REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 01-04-2010	**2. REPORT TYPE** Master of Military Studies Research Paper	**3. DATES COVERED** *(From - To)* September 2009 - April 2010

4. TITLE AND SUBTITLE
DEPARTMENT OF DEFENSE'S ENHANCED REQUIREMENT FOR OFFENSIVE CYBER WARFARE OPERATIONS

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Major Paul M. Mattear

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

12. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT

Thesis: The Department of Defense (DoD) needs to further develop its offensive cyber warfare capabilities at all levels. In an asymmetric environment, understanding an enemy's information capacity and disrupting his information flow is a key enabler for success on and off conventional and non-conventional battlefields. If the DoD does not prosecute offensive cyber warfare tactics then the DoD has effectively allowed a significant advantage to be given to an adversary.

Discussion: The DoD's cyber networks are under constant probing and attack from state supported and non-state supported entities. This style of warfare is only expected to expand in scope and sophistication.

Several near peer states have well developed military units in support of offensive cyber warfare operations. These states utilize their cyber warfare capabilities to support their national, operational and strategic objectives.

Conclusion: Near peer nations such as China and Russia have well developed offensive cyber warfare capabilities and doctrine within their militaries. The DoD needs to establish like units to continue its tactical, operational and strategic dominance over its adversaries.

15. SUBJECT TERMS
Cyber, Cyber War, Cyber Warfare, Cyber War-Fare, Offensive Cyber War, Offensive Cyber Warfare, Russia, China,

INSTRUCTIONS FOR COMPLETING SF 298

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 30	19a. NAME OF RESPONSIBLE PERSON Marine Corps University / Command and Staff College
a. REPORT Unclass	b. ABSTRACT Unclass	c. THIS PAGE Unclass			19b. TELEPONE NUMBER (*Include area code)* (703) 784-3330 (Admin Office)

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at lest the year and be Year 2000 compliant, e.g., 30-06-1998; xx-08-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. 1F665702D1257.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. AFOSR-82-1234.

5d. PROJECT NUMBER. Enter al project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORS AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE: DEPARTMENT OF DEFENSE'S ENHANCED REQUIREMENT FOR OFFENSIVE CYBER WARFARE OPERATIONS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIRMENTS FOR THE DEGREE OF MASTER OF MILITARY STUDIES

AUTHOR: MAJOR PAUL MATTEAR

AY 09-10

Mentor and Oral Defense Committee Member: Dr. Erickson, E.
Approved: Edward
Date: 10 April 2010

Oral Defense Committee Member: Dr. Otis, P.
Approved: Paulette Otis PhD.
Date: 10 April 2010

Executive Summary

Title: Department of Defenses enhanced requirement for offensive cyber warfare capabilities.

Author: Major Paul M. Mattear, United States Marine Corps

Thesis: The Department of Defense (DoD) needs to further develop its offensive cyber warfare capabilities at all levels. In an asymmetric environment, understanding an enemy's information capacity and disrupting his information flow is a key enabler for success on and off conventional and non-conventional battlefields. If the DoD does not prosecute offensive cyber warfare tactics then the DoD has effectively allowed a significant advantage to be given to an adversary.

Discussion: The DoD's cyber networks are under constant probing and attack from state supported and non-state supported entities. This style of warfare is only expected to expand in scope and sophistication.

Several near peer states have well developed military units in support of offensive cyber warfare operations. These states utilize their cyber warfare capabilities to support their national operational and strategic objectives.

Conclusion: Near pear nations such as China and Russia have well developed offensive cyber warfare capabilities and doctrine within their militaries. The DoD needs to establish like units to continue its tactical, operational and strategic dominance over its adversaries.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPREESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINES CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED THE PROPER ACKNOWLEDGEMENT IS MADE

Table of Contents

Contents

Introduction

In the early 1990's the Department of Defense (DoD) created the Nonsecure Internet Protocol Router Network (NIPRNet) to exchange sensitive but unclassified electronic information between internal users but still allow those internal users access to the external internet or world wide web. Since then the DoD has developed and continues to develop a multitude of networks with varying security classifications such as the Secure Internet Protocol Router Network (SIPRNet) and the Joint World Intelligence Communications System (JWICS). With the DoD's increased dependence upon the aforementioned networks for content staging, information sharing and collaboration, so too has risen the desire for state and non-state actors to gain that information. The Central Intelligence Agency (CIA) in 2000 stated that they were "detecting, with increasing frequency, the appearance of doctrine and dedicated offensive cyber warfare programs in other countries."[i] Today the DoD continues to be inundated by offensive cyber attacks purportedly from state supported, non-state supported antagonists and hacktivists. The DoD needs to further develop its offensive cyber warfare capabilities at all levels to match near state competitors or risk providing those competitors a lucid advantage in offensive cyber warfare.

Key attacks have been noted across United States key civilian and government non-secure and secure networks. In April 2009 Air Force Gen. Kevin P. Chilton stated in the *Information Management Journal* that the DoD had spent more than $100 million in the last six months fighting off daily cyber attacks against DoD computer systems.[ii] The amount of money and effort spent on defense coincides with the current administrations stance on how to combat offensive cyber attacks. In a New York Times article titled *U.S and Russia Differ on Treaty for Cyberspace* published on 28 June, 2009, an unnamed State Department Official was quoted as saying "We really believe it's defense, defense, defense," when talking about the best way to counter the continuing and evolving threat of cyber attacks.[iii] This line of thinking and approach to cyber warfare shows an almost monolithic government stance that does not take into account the clear benefits of offensive cyber operations.

As the United States faces more and more combatants on an asymmetric warfare plane, defense alone will not be enough to combat the threats of cyber warfare. Across the information and technology (IT) field, government and non-government technical experts agree that the DoD's offensive capabilities are lack luster. MajGen William Lord (provisional commander of Air Force Cyber Command) similarly expressed this belief in a *Defense Technology International* article; his concerns are that current policies and laws may negate the ability of experts to launch cyber attacks.[iv] In order to better understand an antagonist, an offensive posture must be adopted that allows for cataloging of network weaknesses/gaps and intelligence gathering. This style of information gathering is no different than a CIA officer working an asset for information. An offensive cyber action would be utilized to determine what an antagonist knows and what they are doing with that information and with whom they are sharing the information.

In a May 2009 speech from President Obama, he highlighted the extreme importance of cyber security stating that cyber security is one of Americas "most serious economic and national security challenges."[v] In direct response to the President's concerns, on June 23, 2009, the Secretary of Defense ordered the DoD to establish a unified command, United States Cyber Command (USCYBERCOM), to centralize cyber capabilities and operations. USCYBERCOM, located at Fort Meade, Maryland, is expected to be fully operational capable by October 2010. Although this is a tremendous step forward in integrating cyber operations for the DoD at a

Combatant Commander/Strategic level (under United States Strategic Command), this organization has been created several years after Russia, China and several other near peer nations created similar agencies. Because of this time lapse, the DoD has significant shortcomings in service and joint doctrine as it pertains to offensive cyber attack/cyber warfare and how to prosecute offensive cyber actions.

