AU/ACSC/SMITH, FI/AY16

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Airpower History and the Cyber Force of the Future

How Organization for the Cyber Domain Outpaced Strategic Thinking and Forgot the Lessons of the Past

by

Zachary M. Smith, Major, USAF
Master of Science, Strategic Intelligence, National Intelligence University

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisors: Lt Col Daniel A. Connelly and Dr. Panayotis Yannakogeorgos

Maxwell Air Force Base, Alabama

June 2016

Disclaimer

Abstract

The rapid growth in the importance of the cyber domain to US military operations spurred a reaction by the Department of Defense to organize cyber forces before the US Government had fully digested the nature of cyberwarfare. This paper uses the emergence of the air domain to understand how new technology changes warfare, and how the US reacts to technological changes through the organization of military forces. The research looked at the government documents and studies related to military organization written during the interwar years through the time right after the National Security Act of 1947 to determine how and why the airplane led to the reorganization of air forces within the military. Furthermore, cyberspace forces were organized around a functional command construct instead of integrated into the existing geographic commands. This paper will also explore how this affected the employment of airpower after the air forces were given greater autonomy based on their perceived strategic capabilities. The fusion of this historical analysis shows a highly questionable effectiveness for the future of the current organizational construct of cyber forces. This paper explores the idea of an independent cyber service, through the lens of how new domains were organized in the past. Though not in tactics or warfare theory, the similarities with the debates surrounding air forces and cyber forces organization is striking, especially with arguments against independent organization and the role of emerging technology in warfare. The conclusion is that cyber force organization has actually made both of the major mistakes that airpower organization did once before, and this should serve as a warning of potential strategic surprise and disruption of the joint force in war.

Airpower History and the Cyber Force of the Future

How Organization for the Cyber Domain Outpaced Strategic Thinking and Forgot the Lessons of the Past

"One day there will be competent and robust specific general theories of space power and cyber power, but they do not exist as of yet. This hugely immature theory is a problem if one seeks essentially to fold space power and cyber power into airpower theory and doctrine, as has been the recent case in the USAF. The potential is high for serious error leading to much gratuitous strategic self-harm." – Colin Gray[1]

The emergence of new technology, the airplane, once opened an entirely new domain in the air that revolutionized warfare. The countries that figured out how to operate in and leverage the power of this new domain had the advantage in joint warfare. The US did not lead the charge to take advantage of the new technology and its associated domain, and suffered devastating losses at Pearl Harbor. New technology has now opened cyberspace as a warfighting domain. Some countries have figured out how to leverage this new domain's power. The US is not one of them, and is now repeating the same struggles to organize cyber forces as it once did with the air domain. In order to navigate the confusing territory of a new domain that is not well understood, we can look backward to see how decision-makers dealt with a very similar problem, and learn from their failures.

Airpower became most effective when a force for the air domain was organized into a professional independent organization, built for air warfare, that in war was fused with the joint force under a single military commander, who had responsibility over all the domains of warfare. The forces for the cyber domain should now be included, as airpower is, in the joint force structure because the joint force is most unified in effort and effective in combat when all domains work seamlessly together without functional autonomy. Unity of command is only achieved when all military domains are leveraged together to maximize the joint capabilities for a unified military purpose, but cyber has not been organized this way. In past conflicts, airpower

has been employed autonomously or, more effectively, as part of geographic joint forces. The emergence of new warfighting domains has always complicated our understanding of how to organize for joint warfare, but the story of how the air became a coequal domain demonstrates the difficulty the cyber domain will face on a path to equal status. The result of failing to understand what was needed for the new domain of air should serve as a cautionary tale in cyber force organization. An independent cyber service presents several advantages that might avoid the mistakes of airpower's past. As the US military heads into the cyber domain, it should take with it the lessons of the past: that the military is most effective when each warfighting domain has an independent service responsible for building the forces and tactics needed for each domain, but provides forces to a joint commander to serve alongside the forces from all other domains and unify military power.

The primary goal of a military organizational structure is to maximize effectiveness in war. Although peacetime military operations can be significant, they should not be the driving factor for any military organizational structure and distract from military readiness. However, the US is not at war in cyberspace, despite many claims to the contrary. Peacetime operations may be an enticing lure for a cyber force that is not at war with any nation, but the ultimate purpose of any military is to win the nation's wars. As such, maximizing our ability to fight in war should be the most important principle behind cyber force organization. Foreign policy in a single domain cannot be separated from the overarching foreign policy of a nation. This paper will attempt to determine if our cyber force organization is maximized to fight joint warfare or is now about to repeat the mistakes of airpower's past.

THE ORGANIZATION OF CYBER FORCES AND UNITY OF COMMAND

"Well, let me tell you, this doctrinal bickering is horse manure. First of all, in Desert Storm we had one ground force commander for each of the two forces and they approved every target…they trusted their air component to organize a daily air campaign, which they reviewed as land component commanders, and then as CINCs either changed or approved…Secondly, all subordinates in a war must understand that no joint force commander wants to lose. He hopes to use air, land, sea, and space assets in a way that will bring victory on the battlefield. So back at the Pentagon, quit writing doctrine that is a compromise between the way each separate service wants to fight wars, because they don't fight wars. Unified commanders…are in charge. If we follow the doctrines of compromise published by the services and the Joint Staff, we will end up with 'war fought by committee' –a sure loser."

-Chuck Horner, JFACC for DESERT STORM[2]

The organization of cyber forces intended to unify the capabilities of the Army, Navy, Air Force, and Marines into a warfighting organization that would be responsible for fighting the nation's wars in cyberspace, but the amalgamation of the services' cyber capabilities created only the semblance of unified power. The creation of the United States Cyber Command (USCYBERCOM) was a necessary step forward in cyberspace organization, but it is not a truly joint organization. If anything, creation of a combatant command only created a functional stovepipe for cyber operations to occur separately from other domains reducing the incentive for the Geographic Combatant Commander to understand how cyberwarfare may affect the totality of military operations. Cyberspace challenges our fundamental understanding of joint warfare itself, and threatens to model itself around a function instead of joint purpose. Instead, cyber force organization may be creating unity of command specific to only one problem, and leaving joint warfare behind as an idea of the past. There is certainly a need to grow, develop, and maintain a force ready to fight wars in the cyber domain, but we must be careful to create an organization responsive to our nation's needs. Although the DoD created USCYBERCOM, it provides only the semblance of a solution and falls short of being able to build the capabilities needed to support the joint force in the cyber domain.

Cyber forces should maximize the advantages of the domain, but still remain part of the overall objectives of the joint (land, air, sea, space) force. Instead of a focus on where cyber fits in the joint force, much of the discussion about cyber force organization has become polarized, focused on whether cyber should be an independent or supporting force. Many of the same arguments during the debates of the interwar years about airpower resonate in these cyber debates of today. One notable argument from 1913 compares the emerging air domain to the older land domain. Assistant Secretary of War Breckinridge regarded military aviation as "merely an added means of communication, observation, and reconnaissance" which "ought to be coordinated with and subordinated to the general service of information and not erected into an independent and uncoordinated service."[3] Discussions about the air domain may seem familiar to some concepts of cyberpower, but most decision-makers recognize cyber as strategically important, if confusing. Many of the debates about the importance of cyber have clearly resonated with senior government officials. Cyber forces were looked at as something so new they had to be given a great deal of autonomy within a single warfighting command. The sheer magnitude of cyber incidents certainly demanded something be done to address the imminent threats in cyberspace, but unlike the air domain, the cyber domain arose after the Goldwater-Nichols reconstruction of the Department of Defense. As such, with all the best intentions, cyber forces were disconnected from the command structure of the Geographic Combatant Command (GCC).

If unity of command is the organizational principle of how we fight our nation's wars, we have to ask ourselves if that is really what we have created, or just the appearance of unity and a new way to segregate cyber operations from the joint force while we convince ourselves that our adversaries will do the same. There is a significant difference between the independence of an

organizational structure to train, organize, and equip and the independent action of a global organization. Since USCYBERCOM now exists, it may serve as a hindrance to serious study of cyber force organization. After an organizational decision is made and it appears the problem is still not solved, it may seem easier to invest more resources and empower the organization even more instead of questioning whether the current heading is going to meet the needs of the joint force and national leadership.

One of the potential indicators of an organizational problem may be the quest to reform major government processes such as laws and authorities that are restricting the organization. In the US constitutional system, Congress has already granted the President the means to defend the nation from foreign threats. There are no authority limitations preventing civilian leadership from conducting the operations needed to defend the nation. The legal structure that was not built for cyberspace is still sufficient to meet the needs of the new domain.[4] The greater considerations are policy concerns for organizational roles. As is the case for any other domain inhabited by civilians, cyber militarization remains a constant concern for policymakers.[5] Granting more authority to a military warfighting organization may move in exactly the wrong direction from a national policy perspective. Cyber should, perhaps, be no different than any other form of military power, and be built and stand ready for a day that political leaders all hope will never come. However, if one thing is resoundingly clear from over 3000 years of military history, the era of nation-state warfare has not ended. The nation's next wars against another nation will undoubtedly include a cyber component, and the inclusion of cyber power into the joint forces will be a critical part of what the US military must be ready for.

In the post-Goldwater-Nichols era, unity of command is essential to the projection of military power and the coordination of joint warfare. Unity of command is one of the

fundamental beliefs of the US military, was based on painful experience, and is now at the core of joint force organization.

