Whither Cyber Force?

CW3 Jakob K. Kaivo
uscf@jkk.org

April 12, 2021

The US military is at a crucial turning point in its history. For the first time ever, a man-made domain of warfare is accessible. Existing branches of service are attempting to operate in this domain. This paper argues, with examples primarily taken from the Army, that their efforts are insufficient, and the inevitable conclusion is the establishment of a United States Cyber Force.

Contents

1 Introduction

The need for US military operating in the cyber domain is evident by the fact that every existing branch of service has established a cyber component. The existence of United States Cyber Command (USCC) further amplifies this need. It is my contention that the service cyber components and USCC are not enough, and the nation is in desperate need of a new branch of service, which I will consistently call United States Cyber Force (USCF).

For background information, I am a Chief Warrant Officer 3 in the Army with over 19 years of service. Of those 19+ years, the last 10 have been primarily focused in cyber operations. From 2011 to 2014, I served as an operator in the Remote Operations Center (ROC) at National Security Agency-Hawaii (NSAH). From 2014 to 2017, I was a participant in Computer Network Operations Development Program (CNODP). Since early 2019, I have been a developer in the Cyber Solutions Development Detachment (CSD). Beyond that, prior to enlisting, I spent five years (1996-2001) working in the private sector at an Internet Service Provider (ISP), doing system and network administration, network security, and network programming. I have a Masters degree in Computer Science from The George Washington University. All of which is to say, I am very familiar with the cyber realm, and especially how the Army, National Security Agency (NSA), and USCC operate in it.

In this paper, I will advocate for the establishment of USCF. I will use examples based on my experience to show where the Army is institutionally incapable of properly executing the nation's cyber missions. I will not make explicit parallels with other branches of service, but my conversations with service members from the Air Force, Coast Guard, Navy, and Marine Corps indicate that the institutional problems faced by the Army are not unique. It is safe to assume that wherever I reference an Army-specific term, the service-equivalent of each branch can be substituted with approximately the same results.

In addition to using the term USCF as established fact, I will also refer to Hackers (with a capital H) to refer to members of this theoretical organization, in the same manner in which Soldier is a referent to a member of the Army.

This paper is not organized in any particular fashion. Most sections, apart from this introduction, can be taken as stand-alone mini essays. The order of their presentation has no significance. The tone is informal. I do not use The Army Writing Style, for reasons that should be readily apparent. You may have already noticed that occasionally I use first-person. Sometimes I'll even use humor. I will not apologize.

2 Army Air Corps 2.0

The parallels between the current evolution of Army Cyber Command (ARCYBER) and the Army Air Corps are astounding. Both were prompted by human invention enabling access to a new domain. Both were originally subordinate to the Army's Signal Corps. Both represent highly technical fields. Both re-

quired establishing new work roles to handle those technical tasks. Both led to establishment of new incentive programs to recruit and retain those specialized technical workers (flight pay for aviators; Cyber Assignment Incentive Pay (CAIP) for Hackers). And, just as the Army Air Corps inevitably led to the establishment of the US Air Force, the only logical conclusion of ARCYBER (and, indeed, all of USCC) the creation of USCF. For these reasons, I have frequently referred to the current status quo as "Army Air Corps 2.0".

The question is how long will it take? From the Wright Brothers' first flight at Kitty Hawk in 1903 to the establishment of the Air Force in 1947, the Army Air Corps went through 44 years of growing pains[1]. It's more difficult to define the start of the cyber era, though. Do we use the connection of the first ARPANET nodes in 1969? If so, USCF is already 8 years late in coming. Maybe the transition to Internet Protocol (IP) based protocols in 1983? Or the transition from government controlled ARPANET and NSFNET to the open Internet in 1989? At the very latest, we have to point to June 1998, when B Company 742nd MI Battalion was designated as the Army's first computer network operations element. By that timeline, we are 23 years into Army Air Corps 2.0. It is my sincerest hope that it will not be another 21 years before USCF is realized.

3 Domains

Warfare is separated by domains. Historically, nations establish different militaries responsible for different domains. Land is the oldest domain. Land warfare and the existence of armies predates written history, and likely dates to the first stone-age tribes squabbling over a limited resource, taking up stick and stone to establish dominance. Navies followed the invention of boats quickly. And air forces came into being within a half-century of the first man-powered flight.

The existence of separate branches reflects the inherit core differences that exist when operating in separate domains. Land warfare is just fundamentally different to naval warfare, and air warfare is radically different from the others. The recent establishment of the US Space Force is, at least in part, predicated on this same notion.

