AIR WAR COLLEGE

AIR UNIVERSITY

CYBER FOR THE MIDDLEWEIGHT FIGHTER:

Recommendations for Cyberspace Capabilities for the United States Marine Corps

by

Mark S. Revor, Lt Col, USMC

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Col Mark Nelson

14 February 2013

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 Colonel Mark Revor is a U.S. Marine assigned to the Air War College, Air University, Maxwell AFB, AL. He was designated a Naval Aviator in 1996 and qualified in the CH-53E and CH-53D. He deployed with a Marine Expeditionary Unit and with a Special Purpose Marine Air Ground Task Force. He also has deployed in support of Operations Iraqi Freedom and Enduring Freedom. He commanded Marine Heavy Helicopter Squadron 363. He graduated from the U.S. Naval Academy in 1994 with a Bachelor of Science degree in Mathematics and the Naval Postgraduate School in 2004 with a Master of Science Operations Research degree.

Abstract

One of the issues that the senior leadership of the Marine Corps is wrestling with is the future of cyberspace operations and the degree to which the Marine Corps invests in cyber forces. The Marine Corps is drawing down from 202,000 Marines to 182,100 as Operation Enduring Freedom comes to a close. At the same time, nations around the world are arming for operations in cyberspace, non-state actors are increasingly threatening, and U.S. forces are becoming dependent on computer technology and their associated networks. The Marine Corps of the future must be prepared not only to defend its networks and to add offensive cyberspace operations to its combined arms fight but, to do so in a way that supports it expeditionary nature and its reputation for being frugal.

The Marine Corps needs to determine the extent of its involvement in cyberspace operations. Because of the highly technical nature of certain aspects of both defensive and offensive cyberspace operations, as well as the global and near instantaneous nature of cyber operations, the Marine Corps can forgo a heavy cyber workforce and structure by making use of deployed planners and liaisons to U.S. Cyber Command. However, due to the its expeditionary nature, the Marine Corps must have forward deployed Marines trained to support the cyber requirements of the MAGTF in order to have reliable networks as well as the ability to restore network access following a disruption,. The efficiencies gained by using support from U.S. Cyber Command and the need to have robust access to the global information grid requires that the Marine Corps take a middle weight approach to its cyber future; neither to heavy nor to light.

Introduction

My promise to Congress is that at the end of the day, I will build and maintain the best Marine Corps our Nation can afford with the resources it is willing to invest. –General James F. Amos

The United States Marine Corps, along with the rest of the department of Defense, is in the midst of a post-war drawdown accelerated by an impending fiscal crisis. The decade plus focus on counter-insurgency is coming to a close and a pivot to the pacific is beginning. The result is a re-examination of roles and missions for all the services. At the same time a new domain of warfare is rising in prominence, adding demands for resources and attention. The cyber domain, one that cuts across all other domains, has been a rising specter to be defended against as well as a powerful new weapon in the arsenal. This paper explores the possibilities and makes recommendations on the role and extent of cyberspace operations in the Marine Corps.

The USMC exists to be America's expeditionary force in readiness, forward deployed as a Navy-Marine Corps team giving the President and the Geographic Combatant Commanders a multi-domain force with a small footprint and little need for infrastructure ashore. The Commandant of the Marine Corps describes the Corps as "the middleweight force from the sea…that is light enough to arrive rapidly at the scene of a crisis, but heavy enough to carry the day and sustain itself upon arrival."[1] As a middleweight force that intends to "fight across all domains with out optimizing on one in particular", the Marine Corps must ensure it makes balanced decisions in using the 8.2% of the Defense Budget it is allocated.[2] Marine Corps capabilities in the cyber domain are no different. This paper will argue that cyber capabilities in the Marine Corps should focus on security of and access to its networks and leave offensive cyber operations as a reach-back capability supported by US Cyber Command.

First, I will provide a brief background of cyberspace as a warfighting domain and of cyber organizations as they exist today. This will also include a brief overview of United States Cyber Command and cyber forces in the Marine Corps. Next, cyber threats, requirements and opportunities will be explored, followed by arguments against significant investments in cyber and against a minimal cyber future.

Cyber as the Fifth Warfighting Domain

Cyber and cyber war have become a hot topic for everyone involved in national security. From military and defense related bloggers and journalist, all the way up to those who craft grand strategy and set requirements for military organizations, cyber has become a pervasive issue. However, as recent as 2003, the threat of a cyber attack was viewed as a bit overblown.[3] Cyber attacks were seen as a website defacement or bit of intermittent Internet inaccessibility.[4] Though doubters persisted, the concern about the possibility of a real cyber threat continued to grow. By 2006 little doubt remained as to the seriousness of the cyber threat and the term "cyber" appeared for the first time in the National Security Strategy (NSS). It was only mentioned in a parenthetical description of Disruptive Threats, but its inclusion reflected the growing seriousness of the cyber threat.[5] [6]

