REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 03-05-2010	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE **Cyberspace and the Operational Commander**	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Gerald L. Tritz**	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Military Operations Department Naval War College 686 Cushing Road Newport, RI 02841-1207	**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
DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Cyberspace and the Operational Commander. Cyberspace, now considered a domain in warfare, represents a new frontier for the operational commander. Given global dependence on emerging technologies and the Internet, to achieve military objectives operational commanders must integrate cyberspace operations into planning and execution. This paper explores cyberspace and its importance to the operational commander and the operational level of warfare. First, it examines U.S. vulnerability to computer network attack and the importance of cyberspace to the operational commander. Secondly, the paper investigates the role of cyberspace in future operations by exploring recent international military conflicts. Next, it discusses the theory of cyberspace and its application to operational warfare. Finally, the paper presents recommendations for further integrating computer network operations into the operational level of war.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Chairman, JMO Department
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED		**26**	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3414

NAVAL WAR COLLEGE
Newport, R.I.

CYBERSPACE AND THE OPERATIONAL COMMANDER

by

Gerald L. Tritz

Lieutenant Commander, USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ____________________

3 May 2010

Contents

Abstract

Cyberspace and the Operational Commander. Cyberspace, now considered a domain in warfare, represents a new frontier for the operational commander. Given global dependence on emerging technologies and the Internet, to achieve military objectives operational commanders must integrate cyberspace operations into planning and execution. This paper explores cyberspace and its importance to the operational commander and the operational level of warfare. First, it examines U.S. vulnerability to computer network attack and the importance of cyberspace to the operational commander. Secondly, the paper investigates the role of cyberspace in future operations by exploring recent international military conflicts. Next, it discusses the theory of cyberspace and its application to operational warfare. Finally, the paper presents recommendations for further integrating computer network operations into the operational level of war.

INTRODUCTION

The growth of technology has “snowballed” since the introduction of the Internet. In modern countries, technology has changed every facet of human life including shopping, banking, and entertainment. Communication over the Internet has evolved from simple email to websites to social networking sites like Facebook and Twitter. The term “friends” now refers to people being connected only through a website who rarely if ever actually use verbal communication. Parallel to the web based social revolution, a technological transformation has occurred in warfare. Capitalizing on the advantages of instantaneous electronic communication and the ability to link platforms across the military services, the U.S. military has fundamentally changed the way it accomplishes its missions. Instead of ships communicating with flags or light signals, modern sailors monitor computer chat rooms and Internet sites. Leaps in connectivity have produced tremendous advantages but have also exposed new vulnerabilities for the modern military. Given global dependence on emerging technologies and the Internet, to achieve military objectives operational commanders must integrate cyber operations into planning and execution.

BACKGROUND

Discussing events in cyberspace requires an understanding of a few terms unique to the cyber environment. According to the Department of Defense (DOD), “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.”[1] It further defines computer network operations as the combination of computer network attack, computer

[1] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, 12 May 2001 as amended through 31 October 2009), 139.

network defense and computer network exploitation.[2] In other words, computer network operations include the offense, defense and exploitation occurring in the domain of cyberspace.

AMERICAN MILITARY VULNERABILITY

Since the fall of the Soviet Union, the United States has possessed an unrivaled military power. Most countries in the world would not dare challenge America in a direct military confrontation. Instead, both state and non-state actors look to achieve political and military objectives through asymmetric warfare. This type of warfare became painfully obvious to the American public on September 11, 2001 and has continued with insurgencies in Iraq and Afghanistan. The current and future frontier for asymmetric warfare lies in cyberspace because the DOD relies on it to achieve national military objectives in the areas of military, intelligence and business operations.[3] U.S. dependence on cyberspace will continue to increase as DOD force transformation focuses on a move toward net-centric operations.[4] The combination of American reliance on cyberspace and her enemies' strategy of asymmetric warfare make the U.S. susceptible to computer network attack; operational commanders (Geographic Combatant Commanders and Joint Task Force commanders) should expect it in all future military operations.

American military leadership recognizes the potential vulnerability of future operations to computer network attack. Deputy Secretary of Defense William J. Lynn III said, "I'm often asked what keeps me up at night. No. 1 is the cyber threat. If we don't maintain our capabilities to defend our networks in the face of an attack, the consequences

[2] Ibid., 111.

[3] Chairman, U.S. Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations*. (Washington, DC: CJCS, December 2006), 21, http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf, (accessed 20 February 2010).

