AU/ACSC/HELMS /AY15

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

THE DIGITAL GCC: USCYBERCOM AS A COMBATANT COMMAND

by

Christian P. Helms, Major, United States Air Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Group Captain (RAF) Graem Corfield

Maxwell Air Force Base, Alabama

April 2015

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 or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

This thesis examines the organization and authorities of U.S. Department of Defense (DoD) cyber forces. The results of this examination indicate that the existing organization of American cyber forces does not have the authorities required to adequately provide for the prevention of cyber-attacks nor does it effectively project U.S. interests through cyberspace.

U.S. Cyber Command (USCYBERCOM), as it presently stands, has the general framework and knowledge base to protect and defend the United States from cyber threats. As a subordinate unified command however, USCYBERCOM's organization is fragmented, yoked with multiple reporting / directing chains of command, and not a sustainable model for future growth. The Commander USCYEBERCOM is unable to directly advocate for his resource requirements and does not have the logistical capability or to quickly field cyber unique equipment. In order to enable USCYBERCOM with the capability to defend the U.S. against cyber-attacks as well as project American cyber power, the command must be reorganized as a stand-alone Combatant Command with Combatant Command authority (COCOM) granted by a newly legislated Unified Command Plan (UCP).

Contents

USCYBERCOM as a Unified Combatant Command

Legislating U.S. Cyber Command (USCYBERCOM) as a stand-alone combatant command under the Unified Command Plan (UCP) will significantly increase the capability of the U.S. DoD to protect and defend the United States. The current state of our nation's cyber forces is disorganized and lacking the appropriate authorities. USCYBERCOM is a sub-unified command reporting directly to the Commander, U.S. Strategic Command (USSTRATCOM). This subordinate command relationship has left USCYBERCOM open to multiple reporting up-channels headed by competing interest principals and comprised of a variety of fragmented organizations aligned to the specific requirements of the military service departments. A stand-alone USCYBERCOM, empowered with combatant command (COCOM) authority over its own dedicated forces, and task organized in a manner similar to the current U.S. Special Operations Command (USSOCOM) construct would significantly increase the capability of our nation to defend itself and project its national interests through cyberspace.

As it stands the United States is unprepared to face one of the most serious and potentially damaging threats to its sovereignty. Cyber threats to the U.S. have the capability to cripple the core of America's defense, social, industrial, health care, economic, and commercial institutions. Every facet of America's social and military infrastructure is deeply dependent upon cyberspace. With such an entrenchment in the cyber domain, a well-planned, coordinated cyber-attack has the capability to deliver an unrecoverable blow to the American way of life. A recent single incident hack of banking giant JP Morgan Chase & Co. yielded damages in the form of 76 million of its customers' addresses and personal information being compromised.[1] It is not difficult to extrapolate this occurrence to a slightly larger scale and understand how a string of

such attacks on, for example, the American power generation grid could threaten the very survival of the nation.

USCYBERCOM needs to be the organization centrally responsible for the defense of the nation and force projection in cyberspace. In order to demonstrate why it is essential to have USCYBERCOM fill this role through the establishment of a new combatant command, five topics require perusal:

1) What is cyberspace and why it is critical for the U.S. to take cyber threats seriously
2) How are U.S. cyber forces currently organized under USCYBERCOM
3) Why USCYBERCOM's current organizational structure is suboptimal
4) How USCYBERCOM needs to be organized in order to be an effective force
5) How a reorganized USCYBERCOM will enhance U.S. capabilities to protect from cyber threats and project cyber power in support of national interests

Cyberspace as a Warfighting Domain

When considering cyberspace as a both a global information network and a warfighting domain, it is essential to understand what cyberspace is and how it can help the U.S. to achieve its national interests. Viewing cyberspace through the lens of a military planner, Cyberspace is a man-made warfighting domain that transcends borders of nations, space, and time. Through cyberspace, America can protect its forces, project its power, collect intelligence on enemies of the state, and shore up its allies. Cyberspace is a joint operating area, electronic warfare medium, information sharing area, and data repository of America's military cognitive intellectual property. The DoD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe.[2] The DoD also maintains countless antennae, electronic warfare systems, electronic surveillance systems, and cyber intelligence gathering platforms.

