2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

Applying Traditional Military Principles to Cyber Warfare

Samuel Liles
Cyber Integration and Information Operations Department
National Defense University iCollege
Washington, DC
Samuel.Liles@NDU.edu

Marcus Rogers
Computer and Information Technology Department
Purdue University
West Lafayette, IN
rogersmk@purdue.edu

J. Eric Dietz
Purdue Homeland Security Institute
Purdue University
West Lafayette, IN
jedietz@purdue.edu

Dean Larson
Larson Performance Engineering
Munster, IN
deanlarson@larsonperformance.com

Abstract: Utilizing a variety of resources, the conventions of land warfare will be analyzed for their cyber impact by using the principles designated by the United States Army. The analysis will discuss in detail the factors impacting security of the network enterprise for command and control, the information conduits found in the technological enterprise, and the effects upon the adversary and combatant commander.

Keywords: *cyber warfare, military principles, combatant controls, mechanisms, strategy*

1. INTRODUCTION

Adams informs us that rapid changes due to technology have increasingly effected the affairs of the military. This effect whether economic, political, or otherwise has sometimes been extreme. Technology has also made substantial impacts on the prosecution of war. Adams also informs us that information technology is one of the primary change agents in the military of today and likely of the future [1]. There is a difference between using information technology or cyber space as a domain to fight and fighting in the domain of cyber space. Some of the differences appear to be maturity issues in understanding the cyber space domain. The translation of warfare strategies from other domains into an operational art is a process that is simply in its infancy [2]. General Alexander in 2007 said that we currently face many similar issues grappling with cyberspace as a war-fighting domain as the military did during the Interwar years from 1919 to 1938 understanding air-power [2].

This lack of maturity in understanding cyber space appears to be related to other myths of conflict. There are four myths of future land war suggested by Dunlap that are easily applied to cyber warfare; 1) Our most likely future adversaries will be like us; 2) We can safely downsize our military in favor of smaller, highly trained forces equipped with high-technology weapons; 3) We can achieve information superiority and even dominance in future conflicts; 4) Modern technology will make future war more humane if not bloodless. These myths are based the larger quandary known as the "revolution in military affairs" and the "generational constructs" being developed at the same time as it was written by Dunlap [3].

Cyber warfare has many definitions which makes it hard to state exactly what it is when it is many things depending on point of view. One suggested definition is that cyberwar is conducting military operations according to information-related principles while disrupting, destroying and knowing much about an adversary while keeping them from knowing about you [4,5]. Land warfare though has a very similar definition, as we will see in much deeper detail later. This leads into the purpose and scope of this paper:

> Using the conventions for land warfare, what kinds of cyber threats constitute attacks and how do we characterize possible cyber warfare scenarios or attack techniques to provide concepts for a generalized approach that supports situational awareness of the cyber battle space or "terrain"? How does this tool vary for first responders or military operations?

As such it might help to discuss the basic principles of the preeminent land war force in the world. It helps to understand the scope if the principles are detailed. The United States Army in dealing with land warfare has nine principles of war:

> 1) Objective – direct every military operation towards a clearly define, decisive, and attainable objective; 2) Offensive – seize, retain, and exploit the initiative; 3) Mass – concentrate the effects of combat power at the decisive place and time; 4) Economy of force – allocate minimum essential combat power to secondary efforts; 5) Maneuver – place the enemy in a disadvantageous position through the flexible application of combat power; 6) Unity of command – for every objective, ensure unity of effort under one responsible commander; 7) Security – never permit the enemy to acquire an unexpected advantage; 8) Surprise – strike the enemy at a time or place or in a manner for which he is unprepared; 9) Simplicity – prepare clear, uncomplicated plans and clear, concise orders to ensure thorough understanding. [6]