Cyber Warfare

Cyber Warfare has existed in its current form for approximately the last 15 years. One of the reasons an exact date cannot be placed on when the first cyber warfare occurred is the lack of clarity in a globally excepted definition of what is and what constitutes cyber warfare and what constitutes a cyber attack. There is no ubiquitously accepted definition within the DoD for cyber warfare nor is it defined in the *Department of Defense Directory of Military and Associated Terms (JP 1-02)*. This lack of definition has significantly added to the overall confusion within DoD and the civilian sectors. In Joint Publication 1-02 the DoD defines Cyber Operations (CO) as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[vi] The DoD further defines in Joint Publication 1-02 a Computer Network Attack (CNA) as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[vii]

Complicating the matter are the other directives commonly referred to when discussing cyberspace such as Air Force Policy Directive 10-7 (updated 18 December 2009). In this directive the term network warfare operations (NWO's) is defined as "the integrated planning and employment of military capabilities to achieve desired effects across the interconnected analog and digital portion of the battlespace."[viii] This same policy further defines a network attack (NA) as "The employment of network-based capabilities to destroy, corrupt, or usurp information resident in or transitioning through networks."[ix] The previously written definitions are all part of what could constitute portions of cyber warfare but are clearly not the definition of cyber warfare itself.

Across the DoD the various terms being utilized to describe what when put together as a whole is cyber warfare (CO, CAN, NWO's, NA) has and will continue to complicate the matter of understanding cyber warfare. Until DoD publishes a definition it will be increasingly difficult to develop operational and strategic level doctrine and equally important how to work offensive cyber operations within the permissible parameters of military, legal and political systems/law/regulations. Since the DoD does not have a standing definition, for the purpose of this paper the definition that will be utilized will come from *Cyber Warfare Operations: Development and Use Under International Law* "the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves of another state."[x] A concise definition for cyber warfare creates the foundation for an understanding and will promote clarity throughout the rest of this paper.

Why Utilize Cyber Warfare

Although cyber warfare requires utilizing some differing principles than that commonly associated with a kinetic war there are commonalities. In Sun Tzu's *The Art of War* he proposes that you must attempt to manipulate the decision making process or processes of your adversary.[xi] Likewise Clausewitz arguments about inducing the "fog of war" and the "friction of war" coincide with the intentions of utilizing cyber warfare.[xii] Both Tzu and Clausewitz operated in a relatively conventional time period, but their ideas of warfare can be translated and have relevance in the asymmetric world of cyber warfare. This ubiquitous use of terminology lends further credence to the continuance of the battlefield into the cyber domain and information operations.

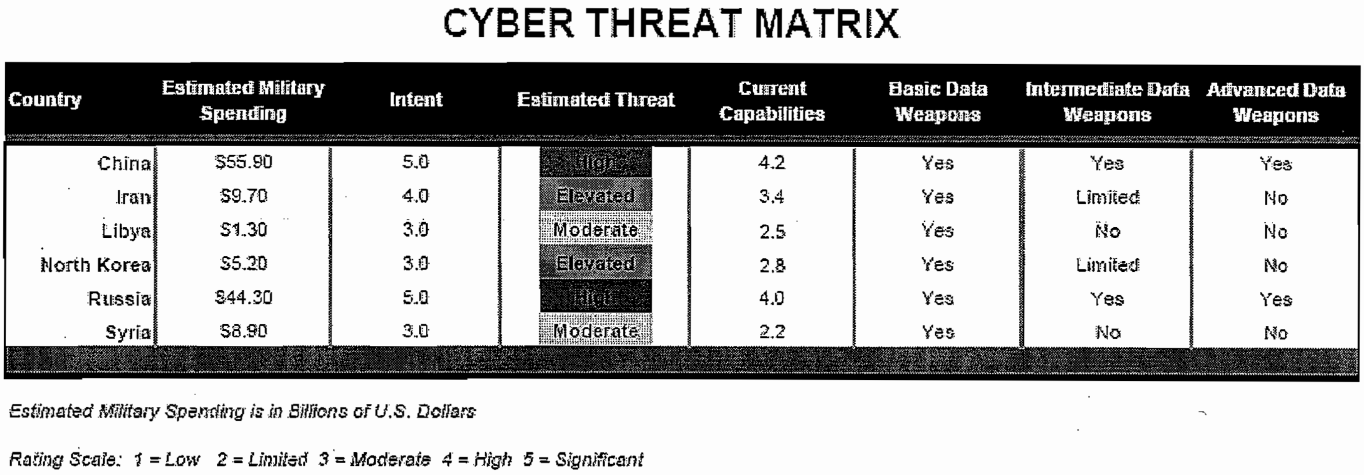
Setting aside the historical relevance of taking advantage of an enemies weaknesses or inducing doubt within the enemy's command and control structure, there are several other reasons why an entity (government and/or non-government sponsored group) would utilize cyber warfare. The primary reason revolves around the most elemental of arguments when discussing war: cost. "Cyber warfare is an inexpensive, highly-effective means for a nation to achieve its political, economic or strategic objectives while maintaining plausible deniability for its actions."[xiii] Cyber warfare is inexpensive because of the tools that are utilized to propagate a cyber attack. The major tools that are utilized for a cyber attack include but are not limited to the below main categories, under these categories can be hundreds of sub-categories and even diffusion between categories:

Tool	Out Come
Insider Attacks	Attack system from inside bypassing layered security. Cloaking/Sniffing/Log manipulation.
Denial of Service (DOS)	Make services unavailable by using up host memory.
Malicious Programs/Software	Disrupt normal functions (virus, Worm, Trojan Horse, etc). Executes malicious code at a predetermined time or after an event. This would include Botnets.
Spoofing	An attempt to gain information by impersonation
IP Packet Manipulation	Gain access to systems by manipulation of source or destination IP, redirect connections, bypass firewall, bypass password access.
Digital Manipulation	Alters an image to reflect new meaning

The monetary cost of each of the tools is relatively minuscule in comparison to the cost of a major end item such as Joint Strike Fighter which now exceeds over $137 million according to a recent article in the *Washington Post.*[xiv] The total purchase for the DoD is 2,458 Joint Strike Fighters at $337 Billion.[xv] The preponderance of cyber warfare tools to a certain level of expertise can be downloaded for free on the internet simply by going to a search engine and searching for a topic relevant to the tool you wish to utilize. This is not to say that all cyber attacks can be simply downloaded and implemented on any network. The complexity of the networks' security parameters will of course influence the complexity of the cyber attack needed to gain the desired effect. Later on in this paper, specific case studies on China and Russia (Estonia and Georgia) will expound upon the complexity of attacking large scale, layered, defense networks.