Cyberspace, as an information network, is also known by a more innocuous name to the common American - the internet. The internet is the amalgamation of global information

networks inextricably tied together by networks of networks, computer systems, and embedded processors and controllers all sharing data at the speed of light.[3] The internet's physical architecture includes millions of interconnected computers, network routers, and fiber optic cables that allow America's critical infrastructures to work.[4]

Cyberspace is therefore both a data sharing network and a warfighting domain. To a college student taking distance learning, the internet houses endless trails of data and resources to advance their education. To a military planner, cyberspace has the "inherent potential to destroy and/or render useless logical, physical, technical, and virtual infrastructure and to damage critical national capabilities such as economic, government, military, educational, health, social, and other capabilities."[5]

Every aspect of American society is touched by, controlled through, or dependent upon the internet. The nation's military's command and control hinges on seamless communication, and zero delay data sharing. Practically every facet of American infrastructure is virtually controlled and monitored by centralized command networks tied together by computer networks. Such a deep reliance on information networks allows the nation to flourish, and thus, the continuous and safe operation of cyberspace is crucial to America's economy and national security.

The nearly total reliance on cyberspace has left the U.S. vulnerable to connectivity disruption, data corruption, and intelligence gathering attacks. The Defense Department uses cyber networks to enable its military, intelligence, and business operations, including the command and control of the Range of Military Operations.[6] As a result of the DoD's reliance on network command and control, there are a number of state and non-state actors that seek to disrupt not only the American military cyber complex, but the civilian virtual networks of

infrastructure, economic institutions, and social networks.[7] These cyber actors seek to destabilize American sovereignty through the exploitation of the nation's cyber vulnerabilities. Iran, for example, is "extraordinarily active in cyber and aspires to use cyber as an asymmetric counterweight to our conventional weight."[8]

The nation's inextricable reliance on networks and cyberspace stands in stark contrast to the inadequacy of our cybersecurity.[9] Volumes could be written on the shortfalls of America's cybersecurity. Critical areas of American infrastructure are routinely penetrated by external cyber actors. The Defense Department's 15,000+ computer stations are unprotected due to a wide variance of computing equipment deployed in highly tribal virtual environments. America's cyber security strategy is largely focused on detecting threats rather than protecting from threats. The government's acquisition process is driven by purchasing bureaucracy that is incapable of rapidly fielding highly technical and specific equipment.[10] The U.S. Government cannot even come to a consensus of what organization – if any – should be tasked with the protection of the nation's critical infrastructure like banking, power generation, and healthcare.

Although USCYBERCOM is a sub-optimally structured organization – it has the capacity and the capability to become America's nexus of cyber security and cyber power projection. With a significant reorganization, USCYBERCOM has the potential to dominate in cyberspace.

Current U.S. Cyber Force Organization

USCYBERCOM is the highest level of government organization tasked to protect and project America's interests in cyberspace. Of the five warfighting domains (land, air, sea, space, cyberspace), cyberspace is the fastest growing, most unique, most dynamic, easiest to access, and

arguably the most misunderstood domain. It is also America's most vulnerable vector of attack, and the only domain in which the U.S. does not decisively exercise supremacy.

The lack of American cyber strength can be directly linked to the U.S. not taking the defense of cyberspace and force projection through cyberspace as seriously as it should. This is evident in the fact that America's lead cyber organization is fragmented, muffled by competing resources among senior leaders, and subordinate to another military combatant command.

