AIR WAR COLLEGE

AIR UNIVERSITY

IS IT TIME FOR A US CYBER FORCE?

by

Corey M. Ramsby, Lieutenant Colonel, United States Air Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Colonel Charles F. Spencer, Jr.

17 February 2015

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
17 FEB 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Is It Time For A U. S. Cyber Force?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air War College,,Air University,,Maxwell AFB,,AL**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

With the doctrinal designation of cyberspace as an operational military domain comes significant implications that include defending, exploiting, and evolving capabilities in pursuit of national objectives. The designation also raises a debate on US military force structure needed to realize its full potential and whether the current construct can support its development. Can the current Department of Defense establishment meet the demands and potential of the cyberspace domain? Or is a separate force, independent of the other services and agencies, needed to project and protect vital US cyberspace interests?

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a REPORT	b ABSTRACT	c THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**26**	

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Corey M. Ramsby is a student at the Air War College, Air University, Maxwell AFB, AL. Lt Col Ramsby is a graduate of Purdue University (Bachelor of Science, Electrical Engineering) and the Air Command and Staff College. He has served at the squadron, group, major command, center, Air Staff, and Joint Staff levels with multiple deployments to Afghanistan in support of Operation ENDURING FREEDOM. His most recent assignment was as the squadron commander for the 375th Communications Squadron at Scott AFB, IL.

Abstract

With the doctrinal designation of cyberspace as an operational military domain comes significant implications that include defending, exploiting, and evolving capabilities in pursuit of national objectives. The designation also raises a debate on US military force structure needed to realize its full potential and whether the current construct can support its development. Can the current Department of Defense establishment meet the demands and potential of the cyberspace domain? Or is a separate force, independent of the other services and agencies, needed to project and protect vital US cyberspace interests?

Using the US Air Force's path to independence as context for an analysis of cyberspace force capabilities, this essay explores whether the services and combat support agencies can meet strategic national objectives. Or, as suggested by retired Navy Admiral James Stavridis, is an independent US Cyber Force needed? Specifically, the existence of four criterions are explored: a unique, strategic military capability unachievable by any of the other services and agencies; corresponding technological advances; an unrestricted battlespace to develop, test, and refine theories, weapons, and tactics; and political champions to maneuver the bureaucratic and legislative terrain needed to pass legislation to create a separate military service.

Introduction

These days, cyberspace is doctrinally designated as an operational military domain.[1] With this designation come significant implications that include defending, exploiting, and evolving capabilities in pursuit of national objectives. The designation also brings with it a debate on how to structure US assets to realize its full potential and whether the current military construct can support its truest development. Can the current Department of Defense establishment meet the demands and potential of the cyberspace domain? Or is a separate force, independent of the other services and agencies, needed to project and protect vital US cyberspace interests?

In a January 2014 *Proceedings* magazine article, "Time for a US Cyber Force", retired Navy Admiral James Stavridis and US Cyber Command planner David Weinstein call for a separate and independent cyber force to fully develop, defend, and exploit America's newest warfare domain.[2] Using US Army Brigadier General William 'Billy' Mitchell and his quest for a separate US Air Force following World War I as a historical contrast, Stavridis and Weinstein build a case of 'been there, done that' and recommend we learn from our lessons, avoid the bitter debates of who and how cyberspace should be managed, and realize a new contested domain requires a separate force free from the other services internal influences, biases, and priorities. In their words, "we are once again on the beach of Kitty Hawk" and "we should not wait 20 years to realize it". Their position is compelling, but the 20 years of debate they prefer us to avoid actually provide a richer historical context to analyze the touchstones necessary to sway lawmakers, military leaders, and the American public to the idea of a separate force to pursue US military interests in cyberspace. In a sense, proof the other services cannot provide the

capabilities a separate armed force can with regards to national defense in the cyberspace domain must be presented.

The time between the creation of the US Army Air Corps in 1926 and the end of World War II framed the air power debate, tested its major concepts and theories, developed distinct air domain technologies, and set the conditions for a separate air force to further US development and exploitation of the air domain. In this context, one can imagine and correlate an analogous path to an independent cyberspace service. Specifically, establishment of a separate cyber force will require at least four criterions: a unique, strategic military capability unachievable by any of the other services and agencies; corresponding technological advances; an unrestricted battlespace to develop, test, and refine theories, weapons, and tactics; and political champions to maneuver the bureaucratic and legislative terrain in the face of extreme scrutiny, opposition, and political parlay.