Another reason to utilize cyber warfare is the anonymity it provides the attacker. Cyber warfare is different from conventional warfare in that it completely relies upon surprise. By virtue of the way the attacks are launched anonymity is significantly easier to maintain. An attacker has a plethora of tools that can assist in keeping his anonymity, from anonymous servers and Internet Protocol (IP) spoofing to hijacking other terminals (botnets). All of that plus many more tools assist in covering the actual attacker from being discovered. The shorter the length of the attack the more difficult it becomes to track the adversary conducting the attack, especially if the attacker is another government or a state sponsored entity.

The DoD received in 56,640 cyber attacks in 2008, that number has rose significantly in the first half of 2009 jumping to 43,785.[xvi] These numbers show an approximate 60% increase in the amount of attacks during the same period of the year prior. Although the origin of most of the attacks cannot be precisely located, the belief by the preponderance of IT security professionals is that the attacks are state sponsored originating from China and Russia. The below matrix was taken from a report sponsored by *The Technolytics Institute,* which highlights both China and Russia as being the greatest threat to the safety and security of American networks.



CYBER THREAT MATRIX

Country	Estimated Military Spending	Intent	Estimated Threat	Current Capabilities	Basic Data Weapons	Intermediate Data Weapons	Advanced Data Weapons
China	$55.90	5.0	High	4.2	Yes	Yes	Yes
Iran	$9.70	4.0	Elevated	3.4	Yes	Limited	No
Libya	$1.30	3.0	Moderate	2.5	Yes	No	No
North Korea	$5.20	3.0	Elevated	2.8	Yes	Limited	No
Russia	$44.30	5.0	High	4.0	Yes	Yes	Yes
Syria	$8.90	3.0	Moderate	2.2	Yes	No	No

Estimated Military Spending is in Billions of U.S. Dollars

Rating Scale: 1 = Low 2 = Limited 3 = Moderate 4 = High 5 = Significant

Case Studies (US/China)

In a report prepared for The U.S China Economic and Security Review Commission titled *Capability of the Peoples Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, the authors note with extreme detail the Chinese desire to expand upon their cyber warfare capabilities. The Chinese have been and will continue to focus its cyber capabilities "on achieving military effects capable of causing economic harm, damaging critical infrastructure, and influencing the outcome of conventional armed conflicts."[xvii]

The author of *Dragon Bytes: Chinese Information-War Theory and Practice,* Timothy Thomas states that "The Chinese have been restructuring their military for over a decade to transform their mechanized People's Liberation Army (PLA) into an "informationalized" force capable of capitalizing on the asymmetric effect of cyberspace."[xviii] Others within the IT field believe the transformation started even prior to the time frame given by Timothy Thomas. In the late 1980's and early 1990's, China began focusing on information warfare as a means to achieve political and economic strategy.[xix] Over the past 20 years China has formulated in-depth cyber strategies and doctrine through simulations, exercises and real world conflicts/actions.

In 2003, an information paper written for the US-China Economic and Security Review Commission stated that "an account of a probable proof of concept initiative in the Guangzhou Military Region to establish IW militia units using local telecommunications companies as a base from which to draw personnel, financial support, and infrastructure access, suggesting that the PLA was tapping its growing pool of civilian commercial IT expertise to aid military information warfare requirements."[xx] It further stated that to support these initiatives four battalions of what had been created within the PLA. Within the U.S. DoD there are no such comparable battalions. China will continue to expand its cyber army as a means of defense and offense as evident by the continual increases in military budgeting "increasing: over 14.7% in 2006."[xxi] They will also continue to focus their cyber research. "In May 2006, China approved a new research and development plan for defense sciences and technologies focusing on solutions involving information technologies."[xxii] The PLA has clearly developed cyber warfare strategic doctrine that does not just preclude itself to a primarily defensive strategy but instead incorporates all aspects of cyber warfare to include state sponsored and non-state sponsored directed offensive cyber operations.

Case Studies (China/Taiwan)

Referring back to the anonymity that a cyber attack provides there is no unclassified evidence that has been released to reflect that the PLA has conducted offensive operations against the United States government. Nor has the government of China directly stated that it has conducted offensive cyber operations against the United States. That being stated, there are numerous cases where attacks have originated from IP addresses within China. Appendix (A) from *Capability of the Peoples Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* report clearly outlines a timeline of significant cyber events aimed at a myriad entities to include France, Korea, Germany, Australia, numerous American agencies and the attacks continue to grow both numerically and in complexity. The DoD stated "that the Chinese government, in addition to employing thousands of its own hackers, manages massive teams of experts from academia and industry in "cyber militias" that act in Chinese national interests with unclear amounts of support and direction from China's People's Liberation Army (PLA)."[xxiii]

In 1999 the president of Taiwan Lee Teng-hui commented that Taiwan deserved to be treated as an equal state by the PRC; following that announcement an exorbitant amount of cyber attacks occurred against Taiwanese government websites.[xxiv] In January 2010, Operation Aurora, better known as the Google hack occurred. This attack is possibly the largest cyber attack ever committed. Initially security experts believed the attack was launched by hackers within Taiwan. However as cyber attack computer forensics professionals further examined the incidents they realized that the attacks were launched through infected servers in Taiwan (botnets). In an article published by examiner.com, it states that "Google has blamed China for the hack attack and all the experts who have studied the Aurora virus, named for a file left on an infected computer, agree that the sophistication of the operation required the resources of either a major corporation or a government.[xxv] The Taiwanese government maintains its belief that these attacks are coming from China through Taiwan, more specifically the PLA.

If Taiwanese government's assertions are correct, that means that the PLA has been conducting coordinated offensive cyber attacks at the strategic level since at least 1999. The start date of 1999 coincides with the first Chinese registered attack in May 1999 listed in (Appendix X) by the *Capability of the Peoples Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* The beginning date of operational and strategic level offensive cyber attacks significantly predates the DoD's attempts to develop offensive doctrine under USCYBERCOM. This clearly demonstrates a considerable difference in developed and mature cyber warfare doctrine by the DoD.

Case Study (Russia/Estonia)

Russia, not unlike China, has developed a significant offensive cyber strategy that aims to infiltrate, degrade and disrupt military and civilian communications capabilities. In 2000 "Vladimir Putin officially adopted the Russian Information Security Doctrine, which addresses issues relating to computer crime and network security from threats both domestic and foreign."[xxvi] This includes the disruption of critical financial markets in order to produce chaos prior to the initiation of more traditional military operations. In 2001 Major General Vladimir Belous of Russia stated:

> "it can be predicted that the battlefield of the future will begin to shift more and more into the area of intellectual effect. An aggressor country is capable of developing, and under certain conditions executing, a scenario of information war against another state in an attempt to demolish it from within. In that way it is possible to force the enemy to surrender without using traditional kinds of weapons."[xxvii]

Russia, along with academia and IT professionals, has and continues to produce a well developed cyber warfare doctrine.[xxviii]

With this well developed doctrine under the early proposed definition of cyber warfare, Russia prosecuted what could be considered the first state versus state cyber war against Estonia in April 2007. The cause of the tension between Russia and Estonia was the Estonian government's decision to move a soviet-era statue that honored Russian soldiers that fought in World War II. At 10:00 p.m. local time on April 26, 2007, the final decision to move the statue was made. At approximately the same time, a massive Denial of Service (DOS) attack was launched that targeted multiple networks to include government, financial and civilian servers. Several other events occurred almost simultaneously to suggest a coordinated effort on a large scale to disrupt, discredit or pressure the Estonian government into changing its stance on the movement of the soviet-era statue.