> "**Organizing Joint Forces**…Sound organization should provide for unity of command, centralized planning and direction, and decentralized execution. Unity of effort is necessary for effectiveness and efficiency. Centralized planning and direction is essential for controlling and coordinating the efforts of the forces."[6]

The above statement was very likely an organizing principle behind the creation of USCYBERCOM, but combining cyber forces from the different branches of service does not truly create a joint construct. Command is not unified unless it combines *all* the components of warfare (i.e. land, air, sea) for a single unity of purpose. USCYBERCOM's focus statement indicates a desire to unify command, but in essence it lists a mix of what should be service and joint force *component* commander responsibilities.

> "The Command unifies the direction of cyberspace operations, strengthens DoD cyberspace capabilities, and integrates and bolsters DoD's cyber expertise. USCYBERCOM improves DoD's capabilities to operate resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace. USCYBERCOM is designing the cyber force structure, training requirements and certification standards that will enable the Services to build the cyber force required to execute our assigned missions. The command also works closely with interagency and international partners in executing these critical missions."[7]

Although this may appear to provide the unity of action in cyberspace that was so desperately needed, instead it created a flaw in the foundational statement, by using the word "cyberspace" as something separate from the other aspects of military power. There is no such thing as cyberwar. There is only war, of which cyber is a component. USCYBERCOM does not create unity of command, except in cyberspace.

USCYBERCOM executes joint warfare in cyberspace disconnected from the command structure of all other aspects of military operations. The strain from this disconnection can be felt, but may have been welcomed by the joint force due to a severe lack of understanding about

the relevancy of the cyber domain in warfare. Many at the geographic combatant commands (GCCs) understand cyberwarfare as little more than a communication enabler. Without a clear understanding of the role the cyber domain will play in the wars of the future, the disconnected nature of cyber organization leads to the marginalization of cyber forces in joint operational planning. The impact of cyberwarfare on military operations of the future is vague, ranging in prediction from catastrophic to negligible impact. Most combatant commands know that cyber is important and is relevant, but may not truly understand how or why. The focus of cyberwarfare, according to the USCYBERCOM focus statement, is not the responsibility of the GCC since centralized cyberwarfare is not controlled as another coequal component of warfare.

The most fusion of effort may lie in the somewhat painful marriage of USCYBERCOM and NSA. There was a decided lack of expertise in military cyber operations that the shared leadership structure of USCYBERCOM and NSA was intended to solve. The older and more established culture of NSA prescribed rigid standards built for careful, clandestine intelligence operations, and started a journey towards something quite different than joint power integration. Instead of bringing cyber expertise into the COCOMs, USCYBERCOM kept operations and command and control (C2) close to the chest in the model of NSA, which was a model built for a different purpose. The NSA and USCYBERCOM operational platforms are still shared despite years of attempts at separation. NSA Signals Intelligence standards continue to be applied to USCYBERCOM operations, which is now becoming codified in doctrine. This is dangerous as cyber terrain begins to invade every aspect of advanced modern combat systems, and intelligence community standards apply practice meant for a very different purpose into cyberwarfare. These standards may drive USCYBERCOM to a model more conducive to smaller scale special operations than the full-scale cyberwarfare capabilities needed to support combined forces.

Military operations and intelligence operations should be separated and different in a way observable to adversaries. The early infusion of NSA technical expertise into USCYBERCOM was essential, but USCYBERCOM should now evolve and stand on its own to develop the capabilities needed for joint warfare.

GCCs, such as USNORTHCOM, are responsible for executing command and control of joint warfare within their area of responsibility (AOR), with the exception of cyberspace. Cyberspace operations are realized, but separated from the GCC in every posture statement. From these posture statements, many of the GCCs seem to find this a point of contention. USNORTHCOM has a significant amount of focus in their posture statement to the ambiguous cyber environment that they believe will impact their ability to execute their mission. Created out of the fires of the September 11th attacks, USNORTHCOM is responsible for defense of the homeland, except in cyberspace.

> "To address growing cyber threats to our military operations, we rely on the protection of DOD critical systems through cybersecurity efforts and shared situational awareness with our mission partners. Our newly established Joint Cyber Center (JCC), along with our United States and Canada military and interagency partners, recognizes and assesses when malicious cyber activity is being orchestrated against us, and in concert with United States Cyber Command (USCYBERCOM), directs the appropriate cyber measures…We have a wealth of experience in responding to natural disasters in the homeland, but the unpredictable cascading impacts of a cyberspace attack have the potential to easily outpace those of a natural disaster. While our cyberspace mission is defined and limited to protecting our own systems, it would be simplistic to assume that a large scale cyber-attack on the nation's infrastructure would somehow not impact both us and many of our partners' ability to successfully perform the DSCA mission. It makes strategic sense to consider the steps that could be taken to mitigate or prevent these types of attacks before they ever evolve into a DSCA response by DOD."[8]

The posture statement shows that USNORTHCOM considers cyber to be a significant issue for their future mission to defend the homeland and conduct Defense Support to Civil Authorities (DSCA). The command and control during a cyber attack on the homeland is

clearly an issue with the standup of the JCC; however, USNORTHCOM seems to recognize they will not have clear unified control of actions conducted in cyberspace to defend the homeland. Cyber responses will certainly not occur based on USNORTHCOM approval processes. If an attack on the homeland were to occur, USNORTHCOM would rely on USCYBERCOM to conduct the mission of supporting civil authorities, and in the chaos during an attack, it is likely that the split command structure will be strained.

USPACOM is responsible for the execution of joint warfare and military power projection within the Pacific AOR, with the exception of cyberspace. In joint warfare, there is no functional LANDCOMMAND, AIRCOMMAND, or SEACOMMAND, those are component commanders, but there is definitively a CYBERCOMMAND which may even be elevated to the equivalent level of a GCC as USSTRATCOM continues to distance itself from the cyber mission. The statement of the potential impact of this split in the C2 for joint deployed operations is readily evident in the USPACOM Posture Statement:

> "Increased cyber capacity and use, especially by China, North Korea, and Russia, underscore the growing requirement to evolve our command, control, and operational structure authorities. In order to fully leverage the Cyber domain, Combatant Commanders require an enduring theater cyber operational command resourced to provide regional cyber planning, integration, synchronization, and direction of cyberspace forces. The theater cyber operational command will provide direction of operations against increasingly capable threats in coordination with USCYBERCOM, the interagency, and allies and partners. USPACOM sees a future where Joint Force Cyber Component Commands (JFCCC) are aligned regionally under Combatant Commands. JFCCCs will provide staffing and expertise required to oversee persistent operations and defense of theater information networks, synchronization of cyber risk assessments and intelligence, and development of flexible cyber effects."

The segregation of the cyber C2 structure at USPACOM is an example of the strain the cyber domain C2 places on the joint force structure of GCCs. The GCC appears to advocate for a JFCCC, an expert of the domain, unified within the joint military structure as an equal arm of military foreign policy. The GCC is the focus of the nation's military power, but cyber is

currently separated. It could be argued that this segregation occurs because of the unique nature of cyberspace and the skills needed to manage such a complex domain, but all domains are complex to those that are unfamiliar with them, and individual COCOM commanders rarely have expertise in all the subordinate components.

There will never be an AIRCOMMAND despite the complexity of the air domain. Airpower was not segregated from the GCC, but cyberpower was because many believe the cyber domain is independent from geography when this is not the case. Cyber forces will not fight a cyber-on-cyber war while the rest of the joint force conducts separated operations. There are not two foreign policy instruments for military power, national cyberspace forces and geographic forces. Any action in cyberspace against a nation has consequences in all other domains. The loss of cyber forces from the joint command structure that was proven in US warfare history in favor of a functional command structure with the hope that fusion centers will unify action between COCOMs and avoid friction is indeed concerning.

FUNCTIONAL VS GEOGRAPHIC COMMAND AND MILITARY EFFECTIVENESS

"Conquering the command of the air implies positive action – that is, offensive and not defensive action, the very best suited to air power."
-Guilio Douhet[9]

The first great mistake of airpower organization was remaining latched as a subordinate force to land and sea and failing to create an independent service to manage the forces needed for the new domain, but the second great mistake of airpower organization was the creation of a command and control structure for autonomous action independent from land and sea operations. Airpower history may shed light on the consequences of organizational structures that separate functions of military power from joint command. The question of when to enable strategic command versus geographic command is central to how the joint force operates. Functional command creates additional coordination problems, but maintains autonomy. For many military capabilities, this may be more effective. Intertheater mobility (also called strategic mobility) enables the support of numerous geographic commands with the same assets, and is an example of functional command. The other functional commands conduct military tasks such as nuclear warfare and special operations. Not surprisingly, cyber has been compared to these other functional capabilities. Without a foundational theory governing cyber, this confusion has led to organizational decisions based on the uncertainty of where cyber fits in the joint force. Looking at when air domain organizations were effective and when they were not may demystify the cyber domain and explain the tension between geographic and functional commands and control of strategic forces.