As the concern over the threat of cyber grew, so did the recognition of cyberspace as a warfighting domain. In 2005 the Air Force changed its mission to include the ability to "fly and fight in air, space and cyberspace."[7] In the following year the Department of Defense declared that cyberspace was the 5th dimension of warfare.[8] [9] At the same time the services continued to struggle to define what cyber is, and what each of their contributions should be. Even the Air Force, the first service to recognize the cyber domain, expressed doubts about their role. At an Air Force Association sponsored conference in September 2012 the Air Force Chief of Staff,

General Mark Welsh, said in reference to cyber operations, “I'm a believer, I'm just not sure we know exactly what we're doing in it yet, and until we do, I'm concerned that it's a black hole. I'm going to be going a little slow on the operational side of cyber until we know what we're doing."[10]

With the designation of cyberspace as a warfighting domain, doctrine soon followed. In 2006 operations in the cyber domain were described in Joint Publication 3-15, Information Operations[11]. The 2006 version of JP 3-15 listed Computer Network Operations (CNO) as one of five core capabilities of Information Operations (IO) along with Electronic Warfare, Psychological Operations, Operations Security, and Military Deception. CNO was divided into Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE).[12] Since that time cyberspace operations of all sorts have grown dramatically causing the DoD to revise its doctrine and structure. The difficulty in even discussing cyber operations is that the lexicon and responsibilities for cyber have rapidly evolved. In 2009 the Vice Chairman of the Joint Chiefs of Staff, recognizing that the simple division of CNO into attack, defend and exploit lanes was insufficient, issued a memo to define cyber terminology that included 42 terms.[13] In July of 2011 a Government Accounting Office report noted that, “… no single joint publication completely addresses cyberspace operations. While at least 16 DOD joint publications discuss cyberspace-related topics and 8 mention ‘cyberspace operations,’ none contained a sufficient discussion of cyberspace operations.”[14] In the years following the publication of the 2006 version of JP 3-15, IO has moved away from those core functions and it now deals with the employment of Information Related Capabilities (IRC), no longer having responsibility for the cyber domain. The changing lexicon should stabilize now that Joint Publication 3-12, Cyber Space Operations, is signed.[15]

Despite the changing lexicon, it is important to define a couple of key terms before going forward. First, that cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. [16] Cyberspace operations are the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such activities include computer network operations and activities to operate and defend the Global Information Grid.[17]

U.S. Cyber Organizations

The use of cyber in warfare by a nation goes back at least to the cold war when the CIA, according to Thomas Reed's memoirs, allowed the Soviets to steal software designed to control valves and pumps used in an oil pipeline network from a Canadian company after the CIA had inserted malicious code into the software. The malware caused a pump in the Soviet's pipeline system to malfunction and eventually create enough pressure to exceed the limits of the pipeline's joints and welds. The result was an explosion visible from space.[18]

The CIA may have been behind that earliest known cyber operation but today the National Security Agency/Central Security Service (NSA/CSS) is the primary cyber agency. The NSA/CSS has three missions. First is signals intelligence, or collecting foreign intelligence from our adversaries' communications and information systems. Second is information assurance, or, protecting information and information systems critical to US national security. And third, according to their website, the NSA/CSS conducts network warfare.[19]

More recently, the Department of Defense recognized the need to create an organization focused on the complexities, and vulnerabilities, of the cyber domain. In 2009, as the number of probes and attacks against DoD networks continued to rise, United States Cyber Command

(USCYBERCOM) was created as a sub-unified command subordinate to United States Strategic Command. The mission of USCYBERCOM was, and still is, to plan, coordinate, integrate, synchronize, and direct activities to operate and defend the Department of Defense information networks and, when directed, conduct full-spectrum military cyberspace operations.[20] [21] USCYBERCOM and NSA/CSS have the same leader, currently General Keith Alexander, but separate, though supporting missions. As General Alexander stated during congressional testimony, "while there will be, by design, significant synergy between NSA and Cyber Command, each organization will have a separate and distinct mission with its own identity, authorities, and oversight mechanisms."[22]

Cyber in the Marine Corps

In a manner consistent with the Marine Corps' "middleweight fighter" approach, the Corps maintains cyber forces to support the operating forces as well as USCYBERCOM. Marine Forces Cyber Command (MARFORCYBER), along with the other component cyber commands, was created to support and advise USCYBERCOM on the employment and support of service forces. MARFORCYBER consists of a command element, the Marine Corps Network Operations Center (MCNOSC), and the Marine Corps Cryptologic Support Battalion's Company L (MCSB Co. L). The MCNOSC operates primarily to defend the Marine Corps Enterprise Network (MCEN)[23] and is the primary actor in computer network defense for the Marine Corps. MCSB Co. L acts to "provided resources for national and joint kinetic attack requirements."[24] Additionally, the Marine Corps Force Structure Review Group authorized the creation of MCSB Co B as a Direct Support company to fast track Marine Corps cyber requests.[25]

The cyber capabilities already exist in the operating forces; they are communications and signals intelligence specialists. Marines from the communication battalions and communication

squadrons are trained to setup expeditionary communication networks to support the requirements of the MAGTF to include voice and data via radio, satellite and wire. The signals intelligence specialists from the Radio Battalion are able to conduct limited cyberspace operations in addition to signals intelligence and electronic warfare support.[26] Defensive cyber operations in the MAGTF involve managing and maintaining the network. Offensive cyber operations, at the tactical level, are essentially Electronic Warfare; simply managing the spectrum to ensure our own use, while denying it to hostile forces. Additionally, the electromagnetic spectrum is used as a medium for gathering intelligence.