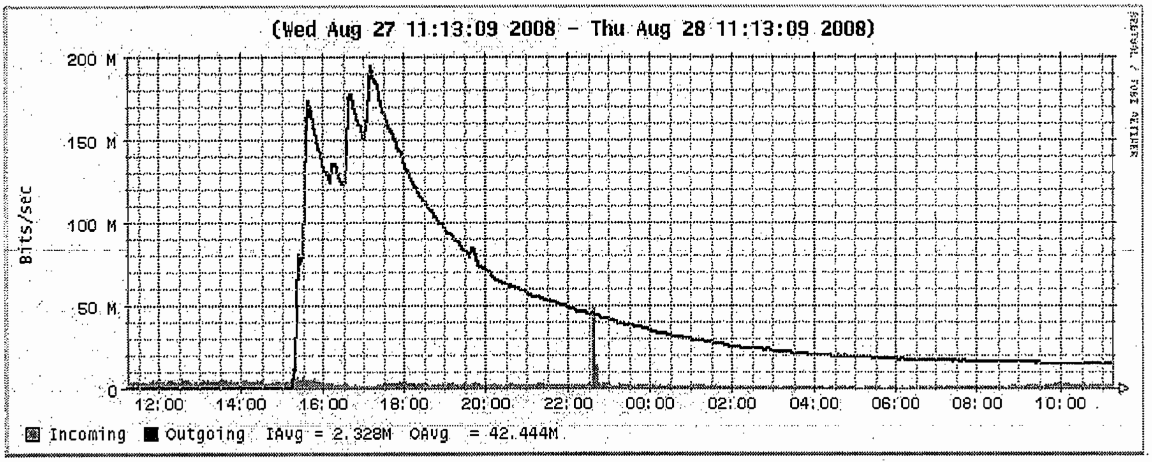
The preponderance of the initial attacks against the Estonian networks were from IP addresses on registered networks within Russia to include specific IP addresses registered to Russian government networks. Prior to the attacks, detailed instructions (in Russian chat rooms/groups) were posted on how to instigate a DOS attack and which Estonian web sites should be attacked.[xxix] Because of the fundamental instructions posted on how to carry out a DOS attack, even the average computer user with internet connectivity could have become a weapon. These attacks dramatically decreased after an official statement from the Estonian government in which the "Estonian Foreign Minister Urmas Paet publically declared that many of the attacks had originated from Russian government computers."[xxx]

A March 2009 statement from Sergei Markov, a State Duma deputy from the Putin's Unified Russia party, pertaining to the 2007 cyber attacks on Estonia confirms that the cyber attack was state sponsored when he confirmed “that attack was carried out by my assistant.”[xxxi] He later went on to clarify his statement adding that at the time his assistant was not working for the Russian government and was launching the attacks as a form of civil disobedience. There is additional evidence that attacks did occur from non-state sponsored actors or hacktivists. But were these attacks coordinated by the Russian government? The general anonymity of cyber attacks in this case would not allow tangible proof that the Russian government had lead/orchestrated the attacks on the Estonian networks so the question remains unanswered, but there continues to be several indicators that these cyber events were state sponsored or at a minimum state directed attacks.

Case Studies (Russia/Georgia)

The war between Russia and Georgia, also known as the 2008 South Ossetia war, officially began on August 7, 2008, and concluded on August 16, 2008, however the beginning of the conflict commenced much earlier in the cyber realm. Georgian web sites, to include government and non-government as well as their telecommunications network, were under cyber attack much earlier. Jose Nazario of Arbor Networks noted “a stream of data directed at Georgian government sites containing the message “win+love+in+Russia””[xxxii]. These attacks occurred several weeks before conventional forces were utilized in the ground invasion on 8 August. The debilitating factor of these attacks on emergency services and government information news portals cannot fully be measured. Even without this salient data, one can clearly understand and ascertain that the ability of the Georgian government to release and update its population was significantly hampered by these attacks. The below graph shows the overall effects on data throughput from a follow on DDOS attack that occurred on August 27, 2008

(Figure A) DDoS Attack Graphs from Russia vs Georgia's Cyberattacks



On key element of the cyber attacks against Georgia was that they were remarkably similar in scope and style to the attacks that occurred against Estonia only a year and a half earlier. The one exception or difference was the follow on actions by the Russian military.

Russia began its conventional invasion by deploying ground troops into South Ossetia, Georgia, on 8 August. Jart Armin, an internationally noted cyber expert who has several cyber articles in Popular Mechanics and Computer World, reported early on in the conflict that traffic destined to some Georgian web sites was actually being rerouted to possible bogus web sites in Russia and Turkey.[xxxiii] He further reported in the same article that the servers receiving the traffic in Russia and Turkey "are well known to be under the control of RBN and influenced by the Russian government."[xxxiv] An excerpt from the article *Shadowy Russian Firm Seen as Conduit for Cybercrime* by Brian Krebs in The Washington Post refers to the Russian Business Network (RBN):

> The company "is literally a shelter for all illegal activities, be it child pornography, online scams, piracy or other illicit operations," Symantec analysts wrote in a report. "It is alleged that this organized cyber crime syndicate has strong links with the Russian criminal underground as well as the government, probably accomplished by bribing officials."[xxxv]

This is important because it shows a relationship between a state actor in the conflict, Russia, and a state sponsored actor, the RBN, being possibly directed or contracted to carry out a cyber attack on another state actor, Georgia.

The conventional war between the two states lasted until a cease-fire was agreed upon on 16 August. Russian troops remained in portions of uncontested Georgia through early October 2008. This time frame is important to understand because that although the conventional forces for all intents and purposes had stopped, fighting the cyber war between the two states continued. This is clearly evident by the DDOS attack graph shown above in figure (a) for the dates of 27 and 28 August 2008.

The complexity of the attacks in Estonia and Georgia suggest a highly evolved cyber warfare doctrine. Russia does have official cyber warfare doctrine and has a Record of hacking other nations (see appendix B). This combined with the relationship the government of Russia has with the RBN is considerable reason for alarm for the United States.