At the start of World War II, the Army Air Corps was given a great deal of autonomy for operations. In the time from the start of World War II until reformation of the Armed Forces under the Goldwater-Nichols Act, the US Air Force gained valuable lessons about just

how precarious the balance between joint operations and autonomous strategic effects can be. The organizational lessons became codified in Air Force doctrine:

> Organization is critically important to effective and efficient operations. Service and joint force organization and command relationships—literally, who owns what, and who can do what with whom, and when—easily create the most friction within any operation.
> - Organization and preferred command arrangements are designed to address unity of command, a key principle of war. Clear lines of authority, with clearly identified commanders at appropriate echelons exercising appropriate control, are essential to achieving unity of effort, reducing confusion, and maintaining priorities.
> - The key to successful employment of Air Force forces as part of a joint force effort is providing a single Air Force commander with the responsibility and authority to properly organize, train, equip and employ Air Force forces to accomplish assigned functions and tasks.[10]

The Joint Forces Air Component Commander (JFACC) maintains authority over Air Force forces, but still remains closely linked and subordinate to the Joint Force Commander and the JFC objectives. In Air Force history the range of connection to the Joint Force Commander has varied widely. To understand how cyberpower could be effectively employed or constrained based on its organizational structure, airpower can be used as a case study to determine how organizational structures impacted airpower effectiveness, and with it, the joint force.

Airpower effectiveness is based on the ability of leaders to understand and properly develop theory, implement strategy, and utilize forces to achieve military goals based on the strategic context of the situation. When airpower effectiveness was disconnected by a lack of understanding of the context of how it was needed, it failed to adapt to changes in warfare and exploit new technology. The following three case studies in airpower history may enlighten the spectrum of autonomy of action. When the Army Air Corp was given autonomy to conduct its own operations in WWII, it achieved questionable results through independent action, but was successful in joint operations. Changes in the demands on airpower and strict adherence to past

theory resulted in limited airpower effectiveness as was the case in the Strategic Air Command's C2 of the Linebacker II bombing campaign over Hanoi. Airpower's most effective use in US history might have been the air campaign of DESERT STORM run by the Joint Force Air Component Commander (JFACC) of US Central Command (USCENTCOM) which applied the lessons of how airpower effectiveness was limited in Vietnam and adapted airpower to the context of the first gulf war.

During the interwar period, Giulio Douhet, Billy Mitchell, and Hugh Trenchard strongly advocated for offensive use of aircraft in combat. Both European and American airmen were fascinated by the offensive potential for the aircraft, and the debates about military aviation argued whether it should support the tactical actions of the ground and naval forces or engage in this newly conceived independent strategic attack mission. The autonomy gained after Pearl Harbor gave the Army Air Corps the first opportunity to test their theories regarding strategic attack in a total war setting, and they seized that opportunity to prove an air force can independently achieve a victory. The airmen of the Combined Bomber Offensive (CBO) of WWII endured incredible hardships in the hope of coercing the German government to surrender through independent strategic attack through the air domain. The CBO cost the allies over 18,000 aircraft and 81,000 airmen were lost trying to strike strategic targets to break the German war machine and force the surrender of the government.[11] The German government never surrendered and a land invasion became necessary, of which the Air Corps would play a critical role. Possibly the greatest contribution to allied victory made by airpower was the attritional defeat of the German Luftwaffe during the CBO.[12] The American commitment to daylight bombing of strategically important targets forced the Luftwaffe to attempt to stop the bombers. Because of the introduction of long-range escort aircraft, the allies were able to destroy the

Luftwaffe in the air and gained air superiority. Though the Germans refused to surrender, air superiority allowed the allies to fully support the necessary ground offensive on D-Day. The impact of air superiority allowed the allied ground forces to defeat the Germans on land, directly contributing to the end of the war. As a purely political tool of coercion, strategic bombing for both the American and British failed to work exactly as advertised by Douhet, Mitchell, or Trenchard. Germany had to be invaded by land and conquered, of which airpower played a key supporting role. The advocates of city bombing had greatly misjudged the frailty of enemy morale.[13] In the end, it is unlikely that airpower alone could have led to the political goal of victory in Europe.[14] The unique separation in time between the CBO and the Normandy invasion provided an opportunity to evaluate the effectiveness of autonomous airpower and joint integrated airpower. Despite the focus of the newly autonomous air forces on strategic attack, independent action did not prove successful except at attrition warfare that resulted in the air superiority needed for a land invasion of Europe.

During the Linebacker II bombing campaign over Vietnam, the Strategic Air Command leadership was presented with challenges to the use of airpower, and SAC's strict adherence to theory, poor command structure, and questionable strategy caused significant risk to aircrews and produced highly questionable strategic results. Despite the claims made by Gen Momyer in his book *Airpower in Three Wars*, the air campaign over Vietnam could hardly be considered centrally controlled and de-centrally executed.[15] For the employment of airpower, the Navy, the Army, and the Air Force all retained control of their own aircraft and fought highly disorganized and separate air campaigns leading to divisive arguments and coordination lapses.[16] With the deployment of B-52s during the Linebacker II campaign, this already fractured organizational command structure became even more problematic. According to Marshall Michel, due to the

preeminence of nuclear bombing theory on which the Strategic Air Command (SAC) was founded, SAC maintained C2 of strategic B-52 operations in direct support to the negotiations of the State Department.[17] This proved to be highly ineffective due to the inability of SAC to utilize one of the greatest strengths of airpower, agility. SAC was highly rigid in its adherence to nuclear bombing theory that was not applicable to the context of the situation, and as Colin Gray claims, context matters. The tactics B-52s would employ in nuclear bombing were very different from the tactics needed for repeated bombing runs over Hanoi in an attempt to coerce North Vietnamese leadership. SAC HQ directed the B-52s to repeatedly fly in a straight line to the target, in single file, based on doctrine developed to penetrate Soviet air defenses during a nuclear conflict.[18] This maximized the ability of the North Vietnamese to target the inbound bombers using Surface to Air Missiles (SAMs). SAC HQ did not understand the situation in theater and produced highly ineffective strategic results.

The ineffective strategy of SAC HQ was eventually overcome due to local leadership asserting there was a better way to fight this war, but the organizational command structure required that changes in tactics be routed back to SAC HQ for approval. By the time any changes were approved, crews were already at risk, and the B-52s continued to suffer significant losses in theater. When the B-52s began to ignore SAC HQ direction and adopt bombing runs from multiple approach angles with each aircraft laying down overlapping chaff blankets, the ability of the SAMs to target them became greatly reduced, and B-52 survivability greatly increased.[19] Michel claims that at the end of the war, the overall strategic effectiveness of the bombing campaign was highly questionable.[20] The Vietnamese even built museums to memorialize the victory over the B-52s.[21] The strategic effectiveness of airpower was severely limited due to an ineffective organizational structure and strict adherence to theory intended for other purposes.

In Desert Storm, Gen Chuck Horner, the JFACC, overcame many of the problems suffered during the Vietnam War by effectively organizing the air component and adapting airpower theory to the strategic context of the gulf war under the GCC. One of the most significant lessons that Horner learned from Vietnam was the need to jointly manage the air campaign assets believing that the command of air assets should be centralized under the JFACC to support to the coalition commander.[22] Horner vehemently defended the responsibility of the JFACC to manage all coalition air assets for the needs of the joint force. All targeting in the campaign would be managed by his staff in support of the JFC, without mistakes similar to those of SAC HQ by inappropriately applying doctrine developed for other strategic applications, disconnected from the Geographic Command.

With his organizational C2 structure determined, Horner focused his attention on what strategy would lead to the most effective use of airpower in the conflict. Decades of airpower theory led to the ideas of John Warden's rings theory of targeting. Warden's CHECKMATE team developed a targeting list for Horner based on a foundation of strategic bombing. When this was presented to Horner, he was less than thrilled. Warden's list ignored the fielded forces and support to the land campaign.[23] If airpower did not achieve the strategic effect of coercing the Iraqi government to abandon its defensive position, the superior numbers of the Iraqi army would cause significant casualties for coalition land forces. Though numerous strategic targets were added, Horner rejected the theory that airpower alone could coerce an enemy and ordered an inclusion of ground force interdiction to take full advantage of the edge airpower technology provided over the Iraqi ground forces. This decision led to the success of the ground invasion, and the ultimate strategic success of the operation. If Horner had not adapted airpower theory to

the strategic context of the situation to support the coalition commander, it would have hindered airpower's effective employment and could have led to disaster for the joint force.

The success of the first gulf war air campaign was greatly enabled by sound strategy and a clear C2 structure that took full advantage of the technological advantage of coalition forces, but as the US grows more dependent on cyberspace to fight war, military effectiveness may be highly limited due to the organization of cyber forces. The US has already set down a potentially complicated pathway to manage cyber domain operations. Libicki claims that the creation of USCYBERCOM could potentially send a signal to foreign audiences that the US is prepared, scared, and on the warpath in cyberspace.[24] Whether this is true or not, perceptions matter, and the US has indeed created an organization to fight wars in cyberspace separated from the rest of joint force command. Despite the lessons of Vietnam and the gulf war, USCYBERCOM created national mission forces, separated from the GCC structure under a premise that the US is already under attack in cyberspace, a highly questionable claim. Libicki claims that most of the "attacks" in cyberspace are at most espionage activity with only a handful of events that could be considered potential attacks.[25] The most notable cyber "attack" was the destruction of computers at Sony Pictures by North Korea which resulted in no military response by USCYBERCOM (or PACOM for that matter). What is potentially dangerous is focusing all cyber operational authority and control into a single organization responsible only for cyber power. The concern is that there is unnecessary pressure to use that power independently to justify the organizational existence.