[4] Ibid.

for our military, and indeed for our whole national security could be dire."[5] Lieutenant General Keith Alexander, nominee for commander, United States Cyber Command, admitted that the "current state of our networks presents a strategic vulnerability to the Department and the nation."[6] With 15,000 computer networks spread across 4,000 military installations in 88 countries, the United States' reliance on cyberspace represents a vulnerability that her military's leadership acknowledges.[7]

Military leadership fears computer network attack because state and non-state actors already execute it against the United States. In 2008, the U.S. was the country most frequently targeted by denial-of-service attacks, accounting for 51% of the worldwide total.[8] Since 2006, the victims of computer network attack within the U.S. military include the Non-classified Internet Protocol Router Network (NIPRnet-military unclassified network), Naval War College, National Defense University, and classified networks at U.S. Central Command.[9] Behind the known computer network attacks lies an even deeper vulnerability: attacks the U.S. fails to catch. Many attacks go undetected or enemies penetrate networks with a sleeper virus that may activate at a later date.[10] Additionally, if the enemy can infiltrate a network in order to steal information, they can also use that breach to implant a virus in the network. The difference between computer network exploitation and attack lie

[5] U.S. Federal News Service, "Cybersecurity Seizes More Attention, Budget Dollars," *US Fed News Service, Including US State News,* 5 February 2010, http://www.proquest.com/ (accessed 7 March 2010).

[6] Senate Committee on Armed Services, *Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command,* 111th Cong., 2nd sess., 2010, http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf (accessed 25 April 2010).

[7] Jordan Reimer, "U.S. Cyber Command Preparations Under Way, General Says," American Forces Press Service, 17 March 2010, http://www.af.mil/news/story.asp?id=123195306 (accessed 25 March 2010).

[8] Fossi, Marc ed., *Symantec Internet Security Threat Report: Trends for 2008*, Vol. XIV, April 2009. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet _security_threat _report_xiv_04-2009.en-us.pdf (accessed on 9 April 2010).

[9] James Andrew Lewis, "Cyber Events Since 2006," *Center for Strategic and International Studies,* 3 March 2010, http://csis.org/publication/cyber-events-2006 (accessed on 9 April 2010).

[10] Martin C. Libicki, *Cyberdeterrence and Cyberwar,* RAND Report (Santa Monica, CA: RAND, 2009), 16.

with the motivation of the perpetrator rather than a different skill set or technical expertise.[11] By repeatedly attacking United States military networks, enemies have proven that they have the resolve, capability and experience to commit computer network exploitation and attack.

When computer network attacks occur, the extreme difficulty in identifying the source of the attack compounds the problem. The attacks can be conducted from almost anywhere including cybercafés, open Wi-Fi nodes, or third party computers.[12] Furthermore, they leave next to no physical trace, often leaving attribution to guesswork.[13] The complexity of tracking down culprits usually leads to a lack of consequences for perpetrators.

Operational commanders must expect computer network attacks to occur. The United States' vast military computer network infrastructure makes it an enormous target. Civilian and military leadership acknowledge America's susceptibility to attack. America's enemies constantly attack U.S. military related networks and the lack of attribution or consequences encourages the behavior. Operational commanders need to mitigate American cyberspace vulnerabilities by creating a plan for computer network defense in each operation they undertake.

INTERNATIONAL RECOGNITION OF CYBERSPACE OPERATIONS

The reasons to incorporate computer network operations into operational warfare go beyond American vulnerabilities; future military conflicts will include events in cyberspace.[14] Most world powers recognize the advantages of computer network operations and will execute them during future conflicts. Chinese research, training and experience exemplify the cyberspace capabilities of an advanced nation-state. Russia's conflict with

[11] Ibid.

[12] Ibid., XVI.

[13] Ibid.

[14] Elizabeth H. Manning, "Lessons Learned from the First War Fought in Cyberspace." *The Officer*, 1 February 2009, 37. http://www.proquest.com/ (accessed 25 February 2010).

Estonia demonstrated the potential of computer network attack against an unprepared and vulnerable adversary. In order to maintain U.S. military dominance, operational commanders must employ as effectively in the domain of cyberspace as they do in other domains.

Future military conflicts will include events in cyberspace because most world actors have the capacity to perform computer network attack. In 2007, FBI reports showed that 108 countries possessed dedicated computer network attack capabilities.[15] This number grows constantly due to the low entry barriers (skills and technology required to implement an operation) and an extraordinarily large return on investment for targeting sensitive U.S. information.[16] The rewarding payoff attracts a broader scope of adversaries to cyberspace including rival nation-state, non-state, sub-national and even individual actors.[17] Even entities looking primarily for network security and computer network defense discover that defense and offense in cyberspace utilize identical skills.[18] The same gateways, portals, software holes and other access points that governments discover while trying to protect their own cyberspace can then be used to exploit or attack an enemy's computer networks. The combined effect of low entry barriers and shared skill sets between network attack and defense result in most state and non-state actors possessing a credible cyberspace capability.

China recognizes the benefits of computer network operations and has made significant strides to incorporate them into their military operational planning. China views

[15] Jack M. Germain, "The Art of Cyber Warfare, Part 1: The Digital Battlefield," *TechNewsWorld*, 29 April 2008, 2, http://www.technewsworld.com/rsstory/62779.html?wlc=1256255575, (accessed 25 February 2010).

[16] William Mat, "Chinese Attacks Bring Cyber Spying Into the Open." *Defense News*, 18 January 2010, http://www.proquest.com/ (accessed 24 February 2010).

