REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 06-11-2007	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE
Cyberspace Coercion in Phase 0/1: How to Deter Armed Conflict

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lt Col Russell F. Mathers

Paper Advisor (if Any): CAPT Stephanie Helm

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
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 is a war fighting domain and can be used by joint force commanders (JFC) in Phase 0 (Shape) and Phase 1 (Deter) of their operation to prevent escalation to armed conflict. This paper outlines Byman and Waxman's four coercion mechanisms of power base erosion, civil unrest, decapitation and denial and uses them and Boyd's OODA Loop as a framework to examine how a JFC can use cyberspace capabilities to prevent the use of armed force. The paper also evaluates how Russia and China have used cyberspace operations to coerce their adversaries and place themselves in a position of strength to deter their future adversaries in cyberspace. The paper closes with recommendations to develop joint doctrine for the cyberspace domain, options to move China from a position of coercive strength and the need for the interagency to provide for unity of effort in cyberspace.

15. SUBJECT TERMS
Cyberspace, Coercion, Deterrence, Phase 0/I

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

NAVAL WAR COLLEGE
Newport, R.I.

CYBERSPACE COERCION IN PHASE 0/I: HOW TO DETER ARMED CONFLICT

by

Russell F. Mathers

Lieutenant Colonel, United States Air Force

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: ____________________

6 November 2007

Abstract

Cyberspace is a war fighting domain and can be used by joint force commanders (JFC) in Phase 0 (Shape) and Phase 1 (Deter) of their operation to prevent escalation to armed conflict. This paper outlines Byman and Waxman's four coercion mechanisms of power base erosion, civil unrest, decapitation and denial and uses them and Boyd's OODA Loop as a framework to examine how a JFC can use cyberspace capabilities to prevent the use of armed force. The paper also evaluates how Russia and China have used cyberspace operations to coerce their adversaries and place themselves in a position of strength to deter their future adversaries in cyberspace. The paper closes with recommendations to develop joint doctrine for the cyberspace domain, options to move China from a position of coercive strength and the need for the interagency to provide for unity of effort in cyberspace.

Table of Contents

INTRODUCTION

The purpose of this paper is to explore how a joint force commander (JFC) can direct operations in the cyberspace domain to delay or prevent a conflict from escalating to the use of armed force. The JFC does not have complete control of this decision; the enemy also has a vote. But by understanding an adversary's values, how he thinks and some basic coercion theory, a JFC can structure the enemy's decision and have a strong influence on whether a conflict escalates to the use of armed force. The United States and coalition partner nations benefit from keeping conflict below the threshold of armed conflict, saving countless lives and the expenditure of valuable resources.

This paper will define cyberspace and the operational phases in joint doctrine. It will quickly introduce coercion theory and the Observe, Orient, Decide, Act (OODA) Loop, and then explore how the OODA Loop operates in the cyberspace domain. It will analyze how the JFC can use coercion theory and the OODA Loop model within cyberspace to delay or prevent the enemy's use of armed force. It will examine how Russia and China have coerced in the cyberspace domain and have shaped the international environment to enable their future coercive operations. The paper will close with some challenges to using cyberspace coercion in Phases 0 and I and make recommendations for future improvement.

CYBERSPACE BACKGROUND

Cyberspace has been identified as a war fighting domain. The National Military Strategy for Cyberspace Operations defines cyberspace as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated infrastructures."[1] The definition expands the scope of the cyberspace domain beyond what initially comes to mind, computer networks. The domain includes all electronics such as cellular phones, text messaging devices, radios, video games, electronic warfare, directed energy, and the associated data and information being stored or moved by such devices.

Military forces have used the cyberspace domain throughout history, as early as the U.S. Army executing command and control in the American West with Morse code. And our adversaries have been conducting counter-cyber operations just as long, beginning when the Native Americans cut military telegraph wires. Today's use of the domain is more advanced and evolving faster, and today's military services and combatant commanders must learn how to fight in this domain.

OPERATIONAL PHASES

Joint Doctrine defines joint operations and campaigns as six phases. They are *Shape, Deter, Seize the Initiative, Dominate, Stabilize,* and *Enable Civilian Authority* (reference Figure 1). By breaking an operation into smaller phases, the JFC and his staff can more easily think through the operation or campaign and synchronize the time, space and purpose of each phase. Individual phases also assist the JFC to draft his commander's intent and assign his subordinate components supporting tasks.   The six phases are linked and characterized by their individual focus and weight of effort. The Phases 0 (Shape) and I (Deter) are day-to-day operations addressed in the combatant commander's Theater Security Cooperation Plan, whereas Phases 2 through 6 are addressed in Joint Strategic Capability Plan-directed operational plans.[2]