Analysis

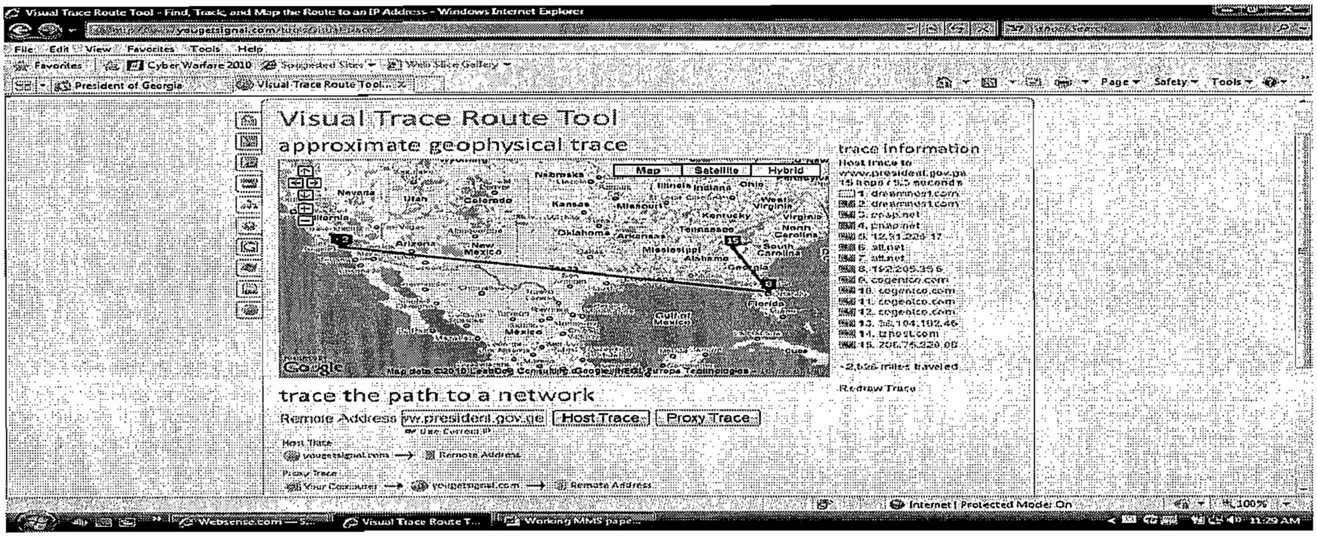
> *Mankind has always been aware of the existence and value of information. It took the invention of heavier-than-air machines to lead to a far greater exploitation of {air as a} dimension of strategy. Similarly, it may have taken the broader exploitation of the electromagnetic spectrum, and in particular the emergence of cyberspace, to realize fully the potential of information power.*
>
> David J. Lonsdale
> *The Nature of War in the information Age*

Offensive operations in cyberspace by the DoD remain a fairly new concept when compared to conventional warfare. The continuing attacks on the DoD, Taiwan, and the attacks suffered by Estonian and Georgia during conflicts with the Russian government, suggest that nations of all sizes and economic stature have already established significant offensive cyber warfare capabilities and doctrine to support their strategic goals. In accordance with appendix (B), both Russia and China have already developed cyber warfare doctrine and have an established record of utilizing this capability.

Both Russia and China have been updating their militaries for over 15 years to establish a high-tech or cyber generation of warriors within their ranks. This was done in reaction to what has become the new and almost constant center of gravity for the American military; Command and Control (C2). Russia's and China's militaries have now grown well beyond the conventional roles within their countries; they have become capable of launching offensive cyber operations when called upon by their governments. Furthermore they have adapted to this new realm by outsourcing to businesses such as the RBN and manipulating hacktivists in their own countries as well as throughout the world to assist in their cyber strategic goals. Hacktivists were a key offensive component in all of the case studies in this paper. Unlike the hackers in the United States the hacktivists in Europe and China seemed to be tied more too state sponsored ideology than to small group interest and reputation establishment.

Focusing on the case studies, one can surmise that the attacker has a clear and almost constant advantage during cyber warfare. Unlike conventional warfare the location of the attack or attacks can be adjusted in milliseconds to continually surprise one's adversary and take advantage of discovered gaps. For the party or network being attacked, that means a constant layered network defense must be implemented as well as updated frequently to match the diversity of cyber attacks prevalent on the net. This can be done by in-house technical support or by outsourcing these responsibilities to a third party.

Georgia hired a third party to host and secure their President's official government web site. In an attempt to reduce the frequency of attacks, the Georgian President's web site was relocated to a server in the United States. The below trace route (cmd tracert), a tool that tracks how IP packets are routed through the Internet, shows the IP routing to the Georgian President's web site, www.president.gov.ge. This trace route terminates at a server farm in Atlanta, Georgia.



Visual Trace Route Tool

approximate geophysical trace

trace information

Host trace to
www.president.gov.ge
15 hops (5.5 seconds)
1. dreamhost.com
2. dreamhost.com
3. pnap.net
4. pnap.net
5. 12.91.226.17
6. att.net
7. att.net
8. 192.205.35.6
9. cogentco.com
10. cogentco.com
11. cogentco.com
12. cogentco.com
13. 38.104.192.46
14. tzhost.com
15. 206.76.220.65

~2,526 miles traveled

Redraw Trace

trace the path to a network

Remote Address vw.president.gov.ge

or Use Current IP

Host Trace
yougetsignal.com → Remote Address

Proxy Trace
Your Computer → yougetsignal.com → Remote Address

One of the reasons to relocate a resource is to secure that resource. The legal implications of attacking intellectual property in another nation are complex and the legal community has not kept pace with the cyber world. Even without clear national and/or international cyber laws one can see by the lack of attacks (see appendix E) on the Georgian server once moved to the United States that the attacker decided it would not be prudent to continue the assault. One could argue that the network defenses were better at the new location their fore the attacks were discontinued. This would be an incorrect assumption; attackers continually look for weaknesses in network defenses as evident by the continual attacks on DoD systems. This appears to be a case of a third party attacker not wanting to escalate the situation by involving the United States.

As shown in the case studies above, the levels, variety and the frequencies of attacks can be manipulated to produce desired responses. This means that an attacker can simply feint a large scale DDOS attack to see what the response will be from the party or network being attacked. This information/intelligence can provide valuable insight to the attacker on how to proceed in future attacks. In other words, how can the attacker make the attack more devastating without launching a full attack? This specifically was the case with the prolonged attacks that occurred in both Georgia and Estonia. In both cases the levels and complexity of attacks increased and culminated with Georgian ground operations.

The anonymity of offensive attacks is another reason why offensive cyber attacks are being utilized by states and non-state actors across the world. Unlike a conventional war where the antagonist is clearly known offensive cyber strikes are extremely difficult if not impossible to corroborate the identity of the attacker. There are multiple ways to masquerade ones electronic footprint. The constant attacks against Taiwan are a clear example of how difficult it is to directly associate an attacker to an attack. In Taiwan's case they believe that the government of China is responsible but cannot prove their culpability to the level that Taiwan could bring international charges against China.

Servers and clients can be taken over by botnets, a group of infected systems utilized unknowingly by the rightful operator/owner to launch attacks on other systems, and utilized against another network or system. There are several other ways attackers disassociate themselves from salient evidence of their attack. These include, but are not limited to, ghosting (utilizing someone else's Media Access Control (MAC) address or IP), outsourcing (RBN), hacktivism (primarily support political or social changes) and physical attack (remove the device initiating the attack from the network). All of the aforementioned are common practice and were utilized by the attackers in the case studies.