[17] General Norton Schwartz, "Space, Cyberspace and National Security," (lecture, Air Force Association, Orlando, FL, 18 February 2010).

[18] Raymond C. Parks and David P. Duggan, "Principles of Cyber-Warfare," *Proceedings of the 2001 IEEE workshop on Information and Security*, (U.S. Military Academy, West Point, NY. 6 June 2001), 124.

cyber operations through a conceptual framework called "Integrated Network Electronic Warfare" (*wangdian yitizhan*) which combines network operations with electronic warfare in coordinated strikes against enemy networks.[19] The Chinese believe that network operations and electronic warfare are the primary modes of attack in information warfare.[20] Furthermore, they envision computer network operations integrated into other war fighting domains and rarely discuss employing them in isolation.[21] China plans to use integrated network electronic warfare in an effort to target enemy computer networks.

Beyond understanding cyberspace operations, the Chinese have incorporated it into their training and doctrine. During a training event in 2004, the opposing force used computer network attack to penetrate and seize control of the Red Force command network minutes after the start of the exercise.[22] Further evidence suggests that the PLA (People's Liberation Army) may strike using computer network operations and electronic warfare instead of conventional attack in the opening phases of a conflict to degrade enemy information systems.[23] In 2007, the PLA's training guidance directed all military services to make training under complex electromagnetic environments the core of its campaign and tactical training.[24] The Chinese emphasis on the theory, training, and doctrine required to successfully execute computer network operations leads to the conclusion that they intend to use them in their future conflicts.

The Chinese incorporation of computer network operations goes beyond employment in information warfare; they also plan to target support systems using cyberspace operations.

[19] Brian Krekal, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, US-China Economic and Security Review Report (McLean, VA: Northrop Grumman, 2009), 13.
[20] Ibid., 14.
[21] Ibid., 23.
[22] Ibid., 16.
[23] Ibid., 23
[24] Ibid., 17.

In a conflict with the United States, the Chinese would likely target NIPRnet-based logistics networks with computer network attack.[25] PLA planners have identified the long logistics tail of the United States military as a center of gravity (key source of strength) and believe that U.S. networks are vulnerable to computer network attack.[26] In addition to targeting military networks, evidence suggests the PLA would also attack potentially vulnerable networks associated with civilian ports, shipping terminals and railheads that support the military's movement of critical supplies.[27] The Chinese plan to use cyber attacks to penetrate American computer networks in an effort to disrupt critical logistics support.

In addition to the theory, training, doctrine and plans to incorporate network operations, the Chinese also have the experience. Since 1999, at least 35 computer network attacks against multiple U.S. government websites including NASA, the Secretary of Defense, the Commerce Secretary and the State Department trace back to the Chinese.[28] Such efforts have proven the Chinese competent and effective in carrying out computer network attacks. It would behoove any operational commander planning military action against the Chinese to adequately integrate computer network operations into an operational scheme.

Not only do the Chinese practice cyberspace operations, the Russians have employed it in their recent conflicts. In 2007, Estonia moved a Soviet war memorial from the capital of Tallinn to a cemetery outside the city enraging the Russian government and citizens.[29] From approximately 27 April 2007 to 21 May 2007 a massive computer network attack aimed at

[25] Ibid., 24.

[26] Ibid.

[27] Ibid., 25-26.

[28] Ibid., 67.

[29] Ian Traynor, "Russian Accused of Unleashing Cyber War to Disable Estonia," *The Guardian,* 17 May 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (accessed 9 April 2010).

Estonia's government websites occurred.[30] Estonia did not successfully defend their system against the Russian attack and multiple websites were defaced or shut down. Finally, the attacks forced the Estonians to secure their cyberspace by disconnecting it from the international community.[31] Although Russia denied responsibility for the attack, Estonia and the international community believe the Russians orchestrated it.[32] The Russian attack against Estonia proved that modern nation-states crush unprepared adversaries in cyberspace.

Judging by the number of international actors who possess cyberspace capabilities, clearly modern militaries will incorporate computer network operations in future conflicts. Chinese planning encourages the use of cyberspace to surprise an enemy and target critical military support infrastructure. Russia on the other hand, proved the value of computer network attack to against an unprepared adversary. The strategy, plans and execution of contemporary militaries involved in conflict prove that future operational plans require computer network operations to harness the full capabilities of military power in order to defeat their enemy across the sea, air, land, and cyberspace domains.

CYBERSPACE COMPLIMENTS OPERATIONAL WARFARE

Since future warfare will include cyberspace operations, operational commanders should incorporate the advantages of cyberspace into an operational scheme for the battle space. The U.S. already incorporates cyberspace for command and control and Information Operations but cyberspace can also compliment operational warfare by contributing to the principles of war and optimizing the operational factors of time, force and space in order to achieve military objectives.

