# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 03-05-2011 | FINAL | |

**4. TITLE AND SUBTITLE**

Operational Art in the Fifth Domain

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**
Lt Charles Hall, USN

Paper Advisor (if Any): Lt Col Justin J. Speegle, USAF

**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**
*For Example:* 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 as a warfighting domain will increase in prominence, and future conflicts will include some aspect of cyberspace operations. Operational art, as a process for planning and executing military operations, is applicable in cyberspace and should be used to develop warfighting principles specific to cyberspace. This paper considers the use of operational art in cyber operations and across the cyberspace domain by analyzing three key elements of operational art: operational factors, critical factors, and center of gravity. Finally, the paper draws conclusions regarding the applicability of operational art in cyberspace, and its application in developing warfighting techniques specific to cyberspace.

**15. SUBJECT TERMS**
Cyberspace, operational art, cyber operations, operational factors, critical factors, principles of war, center of gravity

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Chairman, JMO Dept |
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | | 25 | 19b. TELEPHONE NUMBER *(include area code)* 401-841-3556 |

**Standard Form 298 (Rev. 8-98)**

**NAVAL WAR COLLEGE**
**Newport, R.I.**

# OPERATIONAL ART IN THE FIFTH DOMAIN

**by**

**Charles H. Hall**

**LT, US Navy**

**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: _____**

**May 4, 2011**

**Contents**

Abstract

*Operational Art in the Fifth Domain*

Cyberspace as a warfighting domain will increase in prominence, and future conflicts will include some aspect of cyberspace operations. Operational art, as a process for planning and executing military operations, is applicable in cyberspace and should be used to develop warfighting principles specific to cyberspace. This paper considers the use of operational art in cyber operations and across the cyberspace domain by analyzing three key elements of operational art: operational factors, critical factors, and center of gravity. Finally, the paper draws conclusions regarding the applicability of operational art in cyberspace, and its application in developing warfighting techniques specific to cyberspace.

# INTRODUCTION

The Russian-Georgian War in August of 2008 was the result of years of geopolitical tension between the two nations. While the conflict was cause for alarm internationally, as conventional wars go it wasn't unique. The Russian-initiated conflict included basic aspects of warfare in multiple domains, to include air, land, and sea. The conflict, however, was not limited to conventional aspects alone, or traditional warfighting domains. For what may be the first time in the history of conflict, cyber warfare played a significant role in an otherwise conventional conflict[1]. This synchronization of cyber warfare with conventional combat operations represents a key milestone in modern warfare.

Conflict in cyberspace is no longer a matter of if or when, but rather how. As conflict in cyberspace becomes more prevalent, a lack of preparation for cyber operations, both offensive and defensive, will come at a nation's peril. As militaries and intelligence agencies worldwide develop doctrine for cyberspace operations so must the U. S. In a recent article in Proceedings entitled "Learning to Operate in Cyberspace," Rear Admiral William E. Leigher, Deputy Commander of U.S. Fleet Cyber Command / U.S. Tenth Fleet, makes clear that warfighting principles applicable to cyberspace must be developed [2]. Fortunately, a construct for these principles already exists. This process, known as operational art, has been successfully used to plan and conduct a wide range of military operations across all warfighting domains. The practice of operational art is applicable in cyber warfare and should be used to develop warfighting principles for cyberspace.

## Defining Cyberspace

Cyber warfare is a common term these days, although its true meaning is still in dispute. Public information detailing cyber warfare events is prevalent and includes details of cyber operations against both the United States and other nations, such as Iran and Estonia. Attempted intrusions or disruptions of government networks are reported regularly. Whether you consider these events to be cyber warfare, cyber operations, or internet-based criminal activity, they nevertheless highlight the brave new world that is cyberspace.

This brave new world, recently dubbed the fifth domain, is possibly the most nebulous of the five warfighting domains -- sea, land, air, space, and now cyberspace. The Department of Defense defines cyberspace as, "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 [3]." This brief description, however, fails to truly characterize the domain that is cyberspace.

What makes cyberspace unique from other domains? For one it is manmade, and therefore in a continual state of flux. This endless web of inter-linked global networks is continually growing, its technology rapidly developing. Cyberspace is simultaneously linear and nonlinear. While the concept of the "network" can be easily envisaged, its vastness and unknown reaches prevent precise identification of boundaries. Finally, positively identifying cyber operators, a key aspect of warfare in any domain, can be especially challenging in the murkiness of cyberspace.