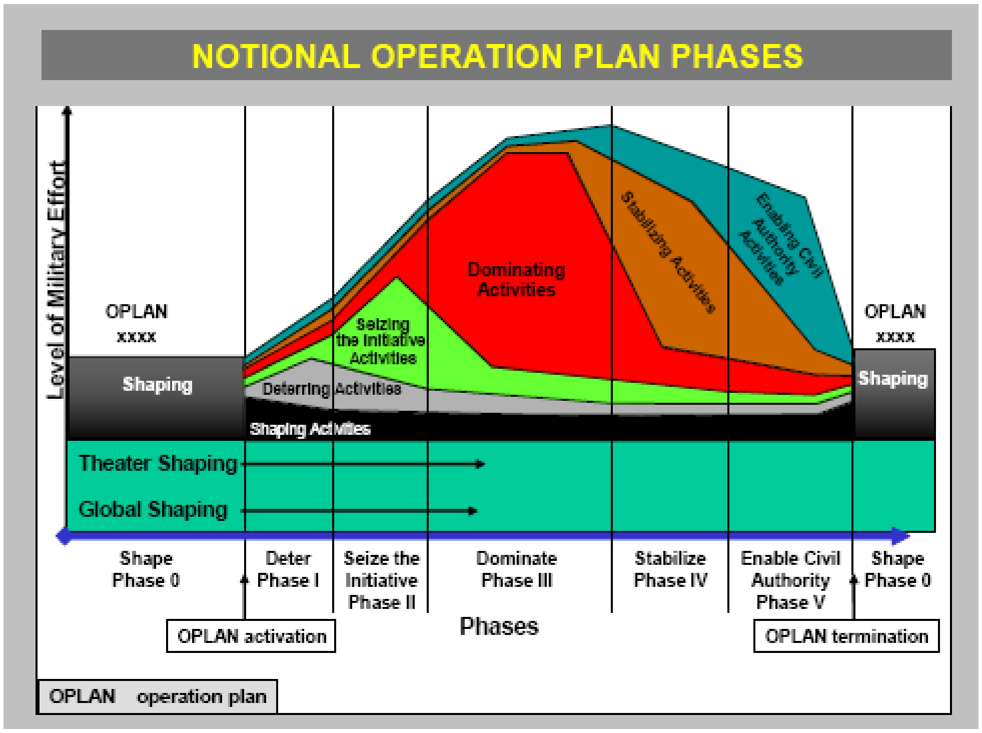


Figure 1: Notional Operation Plan Phases. (Chairman, U.S. Joint Chiefs of Staff, Joint Operations Planning, Joint Publication (JP) 5-0 (Washington, DC: CJCS, 26 December 2006): IV-35.

The JFC's goal in Phase 0 (Shape) is to shape the environment and dissuade potential adversaries, ideally preventing conflict. He also strives to assure and solidify relationships with allies and friends, stabilizing the combatant commander's area of responsibility.[3]

In Phase I (Deter) the JFC's goal is to deter undesirable adversary actions. It differs from the Shape phase because the actions are chosen to deter a specific developing conflict by demonstrating the nation's capabilities and resolve. These actions also prepare the joint force should the operation move into Phase II or beyond.[4]

COERCION THEORY

To effectively shape and deter, the commander and his staff must understand coercion theory. Byman and Waxman discuss coercion with five mechanisms, four of which are applicable in Phase 0/I. These mechanisms are the desired effect of the coercive operations, which should apply pressure to one of the adversary's pressure points. The four applicable mechanisms are *power base erosion, civil unrest*, *decapitation* and *denial*. The fifth, *brute force,* is more suited to Phases II and III.[5]

Power base erosion consists of degrading the relationship with an adversarial leader's core supporters. This was the mechanism used by NATO forces in Serbia to convince President Slobodan Milosevic to accept the Rambouillet peace accords rather than continue his undesired action of a long and brutal ethnic cleansing campaign. NATO military forces targeted the factories and properties of Milosevic's powerful supporters to foster discontent and erode the dictator's power base.[6]

The second mechanism a coercer could exercise is to create *civil unrest* in his opponent's country. The desired objective of this mechanism is to induce dissatisfaction within the population. The Chechen rebels successfully used this mechanism between 1994 and 1996 to allow a de facto secession from Russia. In June 1995 the Chechens attacked the Russian city of Budennovsk, took over 1,000 hostages in a hospital and killed over 100 people. These attacks increased dissatisfaction in Russia; the population felt the war was not worth controlling the country of Chechnya.[7]

If leaders are not accessible by civil unrest, as can be the case in an authoritarian regime, they may be susceptible to the third mechanism, *decapitation*. Decapitation can bring about the desired behavior by assassinating the leader and causing a regime change. Even the threat of a leader's survival or well-being can bring about the desired behavior. This was the case in 1991 during Operation DESERT STORM. Secretary of State James Baker warned Iraqi Foreign Minister Tariq Aziz if anyone ordered the use of weapons of mass destruction each individual would be held responsible and punished appropriately.