An evolving concept, in development by the Cyber Integration Division at the Marine Corps Combat Development Command, is the Cyber / Electronic Warfare Coordination Cell (C/EWCC) concept. The concept recognizes that the deployed MAGTF already has communication and signals intelligence specialists assigned. The C/EWCC combines these already present communications and signals intelligence Marines and adds a planner trained to understand cyber and IO.[27] The C/EWCC is scalable to any sized MAGTF and able to defend their networks and employ tactical electronic warfare to support the scheme of maneuver. If a greater offensive or defensive capability is required then a request for that support is submitted to USCYBERCOM who can provide it from a distance.

Cyberspace Operations and Organizations around the World

It is not just the United States that has developed cyber forces and prepared for operations in cyberspace. US preparations are in part a reflection of the growing threat from other state and non-state actors in cyberspace. Since the Cold War, Russia has become a regular actor in the cyber domain, though not in such a spectacular fashion as the pipeline explosion. Russian cyber attention has been focused on cyber in support of Information Operations and cyber espionage.[28]

From 1997 to 2001, during the Second Russian-Chechen War, both sides used cyber space to engage in IO campaigns to shape public perception. The Russian military, the Federal Security Bureau (formerly known as the KGB), and the Ministry of the Interior have undergone reorganization to more effectively employ and defend against cyberspace operations. Russia is adding graduate courses at their military universities in electronic warfare (EW) and information security. The Russian military expects that EW troops will become an independent combat arm in the future with branches for offensive and defensive IO. To help defend their country from a cyber attack and to better protect themselves from cyber exploitation, Russian law was modified to prohibit Russian Internet operators from passing data to foreign law enforcement agencies, and to prevent foreign entities from acquiring controlling interest in a "strategic company", such as data-encryption services and telecommunications, without the approval of the government. Essentially, the Russian government controls the Internet within their borders.[29] Finally, to further deter information sharing, such as in cooperation with foreign law enforcement, the definition of treason was expanded in November 2012 to include "anyone possessing information *deemed* secret" whether or not the information was passed on or not.[30]

China is the most well known source of cyberspace exploitation and attack operations. The targets of these operations range from the U. S. Government Non-Classified IP Router Network (NIPRnet) to Google's servers. China has also been accused of stealing the classified details of the F-35 Stealth Fighter.[31] The philosophy of China's cyber warfare agenda was outlined in a paper titled "Unrestricted Warfare", written in 1999 by two Chinese colonels who were advocates for warfare in all dimensions. In addition to our five dimensions they added diplomatic, informational, economic and psychological.[32] China, like Russia, has put considerable resources into developing cyber experts in their government, their military and in

their universities. China also makes use of cyber militia, an integration of personnel in the military, at universities and in the private sector.[33]

Unlike the other warfighing domains the price of entry into the cyber battlefield is very low. As a result smaller nations have become actors in cyberspace. In a manner similar to those two nations some thirty other nations across the globe have developed militarized cyber units of various capability and size. For example, Iran, the victim of the well know Stuxnet virus, claims to have the worlds second largest cyber army after standing up a cyber warfare division within the Revolutionary Guards.[34]

Further complicating the threat are the non-state actors. Hamas has been conducting Distributed Denial of Service (DDoS) attacks against Israeli websites. The frequency of the attacks ebbs and flows with the tension between Israel and Palestine. Al-Qaeda, an organization that has not shown its own cyber forces, has called for their followers to conduct cyber attacks on Americans.[35] In addition to terrorists, there are cyber activists to worry about. The hacker group Anonymous has a long list of targets: the Egyptian government during the Arab Spring, the Church of Scientology, Sarah Palin, and the Zetas Drug Cartel. They have also threatened Marine Corps Base Quantico after allegations of abuse arose in the treatment of PFC Bradley Manning –the alleged leaker of classified material to Wikileaks.[36]

The difficulty of attribution, or the ability to identify the originator of a cyber effect, further complicates the question of whether a state or a non-state actor was the perpetrator. In 2007 Estonia decide to relocate a monument dedicated to soldiers of the Soviet Union who died in battle. The backlash from Russia were massive Distributed Denial of Service (DDoS) attacks on websites belonging to two major banks and all government ministries in addition to the parliamentary email server. A similar wave of DDoS and other attacks were unleashed when

Russia invaded Georgia. In these examples the Russian government never admitted to the attacks and stated that they were likely the result of patriotic hackers that they could do nothing about.