Organization of cyber forces would likely be more effective if the DoD had created a separate service to provide a cyber component commander in the GCC structure, fusing cyber power into the joint application of military power as equal with air, land, and sea instead of

creating an entirely new COCOM to manage it separately in more of a SOCOM model. USCYBERCOM is now in danger of becoming the special operations force for cyberspace. Although this may be enticing, it is highly questionable whether the current organization will be effective to fight full scale wars of the future with the command disconnected organizationally from the other components. Special operations have a very unique and different mission than what the nation will need in cyberspace with so vast a range of military operations growing dependent on cyberspace daily. The tendency may be for government leaders to look for the specific and limited capabilities of USCYBERCOM to solve smaller-scale specific problems through clandestine means and ignore the greater military need. Furthermore, USCYBERCOM is dual-hatted with the National Security Agency. Although this was done to exploit the necessity that USCYBERCOM has for intelligence to do its mission, this intelligence need is fundamentally no different than any other GCC, but it gives a functional commander the ability to prioritize the needs of his own operations ahead of the joint force. The molding of USCYBERCOM into a clandestine special operations and intelligence model may have strategic consequences in larger-scale conflict.

The creation of USCYBERCOM seems to have preceded the development of a military strategy for cyberspace or a theory of how cyberspace operations will support national policy; likely to limit US military effectiveness in cyberspace as well. The national strategy focuses on cybersecurity, not on offensive cyber operations, and may have created problems during the organization of the cyber mission forces. Each services created its own interpretation of cyber power. In lack of cyber theory, the USAF has simply applied the principles of airpower to the cyber domain. As Gray states, there is no general theory of cyberpower, one day there might be, but the current trend in the USAF is to apply airpower theory to cyberpower which is dangerous

and may lead to strategic mistakes.[26] Here Gray claims that airpower and cyberpower are not the same and require different approaches, likely true since the employment of cyberspace weapons are very different from how air forces employ weapons. Libicki argues that cyber weapons are unpredictable, and proliferate as soon as they are used.[27] Libicki may only partially be correct; some cyber capabilities are very predictable and controllable and can influence the outcome of conflict without proliferation. Instead it appears cyber weapons are stuck in the context of malware and cybersecurity, causing confusion during employment. Due to lack of a clear understanding of what will happen with the employment of cyber power, leaders have been reluctant to use it.[28] As such, military cyber forces have predominantly focused on providing communication capabilities to land, air, and sea, despite being intended to conduct the full spectrum of military cyberspace operations under centralized control. Future joint capabilities may become even more critically dependent on the defense of the cyber domain. For instance the USAF is entering a transition to Remote Piloted Aircraft (RPAs), requiring effective communications to remain in the fight, and fully capitalizing on the ability to distribute what the pilot is seeing to a wide variety of warriors and intelligence analysts to maximize the utility of airbreathing assets. Although communication services are critical to the way the US now fights war, the inability to understand how cyber operations can be used to maximize military efficiency or disrupt adversary capabilities has severely limited effective employment and may lead to the loss of communications needed during wartime. Lack of understanding by US leaders about how to employ cyberpower has led to disconnects between military strategy and foreign policy that will need to be corrected for cyberpower to be effective in the future.

Airpower leaders have created theory and built organizations to employ strategy effectively through the air domain, and as the US military grows more dependent on

communications to effectively fight, military leaders should now focus on what airpower can teach us about cyberpower, but not transpose airpower theory as a replacement for cyberpower theory development. The lessons of airpower history are a guide for how past leaders have either adapted to the strategic context of their time, or been shackled to organizations and theories of the past. For the USAF to effectively employ military power in the future, it must recognize what has worked and what hasn't and so cyber must learn from this example. There are case studies throughout airpower history that explain the mistakes of too much autonomy for the sake of independent strategic effect, and how joint force employment can achieve war-winning results. The context of the emergence of cyberpower generated USCYBERCOM, which gives only the illusion of the organization that is needed to achieve military effectiveness in the cyber domain. This must be only the start of the conversation about cyber force organization. Cyberpower is still tethered to the cultures of the existing services, and may not be ready for the next major conflict. The existence of USCYBERCOM should not end the debate about cyber organization, but begin it. The creation of USCYBERCOM was a necessary step in a transitional phase that has far to go. Future military leaders will continue to be challenged from the strategic context of their time, and they must realize where organization structures and theories have supported military effectiveness, and where they have limited it, in order to make the decisions needed for the future.

THE EMERGENCE OF A NEW DOMAIN

"History is a conversation the past has with the present about the future"

– Dr. Forsyth, Dean of the Air Command and Staff College[29]

Reorganization of cyber forces may seem like uncharted territory, but there is a surprisingly similar historical precedent in US military history to the challenges now presented by the emerging cyber domain. Analysis of how the emergence of the aircraft as new military technology opened the air domain may shed light on how the military will handle the emergence of cyberspace. The associated debates about airpower importance and its relationship to existing US military services is instructive in present day debates centering on cyber. The historical case of how the US Air Force came about as an independent service, and associated missteps made along the way, is presented below as a precursor to how the US is making similar missteps with respect to cyber. It is critical to understand this historical case in order to avoid further mistakes in the cyber realm. As a cautionary note, the lessons of the formation of the US Air Force and how it rose to meet the challenges of the new air domain are valuable, but the air analogy should only be extended to understand organizational constructs and not to analogize tactics or strategy which are only superficially similar.

Cyber forces have already made the connection between the emergence of the cyber domain and the US Air Force's birth out of the importance of the air domain, but this connection may be founded more on the myth of the creation of the Air Force than the likely reality of why the Air Force found independence. Numerous books were written about the formative ideas of Guilio Douhet, Billy Mitchell and High Trenchard about the strategic attack capabilities that the air domain offered. Perhaps most notable in US Air Force lore are the debates of the interwar years about the promise of the air domain juxtaposed with the iconic image of Billy Mitchell

standing before his court-martial in 1925.[30] One has to question whether it was these very public debates, or if it was the failures of the Army and the Navy to fully exploit the air domain, that led to the creation of the independent air force.

It is most important to understand what was happening in the minds of the people who lived through this time in order to understand the context of the airpower debates. 1925 was a landmark year for the air service debates, as Mitchell published his airpower theory called *Winged Defense*.[31] In 1950, Dr. Earl McClendon completed his book *The Question of Autonomy for the United States Air Arm* which chronicled the major discussions surrounding the issue. McClendon claims the airpower debates actually began as early as 1907, but the year of 1926, much heralded in Air Force lore for the fervor of airpower debates and congressional action creating the Army Air Corps, could not be seen as anything but a victory in defense of the status quo.[32] The establishment of the Army Air Corps, though a significant step, did little to unbind air warfare from a supporting role to the parent services, and the war department seemed less than impressed with airpower. In the 1926 *Annual Report of the Secretary of War to the President*, enabling the offensive strike power of aircraft was hardly a focus of this report. Offensive capabilities were central to the airpower debates of that year, but the Secretary seemed much more interested in topics like finances, inland waterways, and dams.[33] The Secretary's viewpoint on the significance of the congressional legislation pertaining to aviation in 1926 was a small section of the report:

> "Of great importance to the War Department was the enactment during the past session of Congress of the legislation pertaining to the Air Corps of the Army. The War Department has always been emphatic in its opposition to any separation of the air defenses of the Nation from the military forces with which they must be expected to cooperate in time of emergency. It has consistently opposed any proposal for the establishment of a single department of national defense in which the air services would be organized into an independent air force separate and distinct from the Army and Navy."[34]

The mindset of the Secretary considering the value of the air domain seemed to be comprised of two things. First was air defense, and second was support to the Army and Navy. It is completely understandable why the War Department of the interwar years did not have offensive striking power high on its list; the US was looking inward, downsizing the military, and questioned whether the remote possibility of war with a great power was worth the investment. Europe seemed to have completely lost its taste for war, and America now stood as a country with vast distances between its few potential enemies. As the US grew isolationist, its mindset was far more focused on coastal defense, and it was questionable why airmindedness would be needed for the future.

The last consideration for air arm independence stemmed from an environment of cultural resistance to change and a strong desire to end the debates about airpower. The status quo viewed the air domain debates from the framework or perspective of land and sea warfare. With this framework, it became impossible to justify building a strategy that treated the air domain as an equal. In the interwar period, there were congressional hearings, newspaper articles, courts martial, and press conferences about airpower, and because of these theatrics, senior officials may have become weary of hearing about the air domain. In the 1926 report, the Secretary of War goes on to state:

> "The President's Aircraft Board and the two congressional committees upheld the views of the War Department as to the inadvisability of the establishment of an independent air force. Congress too rejected similar proposals. The War Department believes that this action reflects the best thought of the entire Nation after mature and conscientious consideration of the problem."[35]

McClendon argues the final analysis of 1926 Air Corps Act showed that the War Department had won another victory; control, including budgetary control, would remain firmly with the Secretary of War.[36] The tone of the Secretary's report to the President implied finality to the

decision. There was no further need for debate on the issue which had seen the light of day in numerous studies and was now reaching the point of becoming nothing more than a distraction to building air forces to meet the needs of the land domain. The establishment became so entrenched in marginalizing the operations in the new domain despite both public and political focus on its importance. After careful consideration, the defenders of the status quo believed their supporting force structure was sufficient to understanding the value of air operations as long as subordinate airmen advised them; consequently there was no need for a service led by airmen.