Another reason for separate branches is to establish primacy for each domain. Both the Army and Navy have aviation assets, but none of them operate without Air Force liaison, ensuring that combined forces don't accidentally have an Army helicopter, Navy fighter, and Air Force bomber attempting to transit the same air space at the same time.

We have these for the naturally occurring domains. We have an Army for

[1] One of the largest of these pains was the court-martial of MG Billy Mitchell. I sincerely hope nobody has to be court-martialed for USCF to become a reality, especially not me. Then again, if the choice is the status quo for another 20 years, or I get court-martialed and the USCF becomes a reality next year, I would be willing to make that sacrifice. But, please don't court-martial me.

land warfare. A Navy for maritime. An Air Force for the sky. And even a Space Force for the universe beyond our atmosphere. Each a radically different environment that a human being can exist, and conduct warfare, in.

But then we have the cyber domain. It is unique among all others as being the first man-made domain. Sea, air, and space required invention to access, but the domains have always existed. The cyber domain didn't exist prior to the invention of networked computers, and while man has dreamt of flight since time immemorial, networked communications weren't even conceptualized until the 18th century.

Let me emphasize that last point: The very concept of a cyber domain wasn't even possible to think about in the most abstract form until very recently in human history. How, then, can anyone seriously propose applying stratagems that predate the wheel?

We cannot. Everything about the Army is constructed around conducting land warfare. Systems, policies, procedures, regulations, and doctrine all fall short when attempting to manage Hackers and accomplish operations in the cyber domain.

4 Health and Fitness

It's important that members of any military service are healthy. By the very nature of their employment, they can be called upon at any time to participate in stressful activities with tight time constraints. In the cyber realm, this stress can escalate quickly, as the Hacker can be one misstep from accidentally committing the virtual equivalent of shooting Archduke Franz Ferdinand. Being in good health is vital to being able to deal with that stress.

The Army has a focus on fitness. It's important to make a distinction between health and fitness. Fitness is a component of health, but it is not the only one. Mental health plays a major role in overall health, and is arguably more important to Hackers than it is to Soldiers. The Army focus on fitness rather than comprehensive health is a poor fit for Hackers.

It's not even clear that the Army is good at managing fitness. As of this writing, the Army is still struggling to implement the Army Combat Fitness Test (ACFT). The name itself is revealing. It isn't even about fitness, it's about "combat fitness". Hackers don't need to be "combat fit". The average Hacker should never be near combat. Their actions should *prevent* combat.

Focus aside, the ACFT doesn't even seem to be a good fit for measuring fitness. The test it replaced, the Army Physical Fitness Test (APFT), was decidedly not. It didn't measure fitness, only the specific ability to perform the three events that comprised it (push-ups, sit-ups, and a 2 mile run). The ACFT suffers from the same fundamental flaw: it does not measure fitness, only the ability to perform specific tasks. In the case of the ACFT, the tasks are somewhat arbitrary. For instance, the Standing Power Throw. In this task, the Soldier must throw a medicine ball backward over their head some distance. Supposedly, this relates to some Warrior Task and/or Battle Drill. While I

am far from the most deployed Soldier in the Army, in my total 39 months of contingency operations, not once did I need to do anything that even remotely resembled throwing a medicine ball over my head.

There is a reason that Congress has prohibited the Army from implementing the ACFT fully until an independent investigation has been completed.

Even if the ACFT *is* a good way to measure "combat fitness", it's a terrible way to measure the health of Hackers. Again, Hackers should not be involved in combat, they should be involved in preventing (or enabling) combat. A Hacker does not need to be able to throw a medicine ball over 5 meters behind their back over their head; a Hacker needs to be able to move a mouse and type on a keyboard. A Hacker does not need to be able to run two miles in a fixed time. A Hacker does not need to be able to run two miles at all. A Hacker does not need to be able to run two meters. A Hacker needs to have mental endurance to spend hours on a stressful operation without losing focus and physical health to endure the same without having a heart-attack or other cardiovascular trauma.

I don't know the ideal way to manage Hacker health. But the correct place to start is by consulting medical doctors.

5 Incentives

In hist blog post "A Field Guide to Developers", Joel Spolsky opined that "They don't care about money, actually, unless you're screwing up on the other things." While in this case, he was specifically talking about developers, the statement is largely applicable to Hackers. A Hacker tends to get more satisfaction from solving an intellectual challenge than from cashing a paycheck.

This paper is full of examples of the Army "screwing up on the other things." This is a part of the reason CAIP has been successful. But the fact that CAIP was necessary in the first place is an indicator. Hackers notice the many ways in which the Army system fails to mesh with their cyber reality, and CAIP is just enough to make them stick around (in some cases; for others, even CAIP is not enough).