A Suboptimal Organizational Structure

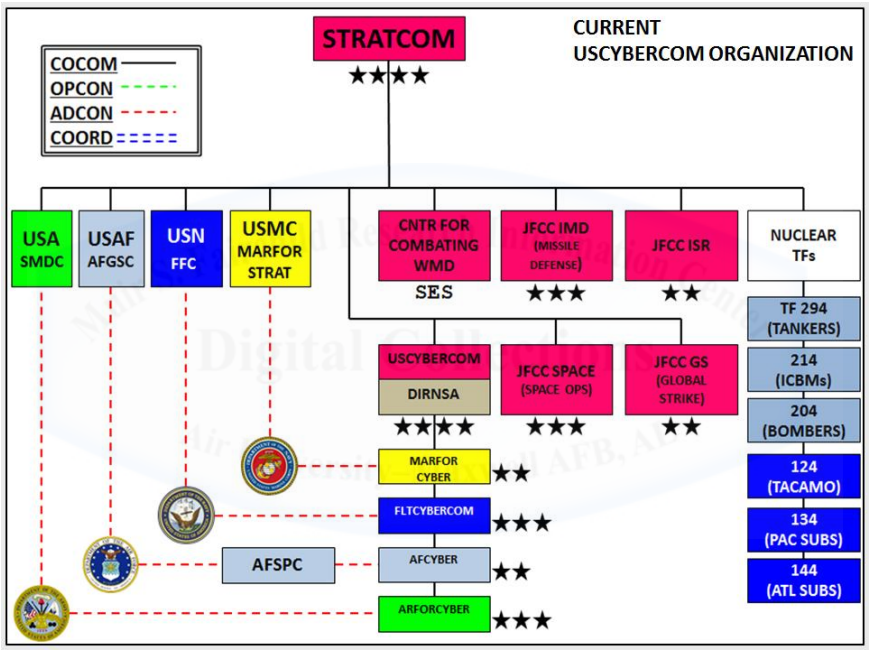

Figure 1: USCYBERCOM Organization Chart

USCYBERCOM is lost in the muddle of U.S. Strategic Command. As a dual-hatted, sub-unified command within STRATCOM, CYBERCOM is on the same organizational level as five other subordinate commands as well as a six-deep nuclear task force responsible for the strategic employment of the nation's nuclear forces (see Figure 1). As a subordinate unified command, USCYBERCOM does not exercise combatant command (COCOM) over its own assigned forces. The lack of COCOM may seem insignificant, however COCOM gives Combatant

Commanders (CCDRs) the ablility to weild substantial power to advocate for their command's requirements and direct its organic forces.

Perhaps the most important aspect of COCOM is the direct line of communication between combatant commanders, the Secretary of Defense, and the Chairman of the Joint Chiefs of Staff. This direct line of communication gives CCDRs an open dialouge with the highest levels of America's military chain of command (see Figure 2).