Saddam Hussein had large stockpiles of chemical and biological weapons and had used these weapons against the Iranians. But Hussein did not use weapons of mass destruction during Operation DESERT STORM, likely because of the direct threat of punishment to himself.[8]

The final mechanism, *denial*, consists of convincing an adversary his desired future benefits are unattainable and he will not succeed on the battlefield. The key in denial is not to defeat an enemy's forces, but to defeat his strategy. Iran demonstrated this mechanism in their 1974 border dispute with Iraq. Iraq had been battling insurgent Kurdish rebels in northern Iraq. Iran began supplying the Kurdish forces with funding and weapons. Iraq battled the rebels for over a year until they realized they could not defeat the guerrilla fighters as long as they were supported by Iran. In 1975 Iraq realized they could not defeat the Iranian-backed rebels and they conceded the contested border regions to Iran, which subsequently ceased their support to the rebels and allowed Iraq to suppress the insurgency.[9]

Equipped with the awareness of the four applicable coercive mechanisms, the JFC must determine how to best achieve them. In order to do so we will examine the OODA Loop, how it applies to the adversary's command and control processes and how it functions in cyberspace.

DECISION MAKING

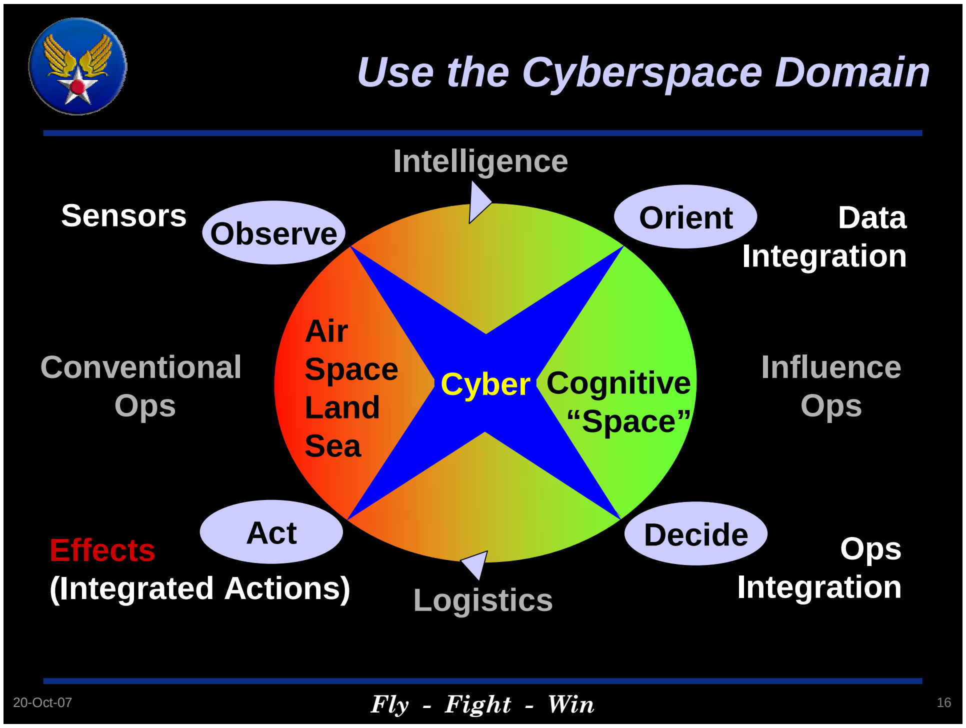
In order to properly apply mechanisms against pressure points, the JFC must know his enemy. Captain Liddell Hart articulated this when he said "The real target in the war is the mind of the enemy commander, not the bodies of his troops."[10] To attack the commander's mind, the JFC must understand how his adversary makes decisions. Once the JFC understands the enemy's decision-making process he can influence the cycle and structure decisions for his adversary and convince him to not choose armed force or delay his decision to do so.

The decision-making process was best illustrated by Colonel John Boyd, USAF, retired, in his OODA Loop model.[11] The continuous, closed loop operates in the following manner. A military commander will *observe* the operational environment and then *orient* both his and the enemy forces with the operational factors present in the operation. The orientation will structure his decision, and he will *decide* which course of action he would like his forces to execute. He will transmit this order to his forces, and they will *act* on his command. The commander will then repeat the closed loop process by *observing* the effect of his force's action, and repeat this process.