For the air domain, the unique capability developed into strategic bombing and the capacity to strike at an adversary's homeland without the need for land invasions or sea battles.[3] The corresponding technological advancement that realized the capability was the long range bomber such as the B-29 with its unrivaled range and delivery of atomic weapons.[4] The battlespace was World War II and the European and Pacific strategic bombing campaigns. And the leadership and proponents for a separate air arm included the likes of Presidents Franklin Roosevelt and Harry Truman, Army Generals Dwight Eisenhower, George Marshall, and Henry 'Hap' Arnold, and Assistant Secretary of War for Air Robert A. Lovett, among others. This is not to say these were the only criterion, just that without them the case for an independent air force would have certainly lacked rationale. And even with the fleshing out of the strategic bombing theories, the advent of long range bombers, World War II, and top US leaders who

backed a separate air force, competing visions and inter-service maneuvering won the day in carving the responsibilities of the air domain amongst each of the combatant arms.

The emergence of a separate cyber force may be as difficult. As Stavridis and Weinstein point out, each of the armed services currently have significant equity in the cyberspace mission. The 2014 Quadrennial Defense Review further entrenches this commitment with the requirement for Cyber Mission Forces sourced via the services.[5] Additionally, the Department of Defense includes the National Security Agency and Defense Information Systems Agency, whose missions heavily reside in the cyberspace domain and in most cases outpace the services capacities and capabilities. The debate for a separate cyber force should not center on whether the cyberspace arm is subservient to the other services similar to the air force debate. The debate should focus on whether or not a separate cyberspace arm can match and exceed existing services and agencies' capabilities without degrading core missions at a resource savings that can overshadow the disruption, disconnection, and overhead costs of establishing a new military branch. Our service creation past suggests these questions will not be answered in the status quo. Altering the nation's military establishment is difficult by design. So much so, a change on the scale of creating a new US military service has occurred once and was preceded by the largest war ever known to mankind.

History shows that the United States rarely built up its military prior to war even in the face of menacing threats (e.g. Germany and Japan prior to World War II).[6] This would indicate the US will unlikely consider such a drastic change to its military force structure that creates a separate cyber force prior to an armed conflict that fully includes cyberspace. And that's assuming cyberspace experts rise to the influential ranks and positions to champion legislation that passes into law. Until then, chances are we'll continue to theorize, debate, and hypothesize

the potential effects of cyberspace power, defend our infrastructure to the best of our abilities, develop and test tactics and techniques short of war, surveille and collect intelligence, and deter others from doing the same to us. The technological advances will also likely lag. Ultimately, nothing shapes and evolves military capabilities like war.

Thesis

This research paper uses a historical case study of the development of a separate US air service after World War II, to assert the establishment of a separate US cyberspace force requires at least four criterions: a strategic military capability unachievable by any of the other services; corresponding technological advances; an unrestricted battlespace to develop, test, and refine theories, weapons, and tactics; and political champions to maneuver the bureaucratic and legislative terrain in the face of extreme scrutiny, opposition, and political parlay.

Cyber What?

Understanding the origins of the term "cyber" help to deconstruct some of its complexity. Today, the term cyber is regularly followed by a pessimistic connotation – attack, warfare, fraud, piracy, espionage, bully, theft, weapon – but can also carry more unexceptional descriptors – café, law, media, shopper, frontier, freedom. The point being, "cyber" is best suited as a prefix. What follows the term "cyber" matters and puts the topic into context. If used alone, "cyber" can, and often, means everything and nothing and complicates the ability to conduct an informed discussion of substance.[7]

Cyber, in its contemporary usage, is a derivative of the Greek word κυβερνητικός (kybernutos) whose meaning relates to government and governing[8] and first popularized by Massachusetts Institute of Technology mathematician Norbert Wiener in his 1948 seminal work on self-regulating mechanisms, *Cybernetics: Or Control and Communication in the Animal and the Machine*.[9] The book introduced, among other things, the theoretical foundation of automata, the principles of digital computing and the benefits of the binary numerical system, the "automatic computing machine", and feedback mechanisms and processes. Wiener's juxtaposition of automata and the human central nervous system foreshadowed today's interconnected world decades before its reality. Wiener wrote, "…automata, whether in the metal or in the flesh, is a branch of communication engineering, and its cardinal notions are those of message, amount of disturbance or noise…quantity of information, coding technique, and so on." Additionally, "They contain sense organs, effectors, and the equivalent of a nervous system to integrate the transfer of information from the one to the other."[10]