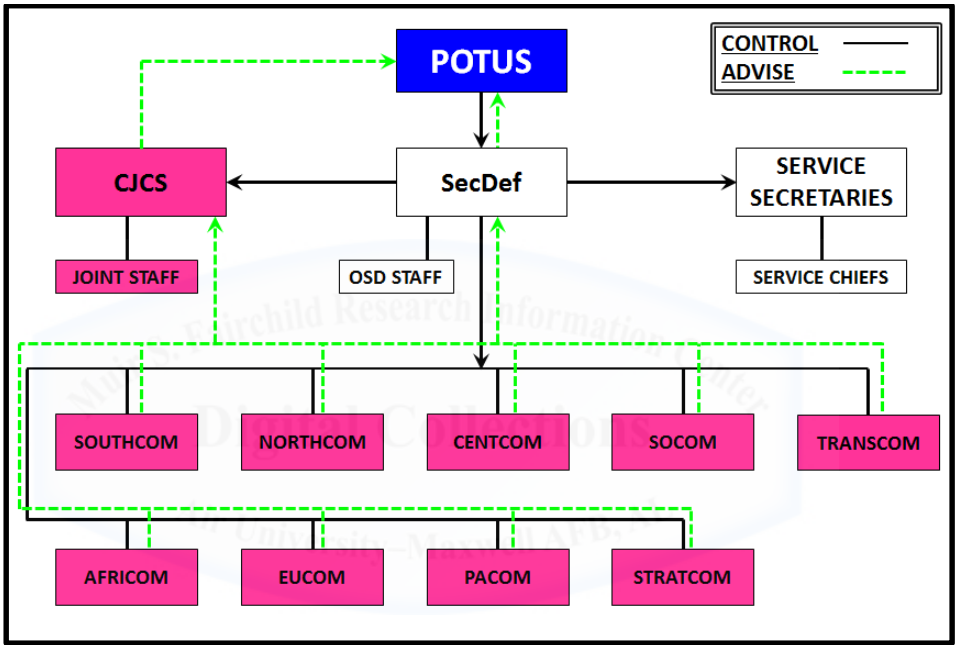

Figure 2: Unified Command Plan Organization

PPBE Limitations

COCOM authority gives Combatant Commanders (CCDRs) an avenue to advise America's senior political leaders on matters directly relating to the DoD's planning, programming, budgeting, and exection (PPBE) process. This process aggregates the nation's economy, industry, and strategy then parses out and allocates resources to the various organizations within the DoD for exectuion. CCDRs are given an opportunity to present the SecDef and the Joint Staff inputs and comments pertinent to their assigned missions throughout

all four phases of the PPBE process. Therefore CCDRs, through the PPBE process, have a direct avenue of communication to the Joint Staff and to the SecDef to ensure their commands are sourced with the ideal equilibrium of personnel, equipment, and support. Combatant commanders are also afforded an open dialogue to the CJCS and the SecDef on a number of command aspects to include, and perhaps most importantly, the CCDR's assessment of risks resulting from the balancing of limited resources and priority taskings.[11]

USCYBERCOM has no fomal avenue of communication to provide inputs on cyber related matters to any senior leaders above the CDR USSTRATCOM. On matters of the PPBE process, the CDR USSTRATCOM takes the advisement of USCYBERCOM in conjunction with other sub-unified commands and task forces. These various requests are aggregated by CDR USSTRATCOM and brought forward to the SecDef along with the other combatant commanders. The SecDef and the joint staff use these submitted recommendation to allocate national resources back to the individual combatant commands and service departments (see Figure 2). Once USSTRATCOM receives its resource allocation from the DoD, it then apportions personnel and equipment throughout its command. In this construct, CYBERCOM's maning and supply is diluted and lost in the shuffle of resources the CDR USSTRATCOM has been allocated. Regardless of how important CYBERCOM's mission may be, how unique and costly the equipment may be, or how critical forces are to fill cyber manning positions, CYBERCOM as a sub-unified command has to compete with other subunified commands for the already constrained resources of USSTRATCOM. The subordinate relationship of CYBERCOM within USSTRATCOM curtails resources and stunts the growth of the Cyber Command into an effective figthing force.

Inadequate Authorities

Aside from advocating for resources and manning, various authorities required to conduct effective cyber operations are neither consolidated nor clearly delineated to USCYBERCOM. Lacking clear guidance and authorities is a result of fragmented roles and missions among a spectrum of U.S. government organizations all in the CYBER arena. As an example, compare the differences in Title 18 and Title 10 authorities then contrast the same given a notional combined Title 18, Title 10 cyber operation.

Title 18 U.S. Code is the legal foundation for federal law enforcement and criminal investigation typically inherent to FBI activities. Title 10 U.S. Code is the legal establishment of the U.S. Armed Forces, its organization, actions, and roles. USCYBERCOM is fundamentally a Title 10 organization. The Posse Comitatus Act of 1878 strictly forbids Title 10 forces from generally engaging in Title 18 actions. With this understanding, place these constraints of a cyber-offensive operations team within a notional example of CYBERCOM attempting to trace and neutralize a Russian computer hacker actively attacking U.S. infrastructure. How does the nation defend against a Russian citizen visiting Arizona on a tourist visa attacking the Pentagon's cyber infrastructure using a host internet router in Germany? A CYBERCOM soldier at a counter-offensive computer terminal has no authority to hit the proverbial *enter* button to forcibly stop such an attack. Such is the state of 21st century cyber activities. The compartmented nature of America's legal framework is well suited to handle 19th and 20th century foreign and domestic issues. 21st century information flow and physical hardware locations will quickly allow the nation's enemies to conduct "lawfare" against the United States effectively using the nation's laws against itself.