Finally, there are also criminals and deviant individuals. In May 2000 the ILOVEYOU virus took the world by storm through an email attachment that eventually caused the Department of Defense and other government agencies, as well as corporations, to shut down their mail servers to deal with the problem.[37]

For nations, terrorist groups, and individuals that are not able to organize a cyber wing to enhance their activities, there is another option; they can simply buy the services of a hacker on the black market. Interested parties can purchase just about anything from malware of all varieties to the services of a hacker to conduct an attack, exploit or just steal some passwords.[38]

Marine Corps Reliance and Opportunities in Cyberspace

The Marine Corps, as a modern military organization, has come to rely on computers, networks and the data that resides on them. In a 2010 Marine Corps Gazette article titled *Feeling the Power*, the author declared that the Marine Corps is too reliant on technology and would have a difficult time operating without GPS and networked command and control systems. His point is excellent. Even in the most austere environment, computers - whether networked or standalone - are ubiquitous and our reliance on technology is complete. For example, GPS devices are assumed to work so well that navigation skills have eroded, manual gunnery for artillery is on the way to becoming a lost art, and calls for close air support depend on it.[39] [40] GPS is also a key element of our command and control system because the Blue Force Trackers depend on it. The author's arguments are made as a warning against the possibility of an electromagnetic pulse that wipes out our electronic devices but the point is also valid because all these electronic devices have computer circuitry behind them.

The Marine Corps relies on networks and computer systems. Command and control systems and global logistics systems rely extensively on a data network. Computer systems are key to nearly every major end item: aircraft increasingly have health and usage monitoring systems and networked radios, artillery fire relies on the computers and software that make up the Advanced Field Artillery Tactical Data System, planners rely on the Joint Mission Planning System. For day-to-day operations Marines rely on computers for email and Internet relay chat. Operations centers make use of the Command and Control Personal Computer program, not maps with acetate coverings, to maintain battlefield awareness.

Though the Marine Corps already relies greatly on its computers and networks, there are even greater opportunities that exist in the cyber domain. Enabling Information Operations through cyber allows the MAGTF Commander to shape the environment. As has been demonstrated repeatedly during a decade of counter-insurgency, one message can incite a violent riot while a timely counter message can diffuse it. Traditional leaflets and handbills are still a tool of information operators but the ability to get targeted messages to the masses via Twitter and the World Wide Web are a great enhancement, as is the ability to deny targeted messages through electronic means.

Offensive cyber operational capabilities are classified, but unclassified examples can be taken from the headlines in the news. A cyber attack could be an alternative to a conventional attack on an air defense system. In 2007, Israel launched aircraft to attack targets in Syria. Instead of jamming the Syrian air defense network, they transmitted malware to the air defense radars. Once the radar received the malware it infected the computer processor. The attack was more subtle than simply jamming the radar; the malware told the computer not to display anything.[41] In addition to air defense systems, anything with computer circuitry is a potential

target. Many modern industrial systems and utilities make use of software designed for remote monitoring and control known as SCADA systems (for Supervisory Control and Data Acquisition) which are susceptible to cyber attack. In 2000, a disgruntled employee of a waste treatment plant in Queensland, Australia wirelessly accessed his former employer's SCADA system and caused a massive spillage of raw sewage. The Marine Corps may not be interested in spilling raw sewage but, unlike bombing key nodes on an electrical grid or communications system, control over the SCADA system could allow for friendly forces to take the network down but not have to rebuild it after hostilities end. Furthermore, these target systems do not need to be connected to the Internet. In the case of the Syrian air defense system the virus was sent through the receiving radar. For Stuxnet, the virus traveled by peer-to-peer networks and via thumb drives as well as over the Internet. Intelligence collection is also enabled by cyber means. The duqu virus, first detected in 2011, made its way into computer systems by the victim opening an email attachment that was able to pass through anti-virus software. Once inserted on the computer it logged keystrokes, took screen shots and exfiltrated data back to whomever sent the virus.

Counter Arguments

After detailing the long list of adversaries that are operating in cyberspace, highlighting the need to defend our own networks as a result of our reliance on technology, and then extolling the possibilities of cyberspace operations; it would seem that a greater investment in cyber is a more logical position for which to advocate. However, a program that would result in a robust cyber force would come at a great, and unnecessary, price. The Marine Corps is presently capped at 182,100 Marines, on the way down from a wartime high of 202,000. The force cap creates a zero-sum game; that is, creating more cyber forces requires a reduction in another area.

The sacrifice in other areas is unnecessary because many offensive and defensive cyber operations are not specific to Marine Corps applications; and therefore can reside elsewhere in the DoD. Furthermore, developing cyber capabilities requires a great investment in dollars and manpower but employing those capabilities does not. Taking our previous example of the Israeli cyber attack on the Syrian IADS, a similar attack was contemplated prior to the 2011 air campaign over Libya, however the cyber attack plan was rejected due to the long lead-time, described as "months or years" to develop the weapon.[42] The reason for the long lead-time is that cyber attack weapons are specific to the target. In some cases the target might be a common system, in which case a particular capability can be reused until the vulnerability in the targeted system is fixed. Then a new weapon needs to be developed. In the case of the Libya air campaign the target system was not vulnerable to any cyber weapon on the shelf. However, if there were a suitable cyber weapon available there would be no need for a cyber warrior to be forward deployed in order to employ the weapon; proximity is not important. What is important to the forward deployed forces is a planner that understands when and where an offensive cyber capability can be used to support the MAGTF commander, and then, if needed, reach-back to the consolidated national assets to employ the capability.