In the early 1980s, cyberpunk science fiction writer William Gibson coined the phrase 'cyberspace' in his short story *Burning Chrome* and follow-on novel *Neuromancer*. In *Burning*

Chrome, Gibson introduced the term as the name of a computer hacker's simulator, the Cyberspace Seven, used to access the "colorless nonspace of the simulation matrix, the electronic consensus-hallucination."[11] Gibson furthers the concept of cyberspace in *Neuromancer* where he develops it as a "Consensual hallucination experienced daily by billions of legitimate operators, in every nation" and a "graphic representation of data abstracted from banks of every computer in the human system" with "unthinkable complexity".[12]

Both Wiener and Gibson theorized the military uses of both cybernetics and cyberspace well before the capabilities existed. Fast forward to the present, and joint doctrine is catching up to those realizations. Take for example, the definition of cyberspace as published in Joint Publication 3-12 (R) Cyberspace Operations (5 February 2013):

> …. Cyberspace, the global domain within the information environment consisting of the interdependent network of information technology (IT) and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[13]

JP 3-12 further goes on to explain cyberspace in terms of three layers: physical network, logical network, and cyber-persona.[14] For the purposes of this essay, this is the definition that will be used to assess and analyze the merits and challenges of establishing a separate US Cyber Force.[15]

Criterion #1: Strategic Capability, Strategic Paradox

Because the missions of the services and the combat support agencies are so ingrained and dependent on cyberspace, the first criterion to be met in the discussion of a separate cyber force is that of a distinct strategic capability unique enough that only a separate service could provide it. Otherwise, a separate cyber force would require a profound cost-benefit analysis so monumental in savings and mission advancement the services and agencies could not refute,

dispute, or refuse its potential. At the present, neither exists. If the former did exist, would we know what it looked like? Chief of Staff of the Air Force General Mark Welsh provided a potential view during his Air Force Update speech at an Air & Space Conference and Technology Exposition in September 2014.

General Welsh stated the Air Force needs "an air component commander capability to sit in the [Air and Space Operations Center] when the big fight starts, hit the cyber easy button and watch the enemy RPAs [remotely piloted aircraft] pool at his feet. Or when the enemy starts to shoot missiles toward friendly forces, employ a tool that allows these missiles to sit and sizzle on the pad or go half way, turn around and go home."[16] He followed the comment with the question of who might be working the solution and how it could be expanded "in a big way." Meant to be forward leaning and thought provoking, Welsh's comments fortuitously highlight two existing aspects of cyberspace: cyberspace power theories are primitive but evolving and, much like the early theories of air power, can be perceived as a panacea above existing weapon capabilities and strategy.

These perceptions of cyberspace seem eerily reminiscent of the interwar air power theories developed by Giulio Douhet and Mitchell. David MacIsaac provides a treasure trove of intellectual analysis on early air power theories in his influential essay *Voices from the Central Blue: The Air Power Theorists*.[17] One of MacIsaac's more interesting cogitations is the visions of air power "invariably outran the reality of the moment" clouding the debate with disappointment and derision based on aspirations that air power could "provide quick, clean, mechanical, and impersonal solutions to problems which others had struggled for centuries." [18] The "cyber easy button" proposed by Welsh bears similar resemblances and therein lies a strategic paradox: the vision of a great capability beyond the means of the services, but

dependent on them to develop it. Douhet and Mitchell well understood this paradox and the reliance on biased army and naval officials to advance air power's role, strategy, doctrine, and capabilities. Though for dissimilar reasons, both surmised air power could not reach its potential while dependent on another service for its development - Douhet called for an "independent air force armed with long-range bombardment aircraft" while Mitchell, less concerned of the particular delivery vehicle, focused on "centralized coordination under the control of autonomous air force command."[19] During their time, both men's ideas eclipsed the strategic utility of the air domain and the airplane remained deferential to land and naval forces.