[30] Bradley L. Boyd, "Cyber Warfare: Armageddon in a Teacup?" (master's thesis, Fort Leavenworth, KS: U.S. Army Command and General Staff College, 12 November 2009), 29.

[31] Libicki, *Cyberdeterrence and Cyberwar*, 1.

[32] Boyd, "Cyber Warfare," 38.

As a manmade domain, cyberspace differs from the classic domains of air, land and sea. Historically, the principles of war (objective, offensive, mass, economy of force, maneuver, unity of command, security, surprise, simplicity) apply to each domain separately and to the battle space as a whole.[33] Cyberspace differs from the other domains because many of the principles of war do not apply or apply differently within network warfare.[34] However, efforts in cyberspace contribute to the application of the principles of war across the battle space.

By synchronizing operations in cyberspace with conventional operations, an operational commander can magnify effects on the enemy. When Russia went to war with Georgia in August 2008, a computer network attack against government websites occurred simultaneously with a conventional military operation.[35] The network attacks crippled Georgia's government websites preventing communication to Georgians and more importantly the international community.[36] After a delay, Georgia used servers located outside their country and changed the format of some of the websites in order to continue their use.[37] By combining a computer network attack with a conventional attack, the Russians effectively amplified the principles of offensive, mass, and surprise across multiple domains to disrupt the information flow for Georgia. The computer network attacks also acted as an operational fire, shaping the battle space by isolating Georgia internationally. When used appropriately, cyberspace allows an operational commander the ability to apply

[33] Chairman, U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication (JP) 1 (Washington, DC: CJCS, 2 May 2007 incorporating change 1, 20 March 2009), I-3.

[34] Parks and Duggan, *Principles of Cyber-Warfare*, 123.

[35] Boyd, "Cyber Warfare," 45.

[36] John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, 12 August 2008, available at http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1 (accessed 25 March 2010).

[37] Boyd, "Cyber Warfare," 57.

the principles of war and operational fires to another domain compounding their effects on the enemy.

In addition to the principles of war, using cyberspace allows a commander the opportunity to optimize the operational factors of time, force and space. Time affects operations in cyberspace much differently than in the other domains. Preparation for computer network attack occurs prior to a conflict through espionage and network analysis so once a conflict begins, the operational commander can use cyberspace options immediately. Once commanded, network attacks move at a rate approaching the speed of light allowing actions in cyberspace to easily integrate with actions in other domains.[38] Sustainability poses a limitation for computer network attack. Typically, after a victim detects an attack, he usually fixes the exploited vulnerability or circumvents the system making long-term sustainability for computer network attack very difficult.[39] By discovering enemy vulnerabilities prior to a conflict, an operational commander can integrate quick, surprise computer network attacks coordinated with operations in other domains to overwhelm an enemy.

Applying force in cyberspace also differs from the classic domains of air, sea and land. Force in cyberspace can achieve similar results to the other domains while minimizing physical damage to targets. Disabling an enemy communication node with a virus denies its use to the enemy in a similar fashion to destroying the node with a bomb. However, the use of a computer network attack makes repairing the node after hostilities cheaper and quicker than physically destroying the node. Taking advantage of cyberspace allows the operational

[38] Richard Clarke, “War From Cyberspace.” *The National Interest*, 1 November 2009. http://www.proquest.com/ (accessed 24 February 2010).

[39] Libicki, *Cyberdeterrence and Cyberwar,* 154.

commander to achieve similar effects while causing less destruction than conventional options.

Cyberspace operations utilize geometric space more efficiently than other domains. Historically, one had to mass men and equipment on the battlefield in order to concentrate military power. Using cyberspace allows an operational commander to geographically disperse a force yet still concentrate the effects of his force on the enemy.[40] By keeping personnel engaged with the enemy but located outside the combat area, an operational commander can influence the enemy while not risking the safety of cyberspace forces.

Computer network operations compliment operational warfare because their effectiveness increases when integrated with other domains. By designing operations to take advantage of the principles of war across air, sea, land and cyberspace, operational commanders can overwhelm enemies. Additionally, commanders can optimize the operational factors of time, force and space in order to achieve objectives with less destruction and less risk to personnel.

CYBERSPACE VERSATILITY IN DIFFERENT MILITARY OPERATIONS

The advantages of cyberspace operations can translate to different types of military operations. From nation-states to non-state actors, virtually every entity relies on cyberspace to function. For example, almost all terrorist and insurgent organizations have a web presence.[41] Because of this web presence, these groups make themselves vulnerable to cyberspace operations. Operational commanders can exploit the enemy's reliance on

[40] Paul Murdock. "Principles of War on the Network-Centric Battlefield: Mass and Economy of Force," *Parameters* 32, no. 1 (1 April 2002): 86. http://www.proquest.com/ (accessed 13 April 2010).

[41] Michele Zanini and Sean J.A. Edwards, "The Networking of Terror in the Information Age," in *Networks and Netwars: The Future of Terror, Crime and Militancy,* ed. John Arquilla and David Ronfeldt (Santa Monica, CA:Rand, 2001), 43.

cyberspace by integrating computer network operations across the range of kinetic military operations from counterinsurgencies to regional wars.