The speed at which the two opposing forces execute their independent OODA Loops is critical. Accuracy is required, but even a sub-optimum solution executed quickly before the enemy can react is preferable to an optimal solution executed too late. The force with the fastest decision-making process will be able to operate proactively and cause the opponent to react. The force with the slower OODA Loop may execute only one cycle while the faster force may execute two, three or more cycles and dominate the battle space.

OODA LOOP IN CYBERSPACE

Operations in the cyberspace domain bring new light to the OODA Loop concept. Cyberspace operates at speeds up to the speed of light and allows for infinitely faster observation, orientation, decision and action. The relationship of cyberspace on the OODA Loop is depicted in Figure 2. The act and observe portions of the model are accomplished in the physical domains of air, land, sea and space. But the orient and decide portions of the cycle are accomplished in the cognitive domain of the decision-makers brain. The



Use the Cyberspace Domain

Intelligence

Sensors

Observe

Orient

Data Integration

Conventional Ops

Air
Space
Land
Sea

Cyber

Cognitive "Space"

Influence Ops

Effects
(Integrated Actions)

Act

Logistics

Decide

Ops Integration

20-Oct-07

Fly - Fight - Win

16

Figure 2: Cyberspace and the OODA Loop (Robert J. Elder, "The Fifth Domain: Cyberspace," Powerpoint, 25 September 2007, Washington, DC: Presentation for Air Force Association, Air and Space Conference.)

cyberspace domain is the man-made domain of electronics and the electromagnetic spectrum which can connect the physical, worldly function and cognitive functions inside the human brain. It is depicted by the four-pointed star inside the OODA Loop, connecting the observe and act functions accomplished in the physical domains with the orient and decide functions done in the cognitive domain.[12]

Command and control OODA Loops utilize networked processes in the electromagnetic spectrum, providing access to the enemy's decision-making process. Sensors (satellites, signal intercepts, SONAR) are used to *observe* the battle space and intelligence organizations process this information and integrate the data (enemy force readiness, order of battle databases, intelligence estimates) into command and control systems to *orient* the commander. Both the sensors and the data integration within command

and control systems are susceptible to manipulation in the cyberspace domain.   As the commander takes in the data and contemplates his decision, he is susceptible to coercion. The commander chooses his course of action and transmits orders to his operational forces (via radio transmissions, cellular phones, electronic orders) which are susceptible to manipulation by the opposing force. His logistics corps supports the effort by deploying forces and moving supplies with electronic databases which can be modified to prevent or delay the arrival of crucial capabilities, fuel and spare parts. Finally, the fielded forces carry out the commander's direction and they can be attacked in the cyberspace domain (electronic attack, directed energy, decoys). The military commander's most critical process, the command and control of the military forces which protect his nation and exercise lethal power, are susceptible at every point throughout the cycle and subject to manipulation like never before.

JFC CYBERSPACE COERCION TOOLS

Today's JFCs have numerous tools they may exercise within their area of responsibility to shape the operational environment in support of their objectives and deter adversaries. The following capabilities are grouped by their most likely mechanism. Many of these platforms can operate in support of several mechanisms; for brevity only the primary mechanism will be addressed. The denial mechanism, which relies on the adversarial commander's perception of whether or not he can achieve his goals, will incorporate the OODA Loop and how the JFC can influence the adversary's decision-making process.

The *power base erosion* mechanism can be achieved with several methods. If the adversarial regime's leadership is supported by wealthy members of the populace, these supporters' bank accounts can be drained of funds and their corporations' credit ratings and stability indicators altered to bring financial ruin. The joint force can fabricate emails and text messages to create rifts among the supporters, distracting their focus and decreasing support for the adversarial leadership. Or the JFC may fabricate and broadcast very realistic video footage of the adversarial leader making inflammatory statements derogatory of his innermost followers, destroying their critical support.

The JFC likely does not wish to cause *civil unrest* during peacetime, but he may choose to use this mechanism to condition the adversarial country's population to not tolerate undesirable behavior by their nation. Traditional peacetime operations such as leaflet drops and loudspeakers are limited in range based on the platform used; cyberspace brings unlimited range, speed and flexibility to influence populations without penetrating the adversary's physical sovereign territory.