Cyberspace visions appear on a similar track. Evolving cyberspace capabilities exist today, but rely on the services and support agencies for their development and thus remain constrained by each accordingly. Additionally, cyberspace maneuvers are largely tactical (precisely targeted) and/or so shrouded in secrecy, they remain useless to the public debate of establishing a separate cyberspace force. Thus, the creation of a separate cyberspace force will unlikely precede the development of a unique strategic cyberspace capability.

Criterion #2: Corresponding Technological Advances

The theory of strategic bombing required technological advancements and weapon systems to progress it from thought and debate to reality. Long-range bombers, advanced bomb sights, and atomic weapons all contributed to its evolution. Strategic cyberspace development must include similar technological advancements whether it be software, hardware, or human presence in the battlespace.

Again, looking at the path to US Air Force independence, the long-range bomber underpinned the ambition and premise for service equality. The ability to attack an enemy's

heartland without a land invasion fundamentally changed America's strategic approach to war and the role of the B-29 Superfortress cannot be overstated in this regard. Considered the "greatest gamble of the war", the $3 billion development and subsequent deployment of the B-29 to the Pacific theater in 1944 marked the point where air domain technology converged with interwar theory and propelled air power into an independent rather than a complementary role in World War II.[20] Commanded by General Arnold and the Joint Chiefs of Staff in Washington DC, the B-29s were organized under the Twentieth Air Force and remained autonomous from the three Pacific theater commanders – Admiral Chester Nimitz, General Douglas MacArthur, and General Joseph Stilwell.[21]

To put the strategic impacts of the B-29 into perspective, "with high explosives alone, the 20th Air Force levelled 2,333,000 homes in Japan, and most of the business and industry in sixty cities."[22] The conventional bombing campaign killed "at least 240,000 and wounded more than 300,000."[23] In March – June 1945 alone, Japanese deaths reached 127,000 in its six largest cities.[24] By any measure, the devastation produced by the B-29 produced strategic options and effects not seen prior to its arrival in the Pacific. Coupled with the atomic bomb, the B-29 provided President Harry S. Truman with a one plane, one crew, one bomb, one city capability that destroyed Hiroshima and Nagasaki, culminated Japan's unconditional surrender, and averted a difficult and costly land invasion. In his words, air power had developed to a point "equal to those of land and sea power" and its contributions to strategic planning was as great.[25]

Technological advances in cyberspace pale in comparison with regards to the overall devastation and political impact of the B-29. However, cyberspace weaponry evolution is well underway with the standard bearers being the precision guided malicious software (malware) of the Stuxnet, Duqu, and Flame viruses. All three employed multiple previously unknown (zero

day) vulnerabilities against Microsoft operating system code using trusted hardware vendor certificates to cloak their presence. Though not publicly attributed to any nation, many believe the US developed Stuxnet in an effort to stem suspected Iranian nuclear weapons efforts at the Natanz nuclear facility.[26] The code, so precisely written, activated only after verifying it was indeed in the Natanz internal network by comparing the exact size and number of centrifuges operating in the facility and has been tagged as the first specifically designed cyber weapon ever deployed.[27] Stuxnet set the Iranian nuclear enrichment program back months to years and accomplished what was only militarily possible via kinetic means prior to it.

The challenge with Stuxnet and other similar cyber weapons is discovery leads to obsolescence and the designs unlock to anyone with the skill set to reverse engineer them. Additionally, secrecy and nonattribution prevail as essential aspects in their development and deployment. These factors highlight the juvenescent state of the cyberspace battlefield, prevailing technologies, and the current capacity of the services and combat support agencies to meet national requirements. Therefore, the impact of creating a separate cyberspace service has not reached a point technologically where the benefits can outweigh the costs in terms of disruption and disconnection from the current service and agency structure. That is not to say cyberspace is uncontested or the US is not dangerously vulnerable. Rather, the risk-benefit analysis, especially with the standup of US Cyber Command and the Cyber Mission Forces, remains in favor of the current military service construct.

