Center for International Maritime Security

CYBER WAR, SPACE

WHY IT IS TIME FOR A U.S. CYBER FORCE

AUGUST 29, 2018 | DAVE SCHROEDER | LEAVE A COMMENT

By Dave Schroeder and Travis Howard

The proposal to create a U.S. Space Force has cyber professionals wondering about the government's national security priorities. While spaceborne threats are very real — some of which cannot be suitably described in a public forum — the threats posed in cyberspace have been all too real for over a decade, and include everything from nuisance hacks by nation-states, to the weaponization of social media, to establishing beachheads on our nation's electric grid, or the internet routers in your own home.

Since 2009, incremental improvements have been made to the nation's ability to operate in cyberspace during this period. The establishment of U.S. Cyber Command (USCYBERCOM) — first subordinate to U.S. Strategic Command, and then elevated to a Unified Combatant Command (UCC) — and the formation of the 133 teams that comprise the Cyber Mission Force (CMF) are chief amongst them.

Yet despite all of the money and attention that has been thrown at the "cyber problem" and for all of the increased authorities and appropriations from Congress, the nation's offensive and defensive cyber capabilities suffer from inefficiency and a lack of a unified approach, slow to non-existent progress in even the most basic of cybersecurity efforts, and a short leash that is inconsistent with the agility of actors and adversaries in cyberspace. Our adversaries continue to attack our diplomatic, information, military, economic, and political systems at speeds never before seen.

The discourse surrounding the formation of a dedicated service for space defense has captured the American imagination, and for good reason. Since World War II, America has shown her ingenuity and innovation, and the success of the U.S. Air Force provides a historical model for how a combat-ready, specialized fighting force can be built around a new warfighting domain. However, a force structure has already taken shape within the U.S. military that would logically translate to its own service, and the operational culture it would both allow and cultivate would greatly enhance the effectiveness of national security.

It is past time to form the U.S. Cyber Force (USCF) as a separate branch of the United States Armed Forces.

America's Position in Cyberspace is Challenged Daily — but it can be Strengthened

It's no surprise that a wider breadth of adversaries can do more harm to American interests through cyberspace than through space, and for far less cost. In the aftermath of the 2008 Russo-Georgian War — the cyber "ghosts" of which are still alive and well in 2018 — Bill Woodcock, the research director of the Packet Clearing House observed, "You could fund an entire cyberwarfare campaign for the cost of replacing a tank tread, so you would be foolish not to."

Deterring and responding to Russian hybrid warfare in cyberspace, countering Chinese cyber theft of U.S. intellectual property, shutting down state and non-state actor attacks, defending American critical infrastructure — including the very machinations of our democracy, such as voting and political discourse and even cyber defense of U.S. space assets are just some of the heavy-lift missions that would occupy a U.S. Cyber Force.

Admiral (retired) Jim Stavridis recently described four ways for the U.S. and allied nations to counter challenges like the weaponization of social media and multifaceted information warfare campaigns on Western democracy: public-private cooperation, better technical defenses, publicly revealing the nature of the attacks (attribution), and debunking information attacks as they happen. A dedicated U.S. Cyber Force, with the proper ways and means to do so, could accomplish all of these things, and be a major stakeholder from day one.

Admiral (ret.) Mike Rogers, former Director, National Security Agency (NSA)/Chief, Central Security Service (CSS) and Commander, USCYBERCOM, in his 2017 testimony before the Senate Armed Services Committee, cautioned against prematurely severing the coupling of cyber operations and intelligence that has been the hallmark of any success the U.S. has thus far enjoyed in cyberspace. General Paul Nakasone, the current DIRNSA/CHCSS and Commander, USCYBERCOM, made the same recommendation in August 2018. Despite increased resourcing of USCYBERCOM by both Congress and the Executive Branch, operational authorities in cyberspace are hamstrung by concerns about blending Title 10 military operations with Title 50 intelligence activities, along with negative public perception of the NSA. The relationship between USCYBERCOM and NSA requires a complicated (and classified) explanation, but blending cyber operations with rapid, fused intelligence is vital, and go hand-in-hand — to separate them completely would be to take the leash that already exists around USCYBERCOM's neck and tie their hands with it as well. Offensive and defensive operations in cyberspace are two sides of the same coin — and intelligence is the alloy between them. Standing up a U.S. Cyber Force would also enable a deliberate re-imagining of this unique symbiosis, and a chance to — very carefully — lay out lines of authority, accountability, and oversight, to both prevent overreach and justifiably earn public trust.