The United States currently executes computer network operations in the fight against violent extremist organizations. Al Qaeda grasped the importance of the Internet from the beginning and tried to harness the power both to further its strategic aims and to facilitate its tactical operations.[42] Al Qaeda utilized the Internet for three critical functions: propaganda (recruitment, fund-raising, and shaping world opinion), terrorist training and operational planning for attacks (using e-mail and open source information).[43] The United States and her allies used computer network attack to cause Al Qaeda to move its website from one Internet service provider to another until it was shutdown completely in 2002.[44] The loss of its website weakened Al Qaeda by impeding its propaganda, training and planning.

Although the U.S. has employed cyber warfare against Al Qaeda, the success has been limited. Al Qaeda still distributes "mujahideen videos" videos over the Internet.[45] The videos communicate messages to sympathizers by depicting the explosions of roadside bombs, giving tactical advice to insurgents and appealing for financial contributions.[46] In testimony to Congress, Bruce Hoffman stated, "To date, at least, the United States, however, has not effectively contested the critical, virtual battleground that the Internet has become to terrorists and their sympathizers and supporters worldwide."[47] In the struggle against terrorism, cyberspace remains one of the most important domains to control because the terrorists need it to communicate their message. Without a medium for communication,

[42] Bruce Hoffman, "The Use of the Internet by Islamic Extremists," Testimony presented to the House Permanent Select Committee on Intelligence, 4 May 2006, (Santa Monica, CA:RAND, 2006), 5.
[43] Ibid., 6.
[44] Ibid., 8.
[45] Ibid., 13.
[46] Ibid., 14.
[47] Ibid., 16.

terrorism will fail.[48] It would behoove operational commanders to place a higher priority on computer network operations in order to prevent known violent extremist organizations from freedom of action in cyberspace.

In addition to insurgencies, regional wars also include cyberspace operations. When Israel invaded Gaza, a parallel battle occurred in cyberspace. Soon after the start of Israel's bombing campaign, Hamas attacked thousands of Israeli government websites.[49] Israel responded by attacking Palestinian media websites and hacking into a Hamas owned television site.[50] Israel employed voluntary "botnet" attacks involving individuals knowingly passing control of their computers to the botnet host server who used them to attack Hamas networks and websites.[51] Both sides also started information campaigns and even used social networking websites like Facebook.[52] Since the war began, Israel has struggled to regain the lead in the information war against Hamas. Israel now acknowledges that cyberspace is another war zone.[53] The information war fought in cyberspace played a critical role in the Israeli invasion of Gaza.

Operational commanders cannot foresee how their forces will be used in future military conflicts. However, recent history demonstrates that cyberspace operations occur in different types of military operations. By preparing to fight in cyberspace, commanders ensure that their forces can overcome whatever challenges the future holds. Regardless of the type of future U.S. conflicts, the integration of computer network operations into operational warfare will be rewarded.

[48] Ibid., 15.

[49] Jeff Carr, *Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare.* Greylogic Report. 20 March 2009, 8. http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report (accessed 13 April 2010).

[50] Ibid., 13.

[51] Ibid., 4.

[52] Boyd, "Cyber Warfare," 61.

[53] Ibid., 72.

Some might say that integrating cyber operations into the operational level of warfare is inappropriate. Operational commanders can achieve military objectives using air, land and sea based capabilities and the avoidance of cyber operations will help prevent conflicts from escalating. Operational objectives always reside in the physical domains of air, land and space. For an operational computer network attack to work, a potential target has to be accessible and have vulnerabilities that the attacker finds useful.[54] An operational commander cannot force their way into an enemy's cyberspace domain. Targets are limited to what the enemy (or software) leaves vulnerable and to what can be attacked using cyberspace.[55] Even among vulnerable targets it may be difficult to cause an effect in the physical environment. Although future technology may enable cyberspace operations to cause physical results in the classic domains, to date not a single report can confirm a computer network attack caused physical destruction.[56] The restricted nature of computer network operations can lead to an extraordinary amount of effort in order to find a small number of suitable targets with a limited chance of having any effect on the physical environment.

Furthermore, computer network infrastructure stretches beyond a geographic commander's area; the military requires a command with global reach to facilitate computer network defense. U.S. Cyber Command as a subordinate unified command under U.S. Strategic Command is better positioned than an operational commander to ensure that all U.S. forces maintain freedom of operation in cyberspace in order to achieve objectives in the

[54] Libicki, *Cyberdeterrence and Cyberwar*, XIV.

[55] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington, DC: National Academies Press, 2009), 118.