Criterion #3: Unrestricted Battlespace

Over 45 years since researchers at UCLA first connected to a computer at Stanford, and two decades since the explosive internet expansion of the early 1990s, global interconnectedness

has literally changed the political and social fabrics of every developed nation. Today, modern society relies on cyberspace for everything from commerce to education to social networking to, as noted, national security and diplomacy. This interconnectedness has fundamentally shifted the way nations and societies conduct and resolve conflict because it provides a level of engagement, good or bad, at speeds and depths not previously known. Militarily speaking, however, those speeds and depths remain largely undeveloped and untested. As an example, Stuxnet only introduced us to the fringes of what is possible. As best-selling author and cybersecurity researcher Peter Singer puts it:

> "Yet for all the ways it could change how we engage in military operations, cyberwarfare's greatest legacy may not be any single capability or function. More likely, it will be how this new form of engagement mixes with other battlefield technologies and tactics to create something unexpected. The airplane, tank, and radio all appeared during World War I, but it wasn't until the Germans brought them together into the devastating blitzkrieg in the next global conflict that they made their lasting mark."[28]

Stavridis and Weinstein correctly contrast this state as the "beach of Kitty Hawk" with respect to the first powered, controlled, and sustained heavier-than-air human flights by the Wright Brothers in December 1903. Few, if any, could have forecasted four decades later a nation would lay in both physical and political ruins primarily as the result of the weaponized evolution and employment of the air domain. That evolution did not come easy as it covered two world wars, countless billions of dollars of investment, and incredible loss of life. Put another way, the utility and lethality of the airplane of the mid-20th century existed because of the merger of resources, science and technology, courage, and experience underpinned by the political will to push its capabilities through an unrestricted battlespace. This is not unique to the air domain and one can draw similar analogies to the sea and land domains. Examples include the aircraft carrier, submarine, tank, rifle, and the forces organized, trained, and equipped to operate them. All earned their place in America's arsenal through the crucible of war.

Enduring forces, technologies, tactics, techniques, and procedures in cyberspace will likely travel a similar path. The difference between cyberspace and the other domains resides with the direct access to a nation's cities and its people who rely on and share the same infrastructure as military forces. Again, looking to Singer, "By the end of World War II, all sides were engaging in strategic bombing against the broader populace, arguing that the best way to end the war was to drive home its costs to civilians. As cyberwarfare becomes a reality, the same grim calculus will likely hold true."[29] This calculus reflects political will more than technological advancement although each requires the other. When the political will to strike a nation's centers of gravity through cyberspace emerges, so, too, will the reality of its strategic effects and weaponry and with it the competency to engage in an informed dialogue on how best to man, train, and equip US cyberspace forces. Ultimately, much like air power, cyberspace power may not achieve rapid and unrestrained growth without an unrestricted battlespace. Until then, the true effects of a separate cyber force will remain as controversial as Douhet's and Mitchell's prophecies during the interwar years, emotions will play a significant part in the conversation, and the need for a separate cyberspace force will not extend beyond the abilities of the services and agencies to meet US national interests and objectives.

Criterion 4: Political Champions

Assuming there existed a unique strategic capability in cyberspace with corresponding technologies proven in an unrestricted battlespace, the emergence of a separate force still requires leadership to maneuver the political and bureaucratic terrain. Because of the many actors and processes that shape force structure decisions, political champions are necessary both inside and outside the military establishment. In what Air War College Professor David Sorenson classifies as the national interest paradigm, choices about military force levels "stem

from strategic assessments guided by a combination of national interests and international threats to such interests," and, ultimately, competing priorities shape military investment decisions.[30] Simply stated, resources are finite, competition for them is intense, and compromises matter.

Generals Marshall and Arnold fully understood the nation's political and bureaucratic environment. With the advocacy of Presidents Roosevelt and Truman, they built an air force numbering just over 1,200 mostly obsolete aircraft in the Army's smallest combat arms branch at the outset of World War II to its largest by the end – a first in American military history.[31] Along the way they created equal status of the air arm with the publishing of the War Department Field Manual 100-20, *Command and Employment of Air Power,* and gained a seat at the table in the Joint Chiefs of Staff for Arnold, the nation's top Airman.[32] But it didn't come at the expense of the other forces as Marshall was keen on building a balanced force. While building the Army Air Forces (AAF), he also built the largest Army in US history and reorganized the War Department from the "fiefdoms of the chiefs of infantry, cavalry, field artillery, and coast artillery" into the three commands – the army Ground Forces, the Services of Supply, and the AAF.[33] The reorganization streamlined the Army while also providing the AAF with "sufficient clout to move their requirements with dispatch through the War Department General Staff."[34]