Marine Corps cyber defenses need to be robust but, like offensive cyber capabilities, most of the heavy lifting can be done from centralized network operations centers. A large portion of cyber defense is automated monitoring for unusual system activity and searching for signs of known malware, unlike what is depicted in movies such as *Hackers,* where opposing cyber warriors are furiously hacking at their keyboards in attempts to out maneuver one another. When new malware is detected it is isolated and eradicated. At the same time a patch is developed to shore up the exploited system vulnerability and the signature of the malware is

added to a list of things that our anti-virus software looks for. Like the offense, few Marines are required and the heavy lifting is done by the computer industry.

Taking the counter argument the other direction, why have any cyber forces at all? The minimal cyber argument is to forgo having any cyber specialized forces and rely on contractors and the other services. If proximity to the target is not important and experts elsewhere in the government and industry handle the bulk of cyber offense and defense, then the need for any cyber forces in the Marine Corps comes into question. However, a no-cyber program is virtually impossible for a modern force because of the reliance on computer systems and networks. As an expeditionary force, the Marine Corps requires, at a minimum, cyber operators in the form of communications specialists who can create a network in an expeditionary environment, ensure that it works properly and meets the commander's requirements and, if that network is compromised, can make prioritized decisions to keep essential systems up and return the full system as quickly as possible.

Recommendations

The best approach is to take a middle path between the heavy approach and that of a minimalist. The Marine Corps is on the right track to implement the middleweight approach and needs to maintain this course as it shrinks down to 182,100 Marines. Marine Corps Cyber Command exists to support USCYBERCOM but also provides the baseline defense for Marine Corps networks, advocates for Marine Corps needs, and provides opportunities for professional development of Marine Corps personnel in the field of cyber operations. In the operating forces there is a need to have Marines that can setup, monitor and maintain a network and be able to reconstitute it if needed. The MAGTF commander needs to be confident that the systems the MAGTF uses are reliable. The commander and the staff must be as familiar with cyber

operations and capabilities as they are with air, ground and logistics in order to maximize the effects of cyber operations under the single-battle concept. The MAGTF of the future must operate in the fifth domain as comfortably as it does in the first four. To do so, the Marine Corps, along with USCYBERCOM, needs to develop standing operating procedures and policies that allow the forward commander to make use of offensive cyber operations without a long delay in the request process. During pre-deployment training, cyber ranges need to be available for the MAGTF to conduct exercises in order to become familiar with integrating cyber operations. Professional military education needs to include cyberspace and information operations to give future commanders the needed familiarity with the domain.

Growing cyber specialists requires a career path. The Marine Corps needs to analyze the recruitment and retention of the enlisted Marines with cyber specialties in order to keep these highly trained Marines, who have lucrative commercial skills, in the Corps. There is also a need for some cyber specialization in the Officer Corps. Presently cyber officers fall into one of three categories. There are those who work in a closely related field such as communications, signals intelligence or electronic warfare. Officers in these fields are able stay in their primary MOS. There are those in senior management positions that come from a wide variety of fields but are selected for their knowledge of the Marine Corps, leadership and understanding of the MAGTF. Finally, because certain billets require more technical education, there are the Special Education Program graduates who have earned degrees in fields related to cyberspace operations. These are the officers that the Marine Corps needs to retain in the cyber, or IO, field. These officers have spent two years in school and three more years of applied work but need to return to their primary MOS in order to be competitive for promotion. The Marine Corps should consider a

program similar to the acquisition professional, which allows some of these officers to stay in the field and get promoted based on their expertise in cyber operations.

The Marine Corps fights with a combined arms mentality with the goal of placing its enemy on the horns of a dilemma. The MAGTF Commander needs planners that understand how the MAGTF fights to make the best use of offensive cyberspace operations and information operations in combination with kinetic fires.

Conclusion

The cyber domain is a vast new world for military operations. With this vast new world comes the temptation to build vast new requirements. To fully exploit cyberspace; manpower, education and equipment are required. The possibilities are nearly endless and truly represent a "black hole" that is capable of absorbing all resources thrown its way. In the lean times of a post-war budget, especially during an economic crisis, a careful approach needs to be followed to keep requirements and resources defined and balanced. For the Marine Corps, the emphasis needs to be placed on maintaining and defending its critical networks, enabling tactical cyber warfare capabilities, and creating educated and trained cyber planners to make use of national assets in support of MAGTF operations. The Marine Corps needs to resist demand for significant cyber involvement and the temptation to do without it entirely.

Notes

1. Commandant of the United States Marine Corps, *Commandant's 2012 Report to Congress on the Posture of the United States Marine Corps*, (Washington, D.C.: Headquarters Marine Corps, 2012), 6.

2. Commandant of the United States Marine Corps, *Commandant's 2012 Report to Congress on the Posture of the United States Marine Corps*, (Washington, D.C.: Headquarters Marine Corps, 2012), 6.