[56] Timothy O'Hara, "Cyber Warfare/Cyber Terrorism," (research paper, Carlisle, PA: U.S. Army War College, 3 May 2004), 9.

other domains. Also, fears about escalation support the notion of centralizing computer network operations under U.S. Cyber Command rather than an operational commander. Unrestricted cyber warfare between two modern nations has yet to occur. General Chilton, the commander of U.S. Strategic Command, said that in the case of a massive cyber attack, "he would not take an any options off the table" for how the President would respond.[57] Additionally, evidence exists that the U.S. avoided computer network attack during the Iraq war for fear of escalating the conflict in cyberspace.[58] A scenario in which an operational commander's cyber attacks against an enemy lead to retaliation in cyberspace against American business or infrastructure may be unacceptable. In order to contain the ramifications of computer network attacks, U.S. Cyber Command is better positioned and equipped than an operational commander.

Nevertheless, cyberspace represents another domain in warfare. Computer network attack in isolation gives an operational commander very limited options but its integration with operations in the other domains provides a multitude of options. Additionally, a computer network attack against military infrastructure might present a greater threat to the U.S. than an attack against government, civilian or business networks.[59] Operational commanders need to have responsibility for computer network defense because if an enemy succeeds in a computer network attack against theater networks that prevent an operational commander from achieving his objectives, he will be held responsible. The operational commander needs to understand the ramifications of a computer network attack on his operation in order to know how to compensate in other domains for damage taken to his cyberspace infrastructure.   Finally, the idea that cyberspace operations lead to escalation

[57] General Kevin Chilton, interview by Lynn Neary, *Talk of the Nation*, NPR, 10 August 2009.
[58] Ibid.
[59] Libicki, *Cyberdeterrence and Cyberwar*, 6.

relies on the belief that one can control the enemy's use of a capability. If an adversary possesses the capabilities for computer network attack, he alone decides if he will use that capability. The conflict as a whole influences an enemy's decision much more than any decision a U.S. commander might make in a single domain.

RECOMMENDATIONS

To better integrate computer network operations into operational warfare, the United States needs to minimize the seam between U.S. Cyber Command and the operational commanders. Optimizing U.S. military execution in cyberspace requires changes in planning, operational structure and training.

During the planning process, in accordance with doctrine, computer network operations are buried in Information Operations. The Information Operations Estimate Process addresses computer network operations alongside psychological operations and military deception.[60] In order to better integrate computer network operations into the planning process, it needs to be pulled out of the Information Operations estimate and a new Cyber Estimate should be created. For a given operational mission, the Cyber Estimate would include a complete description of U.S. capabilities and vulnerabilities for each state or non-state actor that the mission concerns. The estimate would also include potential targets that computer network exploitation has deemed accessible and vulnerable to computer network attack. By identifying potential targets early in the planning process, the other functional component commanders could synchronize their operations with the relatively limited target set available for computer network attack. A cyber estimate would ensure that

[60] Joint Forces Staff College, *Joint Information Operations Planning Handbook*, Joint Command, Control and Information Operations School. (March 2005), 114.

planners have the information required to fully integrate network operations into operational warfare.

Next, add a Joint Force Cyber Component Commander (JFCyCC) into each geographic combatant command.[61] Currently, each command has a Joint Force Functional Component Commander for land, air and sea operations. To fully integrate cyberspace into operational warfare requires the creation of a separate functional commander. The Cyber Component Commander would specialize in theater cyberspace issues that U.S. Cyber Command might not have the focus or interest in. Although the capabilities for computer network attack are universal, successful execution requires significant analysis of a specific network's vulnerabilities that a Cyber Component Commander should oversee.[62] Having a Cyber Component Commander responsible for the details and progress of theater cyberspace operations eases their integration into campaign plans and execution. Treating cyberspace as a domain requires the incorporation of a separate commander into the command structure in order to synchronize operations across the air, sea, land, and cyberspace domains.

Finally, service components should train in cyber-degraded environments. The training curriculum could start with minor computer network outages and continue to complete non-classified and classified computer network denial (to the utmost of any adversary's capability). Ultimately, all units should receive training in a cyber-degraded environment prior to deployment into a theater of operations. Training in a cyber-degraded environment exposes the entire chain of command to the scope of U.S. dependence on

[61] Martin Stallone, "Don't forget the Cyber! Why the Joint Force Commander Must Integrate Cyber Operations Across Other War Fighting Domains, and How a Joint Force Cyberspace Component Commander Will Help." (research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2009), 14.

[62] Libicki, *Cyberdeterrence and Cyberwar,* 154.

cyberspace. The training would also force operational commanders to clearly communicate orders and intentions to subordinates knowing that command and control could suffer degradation due to computer network attack. Finally, training in a cyber-degraded environment removes the mystery of computer network attack allowing the military to practice employment in spite of limitations in the cyberspace domain. Realistic training for future military operations requires training in a cyber-degraded environment.

Cyberspace represents the newest frontier in warfare. Because the U.S. military leads the world in incorporating computer technology into its forces, its choices in cyberspace will determine American success in future conflicts. Operational commanders need to integrate computer network operations into their planning and execution in order to protect their forces and capitalize on the offensive military power available to them.