China's Asymmetric Military Capabilities

Over the past 20 years the Chinese government has taken great focus on developing the power projection of its military beyond the Asia/Pacific region. Its strategic cyber strategy is a direct reflection of that power projection. Since its inception, China's cyber strategy has remained constant: degrade and disrupt all C2 and national information infrastructures of an adversary.

Under the current political conditions China's military will most likely utilize cyber warfare, specifically cyber reconnaissance to identify and catalogue weaknesses within the United State's military networks for future use. The identification of the weaknesses within the DoD networks would coincide with the stated desire of power projection. The PLA's offensive cyber strategy does not just focus on the DoD; it has a similar cyber strategy that focuses on the rest of the U.S government as well as travel, financial, first responder, and telecommunications networks. Another focus point for the Chinese military cyber reconnaissance would be the identification of advanced technologies that could be used to further Chinese overall interests. This is commonly referred to as "leap-frogging," taking technology illegally to further ones own technological aspirations. By leap-frogging technology, China saves on both development time and economic resources that would have been established to support the development of a technology.

China will continue to focus on networks that provide limited security such as the NIPRNET. This network stores a vast amount of information that when viewed as a whole provides significant insight into the DoD. China utilizes the information that is gleamed from this resource to adjust its current political, economic and military strategies.

It is highly unlikely that China will in the foreseeable future use direct kinetic weaponry against the United States. It is however obvious that China's military will continue to staff, operate and fund units whose mission is to strike at key assets within the DoD's secure and un-secure networks with forces such as the ones already established in the Guángzhou Military Region. The successes that these types of units have enjoyed can only make the PLA more audacious in its desires to create a larger more technical informationalized force.

China's Cyber Army
Global Rating in Cyber Capabilities: 2
Cyber Weapons Capabilities Rating: Advanced
Cyber Warfare Budget: $55 Million USD
Offensive Cyber Capabilities: 4.2 (1 = Low, 3 = Moderate and 5 = Significant)

See appendix (C) for information pertaining to cyber arsenal capabilities.

Russia's Asymmetric Military Capabilities.

Russia's stated cyber warfare doctrine is designed to be utilized in conjunction with conventional force applications. As with any type of symmetric warfare there are varying levels of intensity in its application. Russia has been accused by several governments of utilizing all levels of intensity as it pertains to offensive cyber warfare. Like the Chinese, the Russian government perceives the use of cyber warfare to be an integral part of their overall operational and strategic policies.

Russia's military offensive cyber focus is to disrupt and deny C2 to an adversary and to disrupt and destroy national telecommunications infrastructures of an adversary. This was clearly evident during the Estonian and Georgian conflicts. In both cases government and non-government networks were attacked. The style and manner of attacks were in keeping with the limited published doctrine for the Russian military.

It is unlikely that the Russian government will attempt the same level of cyber intensive attacks against the United States in the near future as it did with Estonia and Georgia. It will however continue to probe DoD's networks for intelligence and vulnerabilities that could be used in the future to prosecute more in-depth cyber operations.

The information that the Russian military gains from the cyber advances on the DoD networks are of significant concern to the United States. Russia has a long history of dealing with nations that the United States considers non-friendly; these nations include China, Iran and Venezuela. It is not known at this time if Russia would sell information it gained from cyber attacks against the United States to foreign countries.

A major concern for the DoD is Russia's willingness to outsource offensive cyber attacks. This concern is highlighted by the fact that the Russian military cyber budget is over double that of the Chinese. The primary recipient of that outsourcing continues to be the RBN. The RBN seems to operate with some level of anonymity within the Russian military and government. This means that along with the inherent capability of the Russian cyber army it also has the capability to expand its size by inculcating the capabilities of the RBN in the future. It is worth mentioning that many IT security professionals believe that the RBN had a significant role to play in the Estonian and Georgian cyber conflicts.

Russia will continue to advance its cyber interests through conventional (military) and non-conventional (outsourcing) means in support of their stated strategic goals. Historical documentation and research shows that the Russian cyber army will continue to receive greater funding as well as more support from within the Russian government.

Russia's Cyber Army
Global Rating in Cyber Capabilities: 4
Cyber Weapons Capabilities Rating: Advanced
Cyber Warfare Budget: $127 Million USD
Offensive Cyber Capabilities: 4.1 (1 = Low, 3 = Moderate and 5 = Significant)

See appendix (D) for information pertaining to cyber arsenal capabilities.