An inappropriately organized cyber force coupled with USCYBERCOM functioning as a subordinate command to USSTRATCOM is an ineffective approach to the nation's cyber protection and projection. The authorities and legal framework of the nation's defense is antiquated and in critical need of review and realignment. In order for the U.S. to apply serious funding, operational capability, and authority to cyberspace, USCYBERCOM needs to be elevated to a stand-alone Combanat Command within the Unified Command Plan through legislated military and homeland defense reform.

Proposed Future U.S. Cyber Force Organization

A reorganized USCYBERCOM would be the ideal organization to project America's national interests both in and through cyberspace. It is the only U.S. Government organization of its design and size equipped to manage America's cyber footprint. CYBERCOM is currently limited in capability due to the aforementioned shortcomings attributed mainly to improper organization and authorities. If CYBERCOM were to undergo a top-down change, and if it were reorganized with unique authorities to conduct cyber operations, the command could be the mainstay of CYBER power America needs it to be. Anything short of this would relegate CYBERCOM to continue on in its current form as a suboptimal fragmented organization.

Cyber Theater Operations Command

To open the idea that USCYBERCOM's reorganization would benefit the U.S, it is necessary to begin at the changes required on the combatant level. To fully realize the capability of a standalone combatant command, USCYBERCOM needs to be organized with subordinate unified commands in each GCC's AOR called Cyber Theater Operations Command (CTOC). These CTOCs beome the event horizon of the DoD cyber domain interface. The CTOCs would be headed by a general or flag officer (typically an O-7). The establishments of the CTOCs

would consolidate the command of all theater cyber effects as well as enhance the cohesion between various elements of cyber forces.[12] Cyber Theater Operations Centers would be the reorganize subordinate unified commands within USCYBERCOM aligning cyber forces with geographic combatant commands. Similar to how SOCOM retains COCOM of their Theater Special Operations Commands, CYBERCOM would retain COCOM of their CTOCS. Geographical Combatant Commanders would therefore exercise OPCON and TACON over CTOCs in order to focus efforts on theater specific cyber requirements (See Figure 3).

CONUS assigned cyber forces would also be under the COCOM of CYBERCOM much like USSOCOM is currently organized. This organizational model allows cyber forces to be commanded and controlled by a single cyber commander with provisions made for each individual service department retaining administrative control of their respective forces (See Figure 3). This unique relationship consolidates cyber forces as well as allows the CDR USCYBERCOM the latitude to reassign forces specific to cyber requirements and, more importantly, prevent highly training specialists from being reassigned to non-cyber related manning positions in other commands or service branches.

Reorganizing USCYBERCOM and standing it up as the tenth independent combatant command would make great strides toward the strengthening of CYBERCOM. In order to give the command the offensive and defensive capability it requires to effectively carry out its mission through and in cyberspace, the authorities and roles of CYBERCOM need to be legislatively changed .

Establishing USCYBERCOM's Independence

On 12 September 1986, the 99th U.S. Congress passed the Goldwater-Nichols Department of Defense Reorganization Act of 1986. This act was arguably the single largest

change to the DoD and its organization since the National Security Act of 1947. The Goldwater-Nichols resolution was enacted to "enhance the effectiveness of military operations and improve the management and administration of the Department of Defense."[13] The legislation was largely successful in that the DoD was realigned from a post WWII institution to streamlined modern organization commensurate with the technologies, policies, and global dynamics of the day. Since the act was put into law in 1986, technology, policy, and global dynamics have once again changed so significantly that legislation in scope on par with the Goldwater-Nichols is required to once again realign and streamline how the DoD and America deals with cyberspace and cyber power. The core of this realignment needs to address USCYBERCOM becoming a stand-alone and independent combatant command.