If mass and economy are related it is important for the combatant commander to understand how cyber enables the mission. The network centric aspects of future battle spaces means that a new weakness has been included too. Effective employment of cyber assets includes an understanding of defending those assets [7]. Parks details several principles of cyber warfare including that cyber warfare must have kinetic effects [8]. Discussing this, Parks says, there are no laws in cyber space, somebody can do just about anything to somebody else given enough authority, tools are dual use, defender and attackers control very little, and cyber space is not consistent. Parks illustrates some of the differences between what the Army doctrine would expect and the capabilities of actual cyber space. Saydjari also looked at the corresponding relationship between information assurance and military doctrinal statements

[9]. Saydjari states that cyber warfare relies on: sensors and exploitation; situational awareness; defensive mechanisms; command and control; strategies and tactics; and then finally science and engineering. The question of effectiveness of attack is in doubt when there is a substantial disconnect between published Army doctrine and the experts opinions on how it all fits together. Attacks from cyber space are cheaper and have substantial impediments to attribution, and as such it is not hard to believe that adversaries of a nation state could attack using information technology in an attempt to manipulate policy and decision makers [10]. Brooks suggested that information operations as a discipline needed to be included in the primary planning phases of operations. Information operations are a form of attack that still fits within the nine principles of military doctrine [10]. This is exactly what China was accused of doing on numerous occasions. Though it appears in most cases infiltration of networks by technology or human agents is done for the exfiltration of information (espionage) [11-15]. Of course, there is also the threat of other nation states such as Russia engaging in espionage through the network [16]. This is not to say that the United States is not also involved in espionage activities. Corn explains that the Pentagon has examined computer communications in transit to determine the modes of operations and goals of fringe groups [17].

The forms of attack are varied and inclusive of goals other than simply winning territory. Conflict is a continuum of strategies into which insurgency rises as a primary strategy. As such irregular warfare and insurgency are old ideas that get applied to new domains of battle repeatedly [18]. The distinctions between irregular warfare, insurgency, low-intensity conflict, guerilla warfare, and terrorism are counterpointed by the merits of each on a continuum of conflict. Gray reminds us that war is basically and simplistically war. The rules of war are applied often after the conflict [18].

Asymmetry, the defining element of insurgency, is not designed to win in the battle-space but to disrupt, distract, disconnect, or debilitate the nation state [19-21]. Relatively speaking the global communications network is nearly exclusively an asymmetric environment where mass and maneuver have minimal meaning. Dion examines the impact of digital capabilities in bringing mass and maneuver to the battle space [19]. This though is a capability not a weapon. Dion is discussing the layering of the digital information technology environment upon the weapons platforms of the Army. This gives the nation-state a significant information edge over the adversary. Layering cyber space capabilities onto terrestrial weapons platforms is not functionally different from using naval forces to support land forces. Another example might be space assets, such as reconnaissance satellites, that support all natural domains (air, land, sea) similar to how cyber supports command and control.

Tying back to the tenets espoused previously, Groh sees military conduct in cyber space as network centric operations and reflecting back to the original tenets of Army doctrine [22]. Specifically he has four information centric statements paraphrased as: 1) Robust networked force improves information sharing; 2) Information sharing and collaboration enhance the quality of information and situational awareness; 3) Shared situational awareness enables self-synchronization; 4) These all increase mission effectiveness. Each point can be brought back to the ideas of speed, maneuver, and unity of command. In this regard network centric warfare is specifically linked to these concepts. As such cyber warfare, which is attacking those channels of information flow, will target the nodes of communication. If taken as information operations

centric, there is some worry of overstating the case. Groh specifically warns that network centric warfare is not a silver bullet as his tenets of network centric warfare limit the doctrinal application to a few areas of specialty.

2. SITUATIONAL AWARENESS TO INFORMATION AS CONTESTED TERRAIN

Cyberspace is not a wholly new area of conflict and is not necessarily a new or nonphysical construct. In fact it is a wholly physical construct much like any other terrain [23]. The advent of cyberspace as a contested domain has significant implications to military doctrine. The strategic understanding of impacts, such as situational awareness removing the fog of war from commanders' current understanding of conditions, are nearly incomprehensible. The strategic and cognitive impacts to leaders' planning and operational capability should be extensive [24,25].