JFCs may condition the adversary's civil population via the electromagnetic spectrum with many of the nation's cyberspace capabilities. United States European Command has demonstrated the ability to communicate via the internet. They engage the Muslim communities on the worldwide web by sponsoring two websites promoting "good news" stories already printed in media. These websites promote stability and seek to counter extremist anti-coalition information posted on the web.[13] The JFC could also shape the environment with video games promoting human rights and democracy. Hezbollah demonstrated this use of media by developing a first-person shooter game titled "Special Forces" where young Hezbollah "warriors" attack Israelis and score points by becoming sacred martyrs.[14] The JFC can also employ EC-130 Commando Solo aircraft to deliver television and radio broadcasts of pro-United States messages to the opponent's population. The State Department's Voice of America broadcasts can be cut to compact discs and distributed to coffee shops in the region, or distributed via the internet as podcasts.

The *decapitation* mechanism can be used to convey threats to an adversarial leader but cannot realistically hold him at risk. Accessing closed control networks to open a dam's floodgates or withdraw the control rods from a nuclear reactor can bring very kinetic effects which could kill a leader if he were in the vicinity, but these technologies would certainly violate the "proportionality" tenets of international law and not be used by joint forces. The November 2006 radiation poisoning of former K.G.B. agent Alexander Litvinenko with the rare polonium 210 isotope is another example of an assassination utilizing the cyberspace domain, though also beyond the scope of the nation's joint forces.[15] Future directed energy weapons may provide more precision with less collateral effects. In the meantime the JFC may use emails, text messages and cellular phone calls to transmit threats similar to those laid before Hussein in order to coerce acceptable behavior.

The JFC can use the *denial* mechanism to degrade the adversary's perception of his battlefield success. Many flexible deterrent options (FDO) fall into this category, especially force deployments. If the JFC publicizes deployment of ISR platforms such as the U-2 or RC-135 platforms, the adversary will realize every movement will be seen or heard, decreasing the likelihood of his success in armed conflict.

In addition to using FDOs as a denial mechanism, the JFC can induce fog and friction to the adversary's OODA Loop, degrading his opponent's command and control operations and confuse their leadership's decision-making. This will slow the opponent's OODA Loop and allow the joint force to operate faster and more lethally than the opponent.

The *observe* function of the loop can be affected in Phase 0/I by deceiving or disrupting the enemy's sensors. According to joint doctrine, this may be accomplished by manipulating or temporarily disrupting information from space-based systems.[16] If the enemy is purchasing third party commercial imagery, the United States could attempt to interrupt the sale of the imagery to non-U.S. government parties with "shutter control."[17] The JFC could also perform the same denial or modifications to weather data, possibly delaying an enemy's combat operation by forecasting poor weather conditions.

The adversary's *orient* function is also susceptible to manipulation. The JFC could place an aircraft carrier or Aegis cruiser radar transmitter on a frigate and divert it from the actual carrier strike group, disorienting the adversary's knowledge of the location or strength of the joint force. Alternatively, the JFC could attack the adversary's data integration with computer network attack. If the JFC can manipulate the opponent's perceived order of battle of the JFC's forces, he may be intimidated by an imaginary force that is not in theater. Or if the adversary's own force readiness levels are reported below what they actually are, the adversary may be confused and delay operations until he perceives his forces stronger. Any of these techniques induce fog into the adversary's decision-making and may alter his decision to engage in armed conflict.

The adversary commander's *decide* OODA Loop function may be influenced in many ways. One simple way may be to establish a communications link (phone, email connectivity or internet chat room between staffs), similar to the red "hotline" between the United States and the U.S.S.R in the Cold War to stabilize tensions. More advanced technology was used in Bosnia to prevent armed force in a peacekeeping role. At the 1995 Dayton Peace Accords the NATO commander demonstrated three dimensional virtual mapping technologies to the presidents of Bosnia, Croatia and Serbia. The presentation simulated a helicopter flight along the 650 miles of their respective borders, with actual helicopter gun film showing border violations by all three nations' forces. The helicopter crew would train their cross hairs on the military vehicles to demonstrate NATO's precision engagement capabilities. This technology presented breathtaking intelligence and military force capabilities and served as a deterrent to cross-border operations because the leaders knew NATO's JFC was watching their forces' every movement.[18] This same technology could be used in Phase I operations to convince adversarial military commanders they cannot escape the eyes of the JFC, and thus deter the adversary's decision to initiate the use of force.

The JFC can degrade the enemy's *act* function within the loop in Phase 0/I by denying the adversary use of the U.S. GPS satellite constellation. This signal is susceptible to cyberspace alteration by uploading erroneous information to the satellite, inducing errors in position, timing and velocity.[19] By refusing the enemy precision navigation in Phase I the adversary will realize his satellite guided munitions will not be effective and his forces will be disoriented. This denial of his military capabilities may serve to convince the adversary the use of armed force is futile and deter him from initiating armed conflict.