3. In a 2003 PBS Frontline Special titled *Cyber War*, James Lewis, a security expert from the Center for Strategic and International Studies referred to cyber threats as "weapons of mass annoyance."

4. Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, (O'Reilly Media, 2009) 7-8.

5. The White House, *2006 National Security Strategy*, (Washington D.C.: March 2006), 43-44..

6. Four years later, In President Obama's 2010 NSS, the phrase 'cyber' appeared more than 20 times.

7. Master Sgt. Mitch Gettle, "Air Force Releases New Mission Statement," *Air Force Print News*, 08 Dec 2005, http://www.af.mil/news/story.asp?storyID=123013440 (Accessed 2 January 2013).

8. House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, *Hearing on National Defense Authorization Act for Fiscal Year 2012 and oversight of previously authorized programs before the Committee on Armed Services, House of Representatives, One Hundred Twelfth Congress, first session: Subcommittee on Emerging Threats and Capabilities hearing on budget request for U.S. Cyber Command*, hearing held March 16, 2011." U.S. G.P.O., 2011. http://purl.fdlp.gov/GPO/gpo13804, 3.

9. The first four domains are maritime, air, land, and space.

10. John Reed, "Air Force Chief wary of cyber 'blackhole'," *Foreign Policy blog Killer Apps*, 18 September 2012, http://killerapps.foreignpolicy.com/posts/2012/09/18/air_force_chief_wary_of_cyber_black_hole , (accessed 11 Nov 2012).

11. Kenyon, Henry S., "Cyber Command Logs In," *SIGNAL Magazine*, August 2007, http://www.afcea.org/content/?q=node/1362 (accessed 11 December 2012).

12. Joint Publication (JP) 3-13, *Information Operations*, 13 Feb 2006, I-7.

13. General James E. Cartwright, USMC, Vice Chairman of the Joint Chiefs of Staff, Memorandum for Chiefs of Military Service, Commanders of the Combatant Commands, and Directors of Joint Staff Directorates, *Joint Terminology for Cyberspace* Operations, August 18, 2009.

14. U.S. Government Accountability Office, *Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities*, Publication #GAO-75-11, (Washington D.C., July 2011), 2.

15. JP 3-12 was signed on 5 February 2013.

16. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010. However small changes can be meaningful. The USCYBERCOM Cyber

Lexicon, 24 July 2012, Version 4.6, Pre-Decisional Draft adds, "…and associated data" to the definition of cyberspace.

17. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010. The USCYBERCOM Cyber Lexicon, 24 July 2012, Version 4.6, Pre-Decisional Draft removes the second sentence in anticipation dropping the term 'computer network operations' from the lexicon..

18. Thomas Reed was the 11th Secretary of the Air Force and an advisor to President Ronald Reagan. The story of the 'logic bomb' referenced in several article that refer to his Memoirs, Reed, Thomas. *At the Abyss: An Insider's History of the Cold War*. Presidio Press, 2005.

19. National Security Agency, "Frequently Asked Questions," http://www.nsa.gov/about/faqs/about_nsa.shtml#about10, (accessed 12 Nov 2012).

20. U.S. Cyber Command, "Factsheet", http://www.stratcom.mil/factsheets/Cyber_Command/printable/, (accessed on 11 December 2012).

21. Fein, Geoff. 2010. "Cyber Intrusions Into Critical Infrastructure Growing, Official Says." Defense Daily 246, no. 11: 2. International Security & Counter Terrorism Reference Center, EBSCOhost (accessed December 11, 2012).

22. US Senate, *Hearing on the Nominations of VADM James A. Winnefeld Jr., USN to be Admiral and Commander, U.S. Northern Command/Commander, North American Aerospace Command; and LTG Keith B. Alexander, USA to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command, S. Comm. on the Armed Services*, 111th Cong., 2nd sess., 2010,157.

23. The Marine Corps Enterprise Network comprises the people, processes, logical and physical infrastructure, architecture, topology, and cyberspace operations.

24. Statement of Lieutenant General George J. Flynn, Deputy Commandant for Combat Development and Integration, 23 September 2010, in House, *Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations: Hearing before the subcommittee on Terrorism, Unconventional Threats and Capabilities*, 111th Cong., 2nd sess., 2010, 37-38.

25. Notes, Land Electronic Warfare Conference, 12 December 2012.

26. Mission statement of 2nd Radio Battalion, http://www.iimef.marines.mil/Units/2ndRadioBattalion.aspx accessed 7 Dec 2012.

27. The planner is a technical Information operations specialist that has completed a two-year course at the Naval Postgraduate School in Monterey, CA.

28. In 1999 U.S. officials accidently discovered that computer system at the Pentagon, NASA, Energy Department, private universities, and research labs had be compromised over the past two years. Russian officials have never admitted involvement but the attacks originated in Russia. The FBI code name for the inquiry was Moonlight Maze.

