFOR) conducting cyberspace missions integrated into all contingency plans
- An Army culture in which cyberspace security, and the ability to operate effectively in cyberspace are viewed as priorities and users think of its information technologies and networks as a contested operational domain
- A convergence of cyberspace and cyber-related operations (IO, EW, Space, IA, etc)
- An cadre of Army cyberspace experts to protect and defend its information networks and critical cyberspace infrastructure backed by investment in the latest technologies to enable our forces to operate in cyberspace under a wide range of conditions, including in contested and degraded environments

PREPARE is the Key to PREVENT and PREVAIL
Required Capabilities: PRESERVE

**Preserve and Enhance All-Volunteer Force.** In order to succeed in today’s wars and prepare for the future, the Department of Defense must ensure the long-term viability of the All-Volunteer Force, its most precious military resource. This requires:

- The Army to develop and prepare cyber forces (both AC/RC) for a broad range of missions and **remain ready to conduct full-spectrum cyber operations** necessary to contribute to the attainment of national policy aims.
- These formations to have enough capacity to support rotational, cyclical readiness models to **provide a predictable and sustainable supply of modular forces** to combatant commanders with a surge capacity for unexpected contingencies.
- Army personnel to have **a greater appreciation for the threats and vulnerabilities** in the cyberspace domain and to have the skills to counter those threats and reduce those vulnerabilities at the user, system administrator, and enterprise levels.
- The Army to have a cyberspace **Training and Leader Development Program** to link the people, skills, and training as the required critical linchpin to achieve required cyberspace capabilities.

**PRESERVE AND ENHANCE is the Key to PREPARE**
Army Cyber Roadmap

LINES OF EFFORT

LOE 1: Operationalize Cyber

LOE 2: Grow Army Cyber Capacity and Capabilities

LOE 3: Recruit, Develop, Retain Army Cyber Professionals

ENABLING ACTIVITIES

People as a Priority

Strategic Communications

Build Headquarters Functional Capacity

VISION:

Professional team of elite, trusted, disciplined warriors defending Army networks, providing dominant full-spectrum cyber, enabling Mission Command and ensuring a decisive global advantage… SECOND TO NONE!
**Operationalize Cyber:** Army Cyber Command will leverage and integrate current capabilities and authorities across the physical, informational, and cognitive dimensions of the information environment to ensure optimal effects in the cyberspace domain, as well as, enable effects in the other domains of air, land, sea, and space.

**MAJOR OBJECTIVES:**
- Develop Cyberspace Intelligence Collection Capability
- Conduct Intelligence Driven Integrated Cyberspace Ops
- Enable Mission Command
- Streamline Army Cyberspace C2
- Advocate for Revised Authorities
Operationalizing Cyber Priorities

- Develop a **Common Cyberspace Operating Picture**
- Develop an **Active Defense Strategy**
- Conduct Cyberspace Operations that **achieve effects Cdrs require**
- Determine and Implement Requirements for **Cyber-Based Intelligence**
- Develop a CONOPs for a **scalable, deployable Cyber JTF**
- Develop supporting **cyberspace planning for key contingency plans**
- Operationalize a **Cyber Center Concept**
- Develop a concept for **Protection of Cyberspace Critical Infrastructure**
- Synchronize with **IO/EW/EMSO and Space** Operational Elements
- Identify and Prioritize **Reserve Component IO and Cyberspace Requirements**
Grow Army Cyberspace Capacity and Capabilities: As the Army’s force modernization proponent for cyberspace operations, Army Cyber Command’s proponent office will define the needed force structure, develop critical doctrine and concepts, and integrate cyberspace operations into the Army’s institutional processes in order to ensure dominance in the new cyberspace domain.

MAJOR OBJECTIVES:
★ Determine and Prioritize Cyberspace Requirements
★ Integrate Cyberspace Operations into Institutional Training
★ Develop the Future Cyber Force
★ Develop Capstone Cyberspace Doctrine and Concepts
★ Develop a World-class Cyberspace Proponent
Priorities for Growing Army Cyberspace Capacity and Capabilities

- Develop an operational concept for a **Responsive Global Army Cyber C2 Structure**
- Develop a **Cyber Center Concept**
- Develop a Long Term **Training and Leader Development Strategy**
- Develop **World Class Cyber OPFOR** (WCCO) Plan
- Prepare an Assessment of the Need for a **Cyber Center of Excellence**
- Conduct Force Management Reviews to Inform Future TAA/POM Cycles
- Conduct a Force Design Update (FDU) at all Echelons.
Recruit, Develop, and Retain Cyber Professionals: While technology plays an important role in the cyberspace domain it is the cyber professionals, not the technology that will win on the 21st century’s battlefields.

MAJOR OBJECTIVES:
★ Determine and Prioritize Cyber Personnel Requirements
★ Develop the Future Cyber Warrior
★ Integrate Reserve Component Units into Cyber Ops
Define **Cyber Personnel, Training, and Leader Development Requirements**

Define a **Cyber Warrior Development Strategy** (AC, RC and DA civilians)

Create **Cyber Programs of Instruction** for Inclusion in Schoolhouses at all levels of Individual Training

Propose an Incentive Plan for HQDA to **Recruit the required Cyber Work Force**

Propose an Incentive Plan for HQDA to **Retain their Cyber Work Force**

Determine the Knowledge, Skills and Abilities **Standards for Future Cyber Personnel**
Enabling Activities are the command’s internal building blocks that support our lines of effort, major objectives and thus permeate all of Army Cyber Command’s operational efforts.

ENABLING ACTIVITIES:

⭐ People as a Priority

⭐ Strategic Communications

⭐ Build Headquarters Functionality
Way Ahead

★ Discussion at Commanders’ Conference (26-27 Aug)

★ Revisions and Staffing (Sept)

★ Roll-Out (Early Oct)

★ Presentation / Display at AUSA Symposium (Oct)
★ COL Thomas Goss (Chief, Strategic Initiatives Group)
  • Thomas.j.goss.mil@mail.mil
★ LTC Karla Brischke (Lead Planner, ARCC Strat Plan)
  • Karla.j.brischke.mil@mail.mil