Command and control warfare is the application of computer information technology for offensive and defensive military operations. Rather than being a primary mode of operations, command and control warfare is an enhancement to the ability of the military unit to operate [26,27]. The cyber assets used by a commander to control can also be used against the commander. As such there is an inherent linkage between the communication infrastructure and the combatant commander. Though there is a relative desire on the part of technologists to say computer information technology it might be important to note that information technology and computers exist at all levels and not simply the desktop personal computer. Many military radios and encryption systems are filled with computers too.

The addition of information technology and computerized capability incurs a set of new risks that are balanced alongside the gains of the new technology. Critics of the technology may overstate the risks. One element likely overstated is the preponderance of "collapse theory" as the primary risk associated with increased information technology capability [24]. Large scale computing systems and communications systems are built with redundancy and scalable capacity. Overwhelming these systems is possible but the idea of collapse theory is that they will not recover from failure.

The ability to utilize ubiquitous computing for decision support and communication through the battle space has substantially increased the scope and vision of the commander in what is becoming known as network centric warfare [28]. There are five tenets to the process of waging network centric warfare according to Adkins 1) Knowledge of the competition, or in the case of the military, the adversary; 2) Near real time shared situation awareness; 3) Communications of the corporate or commander's intent; 4) Decentralized execution of plans; 5) Enabling self-synchronization [28]. This is expanding once again the capability from simply information operations (attacking information flows), past command and control warfare (attacking commanders intent), to utilizing the network to enhance the commander's control. Usually though we see command and control warfare as a strategy to disrupt decision processes.

Command and control in warfare is a strategic issue and tactical conundrum as network

centric capability is realized, though, it is not fully realized, or equally realized across the military enterprise. Acquisition of capability that was commercially available but not within the procurement system slowed and degraded the capability of the Army in Operation Iraqi Freedom. This created an expectation gap of possible versus the operational [29]. Examining this issue in depth Cogan also detailed that tactical communications were degraded by the capability of the end point equipment versus the capability of the backbones bandwidth. From this examination we can deduce two clues about attacking command and control from a cyber warfare denial of service aspect. First, the war, even with degraded capability of the networked equipment, was waged rapidly and successfully. Second, the acquisition process had more effect on the Army capability than the meager attempts to destroy or infiltrate the network. This would be counter to the theorists of collapse theory as discussed by Leonhard [30].

This has left the command and control aspects of warfare much where they were two or three decades ago. Rather than a decrease in capability, the expectations simply have not been met. Where there is increased capability it is held up as an example of superiority. If command is carried out by direction, by plan, or by influence has the automated nature of command and control met those tenets [31]? Command by direction being the oldest method of command, and command by influence being a relatively new construct suggests some maturation of the process. Into this mix cyber warfare as a capability is added.

Metaphors of attack often lack realistic operational thinking. The colloquialism that all elegant metaphors degrade under enough pressure surely must hold true. A favored metaphor of layered defense, or defense in depth, may make metaphorical sense but can be problematic in reality. This is an issue between the logical structure of networks and the physical structure of them. A castle metaphor is good to discuss computer and network security but it lacks certain elegance and sophistication of thinking. Empirical research suggests that layered defense strategies consistently decrease the security of a system. This is based on the increased complexity and increased control services that an adversary could attack [32]. So not only do the cognitive issues degrade but the actual security mechanisms may be degrading, too.

There is also the logical layer in how technology is used. Information systems exist to allow people to communicate and coordinate activities much like any form of technology based communication. Information technology though has some issues with how communication is conducted. Social media and information systems can be exploited through the systems' inherent human centric lag [33]. As an example an insurgency is an inherently social organization with a political purpose. As such a social network approach to understanding them can give clues as to how they are using technology and what that interaction might look like in the real world. Insurgencies are a particular subset of the spectrum of conflict and defy rigid classification [34]. So, the logical and cognitive layers may be both supported by information technology and then exploited (used) by adversaries alike.