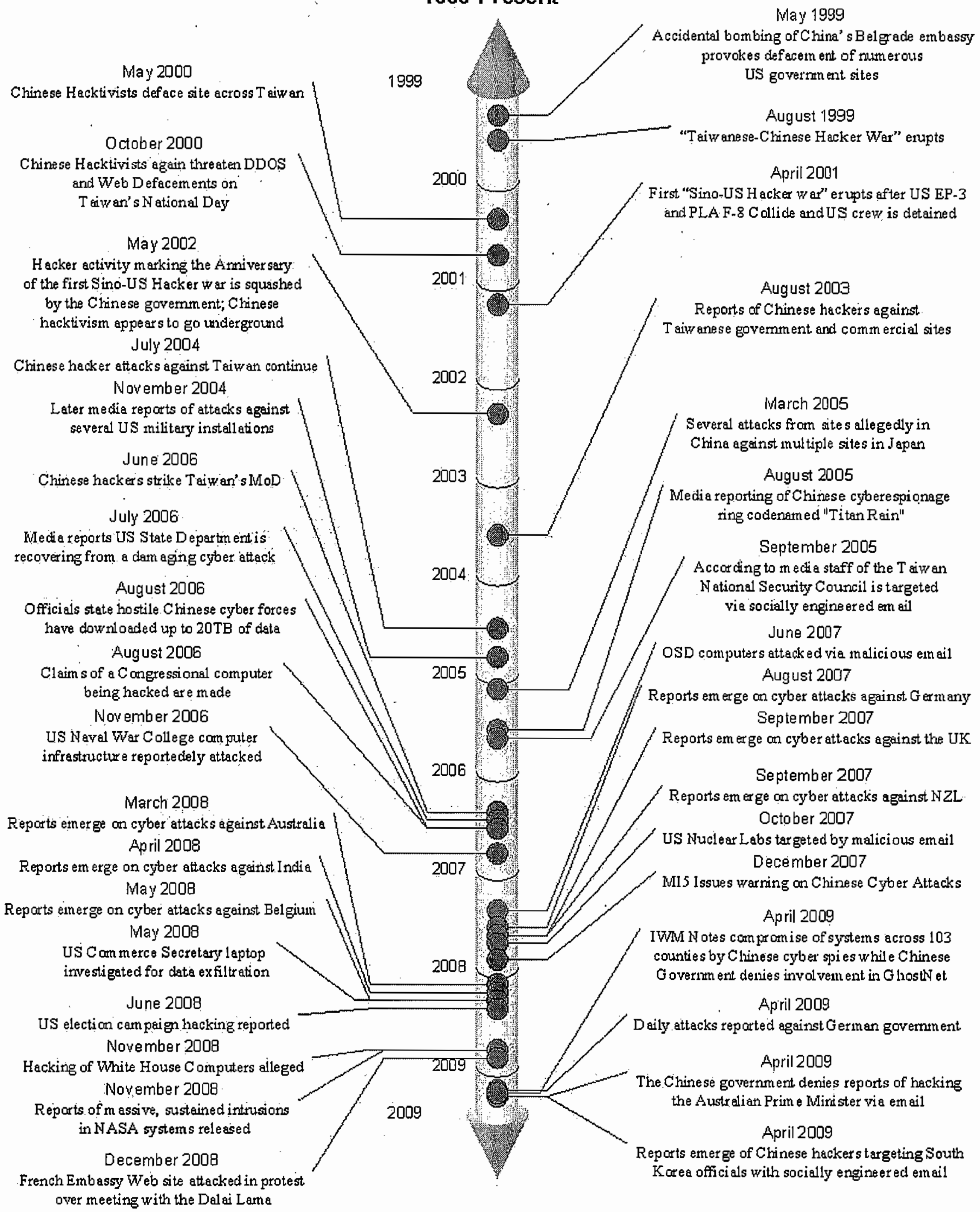
Conclusions

When looking at cyber warfare from a kinetic point of view, it is simple to see that the use of offensive cyber attacks creates significant problems/gaps across the C2 networks. Cyber attacks are increasingly dangerous because of DoD's accelerating reliance upon integrated and distributed networks. The case studies in this paper show that near pear state competitors have created at multiple levels within their militaries offensive cyber units. These units engage in direct attacks, surveillance, intelligence gathering and espionage. This paper further shows that those states are investing greater sums of money and manpower in the continued development of those units responsible for offensive cyber attacks.

The DoD must put forth an increased effort to establish, equip and deploy offensive cyber units to match the offensive cyber units of our near peer nations. By continuing to focus on primarily a defensive strategy the DoD relinquishes any possibility of an asymmetric advantage at the tactical, operational and strategic levels.

Appendix (A)

Timeline of Significant Chinese-Related Cyber Events 1999-Present



May 2000
Chinese Hacktivists deface site across Taiwan

October 2000
Chinese Hacktivists again threaten DDOS and Web Defacements on Taiwan's National Day

May 2002
Hacker activity marking the Anniversary of the first Sino-US Hacker war is squashed by the Chinese government; Chinese hacktivism appears to go underground

July 2004
Chinese hacker attacks against Taiwan continue

November 2004
Later media reports of attacks against several US military installations

June 2006
Chinese hackers strike Taiwan's MoD

July 2006
Media reports US State Department is recovering from a damaging cyber attack

August 2006
Officials state hostile Chinese cyber forces have downloaded up to 20TB of data

August 2006
Claims of a Congressional computer being hacked are made

November 2006
US Naval War College computer infrastructure reportedely attacked

March 2008
Reports emerge on cyber attacks against Australia

April 2008
Reports emerge on cyber attacks against India

May 2008
Reports emerge on cyber attacks against Belgium

May 2008
US Commerce Secretary laptop investigated for data exfiltration

June 2008
US election campaign hacking reported

November 2008
Hacking of White House Computers alleged

November 2008
Reports of massive, sustained intrusions in NASA systems released

December 2008
French Embassy Web site attacked in protest over meeting with the Dalai Lama

May 1999
Accidental bombing of China's Belgrade embassy provokes defacement of numerous US government sites

August 1999
"Taiwanese-Chinese Hacker War" erupts

April 2001
First "Sino-US Hacker war" erupts after US EP-3 and PLA F-8 Collide and US crew is detained

August 2003
Reports of Chinese hackers against Taiwanese government and commercial sites

March 2005
Several attacks from sites allegedly in China against multiple sites in Japan

August 2005
Media reporting of Chinese cyberespionage ring codenamed "Titan Rain"

September 2005
According to media staff of the Taiwan National Security Council is targeted via socially engineered email

June 2007
OSD computers attacked via malicious email

August 2007
Reports emerge on cyber attacks against Germany

September 2007
Reports emerge on cyber attacks against the UK

September 2007
Reports emerge on cyber attacks against NZL

October 2007
US Nuclear Labs targeted by malicious email

December 2007
MI5 Issues warning on Chinese Cyber Attacks

April 2009
IWM Notes compromise of systems across 103 counties by Chinese cyber spies while Chinese Government denies involvement in GhostNet

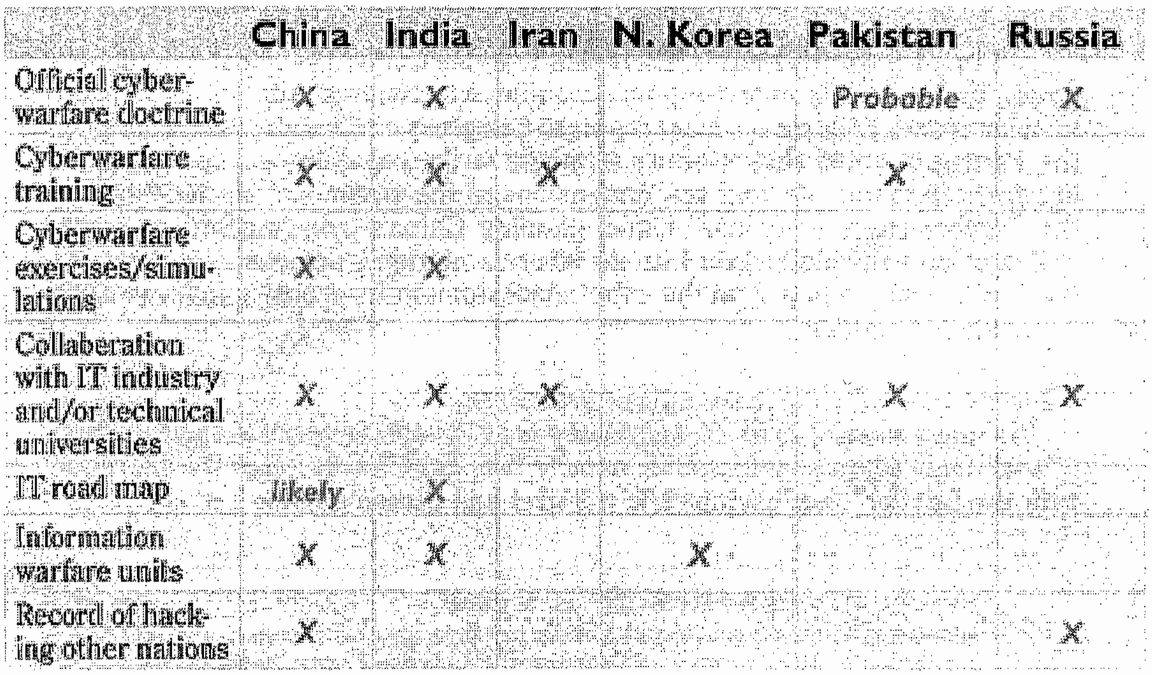
April 2009
Daily attacks reported against German government

April 2009
The Chinese government denies reports of hacking the Australian Prime Minister via email

April 2009
Reports emerge of Chinese hackers targeting South Korea officials with socially engineered email

Appendix (B)

Summary of nation-state cyberwarfare capabilities



	China	India	Iran	N. Korea	Pakistan	Russia
Official cyber-warfare doctrine	X	X			Probable	X
Cyberwarfare training	X	X	X		X	
Cyberwarfare exercises/simulations	X	X				
Collaboration with IT industry and/or technical universities	X	X	X		X	X
IT road map	likely	X				
Information warfare units	X	X		X		
Record of hacking other nations	X					X

Adapted from Charles Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States," Institute for Security Technology Studies, Dartmouth College, December 2004.

