

1. The next war the United States fights will begin in cyberspace.

Cyberattacks will almost certainly be used by an adversary in the opening phases of a crisis or conflict to [target the U.S. homeland](#) and America's ability to project power. U.S. adversaries have already demonstrated the capability and willingness to target critical American and allied infrastructure through cyber means. Establishing a new military cyber service, a dedicated Cyber Force, would best prepare America's national defense to address future threats.

2. Cyberspace is the only warfighting domain without a dedicated military service.

More than two decades ago, the Department of Defense (DoD) defined cyberspace as an operational domain of warfare — joining land, air, sea, and space. Yet cyberspace remains the only domain without a dedicated military service. Now more than ever before, [effective cyber operations](#) require a service branch focused entirely on this vital work. Establishing a Cyber Force would demonstrate a recognition that cyber operations are a core part of America's cutting-edge approach to warfighting.

3. Establishing a Cyber Force would facilitate better use of legal authorities and Guard/Reserve components.

Americans expect their military to protect them from foreign adversaries, but cyberspace is largely owned by companies and private individuals. Accordingly, building out a Cyber Force presents the opportunity to [create structures with different authorities](#) — especially for critical infrastructure protection and homeland defense — that can best leverage the experience and expertise found in the civilian population. Driving attention to the military's relationship with the private sector will enable more effective integration and collaboration with robust Guard, Reserve, and auxiliary components. To attract the best talent, the service would likely need to offer new incentives and flexible career paths tailored to technical experts. Establishing a Cyber Force would best accelerate innovation in recruiting, acquisition, and R&D freed from the weight of traditional service bureaucracies.

4. Responsibility for cyber forces is fragmented across five different services.

The U.S. Army, Navy, Air Force, Marine Corps — and soon, Space Force — are each separately responsible for the recruitment, initial training, promotion, and retention of their own cyber forces. None of the services is optimized to perform this task, and none has prioritized generating and sustaining these service members, resulting in [widespread struggles](#) to recruit and retain top cyber talent. Additionally, while Cyber Command also has training responsibilities, there are limitations to what the command can realistically impose on the services with respect to force generation. Establishing a Cyber Force would best improve military readiness and specialization.

5. Current force generation results in inconsistent cyberspace proficiency.

Because each of the services separately manages its own cyberspace personnel, there is no common understanding of the core competencies, expertise, or standards of conduct expected of cyber warriors, from junior enlisted through senior officers. Accordingly, there are [extraordinary inconsistencies](#), inefficiencies, and shortfalls in the proficiency and [readiness](#) of personnel provided to Cyber Command. Establishing a Cyber Force would best standardize cyberspace capabilities, enhance joint operations, and avoid costly duplication.

6. Cyber force levels are well below what is needed.

The number of U.S. offensive and defensive cyber forces has remained [effectively static](#) over the past 15 years despite growing cyber threats. Over the same period, China has invested heavily in cyber warfare, with cyber troop levels now estimated to be 10 times larger than those of the U.S. military. The current U.S. force generation model [cannot be scaled up](#) quickly enough at a sufficient level of quality to meet this threat. Establishing a dedicated Cyber Force would grow the size and quality of the force in response to the scale of this threat.

7. Cyber warriors are distinctive from soldiers, sailors, airmen, Marines, and Guardians.

The requirements for fighting and winning in cyberspace are different from those of the other warfighting domains, requiring personnel with unique aptitudes and interests. Ideal recruits to serve in cyber roles are more likely to come from the high school computer science club than the football team. Current challenges in recruiting fail to appreciate that cyberspace is a complex, opaque, and dynamic operating environment that requires an ever-changing mix of technologies and [in-depth knowledge](#). Establishing a Cyber Force would best foster a distinct organizational culture that attracts and supports these warfighters.

8. Tasking Cyber Command with force generation is not the answer.

The 1986 Goldwater-Nichols Act established clear roles and responsibilities for the military services as force generators and the unified combatant commands as force employers. While Cyber Command (the force employer) has gained increasing “service-like” authorities, there are [limitations](#) to what it can realistically achieve. For example, when setting standards for the services to meet, the command cannot enforce them. Establishing a Cyber Force would create one entity singularly focused on developing cyberspace warfighting concepts and doctrine as well as attracting and managing the right personnel.

9. Overall cyber readiness is now dangerously limited.

Today’s [critical gaps](#) in recruiting the right people, retaining an adequate complement of quality personnel, and mastering the skills needed to succeed in cyberspace warfighting have left the U.S. military underprepared to conduct defensive and offensive cyber operations. Establishing a Cyber Force would best prioritize recruiting, training, and equipping cyber forces aligned to the evolving demands of the digital environment.

10. The U.S. model is an outlier compared to other cyber powers.

Other cyber powers, including America’s primary adversaries, have established a single military service that is responsible for recruiting, training, and equipping cyber talent. Last year, China disbanded its Strategic Support Forces and established three separate elements, including one solely responsible for cyber. With this change and earlier adjustments, China’s cyber capabilities have grown substantially. Establishing a Cyber Force would bring the U.S. military into alignment with global trends among cyber powers.

For more information, see “[United States Cyber Force: A Defense Imperative](#)” by Dr. Erica Lonergan and Rear Adm. (Ret.) Mark Montgomery, Foundation for Defense of Democracies, March 2024.