One of the issues to the Army and other military organizations is the simple prevalence of the technologies necessary to wage war in cyber space. This is a social problem using technology and not a technology enabling social interaction [35]. The technology in some cases has become the reason rather than the use of the technology. In other cases technology is banned because it is technology rather than the behavior of the misuse. This conundrum has opened

up avenues to exploitation not previously exposed. Whether considered from the prospect of actually using cyber space as a tool to attack, or more likely using cyber space tools to coordinate and communicate a highly desirable capability exists. The ability to raise a mass of socially, technically, networked people with defined purpose is the new *Levee en Masse* [17]. Unfortunately large organizations rarely have the ability to leverage this capability as fast as smaller organizations.

3. APPROACHES TO AN ATTACK IN CYBER SPACE

There are specific behaviors and paths that an attacker will usually take. "An attacker is going to attempt to deny, corrupt, or exploit the adversary's information or influence the adversary's perception" [20]. There is a pretty standard process that will accomplish the prior. The adversary will gather information about the target, plan the attack, and execute the attack. This process is similar to any military activity and only the depth of each step and the conclusions might be different between traditional arms and cyber attacks. Currently there is little in the way of a cyber war rules of engagement. Related to this gap is the missing legal and doctrine development for waging cyber warfare by nation states [36]. The process can take into account each of the nine principles and may be tightly organized around a cross domain approach (utilizing tactics from multiple avenues of attack not simply cyber). This leads to a discussion on strategy and what it means to those nine principles.

For the purpose of considering strategic information warfare Rattray describes three forms of attack: 1) mechanical attacks; 2) electromagnetic attacks; 3) digital attacks. Each of these forms of attack takes on specific strategic aspects and merits [23]. Each of the forms of attack can be directed at or from cyber as the operating weapons system. When considering the merits of attack and defense in the cyber battle space the normal frictions of combat become elusive. Most military doctrine currently understood is about war of attrition, but cyber warfare does not seem as weak to cessation of communication as previously thought [37]. Working around technical disruptions has continued without much in the way of the issue moving forward as a prelude or cyber attack. Various systems and methods of design and infrastructure have been examined to determine an appropriate strategy for dealing with outages [38]. So, even if the attack is successful it may be seen as degradation before it is seen as a serious issue.

When the combatant commander contemplates attack there are serious issues to consider. There is a caution to combatant commanders during the attack phase of command and control warfare to steer clear of imitative deception to commit perfidious acts (false flag operations) as these could be considered war crimes [39]. How this may actually be built into battle plans is not currently discussed outside of classified environments. Actually, not much is discussed in unclassified environments about military training in cyber space. The training of military computer attack teams are classified, but due to the open nature of the technologies involved are likely similar to any other corporate red team capability [40].

4. GENERATIONAL CONSTRUCTS ATTEMPT TO DEFINE CYBER CONFLICT

The revolution in military affairs in many ways is the root of the substantial change and advancement of generational constructs to explain war theory since the mid 1990s [41]. One of the newer concepts suggested is the idea of generational constructs to define conflict strategies and capabilities. Each of the generations of warfare is defined as a capability, technology, or tactic that builds upon the previous generation. For this paper a detailed discussion is not within the scope but see other works by the author for that examination. The concepts and movement of ideas about generational constructs continues to today with work by Hammes. Hammes expands his concepts of generational constructs from fourth to a possible fifth generational component. This fifth generational component is an information operations and cyber enabled population's conflict realm [42]. This work is in addition to the work he did in 2004 where fourth generational related insurgency specific constructs were detailed and analyzed.