For these reasons, and many others, warfighting principles for cyberspace must be developed. Applying existing constructs for developing these principles is a sensible

approach, assuming they are applicable to this nascent domain. Operational art is one such construct that deserves consideration.

**Why Operational Art?**

As theory, operational art is enduring and can be applied across a wide and diverse spectrum. In one form or another, operational art has been used by militaries throughout the world for hundreds of years and has been used to successfully plan and execute a wide range of military operations across all warfighting domains. In the U.S. the process is taught at the individual service war colleges incorporated as part of the Joint Professional Military Education program.

The Department of Defense defines operational art as, "The application of creative imagination by commanders and staffs — supported by their skill, knowledge, and experience — to design strategies, campaigns, and major operations and organize and employ military forces[4]." While this is a good starting point for understanding operational art, another, more concise definition is beneficial. Naval War College Professor Dr. Milan Vego defines operational art as, "A component of military art concerned with the theory and practice of planning, preparing, conducting, and sustaining campaigns and major operations aimed at accomplishing strategic or operational objectives in a given theater [5]." Key aspects of operational art include the consideration of the operational factors of time, space, and force; the determination of critical factors, to include critical strengths and weaknesses; and the determination of enemy and friendly centers of gravity.

**Counter-Argument**

Critics will argue that cyberspace and cyber operations are distinctly unique in nature, and thus require new processes and constructs. Noted cyber-analyst Martin Libicki argues that cyberspace operations are unlike other forms of warfare and should not be defined in military terms [6]. Instead, new methods of planning and execution must be created in order to ensure success in cyberspace. It is likely that similar arguments were made at the advent of military aviation or subsurface warfare. In truth, operational art is an enduring theory that has been used from the Napleonic Wars to the current conflicts in Iraq and Afghanistan. While cyberspace and cyberspace operations are unique in nature, they too can be planned and executed using the process of operational art.

**Operational Factors**

The process of operational art begins with careful consideration of operational factors of space, time and force. Considered both individually and in conjunction with one another, these factors must be carefully balanced in order to accomplish a military objective [7]. As in other warfighting domains, each of these factors can be readily applied to cyberspace.

The operational factor of space is distinctly unique in cyber warfare. According to Vego, "space in itself is both a means and an objective [8]." The same can be said for cyberspace, where lines of communication and lines of operation share the same medium, and interior and exterior lines are blurred, or even non-existent. In any warfighting domain, the operational factor of space includes such considerations as size, distance, boundaries and infrastructure. The relationship between the physical domain and cyberspace also deserves special consideration.

Defining the size of cyberspace is impossible. As a domain, cyberspace is both linear and nonlinear. While the theory of the "network" can be easily envisaged, its vastness precludes precise definition. Size presents unique challenges for cyber operations, and makes conflict in cyberspace more analogous to irregular warfare than conventional warfare. Coordinating the efforts of multiple agencies in such a large environment is difficult. Intelligence preparation of the environment and situational awareness also become increasingly complex. In the U.S., efforts to balance space with force are currently underway. The Defense Department's Cyber Command considers situational awareness a priority, and has made the establishment of a common operating picture (COP) a command priority [9]. This effort mirrors those in other warfighting domains, although its implementation in cyberspace will be especially challenging.

Cyberspace does not easily lend itself to the establishment of boundaries. Data can be routed via multiple paths. Servers supporting one nation's cyber needs may physically reside outside that nation's boundaries. For example, whereas a theater of war or joint operating area would typically include clearly defined areas within the domains of air, sea, and land, no such boundaries can be established for cyberspace. According to Vego, "This has enormous consequences, because the very outcome of a campaign or major operation may depend on offensive and defensive actions conducted far beyond the theater's boundaries [10]." Organizations and procedures to coordinate efforts across multiple areas of responsibility, and potentially between multiple combatant commands, must therefore be established to balance space with force.

