REVISED

CYBER FORCE GENERATION MODEL

IMPLEMENTATION PLAN OVERVIEW

United States
Department *of* War

DEPARTMENT OF WAR 2025

DEPARTMENT of WAR
CYBERCOM 2.0
FORCE GENERATION MODEL

Call to Action

For several years, the Department of War (DoW) has recognized the approach to building cyber talent is not keeping pace with the rapidly evolving and increasingly contested cyberspace domain. Adversaries are investing heavily in cyber capabilities and building forces specifically designed to operate in this domain. Meanwhile, the Department of War is constrained by traditional force generation models that, while effective for conventional forces, fail to fully address the unique requirements of cyberspace operations.

This misalignment has created significant challenges for the Department in recruiting the right people with the right aptitude and skillsets, in retaining our most skilled and experienced operators in the face of lucrative private-sector opportunities, and to providing the hyper-specialized, agile training needed to win against our nation's adversaries. Our legacy force generation model is inconsistent, hindering our ability to adapt at speed and scale to counter threats like Volt Typhoon and Salt Typhoon, and quickly integrate emerging technologies like artificial intelligence. To secure the nation's interests, we must generate cyber forces equipped to operate with precision, agility, and lethality. CYBERCOM 2.0 is the vehicle for achieving that vision.

The CYBERCOM 2.0 Model

The Secretary of War approved CYBERCOM 2.0, a fundamental reimagining of how the Department of war builds and develops the Department's cyber forces. This initiative is not merely an incremental adjustment, but a deliberate and comprehensive overhaul designed to deliver greater operational outcomes for the Joint Force. CYBERCOM 2.0 efficiently synchronizes the authorities provided to Commander, U.S. Cyber Command (USCYBERCOM) in Title 10, U.S. Code, section 167b (the legal authorities that grant the Commander, USCYBERCOM broad authority over cyber mission forces) with the authorities and activities of the Military Departments. As a cornerstone of the Department's broader strategy, CYBERCOM 2.0 works in concert with other initiatives—such as validating and updating our cyber force design and employment models—to ensure maximum operational outcomes for the Joint Force. CYBERCOM 2.0's purpose extends beyond cyberspace; this initiative is an integral Joint Force capability that must be integrated across all warfighting domains, sending a clear message to our adversaries of the Department of War's focus on maintaining cyber superiority in support of our national interests. At its heart, CYBERCOM 2.0 is a commitment to our cyber warriors, providing them with the careers, training, and support they deserve.

DEPARTMENT of WAR
CYBERCOM 2.0
FORCE GENERATION MODEL

Previously, talented military cyber operators might spend three years in a critical cyber assignment before being required to move to an unrelated role, causing their unique skills to atrophy. Faced with a choice between a non-cyber role and a lucrative private sector offer, many chose to leave the service. Under the CYBERCOM 2.0 model, those same operators can build long-term careers in cyberspace. They can deepen their expertise through advanced training and multiple tours, earn incentive pay that recognizes their mastery, and eventually transition to a role where they train the next generation, keeping their invaluable experience in the force.

CYBERCOM 2.0 is founded on three essential pillars that will drive the Department's cyber forces for years to come.

Pillar 1 - Domain Mastery: The DoW is fundamentally shifting away from a compliance-based training paradigm to one that fosters deep, career-long expertise. Our objective is to cultivate a cadre of cyber professionals who achieve true mastery in cyberspace, rather than rotating through cyber assignments as generalists. This approach builds a cyber force better capable of addressing emerging threats, such as adversaries exploiting industrial control systems in critical infrastructure or leveraging artificial intelligence to automate cyberattacks. CYBERCOM 2.0 enables increased influence by the Commander, USCYBERCOM in the talent management of the Department's cyber forces. For example, instead of cyber operators rotating out after a basic qualification, they will have a career path that allows for extended tours in the Cyber Mission Force (CMF), followed by an assignment with a Military Service (Service) cyber unit to broaden their experience and bring their deep expertise back to their Service formations. This model cultivates unrivaled experts who possess a deep portfolio of experience in specific, mission-critical areas.

Pillar 2 - Specialization: The cyber domain is incredibly diverse; as such, a traditional one-size-fits-all approach to force generation is ill-suited to deliver the operational outcomes required. CYBERCOM 2.0 establishes dedicated pathways for our cyber forces to develop deep expertise in highly specialized fields such as cloud security architecture, industrial control systems, and artificial intelligence. This will result in the formation of dedicated units of specialized experts aligned to critical missions, such as a team with expertise in space asset protection or another focused on securing critical energy infrastructure.

Pillar 3 - Agility: The threat landscape in cyberspace evolves with unparalleled speed. As such, the Department requires a force capable of rapid adaptation and dynamic allocation of talent to ensure we maintain a proactive posture against emergent threats. In practice, this means that if a new vulnerability is discovered in a widely used cloud architecture, a specialized team with

expertise in that area can be rapidly assembled and deployed to mitigate the threat, rather than pulling personnel from unrelated, mission-essential tasks.

CYBERCOM 2.0 Attributes

To bring these pillars to life, CYBERCOM 2.0 is built upon seven foundational force generation attributes. While each attribute offers individual merit, their true power lies in their synergy, which creates an exponential effect on our ability to generate and sustain talent.