That being said, USCF would still be well served with a specialized pay system similar to flight pay or medical corps incentive pay. The fact of the matter is that Hackers can, largely, get similar employment in the private sector with a salary an order of magnitude greater than they can in the military. Hacker incentive pay would never be enough to eliminate the gap, but combined with military benefits and a service that *isn't* "screwing up on the other things" could be enough to recruit and retain a force large enough and talented enough to accomplish the nation's cyber goals.

6 Leadership

Across nine enlisted, five warrant officer, and ten officer pay grades, the Army has 28 ranks. Of these, 24 are considered leaders, leaving only four ranks to be

basic Soldiers.

This makes sense, when viewed through the combat arms lens. During operations, there is a very real, ever present threat that the mission leader can be killed. Literally everyone in a combat arms unit needs to be prepared to assume leadership at a moment's notice.

Contrast this with operations in the cyber domain. On any given operation, there is a vanishingly small chance of casualties of any variety. The likelihood that a Hacker will need to take the place of a fallen mission commander is approximately zero.

In the USCF, it's more appropriate for Hackers to focus on their technical role as they progress in rank. Some work roles, such as mission commander, necessarily lend themselves to leadership, and that would be emphasized. But there is no necessary reason for every operator or analyst to be burdened with any sort of leadership role if they don't desire it. There is room in USCF for the equivalent of Vietnam-era Technical Sergeants and the like. Perhaps even an entire Military Occupation Specialty (MOS) devoted to traditional military leadership duties, which would open doors for less technical people to enjoy a fulfilling part in USCF.

7 Location

People often say that in real estate, the three most important things are location, location, and location. While the same cannot be said for military installations, location is still an important factor faced by service members of any branch. It's a huge consideration when it comes to do decide where to go next, or, indeed, whether to continue serving at all.

In the Army, location options are extremely limited for Hackers. We are, effectively[2], limited to Fort Meade, MD, and Fort Gordon, GA. That's not a lot of options, and not a particularly great selection. I know several Hackers whose recent decisions not to continue serving were influenced in part by the lack of location options.

Centralizing people makes some amount of sense for combat arms. You need to be able to amass large amount of troops to overwhelm the enemy with sheer numbers, and those troops need to train as a large unit. The larger the objective, the more troops are desired. Contrast this with operations in the cyber domain: A single computer requires a single Hacker (plus supporting Hackers, but only one on the operational keyboard). A small network can be handled by a single Hacker (plus the same amount of support). A large network can be handled by... a single Hacker (same). The economies of scale are vastly different.

Thus, the need for large numbers of Hackers in any single location is vastly diminished. Couple this with the lessons learned from COVID-19[3], especially

[2]Yes, there are a handful of other options. But these largely have fewer than five billets, making them prohibitively difficult to assign. Hence *effectively*.

[3]At least, I hope we learned these lessons. If we didn't, we're all doomed anyway. Save a hard-copy of this paper, you'll need it for kindling.

the fact that it's possible to collaborate remotely (this is double plus especially true for people working in computer related fields, such as Hackers). We have a recipe for a widely distributed USCF.

A good aim would be at least one location per US state. Not only does this help with recruitment and retention, there are also redundancy benefits. Under the current model, the Army's cyber operations could be absolutely crippled, if not completely destroyed, by two well placed kinetic attacks. Hitting two targets is not terribly difficult for a well equipped adversary. Hitting fifty in a short enough time span to prevent actions at one from alerting the others is considerably more difficult.

8 Serving Many Masters

> No one can serve two masters.
>
> — Matthew 6:24

I don't normally quote scripture, because (1) I am not a member of any organized religion; and (2) I strongly believe that religious doctrine should not be used to form or influence public policy. But this particular quote does serve as a great nugget of wisdom that's been recognized for at least 2000 years. I doubt anything I ever say or write will remembered as long.

To be a Hacker in the Army is to serve at least two masters: The Army itself, and USCC. There is an obvious division in the type of tasks the two masters require. USCC provides the Hacker with missions. Conduct this operation. Analyze this data. Develop this tool. The Army, on the other hand, represents bureaucracy. Take this mandatory training. Go to the dentist. Update your personnel record. The dichotomy is painfully apparent to Hackers, who are, generally speaking, more likely to apply critical thinking to all aspects of their life. It's clear that the Army butters their bread, but as an employer, it doesn't provide meaningful work. All the meaningful work comes from USCC.