FOREIGN STATES CYBERSPACE COERCION

Other nation states are not standing still in the cyberspace arena, at least two have been conducting operations in cyberspace to coerce their adversaries and prepare for future operations. Russia and China have demonstrated capabilities and the intent to carry out cyberspace attacks, giving them credibility should they choose to threaten similar attacks in the future.

Russia conducted a cyberspace attack on Estonia, a former Soviet Republic, for over three weeks in April and May of 2007. The conflict began after the government of Estonia moved a statue commemorating Soviet soldiers for their actions in World War II. The statue was the pride of the minority ethnic Russians in the former Baltic state. On 26 April 2007 ethnic Russians began protesting on the streets and assailants began a denial of service computer network attack against the Estonian networks. The attack was a "botnet" operation, with attackers utilizing thousands of slaved computers in fifty countries to bombard the Estonian networks, overwhelming them into submission. The attacks were conducted by both amateur bloggers and highly skilled specialists with significant resources.[20]

Estonia was aware of the threat of cyberspace attacks and was very well prepared to defend their networks. Estonia is very fluent in computer operations; the World Bank ranked them just behind the United States in internet preoccupation and well ahead of 15 older members of the Western Alliance.[21] Additionally, NATO experts assisted the new member and internet service providers from around the world assisted the country, as they would with any new computer virus or worm. Ultimately, the teams could do little but deploy firewalls to disconnect their network from the rest of the world.[22]

The results of the attack were catastrophic. Hansabank, Estonia's largest bank, lost over one million dollars in the country where 97 percent of bank transactions were conducted online. Parliament, newspapers, universities and the country as a whole were electronically isolated for three weeks. The attackers posted false messages on websites assumed to be authentic, including a fabricated letter of apology from the prime minister for moving the statue.[23]

In this case Russia failed to coerce the Estonians to move the statue, but succeeded in proving they can deliver force in the cyberspace domain. They were "shaping" with the "civil unrest" mechanism in this Phase I-like operation, darkening the citizen's doorsteps in the former “Soviet Bloc” country with their shadow. And every action has multiple audiences; this cyberspace operation, nicknamed “Web War One,” announced to the world Russia has computer network attack tools at its disposal and the wherewithal to use them.[24]

China has also conducted operations in cyberspace, positioning them to coerce future adversaries. The Chinese have developed and tested an anti-satellite weapon, demonstrating its capability by destroying one of their aging satellites. Their perceived benefit from this technology is likely to deny, or threaten to deny, their adversaries the use of platforms in low earth orbit. United States’ assets in this orbit include reconnaissance satellites, commercial satellites, space shuttle orbits and the international space station, potentially denying the JFC vital intelligence and impacting the world’s economy.[25]

The anti-satellite weapon has placed China in a position where they can use coercion in Phase I against the United States to deter us from the use of armed force. One can postulate a scenario with China contemplating action against Taiwan and destroying several satellites in Phase 1. They could blind United States Pacific Command’s (USPACOM) JFC by degrading the “observe” function in within his OODA Loop. China would be exercising the “denial” mechanism, attempting to convince the USPACOM JFC he cannot obtain his objective of preventing China from taking Taiwan and deterring the JFC from intervening with the use of armed force.

CHALLENGES IN CYBERSPACE COERCION

There are challenges to be considered when planning peacetime coercion operations in the cyberspace domain. The primary disadvantage is the highly perishable nature of computer network attack. Once an adversary’s vulnerability is revealed when it is used to access his system, he will search out the vulnerability and repair it.[26] If tensions are rapidly escalating, the JFC will hesitate to use and expose the adversary's known vulnerabilities in Phase 0/I, he will want to save it for access in Phase II (Seize the Initiative) or Phase III (Dominate) when the JFC can integrate the cyberspace capability with conventional combat forces to increase their lethality and possibly save lives.

Another challenge is international law concerning the use of cyberspace and how it relates to the laws of armed conflict. Today's laws do not address computer network attack and how networks interconnect around the world. Computer network attacks can cause physical and economic damage but there is no legal opinion on whether or not this is an "armed attack" and what actions are permissible under self-defense.[27] The JFC will rely heavily on lawyers versed in cyberspace to negotiate this virtual minefield.

A final challenge for the JFC will be to deconflict his operations in cyberspace with other military operations, actions being carried out by other United States governmental agencies, and the actions of coalition partners and allies. The battle space is worldwide and cannot be geographically portioned to different forces; there will inevitably be friendly fire incidents in the global environment at the speed of light. One commander may be attempting to shut down a server, while another commander may be collecting intelligence over the same server and its destruction will eliminate a source of critical intelligence.

RECOMMENDATIONS

Cyberspace is a rapidly evolving domain, changing as often as technologies change. Today's war fighters must be closely tied to commercial industry to know the latest tools and be able to visualize how he can war fight with them, because someone else on the other side of the planet is conceptualizing a way to use that very same new technology against the United States.