Hammes discusses in depth the changing face of war and details the generational warfare construct as an explanatory mechanism. Rather than thinking temporal, each succeeding generation of warfare is advancement in methodology. The first two generations of warfare are answers to technical problems with technology solutions [43]. The third generation of warfare is a change in tactics as Hammes suggests evidenced by mechanization and speed of armor allowed to flourish during World War 2 during the German invasion of Poland[43]. For our purposes in considering the addition of cyber conflict the fourth generation as population centric is especially of interest. The conflict space of fourth generation warfare is that of insurgency or populist aggression against the nation states as Hammes illustrates while discussing Mao [43]. Hammes (2007) builds upon the former to add a cyber and information spectrum for a fifth generational construct.

The realm of cyberspace allows for the fourth generation warfare construct to grow rapidly. When considering the Maoist "displacement strategy" of building "parallel hierarchies" government legitimacy is threatened [44]. Rather than relying on the traditional elements of military warfare such as maneuver, the insurgent in cyber space can use temporal displacement to negate nation state power. The nation-state though should be especially careful as the technological advantage can be lost in a societal shift [45]. Terrorism is especially linked to the idea of legitimacy. Thinking back to the previous discussion on asymmetry when mass and maneuver or not a capability the adversary can leap past them to take on legitimacy of governance. Terrorism via cyber means may break the principles back.

Cyber terrorism as discussed is a relatively inexpensive tool to use in an attack. Yet is wholly an expensive and difficult activity to protect against. Though skeptical Giacomello discussed cyber terrorism in detail as a possibility rather than defined capability [46]. One issue detailed by Giacommello is that the word terrorism is relatively meaningless being defined differently in law and literature. This is supported by in depth by Gordon [47]. In considering the merits of cyber terrorism Giacommello makes a startlingly conclusion that the issue is primarily a cultural phenomenon rather than technical. Perhaps not nearly as startling as expected, as all conflict regardless of the tools is likely cultural in nature.

5. MILITARY OPERATIONS IN CYBER SPACE

Discussing the issues of information in the battle space is nothing new to the Army [45]. There has, however, been a growing scholarship of dealing with information operations from the standpoint of conflict communications. There is also prevalent thread of thought in the international community that suggests information operations can decrease the perfidy of conflict [48].

Simply having computers and using them as communication conduits is not the only issue to combatant commanders considering cyber conflict. The ethics and assumptions of actions taken in cyber space especially computer network attack must be considered. A combatant commander must consider the ideas of discrimination between targets and proportionality of response. [39,49]

6. RESULTS

Coming back to the discussion of how the Army defines conflict and the nine principles of war and combat discussed previously, a series of resulting conclusions can be mapped. These are by no means expected to be the only conclusions that could be derived from the literature. They however do map and can be seen through the lens of the literature. As a cyber conflict space these nine principles have specific allegory to the cyber domain.

The objective in cyber conflict has not substantially changed from the previous consideration of terrestrial conflict. The idea of what attack means and the means of that attack has not substantially changed. The use of generational constructs and information operations has not substantially changed the concept of defining a goal or end-state to an engagement. Relatively simple in statement the where withal to accomplish the task through cyber means can be harder to determine. One element to objective that should not be ignored is that the set of strategic targets and objectives with cyber has been substantially increased in scope.

Taking the offensive is an interesting question. In the idea of generational warfare constructs and low-intensity-conflict, which is related to the tactical choice of insurgency, the offensive may not be similar to previous engagements. To be more specific the forms of conflict are likely to relate more to the fourth and fifth generational models suggesting insurgency and less to high-intensity conflict models where other principles relate closer. It appears taking the offensive may itself be in doubt as limiting war to cyber space may make the principle of offense less obvious. The roles of offense and defense seem to blur within an insurgency model as they do within cyber space.