Military officers in the interwar period believed that the air domain had significant importance for land and sea operations; in fact, they seemed to fully realize how important air operations were to the traditional arms of the military. In 1919, the Secretary of War stated that the attack activities of airplanes during the war were small-scale, but the only indispensable roles were observation and artillery fire control, doctrinally only an extension of the way that land forces fight.[37] What the Secretary stated the military needed was better cooperation between army and navy air arms, but not a unification of the two into a service.[38] The subtext of this statement did not imply that the air domain did not offer innovative new ways to fight; instead, it implied new innovations for air warfare could never eclipse the critical support that air warfare provided to the land forces, and must therefore remain subordinated and focused on those activities. The supporters of the status quo feared that, if autonomous, airmen may choose to ignore or deprioritize their support to other fighting forces. Furthermore, the land forces should be responsible for air doctrine, and innovation in the air domain was not a priority compared with airpower's supporting role to the existing services. For innovation to occur in the air domain, it would do so only under a framework pleasing to leaders of land and sea forces.

Despite vigorous debates for independence, air domain proponents found themselves facing a considerable resistance to innovation and a nearly impossible bar to meet for autonomy. One central theme for many airpower advocates was the promise of new offensive capabilities for the air domain. Although it was questionable how important this was to senior War Department officials during the interwar period, it also seemed very difficult for military officers to conceptualize an air capability of military significance. General Pershing stated that though the air arm was an essential branch of the Army, an air force "acting independently can of its own account neither win a war at the present time nor, so far as we can tell, at any time in the future." He continued that air could not secure a military decision against ground forces and should be treated like other combat branches within the Army.[39] Resistance to change in the status quo was extreme for many officers of the period, and it appeared that officers less familiar with the domain could not envision a way that the domain would actually be capable of winning the wars of the future. The thought implied that since an independent victory probably could not be achieved through the air domain, there was no need for an independent air force.

The value of independence was the ability for air forces to innovate within the domain without having to meet the standards of those unfamiliar with operations and capabilities that did not directly link to other domains. While air forces might not have had the capability then – or possibly ever – to independently win a war, the thought that this is a disqualifier to having an independent service was as wrong-headed then as it remains today. The value of an independent service dedicated to a specific domain is not predicated on the ability of that service to win wars alone. The cyber forces of today struggle to understand the nature of information-based warfare and where they fit in the joint force. The air forces of the US found themselves in a similar situation many years ago when technology opened a new domain to military warfare. Many of

the questions about the relevancy of a new warfighting domain, and what type of organization would be needed to manage it are as relevant today as they were then. Cyber is not just the communications support for the joint force. There must be a debate about the relevance of the cyber domain, and whether USCYBERCOM actually solves the problem it was intended to solve, or just presents only a shadow of a solution. Are the discussions about cyber today framed in the same way airpower was during the interwar period, and if so, what will be the implications for national security? Are we indeed in a new interwar period, and if so, will we be ready for the opening shots of the next war, or will our enemies demonstrate the effectiveness of cyberwarfare for us to learn from?

CONSEQUENCES OF FAILING TO ORGANIZE FOR A NEW DOMAIN

"We were in a state of mind not conditioned to the event at the time."

-Pearl Harbor survivor[40]

Airpower's early history should serve as both a guide and a cautionary tale for the development of new technology impacting military operations and the opening of new warfighting domains. Although we should be careful not to exaggerate the capabilities of a new domain, it is essential to understand how a new domain can change warfare. The consequence of failure to adapt to new warfare environments can lead to strategic surprise and immobilization in times of crisis. Understanding cyber power requires us to follow the journey of airpower from inception to equal status with land and sea power. How airpower became an effective part of the joint force is important, but equally important is the strong cultural resistance to air domain development in favor of the more traditional domains of sea and land. The leaders of the US military before World War II did not grasp the full extent of what would be needed for the air domain. Despite some small organizational wins for air forces, there was a definitive line governing how far airpower would be allowed to go. The concepts for airpower effectiveness did not resonate with the established leadership, and led to strategic consequences. For cyber domain effectiveness, the US should look again at the air domain and avoid fighting wars always one domain behind.

The debate for an independent air force spanned four decades through two world wars, and arguably could have continued indefinitely, if not for a catalytic event. The autonomy of the Air Corps was eventually granted, not because of acceptance of the air domain as a coequal domain based on theory and debate, but because of the complete failure of both the Army and Navy to defend against an air attack. On December 7, 1941, the air defenses of the US

completely failed to defend the nation from an external threat, "the assault, which lasted less than two hours, claimed the lives of more than 2,400 people, wounded 1,000 more and damaged or destroyed nearly 20 American ships and more than 300 airplanes."[41] Despite implementation and availability of advances in technology, like radar, that were needed to understand what was happening in the air that day, the mindset of Army and Navy personnel at the time led to dismissal of critical warnings and actions that could have prevented the failure. The story of Pearl Harbor is a familiar one to many military officers, but what is significant about this moment in history for this case study is that it was the catalyst for the reorganization of how American forces fight in the air domain. After Pearl Harbor, the President granted the Army Air Corps temporary autonomy.[42] Although true independence of the air force was far from complete at this point, the importance of the air domain could no longer be ignored since the US had clearly suffered a strategic attack through the air. The morning after Pearl Harbor, it is uncertain whether the President's decision for air autonomy was based more on the promise of the strategic attack capabilities the air domain offered to gain retribution or fear that the Army and Navy were unable to defend the homeland against a clear external threat, but there may be some clues in the historical record. Immediately following the attack, senior government officials made public statements about how the US might use airpower in a strategic attack role to exact revenge. Senator Thomas Connally, Chairman of the Foreign Relations Committee, said "we shall repay their dastardly treachery with multiplied bombs from the air and accurate shells from the sea."[43] Although statements like his were certainly what the public was likely looking for at the time, in governmental meetings the tone was far different. Civilian leadership sought answers to address the immediate question of how it could have happened in the first place.

To put ourselves into the context of the leaders of the time, for three and a half decades airmen had warned that warfare had changed and the nation would face new threats through the air domain; Pearl Harbor called into question whether the organization of the Army and Navy was adequate to defend the nation from those threats. When convening the Cabinet to discuss the attack, President Roosevelt considered it "the most serious meeting of the Cabinet that had taken place since 1861."[44] Immediately after Senator Connally's previous statement and this Cabinet meeting, the President addressed Congress: "the principal defense of the whole west coast of this country…has been very seriously damaged today."[45] The successful air attack on Pearl Harbor seemed to change how the President viewed the world, and called into question whether the US coast could be defended. Congress also recognized the implications for the military and questioned senior military leaders after the President ended his speech. The Secretary of the Navy, Frank Knox, took the brunt of the questions:

> Connally wanted no excuses. "Hell's fire," he exclaimed, "didn't we do anything?"
> "That's about all," answered Roosevelt.
> Connally turned to Knox. "Well, what did we do?...Didn't you say that our Navy was so well prepared and located that the Japanese couldn't hurt us at all?"
> While Knox struggled for a suitable reply, Roosevelt spoke no word to help him…Connally continued to prod Knox. "Why did you have all the ships at Pearl Harbor crowded the way you did? And why did you have a log chain across the mouth of the entrance to Pearl Harbor, so that our ships could not get out?"
> "To protect us against Japanese submarines," Knox answered shakily.
> "Then you weren't thinking of an air attack?"
> "No," Knox answered.[46]

Politicians were furious at the breakdown of military defenses. The mindset of the Navy did not fully comprehend what could happen in an air attack. Despite being on high alert, specifically because of the threat of a Japanese attack due to ongoing political negotiations, they were completely unprepared for an attack through the air domain. The Navy had focused all their attention on threats from insiders or submarines coming from more familiar traditional domains.

Despite numerous warnings, including those by senior Air Corps leaders, the institutional frameworks of both the Army and Navy were biased to ignore or minimize the impact of threats from the air domain. Accounts from soldiers and sailors that survived the attack were filled with complete disbelief that an air attack could achieve such staggering effects.[47] Many accounts portrayed a belief that it was more likely it was some uncoordinated exercise than an actual attack.[48] The thinking that an attack would come from sea or by land (5th column sabotage) was so ingrained that it took bombs exploding in front of many to finally break down that mindset and take action, but many, including senior officers, had no idea what to actually do against an air threat and proved ineffective.

> As they approached, a middle-aged colonel shouted at Reeves, "Do something Lieutenant! Do something!"
> "What should I do?" countered Reeves.
> "I don't know," the colonel retorted, "but do *something!*"
> This exchange somewhat shook Reeve's faith in his senior officers.[49]

The US military was confronted with the realization that it was unprepared to do anything against the air threat. The military deployed advanced air domain defenses like a state-of-the-art radar-fed air operations center and intercept units needed to defend the airspace over the island, but just lacked the mindset needed to develop the tactics and procedures needed for adequate air defense. They suffered from strategic surprise. The defense of the air domain could not be seen as anything other than total failure; the Japanese had reached the target, inflicted massive damage, and lost only a handful of aircraft.[50]

The defense of the newer air domain contrasted sharply with the defense of the more familiar sea domain. The two-pronged attack on Pearl Harbor included both aerial bombing and midget submarines infiltration, and the Navy was well prepared for submarine warfare. Navy destroyers established defensive zones and did not hesitate to target and destroy merely

unknown, potential subsurface contacts in the defended area.[51] When Navy ships sighted the potential sea threats they did not hesitate to act and eliminate them. The Navy successfully defended the harbor from sea domain attack; the Japanese submarines had failed to penetrate the harbor and all attacking subs were lost.[52] The Navy proved capable of defending Pearl Harbor from a more familiar and expected threat.

