# Building a Cyber Force

## A Roadmap for Implementation

*By Joshua Stiefel, Lt. Gen. Ed Cardon (Ret.), Lauryn Williams, Taylar Rajic, Matt Pearl, and Erica D. Lonergan.*

### KEY TAKEAWAYS

- The United States faces an increasingly severe cyber threat environment shaped by nation-state adversaries, criminal cyber actors, and the rapid advancement of AI-enabled cyber capabilities. China and Russia continue targeting U.S. and allied critical infrastructure, while advances in frontier AI models are accelerating vulnerability discovery, cyber exploitation, and the scale and speed of malicious cyber activity.
- The Pentagon's current approach to cyber force generation remains fragmented across the military services. Cyberspace is the only warfighting domain without a military service responsible for organizing, training, and equipping forces.
- A U.S. Cyber Force should be responsible for generating offensive and defensive cyber forces for the joint force. CSIS recommends a Cyber Force with approximately 20,000 active-duty personnel, 3,500–5,000 National Guard personnel, and roughly 5,000–6,000 civilian and contractor personnel. This could be achieved within 12–18 months following a presidential decision or legislative action.
- The Cyber Force should focus specifically on force generation for offensive and defensive cyber operations, while existing military services retain responsibility for service-specific networks, systems, and internal cybersecurity operations.

## BACKGROUND AND CONTEXT

In September 2025, CSIS, in partnership with the Cyber Solarium Commission 2.0 project at the Foundation for Defense of Democracies, launched the Commission on U.S. Cyber Force Generation. The commission was organized with the following premise in mind: If the U.S. president were to direct the establishment of a Cyber Force—an independent, Title 10 military service focused on force generation for the cyber domain—what would that force look like and how would it be built?

Rather than revisiting debates about whether a Cyber Force should exist, the commission developed a detailed roadmap for standing one up—examining how the United States could generate cutting-edge offensive and defensive cyber capabilities, recruit and retain top talent, and elevate cyberspace as a warfighting domain on par with land, sea, air, and space. The key findings and recommendations from that roadmap are outlined below.

## LEGISLATIVE AND POLICY IMPLICATIONS

The Pentagon's current approach is structurally misaligned with how the U.S. military has organized itself for warfighting since the Goldwater-Nichols Act of 1986. For the land, air, sea, and space domains, a single service holds primary responsibility for organizing, training, and equipping forces—known as force generation. No equivalent service exists for cyberspace, creating an organizational gap that existing reforms have not resolved.

Cyber Force is currently being explored in legislative proposals. As requested under Section 1544 of the 2025 National Defense Authorization Act (NDAA), Congress directed the National Academies of Sciences, Engineering, and Medicine to conduct a study looking at the feasibility of standing up an independent military service dedicated to the cyber warfighting domain. The yet-to-be released study will assess the cost, benefit, and impact of a separate armed service with other options, including enhancing existing cyber forces and alternate organizational models. Additionally, in the 2027 NDAA, Senator Kirsten Gillibrand (D-NY) is planning to introduce an amendment to establish a Cyber Force under the Army, similar to how the Space Force sits under the Air Force and the Marine Corps sits under the Navy.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

## CHALLENGES AND RISKS

The current U.S. cyber force generation model, sourcing personnel directly from four services with their own priorities and culture, is cumbersome and inefficient. No service within the DOD has primacy for cyber force generation, resulting in inconsistent approaches to recruiting, initial training, education, career progression pathways, and compensation for cyber force generation across five different services.

Existing reforms, including CYBERCOM 2.0, are insufficient to address the Pentagon's underlying structural challenges in cyberspace. While CYBERCOM has gradually acquired more service-like authorities, the current model continues to blur the line between force generation and force employment in ways that mirror organizational problems Congress sought to address through the Goldwater-Nichols reforms. A commonly observed issue within the Cyber Mission Force includes officers assigned to junior roles without any relevant training or experience who are expected to figure it out once they check onboard.

These issues reveal dangerous gap between the centrality of cyberspace for modern warfighting and the U.S. military's persistent inability to generate the capabilities necessary to deter, compete, fight, and win in the cyber domain. Absent structural change, the current model will continue to fall short of keeping pace with an increasingly severe cyber threat environment.

## RECOMMENDATIONS

- Update the Department of Defense Directive 5100.01 to formally establish the Cyber Force's mission and responsibilities.
- Determine whether the Cyber Force should be aligned within the Department of the Army or established within a stand-alone Department of the Cyber Force.
- Establish new personnel management, training, and career development pathways optimized for cyber operations.
- Realign existing cyber-related funding and authorities into a unified Cyber Force budget structure.
- Develop transition authorities and implementation timelines that minimize operational disruption to ongoing cyber missions.

## Additional Resources and Contact Information

Joshua Stiefel, Lt. Gen. Ed Cardon (Ret.), Lauryn Williams, Taylar Rajic, Matt Pearl, and Erica D. Lonergan, "CSIS Commission on U.S. Cyber Force Generation," CSIS, June 3, 2026, https://www.csis.org/analysis/csis-commission-us-cyber-force-generation.

For more information, contact **Chloe Himmel** at 202.775.3186 or **chimmel@csis.org**.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

## Force Generation Functions of a Cyber Force

| Function | Key Responsibilities and Activities |
|---|---|
| Man (Organize) | • **Recruitment:** Attract highly specialized technical talent, selecting for quality.<br>• **Personnel Management:** Administer pay, morale, welfare, and medical support.<br>• **Personnel Transition:** Realign personnel from existing services into the new Cyber Force (prioritizing adaptability and rapid experimentation).<br>• **Force Composition:** Manage a ~30,000-person force (20,000 active-duty commissioned and warrant officers, 3,500–5,000 National Guard, and 5,000–6,000 civilians and contractors).<br>• **Career Pathways:** Establish dual-track (technical and managerial) advancement models for mission-, technical-, and capability-focused leaders. |
| Train | • **Force Preparation:** Train and certify offensive and defensive cyber operators.<br>• **Culture and Doctrine:** Develop cyber concepts, doctrine, tactics, techniques, and procedures.<br>• **Education:** Deliver professional military education (PME) and specialized cyber leadership training.<br>• **Readiness:** Assume the role of joint force trainer, providing standardized training for cyber forces<br>• **Cyber Force Generation and Training Command:** Generate, sustain, and certify ready cyber forces for operational employment. |
| Equip | • **Infrastructure:** Operate facilities, systems, and supporting infrastructure.<br>• **Budgetary Control:** Manage dedicated cyber funding (with an initial budget of approximately $10–$11 billion).<br>• **Intelligence Support:** Provide foundational all-source cyber intelligence capabilities. |

Source: CSIS Commission on U.S. Cyber Force Generation.