Mass and economy of force as stated earlier appear to be related within the literature when considering the significant asymmetry of attack strategies and defense requirements. As such, examples of mass jump to the forefront that may not be the best examples. A distributed denial of service appears to be mass when in actually the result is significant but the force behind it is not. That might suggest that technology itself is a force multiplier and in the case of computer information technology substantial. However, that also misses the point that the

effect is primarily against other computer information technology. The user of armor or heavy weapons is technology that has significant impact against people. To be a relevant principle in considering mass and economy of force they would have to effect people. Unfortunately to gain that effect a third element must be rolled in and mass subtracted from the equation. As principles to broadly define military strategic issues they are weakening quickly.

A principle of maneuver exists, as it is not a fact of physical, but also emotional and cognitive. The previously discussed information operations use maneuver to speed combatant commanders and adversaries decisions cycles into appropriate resulting conclusions. Already defined for us through the information operations aspect of current strategic thought we can now apply that same principle of maneuver even faster through computer information technology.

Unity of command as a principle we saw from the literature strongly holds to the use of information technology as the current tool suite used. As seen in several cases command and control are inherently part of this equation and acted upon by computer information technology assets. Those assets are inherently part of the current landscape and the concepts of network centric warfare within the literature are deeply rooted to this basic principle. It then follows that unity of command is a fundamental principle of cyber warfare as it is currently used within computer information technology. Unity of command has used technology for the idea of command and control since smoke signals, semaphore and watch towers as beacons. The advent of computer information technology has only made the cyber landscape faster.

Without a lack of security the computer information technology attack vector might be said to be missing. Unfortunately perfectly perfected computing systems are still perfectly exploitable by people using them for purposes exactly as designed with nefarious results. The literature describes in detail the ideas of cascading failures and the criticisms of that flawed logic. What are not described are insider actions by military entities such as spies and agents. That is likely a classified discussion but a relevant thread for future research.

The act of surprise grows harder and more difficult on the high intensity conflict terrains of the modern battlefield. Observance of the last several incursions by foreign and domestic powers into other sovereign territory have been preceded by massive buildups where the actual attack appears as a pressure cooker finally blowing off steam. Surprise might be characterized as, that it took so long, instead of actually being stealthy. In the computer information technology domain of cyber warfare it becomes rapidly obvious that many attacks are taking place daily. This is supported by numerous literature resources that described earlier the idea of security being lacking. Thus surprise has much to be compared to current terrestrial combat.

Simplicity is in the binary. There is little simpler than the binary of on-off that runs computers. Refuting that point is the systems of systems discussion identified in the literature, which suggested massive scalable systems are created with significant holes in their security. The literature would support that the simplicity assists the adversary through the other principle of economy of force, and that the attacker garners the benefit while the defender is on the opposite side of the simplicity coin. The principle of simplicity as identified in the literature though cascading systems failure and systems of systems approach to design must support the attacker more than it will the defender.

7. CONCLUSIONS

Looking at the conventions of land warfare and the principles of war that constitute strategy and tactics it becomes obvious that there is a substantial disconnect when considering cyber warfare. In fact, there are those who simply say it does not exist [39]. A disconnect between the legal, moral, and ethical considerations perhaps: the conventions for land warfare often refer to the laws of land war, as in the Geneva Convention. However in answering the research question, the author decided to focus primarily on the second part of the research question to answer how the techniques and concepts for generalized approaches to situational awareness might be accomplished.

In ignoring the first part of what constitutes an attack under the law of war, we were able to talk about a variety of attacks. The discussion within this paper answers the idea of attack centered on the types of attack that were possible. Part of this is that perfidy and *jus in bello* in information security simply has not been described succinctly [39]. Simply put the use of the civilian network which is nearly a requirement puts the entire first part of the original research question into a quandary. The civilian network component as described adds possible perfidy to every attack and a nearly defacto risk of violations of the laws of war [25,50].

Finally the last part of the question of how this tool varies is easily answered as discussed previously. The attack is always going to be at an asymmetric advantage that cannot be substantially changed. The level of effort to enter the field of battle no longer requires the nation state. As such the first responder is radically empowered by the scope of their capability to attack but have no real capability at defense when integrated into a corporate or military information enterprise. This is the asymmetric advantage that currently does not erode or seem to erode under scalable systems.