BIBLIOGRAPHY

Akhvlediani, Margarita. “The Fatal Flaw: the Media and the Russian Invasion of Georgia.” *Small Wars & Insurgencies* 20, no. 2 (1 June 2009): 363. http://www.proquest.com/ (accessed 1 March 2010).

Boyd, Bradley L. “Cyber Warfare: Armageddon in a Teacup?” Master’s thesis, Fort Leavenworth, KS: U.S. Army Command and General Staff College, 12 November 2009.

Brenner, Susan. *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York, NY: Oxford University Press, 2009.

Carr, Jeff. *Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare.* Greylogic Report. 20 March 2009. http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report (accessed 13 April 2010).

Clarke, Richard. “War From Cyberspace.” *The National Interest*, 1 November 2009, 31-36. http://www.proquest.com/ (accessed 24 February 2010).

Cornell, Svante E. and S. Frederick Starr, ed. *The Guns of August 2008: Russia’s War in Georgia.* Armonk, NY: Sharpe, 2009.

Dudney, Robert S. “Threats or Capabilities?” *Air Force Magazine*, 1 October 2009, 2. http://www.proquest.com/ (accessed 19 February 2010)

“Europe: A cyber-riot; Estonia and Russia.” *The Economist*, 12 May 2007, 42. http://www.proquest.com/ (accessed 1 March 2010).

Evron, Gadi. “Estonian Cyber-War Highlights Civilian Vulnerabilities; During the Estonia Cyber-war, a Cooperative Effort Prevented Attacks From Taking Down Critical Infrastructure.” *eWeek*, 7 August 2007, 1. http://www.proquest.com/ (accessed 1 March 2010).

Fickes, Michael. “Cyber Terror.” *Government Security 7*, no. 4 (1 July 2008): 8. http://www.proquest.com/ (accessed 1 March 2010).

Fossi, Marc ed. *Symantec Internet Security Threat Report: Trends for 2008*, Vol. XIV, April 2009. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf (accessed on 9 April 2010).

Fulghum, David A. “Digits of Doom.” *Aviation Week & Space Technology* 167, no. 12 (24 September 2007): 74. http://ebsco.com/ (accessed 1 March 2010).

Fulghum, David A., and Douglas Barrie. “Stealthy and Subtle.” *Aviation Week & Space Technology* 171, no. 17 (9 November 2009): 76-78. http://ebsco.com/ (accessed 22 March 2010).

Gates, Robert. Secretary of Defense to Secretaries of the Military Departments. Memorandum, 23 June 2009.

Germain, Jack M. “The Art of Cyber Warfare, Part 1: The Digital Battlefield.” *TechNewsWorld*, 29 April 2008, 2. http://www.technewsworld.com/rsstory/62779.html?wlc=1256255575 (accessed 19 February 2010).

Gorman, Siobhan. “World News: Cyber Attacks on Georgia Used Facebook, Twitter, Stolen IDs.” *Wall Street Journal*, 17August 2009, Eastern Edition. http://www.proquest.com/ (accessed 1 March 2010).

Hille, Kathrin. “Hackers in Frontline of China's Cyberwar.” *FT.com*, 13 January 2010. http://www.proquest.com/ (accessed 19 Feb. 2010).

Hoffman, Bruce. “The Use of the Internet by Islamic Extremists,” Testimony presented to the House Permanent Select Committee on Intelligence, on 4 May 2006. Santa Monica, CA: RAND, 2006.

Joint Forces Staff College, *Joint Information Operations Planning Handbook*, Joint Command, Control and Information Operations School. March 2005.

Kampmark, Binoy. “Cyber Warfare Between Estonia and Russia.” *Contemporary Review*, 1 October 2007, 288-293. http://www.proquest.com/ (accessed 1 March 2010).

Kramnik, Ilya. “Cyberspace Wars: Militarization of Virtual Front.” *Moscow News (in English)*, 23 May 2008. http://www.proquest.com/ (accessed 1 March 2010).

Krekal, Brian. *Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* US-China Economic and Security Review Report. McLean, VA: Northrop Grumman, 2009.

Lewis, James Andrew. “Cyber Events Since 2006,” *Center for Strategic and International Studies*, 3 March 2010. http://csis.org/publication/cyber-events-2006 (accessed on 9 April 2010).

Libicki, Martin C. *Cyberdeterrence and Cyberwar*, RAND Report. Santa Monica, CA: RAND, 2009.

Manning, Elizabeth H. “Lessons Learned from the First War Fought in Cyberspace.” *The Officer*, 1 February 2009, 37. http://www.proquest.com/ (accessed 25 February 2010).

Markoff, John. “Before the Gunfire, Cyberattacks.” *The New York Times*, 12 August 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1 (accessed 25 March 2010).

Mat, William. “Chinese Attacks Bring Cyber Spying Into the Open.” *Defense News*, 18 January 2010. http://www.proquest.com/ (accessed 19 February 2010).