While "human-space" is typically considered relating to the operational factor of space, the cyberspace equivalent may be commercial infrastructure. The rapid growth of

cyberspace is due in large part to commercial interests and ventures. As a result, commercial networks have become intertwined with government networks, sometimes to excess. According to Brigadier General John Davis, U.S. Cyber Command director of current operations, "Ninety percent of what I use to do military missions across DoD rides on the commercial infrastructure [11]." Relying on commercial interests to properly safeguard military information is tantamount to a segmented defense and must be considered a vulnerability. The interests of those commercial companies may also be cause for alarm. For example, China's Huawei Technologies Company has been the target of a congressional investigation for potential ties to the Chinese military following negotiations to provide telecommunications equipment to U.S. companies [12]. The implication of commercial infrastructure in cyberspace operations is akin to dealing with the local populace while conducting counter-insurgency. While the ultimate implications of this so far are unclear, it certainly must be taken into account when planning operations in cyberspace.

The operational factor of time deserves special consideration in cyberspace. Of the three operational factors, time is unique in that lost time can never be regained. This is of critical importance in the rapid-fire tempo of cyber warfare. Time is also directly related to space. In a large domain such as cyberspace, preparation and planning time can be especially challenging. Timing and synchronization must also be considered regarding time.

The military is in a constant period of preparation and planning. The period is ongoing and continues until the outbreak of hostilities. Russian cyber operations conducted during the Russian-Georgian War in August 2008 took time to prepare and plan. These attacks, which were closely synchronized with air, land, and sea operations, successfully targeted the same geographic areas as the conventional elements of warfare. This caused a significant

disruption among the civilian population, disrupting a military response [13]. This successful balancing of synchronization (time) and geographic targeting (space) increased the effectiveness of the attacks. The success of such attacks must have hinged on an accurate intelligence preparation of the environment coupled with extensive operational-level planning.

Timing must also be considered when planning and executing cyberspace operations. According to Vego, there is a distinct "advantage to acting and reacting faster than the opponent[14]." This was clearly demonstrated during the Russian-Georgian War, where Georgia was caught off-guard in all warfighting domains, cyberspace included. As in other warfighting domains, timing is marked by the onset of hostilities and is typically set by the belligerent. Balancing time and force, however, can aid in a successful defense. For example, the establishment of an effective command and control (C2) structure may ensure a swift and balanced response. House testimony by General Alexander, Commander of the recently established U.S. Cyber Command, emphasizes the establishment of an effective operational C2 structure and a Joint Intelligence Operations Center [15]. Perhaps most importantly, the establishment of U.S. Cyber Command consolidates offensive and defensive cyber capabilities under one sub-unified command [16]. As in other warfighting domains, the key to successful C2 of cyber operations will be centralized control and decentralized execution.

At the operational level of war, cyber operations must be synchronized with other lines of operations. This requires detailed preparation and planning, couple with coordinated execution.

When the Israeli Air Force launched long-range strikes against a suspect Syrian nuclear facility in 2007, synchronized cyber operations may have been involved. These operations reportedly targeted vulnerabilities in Syria's integrated air defense system. While electronic attack must have played a significant role in this attack, analysts believe that some sort of cyber operations, involving computer-to-computer attacks, were also included [17]. These operations prevented the Syrian Air Defense network from detecting Israeli aircraft. As a result, Israeli Air Force were able to pass through Syrian airspace unharmed. In this case, the synchronization of cyber operations and air strikes ensured the safety of Israeli aircraft conducting the attack, which resulted in the destruction of the suspected nuclear facility. This scenario also demonstrates the manifestation of tangible cyber effects in physical warfighting domains.

The operational factor of force includes both tangible and intangible aspects. Tangible aspects of force include organization, command and control, and technology. Intangible aspects, which are more difficult to measure, include doctrine, training, and experience.

The composition of cyber forces varies greatly. The U.S. recently established U. S. Cyber Command, a sub-unified command subordinate to U.S. Strategic Command. Cyber Command's mission is to both protect U.S. freedom of action in cyberspace and, when directed, deny an adversary's freedom of action in cyberspace [18]. A cyber component has also been established at each of the four armed services. Determining exactly how U.S. Cyber Command and each service component will support the geographic combatant command is still in development [19]. While U.S. efforts to create a cyber force have been military-centric, other nations may rely on less formal, even mercenary style organizations. Russian cyberspace operations during the Russian-Georgian War of August 2008 were

reportedly conducted by a "cyber militia" [20]. While this may be an effective use of expertise and knowledge, it may also introduce issues of loyalty and motivation. The best solution for establishing a cyber force most likely would include a careful balance of technical expertise and military authority.