As such the research question has been answered in detail with supporting literature from a variety of resources.

REFERENCES:

[1] T. K. Adams, “Radical destabilizing effects of new technologies,” Parameters, vol. 1998, pp. 99-111, 1998.
[2] K. B. Alexander, “Warfighting in cyberspace,” Joint Forces Quarterly, vol. 3rd Quarter, pp. 58-61, 2007.
[3] C. Dunlap, “21st century land warfare: Four dangerous myths,” Parameters, vol. 1997, pp. 27-37, 1997.
[4] J. Arquilla and D. Ronfeldt, Networks and netwars: The future of terror, crime, and militancy. Santa Monica, CA: RAND, 2001.
[5] B. Panda and J. Giordano, “Defensive information warfare,” Communications of the ACM, vol. 42, pp. 31-32, July 1999.
[6] U. S. Army, “FM 3.0 Operations,” T. U. S. Army, Ed., ed. Washington DC, 2001, p. 104.
[7] P. Murdock, “Principles of war on the network-centric battlefield: Mass and economy of force,” Parameters, vol. 2002, pp. 86-95, 2002.
[8] R. C. Parks and D. P. Duggan, “Principles of cyber-warfare,” in 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 2001, pp. 122-125.
[9] S. Saydjari, “Cyber defense: Art to science,” Communications of the ACM, vol. 47, pp. 53-57, March 2004.
[10] P. Brooks, “A vision of PSYOP in the information age,” Special Warfare, 2000.