1. **Targeted Recruiting and Assessments**: The Department is shifting from general recruitment to targeted talent acquisition by leveraging USCYBERCOM's operational insights to enhance the Service recruiting enterprises. By employing advanced tools like a Cyber Assessment Battery, the Department can better identify individuals who possess the inherent aptitude and problem-solving skills for cyber warfare, ensuring the right people are matched to the right work roles. This targeted approach ensures the Department matches cyber talent with mission requirements.

2. **Incentives for Recruitment and Retention**: To remain competitive with the private sector, we are implementing a robust system of incentive pay and retention bonuses designed to reward mastery and specialization. For instance, a master-qualified Cyber Operator might earn a significant monthly bonus, similar to other low-density, high-demand specialties across the Joint Force. We will also standardize incentive pay across all Services, ensuring operators performing the same mission with the same skillset receive equitable compensation.

3. **Tailored and Agile Training**: The Advanced Cyber Training and Education Center (ACTEC) serves as our hub for advanced and specialized training. It delivers mission-specific skills and knowledge on demand, ensuring our forces remain ahead of technological advancements and adversarial tactics. For instance, if a new adversarial tactic is identified, the ACTEC can rapidly develop and deliver a training module—pulled from in-house expertise, industry, or academia—to relevant cyber forces, ensuring they are prepared to counter the threat. The ACTEC ensures our teams aligned against the most consequential targets have the advanced training resources pulled from the most cutting-edge capabilities at the Department's disposal.

4. **Tailored Assignment Management**: The Department is engineering career paths, informed by USCYBERCOM, that enable sustained operational engagement, while ensuring deliberate career progression. This will allow a cyber operator to build a comprehensive portfolio of

experience across multiple mission sets, such as completing an extended tour on a National Mission Team followed by an assignment with a Service's tactical cyber unit. This approach forges unrivaled domain mastery rather than forcing our best talent to move on after a single tour.

5. **Specialized Mission Sets**: We are developing dedicated units of experts focused on highly specialized missions, such as the protection of space assets or the defense of critical infrastructure. These teams will constitute the world's leading authorities in their respective fields. For example, within CYBERCOM 2.0, we can cultivate teams trained specifically to defend satellite communications and GPS systems, while other teams specialize in protecting power grids and transportation networks. Another team might focus on developing accesses for sensitive systems.

6. **Integrated Headquarters and Combat Support**: Our tactical cyber teams will be provided with dedicated headquarters and combat support elements. This structure ensures they have the leadership, resources, intelligence support, and institutional backing necessary to focus on and execute their missions effectively, without being pulled away to perform administrative or other ancillary functions.

7. **Optimized Unit Phasing**: To maintain high readiness and prevent operator burnout, we are instituting a unit phasing model that creates a sustainable operational tempo. CYBERCOM 2.0 will create a rotational cycle where a team member spends a rotation on a mission set, followed by a dedicated period for training and reconstitution. This keeps our personnel fresh and effective over the long term and ensures their operational experience is reinvested across the force.

CYBERCOM 2.0 Enablers

The CYBERCOM 2.0 attributes are driven and supported by three critical enabler organizations:

1. **Cyber Talent Management Organization (CTMO)**: serves as the main integration point between USCYBERCOM and the Service talent management organizations to discover, assess, select, and retain elite cyber talent. By embedding liaison officers with all Service branches, the CTMO will coordinate recruitment strategies and leverage data to identify and fill critical mission gaps across the force.

2. **Advanced Cyber Training and Education Center (ACTEC)**: acts as the central delivery point for advanced, mission-specific training. It rapidly identifies emerging requirements,

maintains a centralized catalog of cutting-edge training from both internal and external partners in industry and academia, and ensures our forces have access to the right knowledge at the time and place needed. The ACTEC will lead USCYBERCOM's effort to drive training and education partnerships with industry and academia, and to deliver those capabilities at the required scale to the operational force.

3. **Cyber Innovation Warfare Center (CIWC)**: designed to deliver end-to-end solutions to the CMF at the speed of need. The CIWC serves as the focal point for our research partnerships and spearheads the development of not just technology, but also non-material aspects such as new tactics, techniques, and procedures and doctrine. By maintaining close ties to the operational force, the CIWC can identify requirements and deliver critical capabilities much faster than traditional military acquisition processes. By pairing rapid technological innovation (material and non-material) to critical operational requirements, USCYBERCOM will be able to adapt to meet the dynamic challenges of the cyber domain.

The Path Forward

A strong and integrated national cyber workforce is essential for protecting the American way of life. The cyber forces developed under CYBERCOM 2.0 will be on the front lines defending the critical infrastructure we all rely on, while simultaneously engaging the most critical threats posed by adversaries who seek to do our nation harm. This initiative directly enhances the security and resilience of our nation against the most consequential cyber threats.

These seven attributes and three enablers are integral to the success of CYBERCOM 2.0. The DoW is implementing foundational force generation initiatives now—such as developing career paths, creating screening assessments, and establishing advanced training—that are essential elements of any cyber force generation model. The success of this new model will be measured by clear metrics, including improved retention rates for critical cyber roles, faster deployment of new cyber capabilities, and enhanced readiness levels across our CMF. The core pillars of mastery, specialization, and agility are indispensable for meeting the Department's strategic objectives, irrespective of any future organizational model decisions. Underpinning all the CYBERCOM 2.0 initiatives is the Department's commitment to a closer partnership with both industry and academia to secure our homeland and harness America's unparalleled strength in talent and innovation.

The true strength of our nation lies in the potential of its people. With CYBERCOM 2.0, the Department of War is unleashing that potential to build and integrate a world-class cyber force across all warfare domains.