Efficient and effective command and control (C2) of forces is critical in any warfare area. The U.S. military tenet for C2 is centralized command and decentralized execution. In the time-constrained, rapid-paced domain of cyber warfare, establishing an effective C2 structure will be critical to mission success. Synchronized cyberspace operations must be coordinated with other warfare areas across the operational level of war. Space, on the other hand, introduces unique challenges to cyber C2. Cyberspace's lack of clear boundaries, coupled with near global access, will introduce challenging coordination issues between operational commanders and supporting geographic combatant commanders and other supporting agencies. Command and control of Russian cyber forces during the Russian-Georgian War of August 2008 appears to be have been effective, and serves as an example of balancing all three operational factors.

The application of force in cyber warfare differs greatly from the other warfighting areas. According to Vego, "The greater the factor of force at the operational level, the greater the operational commander's freedom to act [21]." In cyberspace, force is directly related to technology. Cyber weapons continue to increase in capability and sophistication. Whereas cyber weapons of the past may have simply disrupted operations in cyberspace, the employment of newer, more sophisticated weapons may result in actual kinetic effects [22]. The best, publicly known example of a cyber weapon to date is Stuxnet. Public information regarding Stuxnet was first revealed during the summer of 2010 after multiple infections

were discovered, primarily in Iran. Detailed analysis of Stuxnet has since determined that the weapon's purpose was to sabotage a power facility remotely by taking control of the programmable logic controllers (PLC) and causing them to operate beyond normal limits, resulting in physical damage of industrial components [23]. The implications of Stuxnet are clear. The advent of cyber weaponry capable of causing potentially kinetic effects has arrived. Detecting and defeating such cyber weaponry will be critical to future outcomes of cyber warfare.

Intangible aspects of force include doctrine, training, and experience. It should come as no surprise that in such a nascent warfare area much of these aspects are lacking. Rear Admiral Leigher's article in Proceedings calls for the development of cyber-specific warfighting principles [24]. Indeed, there is no doubt that such efforts are prevalent across the U.S. Department of Defense as cyberspace gains prominence. The establishment of sufficient doctrine will be crucial to effective cyberspace operations undertaken by any nation.

Training and experience is also crucial to effective cyberspace operations. Again, similar doctrine, training and experience will take time to develop. General Alexander, during an address to the House Committee on Armed Services, points this out stating, "there are too few trained Service personnel out there in the first place, and also the Services need to hold on to as many of them as they can [25]." Unfortunately, there is no way to balance time or space with these underdeveloped aspects of force. Establishing doctrine and fielding a well-trained and experienced force will remain a priority until complete.

**Critical Factors**

The next step of operational art is to determine critical factors. Critical factors can be divided into two broad categories: critical strengths and critical weaknesses. Identifying these factors will lead to the determination of critical vulnerabilities. Similar to operational factors, critical factors are as applicable in cyberspace as they are in the other warfighting domains.

Determining and enemy's critical strengths and weaknesses is a challenging endeavor. Yet doing so successfully is essential to the process of operational art. At the operational level, critical strengths are typically associated with a military's combat power [26]. Critical weaknesses are mission-essential capabilities which, for some reason or another, cannot accomplish their assigned function [27]. Conventional examples of both strengths and weaknesses include leadership, firepower, maneuver, equipment, logistics, doctrine, training and experience. Critical vulnerabilities, typically associated with critical weaknesses, are those critical factors which can be exploited to achieve a desired objective.

Critical factors can be logically applied to cyberspace operations as well. Leadership, doctrine, training, and experience all directly correlate to cyberspace operations. Cyber equivalents to firepower, maneuver, equipment, and logistics include technology, infrastructure, network security, and access. While determining critical factors for specific cyber forces is beyond the scope of this paper, pertinent examples of each are readily apparent in previously discussed material.