Mat, William. “Cyber War's 'Front Lines' May Be in Private Hands: ISA.” *Defense News.* 7 December 2009. http://www.proquest.com/ (accessed 19 February 2010).

Mattox, John M. “The Baby and the Bathwater: Changing Times or Changing Principles?” *Military Review*, 1 September 2008, 5-9. http://www.proquest.com/ (accessed 19 February 2010).

Mills, J. “Make Way for the Cyber Fleet!” *United States Naval Institute Proceedings.* January 2010, 64-69. http://www.proquest.com/ (accessed 24 February 2010).

Morgan, John G. and Anthony D Mc Ivor. “Rethinking the Principles of War.” *United States Naval Institute Proceedings*, 1 October 2003, 34-38. http://www.proquest.com/ (accessed 25 February, 2010).

Murdock, Paul. “Principles of War on the Network-Centric Battlefield: Mass and Economy of Force.” *Parameters* 32, no. 1 (1 April 2002): 86. http://www.proquest.com/ (accessed 25 February 2010).

Nguyen, Vinh. “Cyber Capabilities of Major Rising Powers.” Lecture. Naval War College, Newport, RI, 8 April 2010.

O’Hara, Timothy LCol. “Cyber Warfare/Cyber Terrorism.” Research paper, Carlisle, PA: U.S. Army War College, 3 May 2004.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: National Academies Press, 2009.

Parks, Raymond C. and David P. Duggan, “Principles of Cyber-Warfare.” *Proceedings of the 2001 IEEE workshop on Information and Security*. U.S. Military Academy, West Point, NY. 6 June 2001.

Reimer, Jordan. “U.S. Cyber Command Preparations Under Way, General Says,” American Forces Press Service, 17 March 2010. http://www.af.mil/news/story.asp?id=123195306 (accessed 25 March 2010).

Ronfeldt, David. “Netwar Across Spectrum of Conflict: An Introductory Comment.” *Studies in Conflict & Terrorism* 22, no. 3 (July 1999): 189. http://ebsco.com/ (accessed 12 April 2010).

Schaap, Arie J. “Cyber Warfare Operations: Development and use Under International Law.” *The Air Force Law Review*, 1 January 2009, 121-173. http://www.proquest.com/ (accessed 1 March 2010).

Schwartz, Norton. “Space, Cyberspace and National Security,” Lecture. Air Force Association, Orlando, FL, 18 February 2010. http://www.af.mil/shared/media/ document/AFD-100219-034.pdf (accessed 5 April 2010).

Stallone, Martin. “Don’t Forget the Cyber! Why the Joint Force Commander Must Integrate Cyber Operations Across Other War Fighting Domains, and How a Joint Force Cyberspace Component Commander Will Help.” Research Paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2009.

“The Mouse That Roared Cyberwarfare.” *Economist.com / Global Agenda*, 5 September 2007, 1. http://www.proquest.com/ (accessed 1 March 2010).

Traynor, Ian. “Russian Accused of Unleashing Cyber War to Disable Estonia,” *The Guardian.* 17 May 2007. http://www.guardian.co.uk/world/2007/may/ 17/topstories3.russia (accessed 9 April 2010).

U.S. Congress. Senate Committee on Armed Services. *Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command*, 111th Cong., 2nd sess., 2010. http://armed-services.senate.gov/statemnt/ 2010/04%20April/ Alexander%2004-15-10.pdf (accessed 25 April 2010).

U.S. Department of Homeland Security. *Cyber Storm II: Final Report.* Washington, DC. Department of Homeland Security, July 2009.

US Federal News Service. “Cybersecurity Seizes More Attention, Budget Dollars.” *US Fed News Service, Including US State News*, 5 February 2010. http://www.proquest.com/ (accessed 19 February 2010).

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*. Joint Publication (JP) 1-02, Washington, DC: CJCS, 12 May 2001 as amended through 31 October 2009.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United States*. Joint Publication (JP) 1, Washington, DC: CJCS, 2 May 2007 incorporating change 1, 20 March 2009.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *National Military Strategy for Cyberspace Operations*. Washington, DC: CJCS, December 2006. http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed 20 February 2010).

U.S. President. *The National Strategy to Secure Cyberspace.* Washington, DC: White House, 2003

Warner, Gary. "Radical Muslim Hackers Declare Cyberwar on Israel." *CyberCrime and doing time: A Blog about Cyber Crime and Related Justice issues,* entry posted 30 December 2008. http://garwarner.blogspot.com/2008/12/muslim-hackers-declare-cyberwar- on.html (accessed 13 April 2010).

Wright, Austin. "The Unseen Cyber-War." *National Defense,*1 December 2009. http://www.proquest.com/ (accessed 24 Feb. 2010).

Zanini, Michele and Sean J.A. Edwards. "The Networking of Terror in the Information Age," in *Networks and Netwars: The Future of Terror, Crime and Militancy,* ed. John Arquilla and David Ronfeldt. Santa Monica, CA:Rand, 2001.