[11] S. Cooper. (2006) China's secret war. Popular Mechanics. Available: http://www.popularmechanics.com/technology/military_law/3319656.html
[12] J. A. Lewis, Computer espionage, Titan Rain, and China. Washington DC: Center for Strategic & International Studies, 2005.
[13] T. Espiner. (2005, November 17, 2007). Security experts lift lid on Chinese hack attacks. Available: http://news.zdnet.com/2100-1009_22-5969516.html
[14] T. Luard. (2005, November 16). China's spies come out from the cold (International Version ed.). Available: http://news.bbc.co.uk/2/hi/asia-pacific/4704691.stm
[15] D. Sevestopulo. (2007, November 17). Chinese military hacked into Pentagon. Available: http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html?nclick_check=1
[16] B. Drogin, "Russians seem to be hacking into Pentagon: Sensitive information taken--but nothing top secret," in SFGate.com, ed. San Francisco, CA, 1999.
[17] D. Corn. (1996) Pentagon trolls the net. The Nation.
[18] C. S. Gray, "Irregular warfare: One nature, many characters," Strategic Studies Quarterly, pp. 35-57, 2007.
[19] E. Dion, "The e-Forces!: The evolution of battle-groupings in the face of 21st century challenges," Canadian Army Journal, p. 3, October 29-30 2004.
[20] A. J. Elbirt, "Information warfare: Are you at risk," IEEE Technology and Society Magazine, pp. 13-19, 2003.
[21] T. Franz, M. Durkin, P. Williams, R. Baines, and R. Mills, "Defining information operations forces," Air & Space Power Journal, pp. 1-11, 2007.
[22] J. L. Groh, "Network-centric warfare: Leveraging the power of information," in U.S. Army War College Guide to National Security Issues. Third Edition. vol. 1, ed Carlisle, PA: Army War College: Strategic Studies Institute, 2008, pp. 323-338.
[23] G. J. Rattray, Stategic warfare in cyberspace. Cambridge, Massachusetts: MIT Press, 2001.
[24] R. R. Leonhard, "A culture of velocity," in Digital war: A view from the front lines, R. L. Bateman, Ed., ed Novato, CA: Presidio Press, 1999, pp. 131-152.
[25] R. C. Molander, A. S. Riddile, and P. A. Wilson, "Strategic information warfare: A new face of war," Parameters, vol. 1996, pp. 81-92, 1996.
[26] R. F. Erbacher, "Extending command and control infrastructures to cyber warfare assets," in Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 2005.
[27] S. Paradis, A. Benaskeur, M. Oxenham, and P. Cutler, "Threat evaluation and weapons allocation in network-centric warfare," in 7th International Conference on Information Fusion (FUSION), 2005, pp. 1078-1085.
[28] M. Adkins, J. Kruse, and R. Younger, "Ubiquitous computing: Omnipresent technology in support of network centric warfare," in 35th Hawaii International Conference of Systems Sciences, Hawaii, 2002, p. 9.
[29] K. J. Cogan, "A view of command, control, communications, and computer architectures at the dawn of network centric warfare," Issue Paper Center for Strategic Leadership, vol. 2-07, 2007.
[30] R. R. Leonhard, The principles of war for the information age. New York: Presidio Press, 1998.
[31] T. J. Czerwinski, "Command and control at the crossroads," Parameters, vol. 1996, pp. 121-132, 1996.
[32] D. L. Kewley and J. Lowry, "Observations on the effects of defense in depth on adversary behavior in cyber warfare," in Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 2001.
[33] A. Fuxman, P. Giorgini, M. Kolp, and J. Mylopoulos, "Information systems as social structures," in The International Conference on Formal Ontology in Information Systems, Ogunquit, Maine, USA, 2001, pp. 3-9.
[34] B. Reed, "A social network approach to understanding an insurgency," Parameters, vol. 2007, pp. 19-30, 2007.
[35] N. Schachtman. (2007, October 1). How technology almost lost the war: In Iraq the critical networks are social - not electronic. Available: http://www.wired.com/politics/security/magazine/15-12/ff_futurewar
[36] D. B. Hollis, "Title," unpublished|.
[37] M. Herman, "Modeling the revolution in military affairs," Joint Forces Quarterly, vol. Autumn/Winter, pp. 85-90, 1998-99.
[38] B. Hicks, "Transforming avionics architecture to support network centric warfare," in The 23rd Digital Avionics Systems Conference, 2004.
[39] W. J. Bayles, "The ethics of computer network attack," Parameters, vol. 2001, pp. 44-58, 2001.
[40] J. Lasker. (2005, October 1). U.S. military's elite hacker crew. Available: http://www.wired.com/politics/security/news/2005/04/67223
[41] R. Bunker, "Generations, waves, epochs: Modes of warfare and the RPMA," Airpower Journal, pp. 1-10, 1996.

[42] T. X. Hammes, “Fourth generation warfare evolves, fifth emerges,” Military Review, vol. May-June, pp. 14-23, 2007.
[43] T. X. Hammes, The sling and the stone: On war in the 21st century. St. Paul, MN: Zenith Press, 2004.
[44] D. Kilcullen, The accidental guerrilla: Fighting small wars in the midst of big ones. Oxford: Oxford University Press, 2009.
[45] R. J. Harknet, “Information warfare and deterrence,” Parameters, vol. 1996, pp. 93-107, 1996.
[46] G. Giacomello, “Bangs for the buck: A cost benefit analysis of cyberterrorism,” Studies in conflict & terrorism, vol. 27, pp. 387-408, 2004.
[47] S. Gordon, “Cyberterrorism?,” ed. Cupertino, CA: Symantec Corporation, 2003, p. 15.
[48] L. Armistead, Information operations: Warfare and the hard reality of soft power. Washington, DC: Brassey’s, Inc., 2004.
[49] E. V. Leighninger, “Is software warfare d'unthinkableĒ? or is there a rational basis for its adoption?: A proposal for ethical reflection and action,” ACM SIGSAC Review, vol. 9, p. 28, 1991.
[50] J. Mulvenon, “Toward a cyberconflict studies research agenda,” IEEE Security and Privacy, pp. 52-55, 2005.