This paper highlighted many tools a JFC can use in Phase 0 and Phase I operations, but there is no overarching doctrine of how to integrate these cyberspace capabilities. The closest doctrine is the Joint Publication 3-13 series on information operations. The two areas overlap, but there are information operations conducted outside of the cyberspace domain (i.e. leaflets) and cyberspace operations which have nothing to do with information operations (i.e. directed energy attack from an airborne laser or high powered microwave). The Joint Staff must develop a joint doctrine publication on the use of cyberspace and the services must develop targeting, techniques and procedures on how to best use the domain.

The JFC cannot afford a single-point-of-failure such as he has for satellites in low Earth orbit which are threatened by Chinese anti-satellite weapons, and he cannot allow China to be in a position of strength to coerce the United States. The United States must develop alternate sources for intelligence. Possible sources are an "operationally responsive space" concept to quickly launch less capable satellites in the event of a conflict. These additional satellites would augment existing platforms and potentially replace any satellites lost to anti-satellite weapons. A second potential source is an air-breathing concept aircraft which could overfly regions of interest and defeat air defenses. A third source of intelligence would be friendly nations and corporations who also have space-based sensors.[28]

Finally, the interagency should develop a means to develop unity of effort in cyberspace. This paper mentioned the need to deconflict cyber operations in order to prevent friendly fire incidents, but the challenge goes beyond deconfliction. Ultimately the JFC should be contributing towards a unity of effort in cyberspace, coordinating with other governmental agencies, commercial industry, allies and coalition partners. This will provide for unity of effort as the nation attempts to secure the freedom to operate in cyberspace and execute all the instruments of power.

FINAL REMARKS

Cyberspace is not a new domain; it has existed since the invention of electricity. What is new is its relevance as a war fighting domain. The JFCs must begin to visualize this virtual battlefield and understand how it integrates with and flows throughout their traditional domain and of land, sea, air or space.

The cyberspace domain can be used in Phase 0 and Phase I operations to prevent or delay conflict escalation to the use of armed force. The JFC must incorporate a strong knowledge of his adversary to determine which mechanisms to apply. The JFC must also determine how his adversary makes decisions so he can best manipulate or degrade his opponent's OODA Loop. If properly coerced, the opponent may choose not to engage in armed conflict or delay escalating to conflict. This likely will not solve the conflict and create peace, but maintain a stable, predictable stalemate. In many cases deterrence does not provide a victory, it just works.[29]

NOTES

[1] Chairman, U.S. Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (U), (Washington, DC: CJCS, September 2006), p ix. (Secret) Information extracted is unclassified.

[2] Chairman, U.S. Joint Chiefs of Staff, *Joint Operations Planning*, Joint Publication (JP) 5-0 (Washington, DC: CJCS, 26 December 2006), IV-35.

[3] Ibid., IV-35.

[4] Ibid., IV-36.

[5] Daniel Byman and Matthew Waxman, *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might* (Cambridge: Cambridge University Press, 2002), 51-86.

[6] Ibid., 54, 63.

[7] Ibid., 68.

[8] Ibid., 73.

[9] Ibid., 79.

[10] Liddell Hart, *Thoughts on War* (Longon: Faber and Faber LTD, 1944,) 48.

[11] Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War*, (New York, Back Bay Books, 2002), 334-335.

[12] Robert J. Elder, compilation of discussions and meetings during author's assignment at Eighth Air Force Headquarters, November 2006 to July 2007.

[13] United States European Command, "The News and Views of the Maghreb," www.magharebia.com/cocoon/awi/xhtmll/en_GB/homepage/ and "Southeast European Times," www.setimes.com/ (accessed 22 Oct 07).

[14] Daniel J. Wakin, "Video Game Created by Militant Group Mounts Simulated Attacks Against Israeli Targets," *New York Times*, 18 May 2003, http://www.lexis-nexis.com/ (accessed 2 November 2007).

[15] Alan Cowell and Steven Lee Meyers, "Britain Charges Russian in Poisoning Case," *New York Times Europe*, 22 May 07, http://www.nytimes.com/2007/05/22/world/europe/22cnd-Litvin.html?_r=1&oref=slogin (accessed 22 Oct 07).

[16] Chairman, U.S. Joint Chiefs of Staff, *Joint Doctrine for Space Operations*, Joint Publication (JP) 3-14 (Washington, DC: CJCS, 9 August 2002), IV-7, IV-8.

[17] Ibid., A-3.

[18] Timothy L. Thomas, *Cyber Silhouettes,* (Fort Leavenworth, KS: Foreign Military Studies Office, 2005), 109-111.