In the modern age advanced technology directly contributes to warfighting primacy across all warfare areas. The technology-intensive domain of cyberspace is no different. Indeed, technology may provide the advantage necessary to achieve the objective and could be considered a critical strength. The development and deployment of Stuxnet demonstrates

how important technology is in cyber warfare. Detailed analysis of Stuxnet describe it as "of such great complexity - requiring significant resource to develop" and "beyond any threat we have seen in the past [28]." The analysis continues stating that, "we would not expect masses of threats of similar sophistication to suddenly appear [29]." Analysis of a single cyber weapon may not indicate a critical strength alone. Effective training, and development of tactics, techniques, and procedures (TTP) associated with such a weapon will also contribute to its effectiveness in cyberspace operations. However, the development and deployment of Stuxnet indicates how technology may contribute to a force's critical strengths.

Adversely, a lack of technology or technological capability may be considered a critical weakness, especially in an area essential to mission success. Such is the case for U.S. Cyber Command as it seeks to develop a common operating picture (COP) for cyberspace [30]. The development of a COP is a technology-dependent effort in any warfare area. Cyberspace is no different. Once established, a COP will provide the domain awareness necessary to conduct both offensive and defensive cyberspace operations. Until developed, however, the lack of COP represents a critical weakness for a command tasked with conducting offensive and defensive cyberspace operations.

Determining critical vulnerabilities is the crucial next step in operational art. Critical vulnerabilities, when fully exploited, can be used to indirectly attack an enemy's center of gravity and may contribute to an enemy's defeat. During the Russian-Georgian War in August 2008, Russian cyber attacks targeted both internal and external communications of the Georgian government [31]. These efforts demonstrated Georgia's inability to defend its networks, exploiting a critical vulnerability associated with the center of gravity. In his center of gravity analysis, Vego indicates the future importance of computer networks in

operational and tactical centers of gravity [32]. Such was the case here as these synchronized cyber attacks demonstrated.

**Center of Gravity**

The final step in the operational art process is to determine an enemy's center of gravity. The Department of Defense defines center of gravity as, "The source of power that provides moral or physical strength, freedom of action, or will to act [33]." At the operational level of war there is typically understood to be one enemy center of gravity. While aspects of an enemy's center of gravity may reside in cyberspace, it will most likely also include other, more physical aspects, requiring military action in the remaining warfighting domains. Regardless, cyberspace operations may contribute to either direct or indirect attacks on an enemy's center of gravity.

Stuxnet is one example of cyberspace operations contributing to an indirect attack on an enemy's center of gravity. First, we must make two assumptions based on the available reporting. The first assumption is that the objective of Stuxnet was to disrupt or disable Iranian efforts to generate weapons-grade nuclear material. The second assumption is that nuclear weapons in the hands of the Iranian government would be considered the enemy center of gravity.

Available reporting on Stuxnet supports the first assumption. According to detailed analysis, Stuxnet targeted "a specific industrial control system in Iran [34]." Additionally, the vast majority of infections could be traced back to five specific sites, all of which were associated with Iran's nuclear program [35]. Stuxnet is an example of a cyber weapon, targeting physical elements of an industrial process critical to the successful production of

weapons-grade nuclear material, with staggering results. According to the New York Times, "when international inspectors visited Natanz in late 2009, they found that almost 1,000 gas centrifuges had been taken offline, leading to speculation that the attack may have disabled part of the complex [36]." While the exact implications are difficult to determine, Stuxnet is a clear example of cyberspace operations contributing to an indirect attack on an enemy's center of gravity.

**Conclusion**

Cyberspace as a warfighting domain will increase in prominence and future conflicts will include some aspect of cyberspace operations. Recent testimony of General Alexander before the House Committed on the Armed Services supports this theory [37]. While the exact contribution of cyberspace operations has not yet been determined, warfighting principles specific to cyberspace operations must be developed. Operational art is theory and is therefore enduring. It has been successfully used to plan and conduct a wide range of military operations across all warfighting domains. Cyberspace and cyber operations, while unique in many ways, can be planned and executed using the process of operational art.

**Recommendations**

Operational art should serve as the construct for the development of warfighting principles and doctrine specific to cyberspace operations. Additionally, operational-level staffs responsible for planning and executing cyberspace operations should be trained in the practice and practical application of operational art. Finally, cyberspace war-gaming should

include the process of operational art to ensure its applicability and efficacy in the fifth domain.