29. Jeffrey Carr, *Inside Cyber Warfare*, 217-241.

30. Associted Press, "Critics Say New Russia Treason Law Is 'Broad' and 'Dangerous'" *Fox News*, 14 November 2012, http://www.foxnews.com/world/2012/11/14/controversial-treason-law-takes-effect-in-russia-despite-putin-promise-to/.

31. The Economist, "Cyberwar: War in the Fifth Domain." *The Economist*, July 1, 2010. http://www.economist.com/node/16478792.

32. Corn, T. “Peaceful rise through unrestricted Warfare: Grand Strategy with Chinese Characteristics,” *Smallwarsjournal.com*, 5 June 2010, http://smallwarsjournal.com/blog/journal/docs-temp/449-corn.pdf, 3.

33. Jeffery Carr, *Inside Cyber Warfare*, 257.

34. Jeffery Carr, *Inside Cyber Warfare*, 250

35. Catherine Herridge, “Al Qaeda Video Calling for Cyberattacks on Western Targets Raises Alarm in Congress,” *FoxNews.com*, 22 May 2012, http://www.foxnews.com/politics/2012/05/22/al-qaeda-video-calling-for-cyberattacks-on-western-targets-raises-alarm-in/.

36. Wikipedia, the Free Encyclopedia, “Timeline of Events Associated with Anonymous,” (accessed December 10, 2012). http://en.wikipedia.org/w/index.php?title=Timeline_of_events_associated_with_Anonymous&oldid=526426225.

37. Larry Seitzer, “‘I Love You’ Virus Turns Ten: What Have We Learned?” *PCMAG*, 28 April 2010, http://www.pcmag.com/article2/0,2817,2363172,00.asp.

38. Ian Steadman, “The Russian Underground Economy Has Democratised Cybercrime,” *Wired UK*, http://www.wired.co.uk/news/archive/2012-11/02/russian-cybercrime.

39. Captain Joseph P. Steinfels, “The Feeling of Power,” *Marine Corps Gazette* 94, no.8 (August 2010): 25-30.

40. Many may not consider a GPS system to be a computer but there is computer circuitry in all GPS devices. This computer circuitry makes the GPS vulnerable to cyber attacks. On 14 Dec 2012 a Security Blog on the Ars Technica site summarized a report by scientists from Carnegie Mellon that detailed how to disable a GPS system. Typical attacks against a GPS involve blocking or altering the signals received by the GPS. The scientists used a unique approach that not only spoofed the receiver but also attacked vulnerabilities in the firmware of the device. For $2,500 they built a device which was capable of effecting systems up to 30 miles away. The effected GPS not only gave inaccurate location results but also was permanently damaged by having its firmware modified. http://arstechnica.com/security/2012/12/how-to-bring-down-mission-critical-gps-networks-with-2500/

41. Richard A. Clark and Robert K. Knake, *Cyber War, The Next Threat to National Security* (New York, NY: HarperCollins Publishers, 2010), 5-9.

42. Ellen Nakashima, “U.S. Cyberweapons Had Been Considered to Disrupt Gaddafi’s Air Defenses,” *Washington Post*, 18 Oct 2011, http://articles.washingtonpost.com/2011-10-17/world/35276890_1_cyberattack-air-defenses-operation-odyssey-dawn.

Bibliography

Air Force Doctrine Document 2-5, Information Operations, 20 Sep 2002.

Alexander, General Keith, Director, National Security Agency, Commander, U.S. Cyber Command, "U.S. Cyber Security Policy and the Role of U.S. Cyber Command," Center for Strategic and International Studies, Washington, DC, 3 June 2010.

Associated Press, "Critics Say New Russia Treason Law Is 'Broad' and 'Dangerous'." Fox News, 14 November 2012. http://www.foxnews.com/world/2012/11/14/controversial-treason-law-takes-effect-in-russia-despite-putin-promise-to/.

Carpenter, Major Trisha. "About Cyberspace Operations: An Emerging Mode of Warfare." Marine Corps Gazette, April 2012. www.mca-marines.org/gazette (accessed August 26, 2012).

Carr, Jeffrey. Inside Cyber Warfare: Mapping the Cyber Underworld. 1st ed. O'Reilly Media, 2009

Cartwright, General James E. Vice Chairman of the Joint Chiefs of Staff, Memorandum for Chiefs of Military Service, Commanders of the Combatant Commands, and Directors of Joint Staff Directorates, Joint Terminology for Cyberspace Operations, August 18, 2009.

Clark, Richard A. and Robert K. Knake, Cyber War, The Next Threat to National Security. New York, NY: HarperCollins Publishers, 2010.

Commandant of the United States Marine Corps, Commandant's 2012 Report to Congress on the Posture of the United States Marine Corps, 2012.

Corn, T. "Peaceful rise through unrestricted Warfare: Grand Strategy with Chinese Characteristics." Smallwarsjournal.com, 5 June 2010. http://smallwarsjournal.com/blog/journal/docs-temp/449-corn.pdf.

Fein, Geoff. "Cyber Intrusions Into Critical Infrastructure Growing, Official Says." Defense Daily 246, no. 11: 2. International Security & Counter Terrorism Reference Center, EBSCOhost (accessed December 11, 2012).