While building the AAF, Marshal and Arnold had to "continually fend off congressional demands on the question of an independent air force", a trend originated in the interwar years that gained additional traction during the war. With an eye to the future, they successfully deferred the discussion until after the war and concentrated on victory and building the legitimacy of air power and the nucleus of Airmen needed to sustain it.[35] As previously noted, this included the high-risk development of the B-29, the autonomous standup of the 20th Air

Force, and the fusion of the bomber and the atomic bomb that pushed the world into the nuclear age. The underlying goal was not just air force independence, but to establish a United States Air Force in the postwar national security reorganization that allowed for its own budget and to seamlessly fit into a "coordinated organization of ground, air, and naval forces in operational theaters, each under its own commander, and each responsible to a supreme commander."[36] The push for a unified, integrated defense establishment, supported by Truman, General Eisenhower, and many others, became part of the National Security Act of 1947 that established the National Military Establishment (later to become the Department of Defense), Secretary of Defense, Joint Chiefs of Staff, the National Security Council, and the Central Intelligence Agency in addition to the United States Air Force.[37] Air Force independence was established, but in the context of much larger national security changes to deal with the postwar world order.

With the exception of Stavridis, there does not appear to be many leaders, military, congressional, or otherwise, backing the formation of an independent US Cyber Force. Most agree the US is dangerously vulnerable in cyberspace, but do not look at it as a purely military problem that a separate force could solve. From a military perspective, the standup of US Cyber Command as a subordinate unified command under US Strategic Command seems to satisfy the current appetite for restructuring. Looking to the future, the next logical step, as Stavridis points out, may be a modification to the Unified Command Plan (UCP) raising US Cyber Command to full combatant command status.[38] In fact, it's a question the Senate Armed Services Committee asked of Admiral Michael Rogers, current US Cyber Command commander, as part of his confirmation process in March 2014.[39] The question asked: "What are the best arguments for and against taking such action now?" Admiral Rogers stated there were no impediments to an elevation in status other than an increase in staff to accomplish "administrative functions" such

as budgeting and force management at that level. As for the benefits, Admiral Rogers stated, "Elevation to full unified status would improve resource advocacy, allocation and execution by improving input to Department processes and eliminating competition in prioritization. Additionally, alignment of responsibility, authority, situational awareness, and capability under a single commander would improve cyberspace operations and planning."[40] Though this would suggest a change to the UCP, it does not advocate a separate military service.

Furthermore, throughout the 2015 Air War College academic year, influential congressional, government, military, and industry leaders presented numerous views on the threats posed by nations and actors in cyberspace, even suggesting the existence of an ongoing 24/7cyber war. However, not one proposed the need for an independent US Cyber Force to counter the threat. This does not prove one is not needed. Merely, it speaks to the lack of political champions for such change to the military establishment. In fact, when the specific question of a separate force arose, several pointed to the same debate calling for a US Space Force that's existed the past three decades. This common comparison indicates an independent US Cyber Force currently lacks sufficient backing from legislators and military leaders whose support is necessary to draft and pass legislation into law.

Conclusion

Without question, the United States faces unprecedented threats in cyberspace and the military services and combat support agencies continue to feel their way around the terrain developing both offensive and defensive capacity. Because of these threats, and the uneasiness that accompanies them, initial requests for changes in the military force structure have surfaced, to include Stavridis and Weinstein, who call for a US Cyber Force independent of the other services. The basis of their argument is the US traveled a similar path in creating an independent

air force and contrasts the crusade of US Army Brigadier General Billy Mitchell following WWI as a historical context. However, an alternative framework to assess whether the threats warrant a separate cyber force is to analyze key criterion illustrative of the Army Air Forces following World War II. These criterions helped persuade legislators, military leaders, and the American public in justifying an independent air force. Specifically, a unique, strategic military capability with corresponding technological advances honed in an unrestricted battlespace and championed by influential leaders who understood the US government and its bureaucratic and legislative processes.

Using the US Air Force's path to independence as a basis, an analysis of US force structure reveals that the services and combat support agencies currently meet existing national requirements in cyberspace. Also, cyberspace technological advances continue to evolve but remain largely tactical, secretive, and essentially useless in any public debate calling for a change to US military force structure. Finally, though contested, cyberspace remains bound by political will, has not evolved to an unrestricted battlespace, and champions calling for a separate US Cyber Force just aren't very vocal at the present time. Unfortunately, these criterions will likely not be reached until after the first overt, nation state war that extensively includes cyberspace. Much like WWII, that war will look different than anything seen to date, but surely won by the nations who can control cyberspace in a way the Allies ultimately controlled the skies in Europe and the Pacific.