The US was not alone in a difficult path toward air forces independence. Many other countries only reorganized their militaries to maximize the new air domain after they were faced with similar failures. The United Kingdom was one of the first nations to organize an independent air force, but this was only done after they found themselves incapable of stopping the Zeppelin raids over London, followed later by fixed wing raids. The British public was incensed at the inability of the War and Admiralty efforts to defend the air domain, which led to the creation of the Royal Air Force.[53] From the birth of these early air forces, it is apparent that failure was one of the primary motivating factors for political leadership to change the status quo.

Although the US military was not reorganized until after the war, the path to independence was laid by the events on December 7, 1941. The unfortunate truth is that it was unlikely the air domain would ever have been considered an equal warfighting domain without such a destructive, catalytic event as Pearl Harbor. Organizational structuring decisions are always easier in the hindsight of a failure than the prognostication of the future. It is clear that when militaries are presented with challenges from a new domain, there is a deliberate and usually effective effort to prevent the equal status of the new warfighting domain until failure forces change. Furthermore, even when it is realized that the new domain is important, leaders raised in the previous domain will believe their knowledge of the old domain is sufficient for the

new one. Rationalizations based on the biases and perspectives of the importance of the land and sea domains minimized the importance of the air domain and marginalized the need for leaders raised in the new one. The most disturbing aspect is that this tension is rarely resolved until structures, theory, and tactics built for the older domains prove inadequate, ending in catastrophic failure.

BUILDING THE CYBER FORCE OF THE FUTURE IN THE PRESENT

"The culture of hacking in China is not confined to top-secret military compounds where hackers carry out orders to pilfer data from foreign governments and corporations. Hacking thrives across official, corporate and criminal worlds. Whether it is used to break into private networks, track online dissent back to its source or steal trade secrets, hacking is openly discussed and even promoted at trade shows, inside university classrooms and on Internet forums."[54]

The United States should take a serious look at whether it needs the benefits that an independent cyber service could provide. Where the US as a nation continues to grow a robust information technology and cybersecurity culture, many other nations idolize hacking skills and have developed robust industries around offensive tactics. The US may be at a cultural disadvantage to develop ideas needed for both information-based and effects-based warfare in the cyber domain. Strategic surprise may be only as far as the next major nation-state conflict. In remains to be seen if the US has the military organization necessary to develop the theory, strategy, and tactics needed for cyberwarfare as an integrated part of the joint force, or if we have simply tethered ourselves to recycling other domains into cyberspace while subordinating cyber to the more traditional military culture. It is uncertain if the cyber warriors we need for the future will have to mold themselves to fit the expectations of the current establishment while trying to innovate new ideas within the boundaries set by those who grew up in other domains. The full extent of what it might mean to create the US Cyber Service are beyond the scope of this section, and needs much more in depth study, but there are several characteristics of a service that are presented that provide distinct advantages over the current COCOM-centric construct. The DoD created a warfighting organization that continues to focus on organizing, equipping, setting training and tradecraft standards, writing policy, and may even soon have budgetary powers, and has left the services with the responsibility of growing soldiers, sailors, and airmen to operate in the command for a tour before returning to their services.

Cyberspace is no longer a new and emerging field. Alan Turing developed the first computers in the 1930s, and the ARPANET first began talking in 1969.[55] The US is developing a strong culture of cyber security experts, but this does not necessarily translate to the skillset needed to develop and innovate cyberwarfare theory, strategy, and tactics. Many other nations have a broad segment of the population that idolizes these skills that the state can cultivate and draw upon. An entire generation of Americans is growing up as digital citizens with Presidential elections won online perhaps more than in televised debates, yet the US may not be inherently developing the innovative culture needed for cyberwarfare; the US may have to create a culture within the military to do so. Cyber long ago exited its infancy, and is in a state of suspended adolescence. The full impact of creating an independent cyber service is beyond the scope of this paper, but it is time for serious study about whether the need for an independent cyber service has already arrived. Fundamentally, we must ask ourselves if the cyber organizations we already created will achieve the results we intended, and whether there are advantages in efficiency, doctrinal development, workforce development, etc. that a cyber service would provide to the joint force or if USCYBERCOM will simply have to suffice.

USCYBERCOM is a COCOM, an organization of action, and with the current organizational structure, USCYBERCOM may find itself in the position of feeling it has to conduct operations to justify its existence where USPACOM does not. This may put friction within the command structure to force operations that demonstrate the ability to project military power in cyberspace or expand USCYBERCOM operations into missions like espionage and counterespionage that are not the purpose of joint military forces. Expansion into alternate peacetime missions could deemphasize the importance of wartime joint functions like maximizing military combat efficiency through effective cyber-dependent C2, protection through

cyber hardening of military weapons, and ensuring the integration of cyber tactics across the joint force for a contested cyber environment. Overprioritization of offensive operations, especially easily measurable kinetic operations with physical effects, could lead to strategic consequences during joint operations because of unnecessary political risks, with highly questionable effects on the battlefield to support the joint fight and even cause Law of Armed Conflict (LOAC) concerns. With the current construct, coupled with the way that Americans fight wars, we may have sentenced cyberwarfare theory to a state of arrested development of which our adversaries may not be similarly bound.

What is absolutely clear is the critical need for a DoD organization to be responsible for the cyber domain, though a COCOM is the existing, but perhaps less efficient model. USCYBERCOM has focused on organizing cyber forces, creating training standards, and may even soon gain acquisition control similar to USSOCOM, though the intent of USSOCOM acquisition authority was very limited. The latter focus is the clearest signal that there are flaws in the organization of cyber forces. USCYBERCOM continues to leverage the elder partner, NSA, for many of the tools and tactics needed to conduct cyber operations. As this occurs, USCYBERCOM continues to adopt the personality of an intelligence organization, focusing on intelligence-like activities with intelligence-like tradecraft while simultaneously looking at the need to innovate without the ability to develop the typically service-provided platforms needed. It is highly questionable whether the acquisitions process of any existing industrial age military service is adequate to meet the needs of the cyber domain. Although this revelation may further drive decision toward the USSOCOM model, the missions of these two organizations should not be similarly compared. USCYBERCOM is responsible for an entire warfighting domain and needs a service-level train, organize, and equip capability, not limited SOF-like capability.

Instead of simply repeating the mistakes of Vietnam and giving an organization both independence and autonomy in warfighting, the more prudent course would be to identify what qualities a cyber service truly needs and determine if the COCOM model is inappropriate to meet these needs.

The argument against creating a cyber service may be that cyber has not yet matured, but that statement may be the exact reason cyber innovation is stagnating and a continuously increasing bill plagues already existing cyber forces. The joint GCCs should be the focus of joint warfare. The military needs a service to build the forces and theory needed for cyberwarfare, not to slowly follow a path to become a new cyber-SOCOM for limited clandestine actions separate from the joint force. Nor should cyber continue to be just the communication enablers of the joint force. The military needs warriors to look at how adversaries will use cyberwarfare across the spectrum of military domains as part of their joint warfare, and develop the theory, strategy, and tactics needed to defeat them. What is essential to joint warfare is for commanders to accept the cyber domain as a critical enabler to maximize the efficiency and effectiveness of joint operations, and understand where cyber fits in joint warfare with a cadre of professional cyberwarfare experts raised in the domain to fight alongside them. In order to support truly joint operations, the following are the advantages a cyber service affords:

Budgetary Control: A cyber service brings together the experts in the domain and gives them the education, training, tools and resources they need to support the joint warfighter. The bill for cyber has continued to grow, and we have to question whether innovation is keeping pace making us more secure in the cyber domain today. All the signs point to increasing inefficiencies in the system in a time when other domains are forced to do more with less. This cost will continue to inflate as long as all the services continue to acquire their own tools in addition to a

COCOM now entering the budgetary mix. Furthermore, truly innovative capabilities are often deeply buried in budget structures built for land, sea, and air and have difficulty rising to the top for sustainment. In the pressure of a system of forced competition for an annual budget, it becomes difficult to make prudent decisions about the future force, especially when mixed with the mindset of a bar set for other domains. The more prudent course of action would be to consolidate all these service capabilities and eliminate the need for a unique COCOM budget structure.

Cultural Mindset: The traditional military mindset is to argue that cyber can outmatch kinetic forces, but that is an extremely small subset of cyber operations, and possibly the least valuable for the US. In the heart of cyberspace operations lies deception, many offensive cyberspace ops require deception to penetrate targets, but often this mindset extends only to target penetration and not the nature of warfare in an information-based domain. The mindset necessary to truly realize the advantage of competent cyberspace forces has yet to be created within the armed forces of the United States, but needs to be grown quickly as the US is already behind. What exists today is the reuse of doctrine designed for the parent services in an attempt to relate to the leaders of the traditional services. As each service continues to build doctrine fitting their own culture, we grow further away from true domain innovation.