The above challenges could be addressed in part by refining the existing structures and processes, but the real sticking point in USCYBERCOM's sustainment of fully operational cyber forces lies in how we build forces ready to be employed. Force generation of the CMF through the various armed services' manning, training, and equipping (MT&E) their own cyber warriors is an inefficient and weak model to sustain a combat ready force in this highly-specialized and fast-moving mission area.

Cyber resources play second-fiddle to service-specific domain resourcing; for example, the Department of the Navy has an existential imperative to resource the maritime domain such as shipbuilding and warplanes, especially during a time of great power competition. The cyber mission is secondary at best, and that's not the Navy's fault. It just simply isn't what the Navy is built or tasked to do. This same reality exists for our other military services. Cyber will always be synergistic and a force multiplier within and across all domains, necessitating the need for the services to retain their existing internal cyber operations efforts, but feeding the joint CMF is ultimately unsustainable: the CMF must sustain itself.

The Cyber Force is Already Taking Shape

USCYBERCOM, NSA, the 133 teams comprising Cyber Mission Force — are approaching full operational capability in 2019 — and the operational and strategic doctrine they have collectively developed can now more easily transition to a separate service construct that more fully realizes their potential within the joint force. There is a strong correlation here with how the U.S. Army Air Force became the U.S. Air Force, with strong support in Congress and the approval of President Truman. The DoD has begun revising civilian leadership and building upon cyber subject matter expertise, as well, with the creation of the Principal Cyber Advisor (PCA) to the Secretary of Defense — a position that Congress not only agreed with but strengthened in the Fiscal Year 2017 National Defense Authorization Act. Such a position, and his or her staff, could transition to a Secretary of the Cyber Force.

The footprint would be small, and room in Washington would need to be carved out for it, but the beginnings are already there. Cyber "culture" — recruiting, retention, and operations — as well as service authorities (blending Title 10 and Title 50 smartly, not the blurry "Title 60" joked about in Beltway intelligence circles) would all benefit from the Cyber Force becoming its own service branch.

Perhaps one of the greatest benefits of a separate cyber branch of the armed forces is the disruptive innovation that would be allowed to flourish beyond the DoD's traditional model of incremental improvement and glacial acquisition. The cyber domain, in particular, requires constant reinvention of techniques, tools, and skillsets to stay at the cutting edge. In the early 2000s, operating in a cyber-secure environment was thought to mean a restrictive firewall policy coupled with client-based anti-virus software. In 2018, we are developing human-machine teaming techniques that blend automation and smart notifications to fight and learn at machine speed. Likewise, the traditional acquisition cycle of military equipment, often taking 4-6 years before prototyping, just doesn't fit in the cyber domain.

In short, the "cyber culture" is an incubator for innovation and disruptive thinking, and there are professionals chomping at the bit for the chance to be a part of a team that comes up with new ideas to break norms. A dedicated acquisition agency for cyber would be an incubator for baked-in cybersecurity controls and techniques across the entire DoD acquisition community. The Defense Innovation Unit (DIU) — recently shedding its Experimental "x" — is proving that something as simple as colocation with innovation hubs like California's Silicon Valley and Austin, Texas, and a willingness to openly engage these partners, can deliver innovative outcomes on cyber acquisition and much more. Similarly, the Cyber Force must be free to exist where cyber innovation lives and thrives.

Creating the USCF has other benefits that would be felt throughout the military. The Army, Navy, Marines, and Air Force, relieved of the burden of feeding the offensive and national CMF and paying their share of the joint-force cyber bill, can better focus on their core warfighting domains. This doesn't absolve them of the need for cybersecurity at all levels of acquisition, but a USCF can be an even greater advocate and force-multiplier for DoD cybersecurity efforts. Services can and should retain their service-specific Cyber Protection Teams (CPTs), which could be manned, trained, equipped, and tactically assigned to their service but also maintain ties into the USCF for operations, intelligence, and reachback. Smart policies and a unity of effort can pay big dividends here, as the services would naturally look to such an organization as the resident experts.

Extreme Challenges with Existing Forces

Much has been made of the extensive difficulties faced by our military services for the recruiting and retention of cyber expertise in uniform. Brig. Gen. Joseph McGee, Deputy Commanding General (Operations), Army Cyber Command (ARCYBER), described an example in which a talented cyber prospect "realized he'd make about the same as a first lieutenant as he would in a part-time job at Dell." Examples like this are repeated over and over from entry-level to senior positions, and everything in between, on issues from pay to culture. In the military, being a cyber expert is like being a fish out of water.