Gettle, Master Sgt. Mitch Gettle. "Air Force Releases New Mission Statement." Air Force Print News, 08 Dec 2005. http://www.af.mil/news/story.asp?storyID=123013440 (Accessed 2 January 2013).

Goodin, Dan. "How to Bring down Mission-critical GPS Networks with $2,500." Ars Technica, December 14, 2012. http://arstechnica.com/security/2012/12/how-to-bring-down-mission-critical-gps-networks-with-2500/.

Herridge, Catherine. "Al Qaeda Video Calling for Cyberattacks on Western Targets Raises Alarm in Congress." FoxNews.com, 22 May 2012. http://www.foxnews.com/politics/2012/05/22/al-qaeda-video-calling-for-cyberattacks-on-western-targets-raises-alarm-in/.

Joint Publication (JP) 3-13, Information Operations, 13 Feb 2006.

Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 31 October 2009.

Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms. 8 November 2010.

Joint Publication 3-13, Information Operations, 13 Feb 2006.

Kenyon, Henry S. "Cyber Command Logs In." SIGNAL Magazine, August 2007. http://www.afcea.org/content/?q=node/1362 (accessed 11 December 2012).

Liang, Qiao, and Wang Xiangsui. Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House, 1999.
Marine Corps Combat Development Command. Marine Corps Operating Concepts-Third Edition. June 2010.
Marine Corps Strategic Vision Group. Marine Corps Vision & Strategy 2025. DTIC Document, 2008.
Mirenda, Capt Ray J, . "Offensive Cyber Warfare." Marine Corps Gazette, September 2011. www.mca-marines.org/gazette (accessed August 26, 2012).
Mission statement of 2nd Radio Battalion, http://www.iimef.marines.mil/Units/2ndRadioBattalion.aspx (accessed 7 Dec 2012).
Nakashima, Ellen. "U.S. Cyberweapons Had Been Considered to Disrupt Gaddafi's Air Defenses." Washington Post, 18 Oct 2011. http://articles.washingtonpost.com/2011-10-17/world/.
National Security Agency, "Frequently Asked Questions," http://www.nsa.gov/about/faqs/about_nsa.shtml#about10, (accessed 12 Nov 2012).
Notes, Land Electronic Warfare Conference, 12 December 2012.
Office of Force Transformation. Implementation Network-Centric Warfare. Office of the Secretary of Defense, 5 January 2005.
Osinga, Frans. Science, Strategy and War: The Strategic Theory of John Boyd. 1st ed. Routledge, 2006.
Reed, John. "Air Force Chief wary of cyber 'blackhole'." Foreign Policy blog Killer Apps, 18 September 2012. http://killerapps.foreignpolicy.com/posts/2012/09/18/air_force_chief_wary_of_cyber_black_hole, (accessed 11 Nov 2012).
Reed, John. "Army and Marines Creating Systems for Cyber Fire Support | Killer Apps." Killeraps.ForeignPolicy.com, September 10, 2012. http://killerapps.foreignpolicy.com/posts/2012/09/10/pentagon_creating_system_for_cyber_fire_support.
Schwartau, Winn. Information Warfare: Second Edition. 2nd ed. Thunder's Mouth Press, 1996.
Seitzer, Larry. "'I Love You' Virus Turns Ten: What Have We Learned?" PCMAG, 28 April 2010. http://www.pcmag.com/article2/0,2817,2363172,00.asp.
Steadman, Ian. "The Russian Underground Economy Has Democratised Cybercrime." Wired UK, 2 November 2012. http://www.wired.co.uk/news/archive/2012-11/02/russian-cybercrime.
Steinfels, Captain Joseph P. "The Feeling of Power." Marine Corps Gazette, August 2010. www.mca-marines.org/gazette (accessed August 26, 2012).
Steinfels, Captain Joseph P. "The Feeling of Power." Marine Corps Gazette 94, no.8 (August 2010): 25-30.
The Economist. "Cyberwar: War in the Fifth Domain." The Economist, July 1, 2010. http://www.economist.com/node/16478792.
The White House, 2006 National Security Strategy. Washington D.C., March 2006).
U.S. Cyber Command, "Factsheet", http://www.stratcom.mil/factsheets/Cyber_Command/printable/, (accessed on 11 December 2012).

U.S. Government Accountability Office. "Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities." Publication #GAO-75-11. Washington D.C., July 2011.

United States Marine Corps. Warfighting (Marine Corps Doctrinal Publication 1). Quantico, 1997.

US House. Statement of Lieutenant General George J. Flynn, Deputy Commandant for Combat Development and Integration, 23 September 2010, in House, Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations: Hearing before the subcommittee on Terrorism, Unconventional Threats and Capabilities. 111th Cong., 2nd sess., 2010, HASC No. 111-180.

Wikipedia, the Free Encyclopedia, "Timeline of Events Associated with Anonymous." http://en.wikipedia.org/w/index.php?title=Timeline_of_events_associated_with_Anonymous&oldid=526426225 (accessed D December 10, 2012).