Reorganizing the Unified Command Plan (UCP) by elevating USCYBERCOM from its subordinate role to the tenth combatant command would ensure that The United States is adequately prepared to address cyberspace as both a warfighting domain and a critical information network. A reorganized UCP would place a clear responsibility on the CDR USCYBERCOM for accomplishing cyber missions, the formulating cyber strategy, and efficiently employing and advocating for cyber resources. Most importantly, with USCYBERCOM as a combatant command, military advice provided to the President, National Security Council, and the Secretary of Defense would be streamlined and unfiltered.[14]

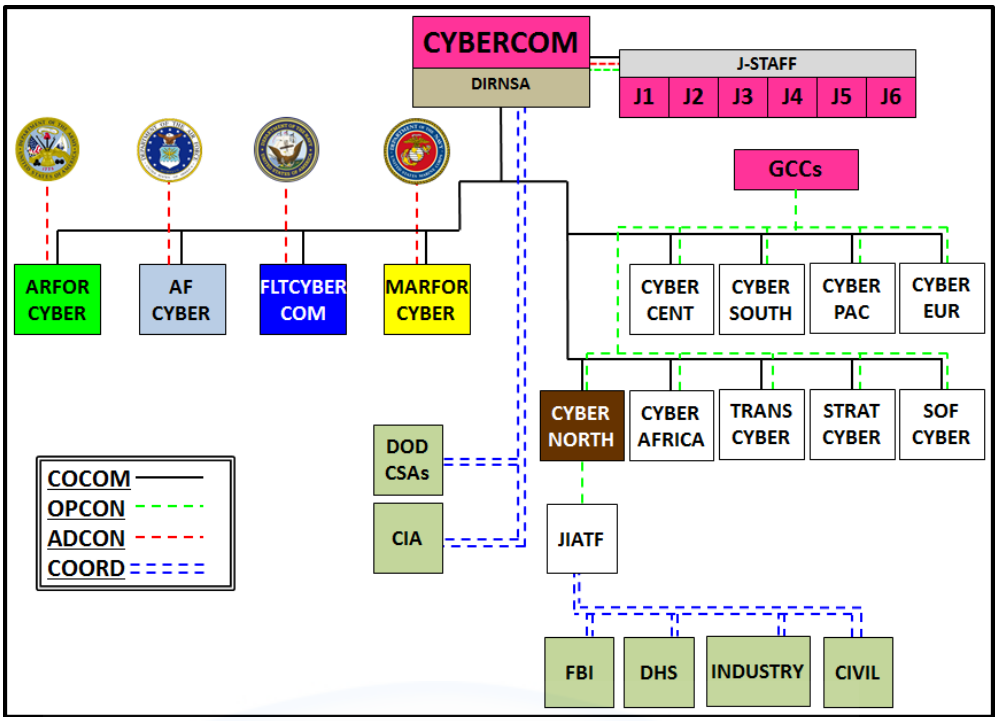

Figure 3: Proposed Future USCYBERCOM Organization Chart

This unfiltered communication avenue is particularly important to the PPBE process. In the current Unified Command Plan the CDR USCYBERCOM's resource allocation priorities are filtered through STRATCOM in competition with its other subordinate commands. As a stand-alone command, CYBERCOM will have the ability to clearly articulate, directly to the SecDef and POTUS, the necessary forces and resources CYBERCOM would need to successfully execute its assigned missions.

CYBERCOM Authorities and Roles

In order to provide the President, Secretary of Defense, and National Security council with the capability to project America's cyber power, paradigms must be broken, and legislation needs to be enacted by the House of Representatives that judiciously and cautiously consolidates significant power and responsibility with the CDR USCYBERCOM. The commander of U.S. Cyber Command is presently dual hatted as both the commander and the Director of the National

Security Agency (DIRNSA). This dual hatted nature gives the commander inherent military and intelligence gathering authorities. This is two of three critical authorities necessary to conduct seamless effective cyber operations. The third is Title 18 authorities. Realizing one of the core tenets of American Constitutional Law is the exclusion of military personnel from conducting law enforcement operations it is unlikely a Constitutional amendment would pass legal review allowing parts of the military to conduct cyber-criminal operations. A more realistic approach to solving the Posse Comitatus impasse would be the establishment of a Joint Inter-Agency Task Force (JIATF).

This JIATF would be charged with the defense of the homeland through the cyber domain and would be task organized under the CYBERNORTH CTOC with OPCON belonging to CDR NORTHCOM. The JIATF North organization would include the physical presence of National Guard, Reserves, DHS, FBI, Industry, and Civil authorities under one directorate thus consolidating homeland cyber defense.