The problem is further exacerbated by the current structure of operational forces. The primary Offensive Cyber Operations (OCO) element in the Army is the 780th Military Intelligence (MI) Brigade (CYBER). It is subordinate to Intelligence and Security Command (INSCOM), not ARCYBER. But its *mission* comes from ARCYBER, not INSCOM. This is a leaky abstraction that hits every member of the brigade at one point or another: Mission needs you to do this thing, but INSCOM is requiring that everyone do this other thing (that has nothing to do with cyber operations).

Recently, I witnessed an Army Captain attempt to diagram the command structure in an attempt to show how the CSD is related to the operational force. The result was woefully incomplete, with no hope of reaching 100%. The best approximation resulted in a non-Euclidean eldritch horror.

This problem fundamentally stems from attempts to shoe-horn cyber operations into a traditional Army structures, with additional requirements imposed

by USCC. It simply doesn't work. Establishing the USCF allows for a clean-slate, creating a simple organizational structure designed to work for Hackers conducting cyber operations from the bottom-up and top-down.

9 Talent Management

It would be dishonest to say that the Army is bad at talent management. To be bad at something, one must first attempt that thing. The Army doesn't attempt to manage talent, because that isn't what the regulations and systems that drive Human Resources Command (HRC) are designed for. HRC is designed to allocate people as interchangeable cogs in the great wheel of combat arms.

To highlight part of the issue, every system at HRC is designed around billets. Billets consists of an MOS and rank/grade, potentially augmented with an Additional Skill Identifier (ASI) or Special Qualification Identifier (SQI). That's about as in-depth as the systems are designed. This works well for combat arms, as it is enough to identify an airborne qualified E-5 in the infantry, or an artillery captain.

It is not sufficient to track and manage Hackers. ARCYBER has identified 26 cyber work roles. All 26 of these are assigned to a single enlisted, warrant officer, or officer MOS (17C, 170A, and 17A, respectively).[4] None of the work roles is identified by an ASI or SQI. Meaning that, systematically, it is impossible for someone at HRC to properly match a Hacker to an operational billet.

And that's just at the most fundamental level. Army systems don't provide good features for further identifying specific talents, such as expertise with an obscure system like VMS. Comment fields in the HRC marketplace don't count, because they don't scale and lack a consistent structure.

A system designed for managing Hackers in USCF would naturally take these things into account. The existing work roles would morph into the service-equivalent of an MOS, and specializations could be captured in the equivalent of ASIs or SQIs. It would be a system designed for managing uniquely talented Hackers, not interchangeable Soldiers.

10 Time Management

When I was young, I remember Army recruiting advertisements claiming that Soldiers get more accomplished before 9 AM than most people do all day. While this hasn't been used in recruiting for quite some time, the sentiment is still pervasive in the Army. The crux is that in typical Army units, the routine is start the day egregiously early with PT, and go from there. Of course you can get a lot done before 9 AM if you've been at work since 5.

[4]The forthcoming 170D warrant officer and 17D officer developer MOS do little to change the situation, but the lack of an equivalent enlisted MOS is extremely telling about how little the Army as an institution cares about managing Hackers.

The problem with this mentality, and especially applying it to Hackers, is that it forces everyone to conform to a single schedule. Human beings didn't evolve this way. Since pre-history, humanity has evolved so that some are prone to being up early in the day (and getting all sorts of things done before 9 AM), where others are naturally more active late into the night (often called "night owls"). It's a defense mechanism, ensuring that a tribe will typically have at least one person awake and active to be alert for predators.

The interesting thing is that in contingency operations, Army units will fall back to this, setting up rotating shifts to ensure that someone is always alert to hostile engagements. Ironically, leaders invariably attempt to spread shift work equitably, rather than making an attempt to identify the natural diurnal cycles of individual Soldiers, to the detriment of all.

Why is this broad application of forced morning person particularly damaging to Hackers? For one thing, recall that operations in the cyber domain never stop. There is no deployment or redeployment to clearly delineate the beginning and end of operations. Right now[5], someone is actively trying to compromise American computer systems. Right now[6], there is a need for an American Hacker to be conducting an operation against a hostile nation or terrorist group in order to prevent physical hostilities. Cyber operations are necessary 24 hours a day, 365 days a year, year in and year out. We need Hackers to be able to work any time, not just in sync with the Commander's schedule. Notably, there is significant segment of the Hacker population that falls in the "night owl" category. I myself did my best undergrad work between the hours of midnight and 4 AM. The USCF would do well to incorporate flexible schedules, largely accommodating Hackers' natural proclivities. Of course, some time management is required to ensure that the 24/7/365 coverage that is so desperately needed is fulfilled, but by giving Hackers options, it's easier than it might seem.

