



Space to the Air Force, Underwater to the Navy: Why Cyber Belongs to the Army

Published on 04/06/2026

The debate on the governance of new conflict domains is heating up globally. In the United States, the bipartisan proposal to place the nascent **Cyber Force** under the aegis of the U.S. Army (within the National Defense Authorization Act) outlines a path that many Western allies, including Italy, are watching closely.

Why is this tripartition – **Space to the Air Force, Underwater to the Navy, and Cyber to the Army** – not just a bureaucratic division, but a doctrinal choice that is symmetrical, balanced, and strategically coherent?

The Symmetry of Domains: Natural Extensions

The assignment of traditional and emerging domains follows a logic of "natural extension" of the historical competencies of the individual Armed Forces.

- **Air Force and Space:** Orbital space is the vertical continuation of the atmosphere. Those who dominate the third dimension (flight) already possess the technological culture, management of vectors, satellites, and radar surveillance systems necessary for the *Space Economy* and *Space Defense*.
- **Navy and Underwater:** The underwater world (the so-called *underwater*) is the abyssal continuation of the sea surface. The protection of underwater data cables, pipelines, and acoustic warfare requires an environmental culture that only those who navigate possess.
- **Army and Cyber:** At first glance, cyberspace seems immaterial. In reality, **the network rests on the mainland**. Server farms, communication nodes, fiber optic backbones, and critical infrastructures are physically rooted in the territory. The Army, the territorial force par excellence, has the mission of protecting and controlling the mainland, making it the natural guardian of the physical infrastructure of the web.

The 3 Good Reasons to Give Cyber Leadership to the Army

Beyond geographical continuity, there are operational, demographic, and doctrinal reasons that make the Army the ideal candidate for the *leadership* of the Cyber domain.

The Centrality of the "Human Factor" (Manpower and Recruitment)

Cyber warfare is not conducted with machines, but with minds. As highlighted by recent analytical studies (including those by the *Foundation for Defense of Democracies*), a Cyber force requires a critical mass of personnel (about 10,000 units for an autonomous structure).

The Army, historically being the largest Armed Force in terms of personnel, possesses the logistical, academic, and large-scale recruitment structure suitable for absorbing, training, and managing a vast number of specialists without cannibalizing its internal operational capabilities.

Cyber as "Modern Artillery" in Land Combat

In contemporary wars, the Cyber attack is not just a tool of espionage, but a tactical support weapon. Shutting down enemy radars, hacking adversary drones, or disrupting a headquarters' communications before an attack are operations comparable to the use of artillery or military engineering. The integration of *cyber effects* into the doctrine of land combat (combined arms) is vital for the Army to protect its soldiers and assets on the field.

The Resilience of National Critical Infrastructures

In the event of a massive cyber attack that cripples a country's electricity, water, or transport networks, the response does not occur in the virtual world, but in the streets. The Army is the only force equipped with heavy logistical capabilities and territorial capillarity to ensure the continuity of the State, protect the physical nodes of the network, and exercise civil defense while technicians restore systems.

A Balance of Mirrors

Entrusting the *lead* of Cyber to the Army does not mean diminishing the role of the Navy and Air Force (which will still maintain their indispensable specialized cyber components for ships and aircraft), but it means creating a **perfect triumvirate of emerging domains**.

In this scheme, each Armed Force receives the responsibility of the domain that best suits its intrinsic nature:

Armed Force	Traditional Domain	Emerging Domain	Strategic Focus
Air Force	Air	Space	High vectors and orbital surveillance
Navy	Sea	Underwater	Protection of seabeds and marine communication lines
Army	Land	Cyber	Defense of the physical infrastructure of the web and tactical support

This distribution ensures a perfect balance of inter-force power, avoids overlaps, and ensures that no domain is neglected. Cyber needs mass, land, and tactical integration: three elements that the Army has had in its DNA for centuries.

News link: <https://www.defenseone.com/policy/2026/05/cyber-force-service-branch-proposal/413863/?oref=d1-homepage-river>