Cyberspace is different from traditional warfare since it is a battle over the operational efficiency of the armed forces through the control and manipulation of information. It is less about direct conflict as is the case of every other domain. Cyber may only occasionally have a role causing direct effects in other domains, but could greatly influence the effectiveness of traditional forces. If a boxer faces a chess player in a physical contest, there is usually an obvious conclusion. Cyber is not a chess player in a boxing match. The much better analogy is when two

boxers fight, one clearly outmatches the other, but the stronger boxer fights confused and tired with his vision clouded, having been manipulated through actions outside of boxing. The weaker boxer is then able to exploit the stronger boxer's weaknesses more efficiently, needing less strength and speed to win. Cyberwarfare changes capabilities and perceptions of the boxers or the conditions of the boxing ring itself. Cyber operations will only rarely directly strike enemy targets, but they do disrupt enemy situational awareness and logistics chains or insert doubt or confusion into enemy decision-making processes.

It is questionable whether a physical-based kinetic mindset, which could be called air-mindedness for the Air Force, will be optimal to understanding the linkages in how information moves and is handled to achieve cyber effects. Cybermindedness is built for an information-based domain. In an information-based domain, both counterintelligence and intelligence ideas about obtaining or controlling what an enemy knows using information as a weapon may play as important a role as kinetic-effects cyber ideas in a future cyber service structure. Instead though, the same standards that air forces once had to meet may be applied to cyber theories. Cyber forces are being asked to prove joint value by demonstrating the capability to achieve independent decision over land, air, or sea forces through unproven kinetic effects. The most value for cyber forces occurs when they are treated the same as all other military forces, fighting in unified and joint action to preserve or provide cyber advantage to the joint force. Cyber is not a function to be separated from the joint force, it is meant to enhance our own forces and degrade the adversary.

Doctrine: We fight in cyberspace in a completely different way than any other domain, but this occurs not because of the unique tactics needed for the domain, but because of the decision to subordinate cyber forces deep within each service. Established through joint doctrine,

cyber forces also possess near autonomous action as a functional combatant command outside the traditional GCC structure. In essence, the joint doctrine for cyberspace runs counter to all other joint doctrine and is inherently deficient to fight most of the battles in the cyber domain of the future. Cyberwarfare is efficiency warfare, built to enable more effective friendly forces and disrupt opponents. The fact that cyberwarfare can have direct kinetic effects (fires) has caused the joint community most familiar with other domains to focus on the kinetic side of cyberwarfare, instead of the information-based side. Cyber domain doctrine does not easily link up military units to the interagency or civilian sector, which is essential for cyberwarfare. Numerous senior military officers over the last decade have stated, "we are at war in cyberspace."[56] Joint planning focuses on phase 0 operations for this state of undeclared war, when in fact, a state of war only exists in cyberspace when political leaders consider us to be in an overall state of war. Operations with an underlying tone of an already existing war betray the more accurate state of foreign espionage activity in the cyber domain. The fact that foreign spies are operating in the United States within the military does not mean we are at war. Cyber doctrine may have been founded on a misconception about the state of conflict in cyberspace. The idea of warfare functionally disconnected from the rest of the joint force has rarely proven successful and so there is no reason to believe cyberspace will be different. The intent of joint planning is not to lead to a state of conflict when one does not exist. If cyber espionage is impacting national security, appropriate tools should be use to counter that threat and not escalate the state of conflict. This doctrinal and joint planning disconnect may indicate a need for new doctrinal approaches for joint operations in and through the cyber domain that a service should develop.

Recruiting: The ability to recruit service members may be the most important advantage of a separate service. During the recruiting process, military members are attracted to the culture and the mission of their particular chosen service. No potential recruit can choose to become a member of USCYBERCOM, but they can choose to become a member of the USAF. If they are interested in gaining the skills needed to win the nation's wars in cyberspace, they must first obtain selection for a cyber-related career field balanced with the needs of the rest of the Air Force, even if they possess the necessary prerequisites. Every service will fill its needs based on the priority structure of their missions. The same potential recruit may have exactly the right background and aptitude to be either a cyber operator or an aircraft electronics technician or even a boom operator. As is common with many who possess some of the best aptitude to be cyber operators, they may not have interest in the chance of other careers fields. They may be interested in military service specifically to obtain the training and education necessary to operate in cyberspace, possibly in a civilian career after service. Although there is a potential wide range of professions needed for successful cyber operations including intelligence analysts, hackers/penetration testers, network administrators, malware engineers, software developers, and even law enforcement/counterintelligence agents, all of these may have an attraction based on their involvement in the cyber domain. In China, hacker culture is cultivated and encouraged, with military competitions; many civilians aspire to become hackers for China's military.[57] The ability of a service to tailor their personnel needs and compete for recruits is the greatest advantage that services employ that COCOMs cannot.

Advocacy: Cyberspace operators have found no shortage of advocates to argue that cyberspace will be important to the wars of the 21st century; however, what those voices lack is unity. If the senior officers were polled on whether cyber is important to the US military, almost

all would emphasize its importance. But if the same group was asked *why* they think cyber is important and *what* they need to fight in cyberspace, they would likely have a vast array of answers. The most complicated and rarely asked question might be *how* do you fight in cyberspace; the array of answers from military leaders might vex senior civilian leadership, and certainly cause hesitation to approve operations. Even more complicated is the way USCYBERCOM was created tethered to NSA. The result is constant speculation about conflict of interest between each side of the facility at Ft Meade. Intelligence culture may be the more potent and established force, and adoption of operational models and policy intended for the intelligence community is a natural state for such complex matters. Advocacy may be split between the needs of military power projection, joint force support, and intelligence gathering. These positions may be fundamentally at odds, and prone to internal competition, and may influence the perceptions of top military leaders.

Training: We should ask ourselves if the four different service training pipelines are preparing our cyber operators for the right fight. The most practiced cyber tradecraft was developed long ago by NSA, and that has certainly transferred to USCYBERCOM. It remains uncertain if this is the right approach. The tactics necessary to attack and defend in a heavily contested domain may not yet be developed. The current status of training may be merely preparing a force to conduct clandestine cyber intelligence operations and limited cyber special operations. If faced with a large-capacity nation-state adversary with robust integration of information-based effects, cybersecurity may be overwhelmed, and offensive cyber actions may have little effect on disrupting the scale of attacks and penetrations supporting a joint force. The tactics employed will be very different when coupled with conventional forces instead of training for cyber on cyber engagements. Although necessary, clandestine penetration is only a fragment

of the skills needed for true warfare with a cyber component. What is needed more than training is professional military education for the cyber domain. Every service has different levels of schools to focus on their respective domain focus. Cyber education is still in a state of evolution, and may not be sustained without dedicated service backing.

Career Management and Preservation of Expertise: It is natural for leaders to look at themselves to determine what makes an effective leader. In this way, current leadership looks for their same qualities and expertise in the next generation. This works relatively well in an established organization, but when new missions, innovation, and adaptation for a new domain is needed, this can cause great friction between current leadership and future leaders. There is no easy way to solve this dilemma. It is one of the problems that led to Billy Mitchell's courts martial, and was a constant complaint of many early airmen. One of the formative principles of the Air Force was that it would be led by airmen. Even when missions change, it is natural for the organization to have resistance to changes in leadership makeup. The Cyber domain was of national importance since at least the Reagan Administration, but yet the military still struggles to develop effective cyber strategy and build the cyber officers needed to pioneer the theory and tactics for the new domain.

The Services inherently plan and manage the careers of the officers and enlisted based on the needs of the service. There is little incentive for cyber innovation since every innovation is unlikely to offer significant career advancement when confronting the status quo. If one culture and mission is the dominant one, the careers most directly related to that mission will be paramount, especially at the senior ranks were doctrine and strategy decisions will be made. In nearly all cases in the existing services, cyber experts are not in charge of cyber organizations. Space operators dominate the senior levels of the AFSPACE-owned cyber force structure of the

Air Force. Without cyber professionals, which are different than communications professionals, at higher ranks it is likely doctrine and strategy will reflect the views of the dominant culture. Even if cyber experts are involved, their influence may be limited. Essentially, having a dedicated cyber service builds enduring institutional expertise and professional focus on a domain with leaders who are raised in the domain.

HEADING INTO THE FUTURE IN THE CYBER DOMAIN

"The best way to predict the future is to invent it."

-Alan Kay, Innovator and Computer Scientist[58]

Today, the United States Air Force is an accepted component of US military power, but the creation of an independent air force occurred despite staunch resistance to change from throughout the War Department. The USAF is a valuable case study for the organization of cyber forces. The USAF is now responsible for delivering capabilities to the geographic combatant commands as an institution built around the unique capabilities of the air domain, as cyber forces should be built around the cyber domain. The cyber forces of the Department of Defense are organized differently than all other military domains. As early airpower advocates once claimed about the air domain, cyberspace appears to offer a new domain that promises a revolution in military affairs. When the nation was presented with legitimate air threats, we were uncertain of what the emergence of the air domain would mean for the joint force of the future, and this uncertainty is also present in the cyber domain today. The US has invested heavily in cyber forces, but we have to ask if the cost of our military cyber organization has produced the force the nation needs. The US military was reformed around the cyber domain before an effective theory for employment of cyber forces was developed.

The decision to create USCYBERCOM was based on the best information available at the time, but today we should know better. Instead of addressing the limitations of the organizational construct by building the organizations we actually need, we find ourselves doubling down on our past decisions in cyber organization, granting more authorities, more resources, and more budgetary and acquisition control to a construct built for other domains and prone to failure. The cost of conducting operations in cyberspace through the current COCOM

model can only increase and invite friction within our own forces and create seams for our adversaries to exploit. Worse, if a catastrophic event were to occur, we may tell ourselves we simply didn't invest enough. Finally, the pressure to make the current system work intensifies with every dollar added to cyberspace forces.