One final note on time management: Regardless of a Hacker's work schedule, the Hacker's leader would do well to note that work time is work time, and leave it at that. Attempts to micromanage work time by delineating specific hours for specific tasks, will be immediately seen as just that: micromanagement. Micromanagement is a sign of distrust, and will inevitably lead to lower morale and decreased retention.

11 Training

Training can be a fantastic thing. There are a lot things in the cyber domain that are just plain hard, and many can't be accomplished without some amount of training. The Hacker might not know what they don't know otherwise.

That being said, the Army places perhaps too great an emphasis on training. From a big Army perspective, the emphasis on training makes sense. A typical

[5]Without involving time travel, this instance of the "right now" refers both to the time I am typing these words and to the time you are reading them, no matter the temporal displacement between the two.

[6]Same.

combat arms unit can't execute it's mission 100% of the time (ideally, far less than 100%; it's in the national interest to have the amount of time combat arms units devote to operational employment approach zero), and conducting land warfare is a perishable skill. Thus, combat arms units spend their time training. Or, maybe more accurately, practicing and rehearsing things they have already trained in. But rehearsals and practice get lumped into "training", so training is how they're seen. Even during contingency operations, many units operate in cycles: one year focused on individual training, one year focused on collective training, one year doing actual operations. Rinse, repeat. Two-thirds of the combat arms unit's time is spent in training.

Contrast with operations in the cyber domain. Without exaggeration, real-world operations are happening 24 hours a day, 7 days a week, 365 days a year (and 366 days in Leap Year – no rest for the weary here!). Less time is necessary for practicing or rehearsing because there are actual operations to take care of. Skills do not have time to atrophy when they are applied on a daily basis.

And yet, I constantly see Army leaders looking for more training to put on the calendar. Lacking relevant training, the calendar will be filled with irrelevant Army training. Things like land navigation. There is no excuse to take a Hacker out of operations to practice using a map and compass. Generally speaking, Hackers don't deploy. In the event that they do, it's far more likely that they'll (1) have a GPS device or (2) be attached to another element that is staffed with people who routinely practice land navigation because it's relevant to their mission, and can simply follow their lead. Ticking off Army training boxes does nothing to improve the readiness of Hackers to conduct their mission, but it does detract from the time they have to accomplish said mission.

USCF training goals are focused primarily on initial training. Hackers need to be brought up to speed on how things work in USCF, especially as it contrasts to the private sector. After that, however, skills are primarily maintained through constant use. You don't need to practice things you do for real on a daily basis. As new technologies emerge that fundamentally change how operations are accomplished, there is room for more training. Otherwise, it should be a low priority.

12 Uniforms

Uniforms are a necessary part of any military, especially those hoping to enjoy protections under the Geneva Conventions.

Do Hackers need to wear a *camouflage* uniform?

Given that the average Hacker will spend their entire career inside a secure facility, it seems silly to dress them in camouflage. What are they blending in to? Not their office chair, that's for sure.

The USCF would be better served with something more like a polo shirt and comfortable slacks as a daily uniform. Something resembling what thousands of Information Technology (IT) professionals around the world wear on a daily basis, with just enough insignia to make it readily identifiable as a military

uniform. Just make sure you don't ask Hackers to wear anything resembling a suit on a regular basis. There's a substantial overlap in the Venn diagram between skilled Hackers and people who will only wear a suit under duress, and that would be a sure-fire way to destroy recruitment and retention.

13 Conclusion

TL;DR: The current strategy of forcing the square-peg of cyber operations into the round, triangular, or trapezoidal shapes of existing services is insufficient in a multitude of ways. Establishing the USCF is the inevitable conclusion of all efforts on this front. The sooner this happens, the better.

Appendices

A Acronyms

ACFT Army Combat Fitness Test

ARCYBER Army Cyber Command

APFT Army Physical Fitness Test

ASI Additional Skill Identifier

CAIP Cyber Assignment Incentive Pay

CSD Cyber Solutions Development Detachment

CNODP Computer Network Operations Development Program

HRC Human Resources Command

INSCOM Intelligence and Security Command

IP Internet Protocol

ISP Internet Service Provider

IT Information Technology

MI Military Intelligence

MOS Military Occupation Specialty

NSA National Security Agency

NSAH National Security Agency-Hawaii

OCO Offensive Cyber Operations

ROC Remote Operations Center

SQI Special Qualification Identifier

TL;DR Too Long; Didn't Read

USCC United States Cyber Command

USCF United States Cyber Force