The service cyber and personnel chiefs have made a clear case before the Armed Services Committees of both houses of Congress for the urgent need for flexibility on issues such as rank and career path for cyber experts specifically. Cyber needs were repeatedly cited as the rationale for the need for changes to restrictive military personnel laws. Many of these items were indeed addressed in the Fiscal Year 2019 (FY19) National Defense Authorization Act (NDAA), with provisions which may now be implemented by each service in what is hailed as the biggest overhaul to the military personnel system in decades:

- Allow O-2 to O-6 to serve up to 40 years without promotions, or continue service members in these grades if not selected for promotion at a statutory board
- Ability for service members to not be considered at promotion boards "with service secretary approval" — for instance, to stay in "hands on keyboard" roles
- No need to meet 20 years creditable service by age 62 for new accessions (no need for age limit or age waiver above 42 years old for direct commissions)
- Direct commissions or temporary promotion up to O-6 for critical cyber skills

But even these provisions do not go far enough, and the services are not obligated to implement them. When the challenges of pay, accessions at higher rank, physical fitness, or military standards in other areas come up, invariably some common questions are raised.

A common question is why don't we focus on using civilians or contractors? In the case of naval officers, why don't we make them Staff Corps (instead of Restricted Line), like doctors and lawyers who perform specialized functions but need "rank for pay" and/or "rank for status?" What about enlisted specialists versus commissioned officers?

The answer to the first question is easy in that we do use civilians and contractors across the military, extensively. The reason this is a problem is that we also need the expertise in uniform, for the same legal and authorities reasons we don't use civilians or contractors to drive ships, lead troops, launch missiles, fly planes, and conduct raids.

As for making them Staff Corps officers or equivalent in the other services, the Navy, for instance, has been talking about going the other direction: making officers in the Navy Information Warfare community designators (18XX) unrestricted line, instead of restricted line, like their warfare counterparts, or doing away with the unrestricted line vs. restricted line distinction altogether. This is a matter of protracted debate, but the reality is that some activities, like offensive cyberspace operations (OCO) and electronic attack (EA), are already considered forms of fires under Title 10 right now — thus requiring the requisite presence of commissioned officers responsible and accountable for the employment of these capabilities. The employment of OCO creates military effects for the commander, and may someday be not just a supporting effort, or even a main effort, but the only effort, in a military operation.

Under the Navy's Information Warfare Commander Afloat Concept, for the first time the Information Warfare Commander of a Carrier Strike Group, the Navy's chief mechanism for projecting power, can be a 18XX Officer instead of a URL Officer. If anything, we're shifting more toward URL, or "URL-like", and the reality of the information realm as a warfighting domain is only becoming more true as time goes on, if not already true as it stands today.

So what about our enlisted members? They're doing the work. Right now. And the brightest among them are often leaving for greener pastures. But still for reasons of authorities, we still need commissioned officers who are themselves cyber leaders, subject matter experts, and practitioners.

None of this is to say that direct commissioning of individuals with no prior service as officers up to O-6 is the only solution, or that it would not create new problems as it solves others. But these problems and all of the concerns about culture shock and discord in the ranks can also be solved with a distinct U.S. Cyber Force which accesses, promotes, and creates career paths for its officers as needed to carry out its missions, using the full scope of flexibility and personnel authority now granted in the FY19 NDAA.

Another major challenge is the lack of utilization of our reserve components. Many members of our reserve force have multiple graduate degrees and 10-15 years or more of experience, usually in management and leadership roles, in information technology and cybersecurity. We have individuals in GS/GG-14/15 or equivalent contractor and other positions, who are doing this work, every day, across the Department of Defense (DOD), the Intelligence Community (IC), academia, and industry.

Yet reservists are currently accessed at O-1 (O-2 under a new ARCYBER program), need to spend 3-5 years in training before they are even qualified to mobilize, or for the active components to use in virtually any operational or active duty capacity. And that's after doing usually a year or more of non-mobilization active duty, for which nearly all employers don't give differential pay because of existing employment policies, including in federal GS/GG positions.

We have very limited mechanisms and funding sources to even put reservists on active duty at NSA or USCYBERCOM, where our service cyber leadership repeatedly states we need people the most. And in the rare instances we manage to put people on some type of active duty in a cyber role in their area of expertise, it often is not a "mobilization" under the law — which means a person is now an O-2 or O-3, and with that "level" of perceived authority and experience to those around them. And they often just left their civilian job where they are recognized as a leader and expert — and easily make $200k a year.