Bibliography

Clark, Richard A. and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do about It.* New York: Harper Collins Publishers, 2010.

Coffey, Thomas M. *Hap: The Story of the US Air Force and the Man Who Built It.* New York: The Viking Press, 1982.

Cray, Ed. *General of the Army: George C. Marshal, Soldier and Statesman*. New York: WW Norton and Company, 1990.

Frank, Richard B. *Downfall: The End of the Imperial Japanese Empire,* New York: Penguin Books, 1999.

Gibson, William. *Burning Chrome*, can be accessed at: http://mith.umd.edu/digitalstorytelling/wp-content/uploads/GibsonW_Burning_Chrome.pdf

Gibson, William, *Neuromancer*, New York, NY: ACE, 1984

Glosbe Greek-English Dictionary, https://en.glosbe.com

Greenert, Jonathon. *Wireless Cyberwar, the EM Spectrum, and the Changing Navy*, Breaking Defense Online, 3 April 2013, http://breakingdefense.com/2013/04/adm-greenert-wireless-cyber-em-spectrum-changing-navy/

Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986-2012*. Washington, DC: Atlantic Council, 2014.

Hurley, Alfred F. *Billy Mitchell: Crusader for Air Power*, Bloomington: Indiana University Press, 1975.

Joint Planning 3-12(R), Cyberspace Operations, 5 February 13.

Joint Chiefs of Staff. National Military Strategy for Cyberspace Operations. Washington, DC: DOD, 2006. http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.

MacIsaac, David. *Voices from the Central Blue: The Air Power Theories*, in *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, edited by Peter Paret, Princeton, New Jersey: Princeton University Press, 1986.

Newitz, Annalee, *The Bizarre Evolution of the Word 'Cyber'*, iO9, 13 September 2013, http://io9.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487, accessed 10 October 2014.

Singer, PW and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know,* New York: Oxford University Press, 2014.

Singer, Peter W. *The War of Zeros and Ones,* Popular Science online, posted 8 September 2014 at http://www.popsci.com/article/technology/war-zeros-and-ones

Sorenson, David S. *The Politics of the American Weapons Acquisition Process*, in *The Process and Politics of Defense Acquisition*. Westport, CT: Praeger Publishers, 2009.

Stavridis, James and David Weinstein. *Time for a US Cyber Force,* Proceedings, vol. 140/1/1,331, US Naval Institute, January 2014. http://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force

Stavridis, James. *The New Triad: It's Time to Found a US Cyber Force,* Foreign Policy, 20 June 2013. http://www.foreignpolicy.com/articles/2013/06/20/the_new_triad

Truman, Harry S. *Memoirs, vol. 2, Years of Trial and Hope,* Garden City: Doubleday and Co., Inc., 1985.

US Department of the Air Force, *Cyber Vision 2025,* AF/ST TR 12-01, 13 December 2012.

US Department of Defense, *Strategy for Operating in Cyberspace*, July 2011.

US Department of Defense, *Quadrennial Defense Review*. Washington, DC: Office of the Secretary of Defense, March 2014. http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf

US Senate Armed Services Committee, *Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command*, Washington, DC, 2014. http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf

Wiener, Norbert. *Cybernetics: Or Control and Communications in the Animal and the Machine*, 2nd rev. ed., Cambridge, MA: MIT Press, 1961.

Williams, Brett, *Cyberspace: What is it, Where is it, and Who Cares?*, Armed Forces Journal, 13 March 2014, http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/.

Welsh, Mark, *Air Force Update* speech at the Air Force Association's Air & Space Conference and Technology Exposition, September 2014. http://www.af.mil/Portals/1/documents/af%20events/Speeches/16SEP2014-CSAF-GenMarkWelsh-AFUpdate.pdf?timestamp=1410982866264

Wolk, Herman S. *Reflections on Air Force Independence*, Washington, DC: Air Force History and Museums Program, 2007

Yannakogeorgos, Panayotis A. and Adam B. Lowther. *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Boca Raton: Taylor & Francis, 2014.

Notes

[1] Joint Publication 3-12(R), 5 February 2013, p I-1.