**End notes:**


1. Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, 6 January 2011, http://smallwarsjournal.com/blog/2011/01/cyberwar-case-study-georgia-20/, (accessed 4 March 2011), 1.

2. Leigher, William E. "Learning to Operate in Cyberspace." *Proceedings*, Vol. 137/2/1,296, 33.

3. U.S. Office of the Chairman of the Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms (JP 1-02)*. Washington, DC: CJCS, 8 November 2010, 92.

4. Ibid, 93.

5. Vego,. *Joint Operational Warfare Theory and Practice and V. 2, Historical Companion*. City: United States Dept. of Defense, 2009, I-4.

6. Eric Beidel, Cyberwars Should Not Be Defined in Military Terms, Experts Warn, 5 April 2011, http://www.nationaldefensemagazine.org/blog/lists/posts/post.aspx?ID=363, (accessed 6 April 2011).

7. Vego,. *Joint Operational Warfare Theory and Practice and V. 2, Historical Companion*. City: United States Dept. of Defense, 2009, III-3.

8. Ibid, III-7.

9. Meg Beasley, DoD wants common cyber picture, *Federal News Radio*, 24 February 2011, http://federalnewsradio.com/?nid=35&sid=2283664, (accessed 2 March 2011).

10. Vego,. *Joint Operational Warfare Theory and Practice and V. 2, Historical Companion*. City: United States Dept. of Defense, 2009, III-5.

11. Meg Beasley, DoD wants common cyber picture, *Federal News Radio*, 24 February 2011, http://federalnewsradio.com/?nid=35&sid=2283664, (accessed 2 March 2011).

12. Lococo, Edmond, U.S. Lawmakers Request FCC to Review China's Huawei, ZTE, *Bloomberg News*, 19 October 2010, http://www.bloomberg.com/news/2010-10-20/u-s-lawmakers-request-fcc-to-review-china-s-huawei-zte-on-security-risks.html, (accessed 12 March 2011).

13. Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, 6 January 2011, http://smallwarsjournal.com/blog/2011/01/cyberwar-case-study-georgia-20/, (accessed 4

March 2011), 8.

14. *Vego,. Joint Operational Warfare Theory and Practice and V. 2, Historical Companion*. City: United States Dept. of Defense, 2009, III-29.

*15.* General Keith B. Alexander, "Testimony," House, *United States Cyber Command before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services*, 112th Cong., 1st sess, 2011, 3.

16. Molly Bernhart Walker, Gen. Alexander: CYBERCOM structure will ensure seamless response to cyber crisis, Fierce Government IT, 23 February 2011, http:/ / www.fiercegovernmentit.com/story/gen-alexander-cybercom-structure-will-ensure-seamless-response-cyber-crisis/2011-02-23,(accessed 25 February 2011).

17. R.K., Clarke,. *Cyber war: the next threat to national security and what to do about it*. City: Ecco, 2010, 5.

18. General Keith B. Alexander, "Testimony," House, *United States Cyber Command before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services*, 112th Cong., 1st sess, 2011, 14-15.

19. Ibid, 13.

20 Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, 6 January 2011, http://smallwarsjournal.com/blog/2011/01/cyberwar-case-study-georgia-20/, (accessed 4 March 2011), 5.

21. *Vego,. Joint Operational Warfare Theory and Practice and V. 2, Historical Companion*. City: United States Dept. of Defense, 2009, III-33.

22. General Keith B. Alexander, "Testimony," House, *United States Cyber Command before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services*, 112th Cong., 1st sess, 2011, 6.

23. Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier, Symantex Security Response (Cupertino, CA: Symantec Corporation, 2011), 2.

24. Leigher, William E. “Learning to Operate in Cyberspace.” *Proceedings*, Vol. 137/2/1,296,
33.

25. General Keith B. Alexander, “Testimony,” House, *United States Cyber Command before the*
*Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services*,
112th Cong., 1st sess, 2011, 16.

26. Vego,. *Joint Operational Warfare Theory and Practice and V. 2, Historical Companion*. City: United States Dept. of Defense, 2009, VII-15.

27. Ibid, VII-16.

28. Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier, Symantex Security
Response (Cupertino, CA: Symantec Corporation, 2011), 54.