[19] Chairman, U.S. Joint Chiefs of Staff, *Joint Doctrine for Space Operations*, Joint Publication (JP) 3-14 (Washington, DC: CJCS, 9 August 2002), IV-9.

[20] Rebecca Grant, *Victory in Cyberspace*, special report (Arlington, VA: Air Force Association, October 2007), 4-6.

[21] Ibid., 5.

[22] Ibid., 5.

[23] Ibid., 5-6.

[24] Ibid., 4.

[25] Amy Butler, “Secret Steps,” *Aviation Week and Space Technology* 167, no. 15 (15 October 2007): 40.

[26] Sebastian M. Convertino, Lou Anne DeMattei, and Tammy M. Knierman, *Fly and Fight in Cyberspace* (Maxwell AFB, AL: Air University Press, 2007), 55.

[27] Christopher Joyner and Catherine Lotrionte, “Information Warfare as International Coercion: Elements of a Legal Framework,” *European Journal of international Law* 12 (1 December 2001), 864, http://proquest.com/ (accessed 20 October 2007).

[28] Ibid., 40.

[29] Grant T. Hammond, “Deterrence for the 21st Century,” Powerpoint, 15 December 2006, Barksdale AFB, LA: Air University, Director, Center of Strategy and Technology.

BIBLIOGRAPHY

Butler, Amy. “Secret Steps.” *Aviation Week and Space Technology* 167, no. 15 (15 October 2007): 39-40.

Byman, Daniel, and Matthew Waxman. *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might.* Cambridge: Cambridge University Press, 2002.

Convertino, Sebastian M., Lou Anne DeMattei, and Tammy M. Knierim. *Flying and Fighting in Cyberspace.* Maxwell Paper No. 40. Maxwell AFB, AL: Air University Press, July 2007. 76 p.

Coram, Robert. *Boyd: The Fighter Pilot Who Changed the Art of War.* New York, NY: Back Bay Books, 2002.

Cowell, Alan, and Steven Lee Meyers. “Britain Charges Russian in Poisoning Case.” *New York Time Europe*, 22 May 07. http://www.nytimes.com/2007/05/22/ world/europe/ 22cnd-Litvin.html?_r=1&oref=slogin (accessed 22 Oct 07).

Eighth Air Force Headquarters. “Concept of Cyber Warfare.” Concept of Operations Paper, Barksdale AFB, LA: Eighth Air Force, 1 June 2007.

Elder, Robert J. "The Fifth Domain: Cyberspace." Powerpoint. September 25, 2007.

Fulghum, David A. “Massed Airborne Forces Aimed at Heart of Haiti.” *Aviation Week and Space Technology,* 141, no. 15 (10 October 1994): 71-72.

Grant, Rebecca. *Victory in Cyberspace.* Special Report. Arlington, VA: Air Force Association, October 2007.

Hammond, Grant T. "Deterrence for the 21st Century." 8th Air Force Deterrence Seminar. Barksdale AFB, LA. Powerpoint. December 15, 2006.

Hart, Liddell. *Thoughts on War*. London: Faber and Faber LTD, 1944.

Joyner, Christopher, and Catherine Lotrionte, “Information Warfare as International Coercion: Elements of a Legal Framework,” *European Journal of International Law* 12 (1 December 2001): 864-865. http://www.proquest.com/ (accessed 20 October 2007).

Jannarone, Greg. "Behavioral Influences Analysis." 8th Air Force Deterrence Seminar. Barksdale AFB, LA. Powerpoint. December 15, 2006.

Rattray, Gregory J. *Strategic War in Cyberspace.* Cambridge, MA: Massachusetts Institute of Technology, 2001.

Thomas, Timothy L. *Cyber Silhouettes*. Fort Leavenworth, KS: Foreign Military Studies Office, 2005.

U.S. European Command. "The News and Views of the Maghreb," www.magharebia.com/cocoon/awi/xhtmll/en_GB/homepage/ and "Southeast European Times," www.setimes.com/ (accessed 22 Oct 07).

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations.* Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Doctrine for Space Operations.* Joint Publication (JP) 3-14. Washington, DC: CJCS, 9 August 2002.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Operation Planning.* Joint Publication (JP) 5-0. Washington, DC: CJCS, 26 December 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *The National Military Strategy for Cyberspace Operations* (U). Washington, DC: CJCS, Sept 2006. (Secret) Information extracted is unclassified.

Wakin, Daniel J. "Video Game Created by Militant Group Mounts Simulated Attacks Against Israeli Targets." *New York Times,* 18 May 2003. http://www.lexis-nexis.com/ (accessed 2 November 2007).