[2] James Stavridis, David Weinstein, *Time for a US Cyber Force,* Proceedings, January 2014, http://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force, accessed 15 October 14.

[3] Herman S. Wolk, *Reflections on Air Force Independence*, (Washington, DC: Air Force History and Museums Program, 2007), p 55.

[4] Wolk, p. 67-68.

[5] Department of Defense Quadrennial Defense Review 2014, p 41, http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf, accessed 14 Oct 14.

[6] David S. Sorenson, "*The Politics of the American Weapons Acquisition Process*," in The Process and Politics of Defense Acquisition, (Westport, CT: Praeger Publishers, 2009), p 91.

[7] For a more in-depth view on this see Maj Gen (R) Brett Williams' article published in The Armed Forces Journal in March 2014. http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/

[8] Glosbe Greek-English Dictionary, https://en.glosbe.com/el/en/κυβερνητικός, accessed 13 Dec 14.

[9] Norbert Wiener, *Cybernetics: Or Control and Communications in the Animal and the Machine*, 2nd rev. ed. (Cambridge, MA: MIT Press, 1961).

[10] Ibid, pg 42-43.

[11] William Gibson, *Burning Chrome*, p 197, (http://mith.umd.edu/digitalstorytelling/wp-content/uploads/GibsonW_Burning_Chrome.pdf) accessed 13 Dec 14.

[12] William Gibson, *Neuromancer*, (New York, NY: ACE, 1984), p 67.

[13] Joint Publication 3-12(R), p I-1.

[14] Ibid, p I-2.

[15] A differing view, and one the author subscribes to, characterizes cyberspace as not the domain, but rather the tools and platforms used to operate within the domain of the electromagnetic spectrum. Some current senior military leaders, such as Chief of Naval Operations Admiral Jonathon Grennert, share a similar perspective. Admiral Grennert published his viewpoint in an Op Ed titled "Wireless Cyberwar, the EM Spectrum, and the Changing Navy" which was posted on Breaking Defense website on 3 April 2013 and can be found at: http://breakingdefense.com/2013/04/adm-greenert-wireless-cyber-em-spectrum-changing-navy/.

[16] Mark Welsh, chief of staff, US Air Force (address, *Air Force Update* speech at the Air Force Association's Air & Space Conference and Technology Exposition, Washington, DC, September 2014) http://www.af.mil/Portals/1/documents/af%20events/Speeches/16SEP2014-CSAF-GenMarkWelsh-AFUpdate.pdf?timestamp=1410982866264,

[17] David MacIsaac, *Voices from the Central Blue: The Air Power Theories*, in Makers of Modern Strategy from Machiavelli to the Nuclear Age, edited by Peter Paret, (Princeton, New Jersey: Princeton University Press, 1986), p 624-647.

[18] Ibid, p. 626

[19] Ibid, p. 631

[20] Wolk, p. 45, 59

[21] Ibid, p. 48-49

[22] Coffey, p. 374

[23] Ibid

[24] Richard Frank, *Downfall: The End of the Imperial Japanese Empire*, (New York: Penguin, 1999), p. 334

[25] Harry S. Truman, *Memoirs, vol. 2, Years of Trial and Hope*, (Garden City, Doubleday and Co., Inc., 1956), p. 46.

[26] PW Singer, Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, (New York, Oxford University Press, 2014), p. 114-118

[27] Ibid, p. 118

[28] Peter W. Singer, *The War of Zeros and Ones*, Popular Science online, posted 8 September 2014 at http://www.popsci.com/article/technology/war-zeros-and-ones, accessed 13 February 15.

[29] Ibid
[30] Sorenson, p 90.
[31] Wolk, p. 3.
[32] Wolk, p. 30; Coffey, p. 259
[33] Ed Cray, *General of the Army: George C. Marshall, Soldier and Statesman*, (New York and London, WW Norton and Company, 1990), p. 279.
[34] Wolk, 27.
[35] Ibid
[36] Wolk, p. 78.
[37] Wolk, p. 96-97.
[38] Stavridis, *Time for a US Cyber Force.*
[39] Senate Armed Services Committee, Advance Questions for Vice Admiral Michael S. Rogers, USN Nominee for Commander, United States Cyber Command, http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf, accessed 15 Feb 2015, p. 29-30.
[40] Ibid.