NSOC watch floor circa 1985

National Security Operations Center (NSOC) c. 1985 — National Cryptologic Museum

Most people appreciate that you can't just magically appear as an O-6, and have the same depth, breadth, and subtlety of experience and knowledge as a O-6 with 25 years in uniform. Yet these O-6s, as well as general and flag officers, routinely retire and assume senior leadership positions in all manner of public and private civilian organizations where "they don't know the culture" — because they're leaders.

So while a person off the street doesn't have the same level of understanding of the military culture, it's incorrect to say they can't innovate and lead on cyber matters — to include in uniform as a commissioned officer. We're not so special to imply that you can't lead people and do the critical work of our nation, in uniform, unless you've "put in your time" in a rigid career path. It's time to change our thinking, and to establish a military service to support the realities of that shift.

Recommendations

The call for a dedicated cyber branch of the U.S. Armed Forces is not new. Admiral (ret.) Jim Stavridis and Mr. David Weinstein argued for it quite passionately in 2014, calling on national leaders to embrace cyber innovation and imploring us to "not wait 20 years to realize it." Great strides have been made in the four years since that argument was made, and we are closer than ever to realizing this vision. It will take a focused effort by Congress and the president to make this happen, as it did with the U.S. Army Air Forces becoming the U.S. Air Force in 1947. A tall order, perhaps, in today's political environment, but not impossible, especially given the desire to compromise on issues of national defense and when both Republicans and Democrats alike are seeking wins in this column.

To summarize: the threat is eating our lunch, USCYBERCOM and the CMF are nearly ready to transition to their own service branch, and the benefits of doing so are numerous:

- Sensible use of resources spent on cyberspace operations
- An incubator of disruptive and rapid innovation in the cyber domain
- Improved oversight and accountability by policy and under U.S. Code
- More efficient and sustainable force generation and talent retention

- Better alignment of service-specific core competencies across all warfighting domains
- Synergy with a unified space commander (such as cyber protection of satellite constellations)

The United States House of Representatives recently ordered the Government Accountability Office (GAO) to begin an assessment on DoD cyberspace operations as part of the FY19 NDAA. This study, due to Congress in 2019, should prove enlightening and may become a foundational effort that could be built upon to explore the feasibility of establishing the U.S. Cyber Force as a new branch of the Armed Forces. Congress could order this as soon as FY21, with the Cyber Force fully established by the mid-2020s (blazingly fast by federal government standards, but no faster than the proposed Space Force).

Conclusion

The President has also now relaxed rules around offensive cyberspace operations, perceiving the urgent need to respond more quickly to cyber threats and cyber warfare directed at the United States. We have a great stepping stone in USCYBERCOM, but with no plans to take it to the next step, even a dedicated combatant commander for the cyber domain will face challenges with the above issues for the duration of its lifespan. Similar to how we are just becoming aware of space as a distinct warfighting domain, cyber has *already been* a warfighting domain since the beginning of the 21st century. The time for a U.S. Cyber Force is now. The threat in cyberspace, and our underwhelming response to it thus far, cannot wait.

Travis Howard is an active duty Navy Information Professional Officer. He holds advanced degrees and certifications in cybersecurity policy and business administration, and has over 18 years of enlisted and commissioned experience in surface and information warfare, information systems, and cybersecurity. Connect with him on LinkedIn.

Dave Schroeder served as a Navy Cryptologic Warfare Officer and Navy Space Cadre, and is Program Manager for IWCsync. He serves as a senior strategist and cyber subject matter expert at the University of Wisconsin–Madison. He holds master's degrees in cybersecurity policy and information warfare, and is a graduate *of the Naval War College and Naval Postgraduate School. Find him on Twitter or LinkedIn.*

The views expressed here are solely those of the author and do not necessarily reflect those of the Department of the Navy, Department of Defense, the United States Government, or the University of Wisconsin–Madison.

Featured Image: National Security Operations Center floor at the National Security Agency in 2012 (Wikimedia Commons)

SHARE THIS:

Email Tumblr Print Facebook 295 LinkedIn Google Twitter Reddit Pinterest

LIKE THIS:

Like

Be the first to like this.

Related

Towards A National Cyber Force "Department of the Air Force – US Cyber Corps"
December 21, 2015
In "Capability Analysis"

The Lawless Trons of Cyberspace
January 5, 2017
In "Cyber War"

Sea Control 143 - Cyber Threats to Navies with Dr. Alison Russell
September 6, 2017
In "Cyber War"

CYBER FEATURED NSA SPACE USCYBERCOM