We have to ask ourselves if we have actually built the cyber organization for the COCOMs to utilize in joint warfare, and that answer may be strategically dangerous if wrong. The perception that an organization exists to prevent a major cyber incident betrays the fact that we may have created the exact conditions necessary for an adversary to exploit. When we look back at this time in the history of cyber force organization, we may decide we were lucky, at best, that a significant incident did not happen, with the history of airpower as a warning. We may question our understanding of cyberwarfare, looking back on the strategic attack theories of cyberspace and their disconnection from joint force operations. At worst, we will realize through failure that an adversary figured out first how to incorporate cyberwarfare into joint warfare. We may then learn from their example of cyber power. The lessons of the past are already there for us to see how to manage a new domain. We must resist the human condition that makes us defend a potentially inefficient or ineffective status quo that feels politically more comfortable. If we wait to make decisions based on our current criteria, those decisions may come too late. The US needs to repurpose a cyber command into a cyber service, and join that domain to the geographic joint force. A more effective organizational structure for cyber forces can be created. It will not become easier to reverse our current course as more of the military culture becomes indoctrinated in the mindset of the organizations they grew up in. If the current system is not working, then it needs to change before we prove to ourselves that we were not ready for the challenges of the 21st century.

Today we stand paralyzed in fear of the unknown, transfixed on the future but afraid of making the wrong decision about something we do not understand. So we stand firm preserving the status quo, creating stovepipes and calling it innovation. We fail to remember the same mistakes we made once before and the consequences of failure in vision. We will marginalize true innovation when it gives cultural discomfort, and we convince ourselves that our experience in unrelated domains make us experts in leading forces in new ones. Instead of thinking about where we want to go, we convince ourselves that we can solve our cyber problems with broader powers, more authorities, laws that enable more intrusive capabilities, and heavily investing resources instead of thinking about whether we are building a structure already known to fail. If we stay the course, the only option may be to grant highly intrusive authorities normally reserved for intelligence and counterintelligence forces that will allow autonomous action even when not needed to support joint warfare. This may end up being a greater threat to the American way of life than threats which we hope to defend against.

---

[1] Colin Gray, *Airpower for Strategic Effect* (Maxwell AFB, AL: Air University Press, 2012), 35.
[2] Tom Clancy, *Every Man a Tiger* (New York, NY: G.P. Putnam and Sons, 1999), 474-475.
[3] Breckinridge o Scriven, 7 Aug 1913, in Sig. C. files, 29278, in National Archives in *The Question of Autonomy for the US Air Arm, Part 1: 1907-1945.* 31-35.
[4] Charles J. Dunlap Jr., "Perspectives for Cyberstrategists on Cyberlaw for Cyberwar," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos et al. (Boca Raton, FL: Taylor & Francis Group, 2014), 214-215.
[5] "International Engagement in Cyberspace Part 4" https://www.youtube.com/watch?v=3MF9JjnYGDE (accessed 10 February 2016).
[6] Joint Publication 1, IV-2.
[7] "US Cyber Command" https://www.stratcom.mil/factsheets/2/Cyber_Command/ (Accessed online 24 Jan 2016).
[8] Senate Armed Services Committee, "Statement of Admiral William E. Gortney, United States Navy, Commander, United States Northern Command and North American Aerospace Defense Command Before the Senate Armed Services Committee" (Washington, DC: March 12, 2015), 12.
[9] Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (1942; new imprint, Washington, DC [or D.C.]: Office of Air Force History, 1983), 19.
[10] Curtis E. LeMay Center for Doctrine Development and Education, "Air Force Doctrine Volume III – Command" https://doctrine.af.mil/download.jsp?filename=Volume-3-Command.pdf (June 5, 2013), 43.
[11] Mark Kendall Wells. *Aviators and Air Combat: A Study of the 8th Air Force and R.A.F. Bomber Command*. (Department of War Studies, Kings College, July 1992), 2-3.
[12] Colin S. Gray, *Airpower for Strategic Effect* (Maxwell AFB, AL: Air University Press, 2012), 138.
[13] Ibid, 137.

[14] Ibid, 137.
[15] William Momyer, *Airpower in Three Wars* (Maxwell AFB, AL: Air University Press, 2003).
[16] James Kitfield, *Prodigal Soldiers: How a Generation of Officers Born of Vietnam Revolutionized the American Style of War* (Washington, DC: Potomac Books, 1997), 358.
[17] Marshall Michel, *The 11 Days of Christmas: America's Last Vietnam Battle* (San Francisco, CA: Encounter Books, 2002), 55-57.
[18] According to B-52 crews at the time, this was based on limitations to the bombsite technology developed for nuclear warfare that could have been overcome. The bombsite on the B-52 needed a set period of time to stabilize the gyros. If the aircraft was performing maneuvers to throw off enemy targeting, the gyros in the bombsite could not compensate, and would result in less than optimal precision. This would have been unacceptable to SAC leadership at the time who regarded this as a measure of bomb crew skill. In actuality this only meant the last minute of the bomb run had to be straight and level. Interview with B-52 Bombardier/Navigator Instructor from 1979.
[19] Marshall Michel, *The 11 Days of Christmas: America's Last Vietnam Battle*, 193-201.
[20] Ibid., 222-224, 229-231.
[21] Ibid., 232-233.
[22] Tom Clancy, *Every Man a Tiger*, 212-217.
[23] Ibid., 263.
[24] Martin Libicki, *Crisis and Escalation in* Cyberspace, (Santa Monica, CA: RAND Corporation, 2012), 66.
[25] Ibid., xi, 1.
[26] Colin Gray, *Airpower for Strategic Effect,* 35.
[27] Lecture in Wood Auditorium (Maxwell AFB, AL: 23 Nov 2015).
[28] Michael V. Hayden, "The Future of Things Cyber," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos et al. (Boca Raton, FL: Taylor & Francis Group, 2014), 5-6.
[29] Dr. James Forsyth speaking before the Air Command and Staff College.
[30] Alfred F. Hurley, *Billy Mitchell: Crusader for Airpower*, 72-73.
[31] William "Billy" Mitchell, *Winged Defense* (Tuscaloosa, AL: The University of Alabama Press, 1925).
[32] R. Earl McClendon, *The Question of Autonomy for the US Air Arm, Part 1: 1907-1945* (Maxwell AFB, AL: Air University Document Research Study, 1950), 101.
[33] Annual Report of the Secretary of War 1926.
[34] Annual Report of the Secretary of War 1926. 33.
[35] Annual Report of the Secretary of War 1926. 34.
[36] R. Earl McClendon, *The Question of Autonomy for the US Air Arm,* 135.
[37] R. Earl McClendon, *The Question of Autonomy for the US Air Arm,* 81. Citing the *Annual Report of the Secretary of War 1919*. 68-75.
[38] R. Earl McClendon, *The Question of Autonomy for the US Air Arm,* 84-85. Citing the *Annual Report of the Secretary of War 1919*. 68-75.
[39] R. Earl McClendon, *The Question of Autonomy for the US Air Arm,* 95. Citing the *Report of the Director of the Air Service*, 1920.
[40] Gordon W. Prange, Donald M. Goldstein and Katherine V. Dillon, *December 7, 1941: The Day the Japanese Attacked Pearl Harbor* (New York, NY: McGraw-Hill Book Company, 1988), 204.
[41] Barbara Maranzani, "5 Facts About Pearl Harbor and USS Arizona" (2011) http://www.history.com/news/5-facts-about-pearl-harbor-and-the-uss-arizona (Accessed 30 Jan 2016).
[42] R. Earl McClendon, *The Question of Autonomy for the US Air Arm, Part 1: 1907-1945*, 8.
[43] Gordon W. Prange, Donald M. Goldstein and Katherine V. Dillon, *December 7, 1941*, 387.
[44] Ibid., 387.
[45] Ibid., 388.
[46] Ibid., 388.
[47] Ibid., 166.
[48] Ibid., 204.
[49] Ibid., 243.
[50] Ibid., 159.
[51] Ibid., 92.

[52] Ibid., 362-377.
[53] John T. Farquar, *Trenchard, Slessor, and RAF Doctrine before World War II.*
[54] Edward Wong, "Hackers Find China is Land of Opportunity" (New York Times, 22 May 2013) http://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html?_r=0 (accessed 28 Jan 2016)
[55] Computer History Museum, "Internet History: 1962-1992," http://www.computerhistory.org/internethistory/1960s/ (accessed December 20, 2015)
[56] Gen. Stephen R. Lorenz, Air Education and Training Command commander, "Lorenz on Leadership: At War in Cyberspace," (Randolph AFB, TX: 9 Jan 2009) http://www.goodfellow.af.mil/News/Commentaries/Display/tabid/361/Article/375382/lorenz-on-leadership-at-war-in-cyberspace.aspx (accessed 17 February 2016).
[57] Edward Wong, "Hackers Find China is Land of Opportunity" (New York Times, 22 May 2013) http://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html?_r=0 (accessed 28 Jan 2016)
[58] Alan Kay "Alan Kay: Educator and Computing Pioneer" https://www.ted.com/speakers/alan_kay