The standup of USCYBERCOM as an independent combatant command would consolidate the defense of the homeland into a JIATF and allow GCCs the ability to direct cyber effects relevant to their areas of responsibility. USCYBERCOM as a standalone combatant command would give the CDR USCYBERCOM a voice in the PPBE process as well as control the resourcing of the command to adequately fulfill the cyber policies of the President and SecDef.

Conclusion

Legislative action by the U.S. Congress commensurate with the Goldwater Nichols Defense Reorganization Act of 1986 is truly necessary to make CYBERCOM what it needs to be. Politics and tribal interests need to be set aside along with shifting the current

USSTRATCOM paradigm of owning America's cyber capability. In order to affect real change that is critical to the protection of America and its interests in the cyber domain, CYBERCOM needs to be an independent combatant command staffed with competent cyber warriors and armed not only with technology and capability, but the authority to conduct operations commensurate with 21st century cyber threats.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography)

[1] Glazer and Yadron, *JP Morgan Says About 76 Million Households Affected by Cyber Breach*
[2] White House Communications Agency, *Department of Defense Strategy For Operating in Cyberspace*, 1
[3] JP 1-02, DoD Dictionary of Military and Associated Terms, 63
[4] White House Communications Agency, *The National Strategy to Secure Cyberspace*, vii
[5] Hollis, USCYBERCOM: The Need for a Combatant Command versus a Subunified Command, 48-53
[6] White House Communications Agency, *The National Strategy to Secure Cyberspace*, 1-2
[7] White House Communications Agency, *Department of Defense Strategy For Operating in Cyberspace*, 4-5
[8] Dempsey, *General Dempsey's Remarks at a [sic] Notre Dame, Questions and Answers*
[9] White House Communications Agency, *Department of Defense Strategy For Operating in Cyberspace*, 8
[10] Jabbour, Cyberspace Threats
[11] Chairman Joint Chiefs of Staff, *CJCSI 8501.01B, Participation In The Planning, Programming, Budgeting And Execution Process*, A-1 – A-8.
[12] Shelton, Coming of Age: Theater Special Operations Commands, 50-52
[13] U.S. House of Representatives, *Goldwater-Nichols Department of Defense Reorganization Act Of 1986,* 3-5
[14] Ibid., 22-30

References

Chairman Joint Chiefs of Staff. *CJCS Instruction 8501.01B, Participation In The Planning, Programming, Budgeting And Execution Process.* J-8, Joint Staff, Washington, D.C.: DTIC, 2012.

Emily Glazer, and Danny Yadron. *JP Morgan Says About 76 Million Households Affected by Cyber Breach.* October 2, 2014. http://online.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372#printMode (accessed October 3, 2014).

Hollis, David M. "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command." *Joint Forces Quarterly*, no. 58 (3rd Quarter 2010): 48-53.

Jabbour, Kamal. "Cyberspace Threats." Maxwell AFB, AL: Unclassified data extracted from a classified briefing, October 22, 2014.

"Joint Pubication, 1-02: Department of Defense Dictionary of Military and Associated Terms." *Joint Electroinic Library.* July 16, 2014. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed September 20, 2014).

Henry H. Shelton, "Coming of Age: Theater Special Operations Commands." *Joint Forces Quarterly*, Winter 1996-97: 50-52.

Martin E. Dempsey, *General Dempsey's Remarks at a [sic] Notre Dame, Questions and Answers.* September 06, 2014. http://www.jcs.mil/Media/Speeches/tabid/3890/Article/11087/general-dempseys-remarks-at-a-notre-dame-questions-and-answers.aspx (accessed October 2, 2014).

U.S. House of Representatives. *Goldwater-Nichols Department of Defense Reorganization Act Of 1986.* Conference Report, 99th Congress 2d Session, Washington, D.C.: United States Congress, 1986, 1-164.

White House Communications Agency. "Department of Defense Strategy For Operating in Cyberspace." Washington, DC, 2011.

White House Communications Agency. "The National Strategy to Secure Cyberspace." Washington DC, 2003.