29. Ibid, 54.

30. Meg Beasley, DoD wants common cyber picture, *Federal News Radio*, 24 February 2011,
http://federalnewsradio.com/?nid=35&sid=2283664, (accessed 2 March 2011).

31. Hollis, David. “Cyberwar Case Study: Georgia 2008.” *Small Wars Journal*, 6 January 2011,
http://smallwarsjournal.com/blog/2011/01/cyberwar-case-study-georgia-20/, (accessed 4 March 2011), 5.

32. Vego,. *Joint Operational Warfare Theory and Practice and V. 2, Historical Companion*. City: United States Dept. of Defense, 2009, XIV-11.

33. U.S. Office of the Chairman of the Joint Chiefs of Staff. *Department of Defense Dictionary*
*of Military and Associated Terms (JP 1-02)*. Washington, DC: CJCS, 8 November 2010, 48.

34. Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier, Symantex Security
Response (Cupertino, CA: Symantec Corporation, 2011), 2.

35. John Markoff, Malware Aimed at Iran Hit Five Sites, Report Says, *The New York Times*, 11 February, 2011, http://www.nytimes.com/2011/02/13/science/13stuxnet.html, (accessed 2 February 2011).

36. Ibid.

37. General Keith B. Alexander, "Testimony," House, *United States Cyber Command before the*
*Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services*,
112th Cong., 1st sess, 2011, 15.

**Bibliography:**


Eric Beidel, Cyberwars Should Not Be Defined in Military Terms, Experts Warn, 5 April 2011, http://www.nationaldefensemagazine.org/blog/lists/posts/post.aspx?ID=363, (accessed 6 April 2011).

General Keith B. Alexander, "Testimony," House, *United States Cyber Command before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services*, 112th Cong., 1st sess, 2011, 3.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, 6 January 2011, http://smallwarsjournal.com/blog/2011/01/cyberwar-case-study-georgia-20/, (accessed 4 March 2011), 1.

John Markoff, Malware Aimed at Iran Hit Five Sites, Report Says, *The New York Times*, 11 February, 2011, http://www.nytimes.com/2011/02/13/science/13stuxnet.html, (accessed 2 February 2011).

Leigher, William E. "Learning to Operate in Cyberspace." *Proceedings*, Vol. 137/2/1,296, 33.

Lococo, Edmond, U.S. Lawmakers Request FCC to Review China's Huawei, ZTE, *Bloomberg News*, 19 October 2010, http://www.bloomberg.com/news/2010-10-20/u-s-lawmakers-request-fcc-to-review-china-s-huawei-zte-on-security-risks.html, (accessed 12 March 2011).

Meg Beasley, DoD wants common cyber picture, *Federal News Radio*, 24 February 2011, http://federalnewsradio.com/?nid=35&sid=2283664, (accessed 2 March 2011).

Molly Bernhart Walker, Gen. Alexander: CYBERCOM structure will ensure seamless response to cyber crisis, Fierce Government IT, 23 February 2011, http://www.fiercegovernmentit.com/story/gen-alexander-cybercom-structure-will-ensure-seamless-response-cyber-crisis/2011-02-23,(accessed 25 February 2011).

Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier, Symantex Security Response (Cupertino, CA: Symantec Corporation, 2011), 2.

R.K., Clarke,. *Cyber war: the next threat to national security and what to do about it*. City: Ecco, 2010, 5.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms (JP 1-02)*. Washington, DC: CJCS, 8 November 2010, 92.

Vego,. *Joint Operational Warfare Theory and Practice and V. 2, Historical Companion*. City: United States Dept. of Defense, 2009, I-4.

**Definition of Terms:**

Center of gravity — The source of power that provides moral or physical strength, freedom of action, or will to act. Also called COG. See also decisive point. (JP 3-0)

Critical capability — A means that is considered a crucial enabler for a center of gravity to function as such and is essential to the accomplishment of the specified or assumed objective(s). (JP 5-0)

Cyberspace — 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. (CJCS CM-0363-08)

Cyberspace operations — The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. (JP 3-0)

Operational art — The application of creative imagination by commanders and staffs — supported by their skill, knowledge, and experience — to design strategies, campaigns, and major operations and organize and employ military forces. Operational art integrates ends, ways, and means across the levels of war. (JP 3-0)