The Journal of International Security Affairs, The Art of (Cyber War) Brian M. Mazanec Spring 2009 Number 16

Appendix (C)

China

Cyber Weapons Capabilities Rating: Advanced
Cyber force Size: 10,000 +
Broadband Connections: More than 55 million
China's Hacker Community: Honker Union, Red Hackers Alliance (The 5th largest hacking organization in the world.)
China's Software Industry: In Q1 2007, the software industry RMB 96.7 billion with a year-on-year increase of 26.9%.

Cyber Weapons Arsenal:
In Order of Threat — Large, advanced BotNet for DDos and espionage
Electromagnetic pulse weapons (non-nuclear)
Compromised counterfeit computer hardware
Compromised computer peripheral devices
Compromised counterfeit computer software
Zero-day exploitation development framework
Advanced dynamic exploitation capabilities
Wireless data communications jammers
Computer viruses and worms
Cyber data collection exploits
Computer and networks reconnaissance tools
Embedded Trojan time bombs (suspected)
Compromised microprocessors & other chips (suspected)

Appendix (D)

Taken from: http://defensetech.org/2008/05/27/russias-cyber-forces/
Kevin Coleman, Russian Cyber Forces May 27, 2008
Russia's 5th-Dimension Cyber Army:
Military Budget: $40 Billion USD
Global Rating in Cyber Capabilities: Tied at Number 4
Cyber Warfare Budget: $127 Million USD
Offensive Cyber Capabilities: 4.1 (1 = Low, 3 = Moderate and 5 = Significant)

Cyber Weapons Arsenal in Order of Threat:

- Large, advanced BotNet for DDoS and espionage
- Electromagnetic pulse weapons (non-nuclear)
- Compromised counterfeit computer software
- Advanced dynamic exploitation capabilities
- Wireless data communications jammers
- Cyber Logic Bombs Computer viruses and worms
- Cyber data collection exploits Computer and networks reconnaissance tools
- Embedded Trojan time bombs (suspected)

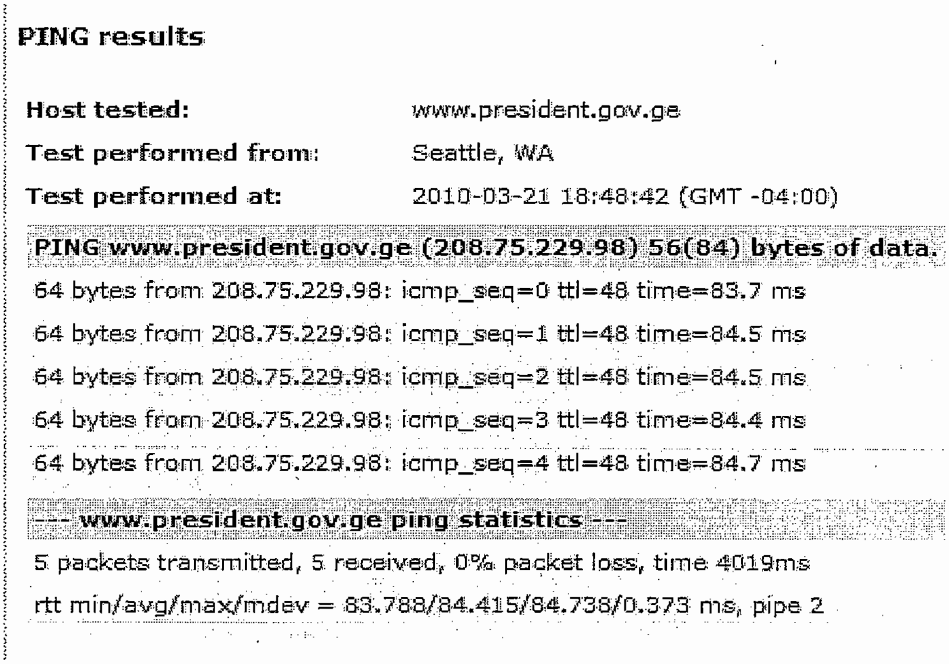
Cyber Weapons Capabilities Rating: Advanced

Cyber force Size: 7,300 +

Reserves and Militia: None

Broadband Connections: 23.8 Million +

Appendix (E)



PING results

Host tested: www.president.gov.ge

Test performed from: Seattle, WA

Test performed at: 2010-03-21 18:48:42 (GMT -04:00)

```
PING www.president.gov.ge (208.75.229.98) 56(84) bytes of data.
64 bytes from 208.75.229.98: icmp_seq=0 ttl=48 time=83.7 ms
64 bytes from 208.75.229.98: icmp_seq=1 ttl=48 time=84.5 ms
64 bytes from 208.75.229.98: icmp_seq=2 ttl=48 time=84.5 ms
64 bytes from 208.75.229.98: icmp_seq=3 ttl=48 time=84.4 ms
64 bytes from 208.75.229.98: icmp_seq=4 ttl=48 time=84.7 ms

--- www.president.gov.ge ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4019ms
rtt min/avg/max/mdev = 83.788/84.415/84.738/0.373 ms, pipe 2
```

Appendix (F)

Acronym List

CNA	Computer Network Attack
CO	Cyber Operations
DoD	Department of Defense
DOS	Denial of Service
DDOS	Distributed Denial of Service
JWICS	Joint World Intelligence Communications System
MAC	Media Access Control
NA	Network Attack
NIPRNET	Nonsecure Internet Protocol Router Network
NOW's	Network Warfare Operations
PLA	Chinese Peoples Liberation Army
PRC	Peoples Republic of China
RBN	Russian Business Network
SIPRNET	Secure Internet Protocol Router Network
IP	Internet Protocol
IT	Information Technology
USCYBERCOM	United States Cyber Command

Endnotes

[i] John A. Serabian, Jr. Statement for the Record Before the Joint Economic Committee on Cyber Threats and the Us Economy, February 23, 2000. https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html (accessed December 12, 2009).

[ii] *Information Management Journal,* Cyber attacks on U.S. government rise. Volume: 43 Issue: 4 Page: 7 July 1 2009.

[iii] John Markoff and Andrew Kramer. "U.S and Russia Differ on Treaty for Cyberspace." *N.Y. Times.* June 27, 2009. http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=1

[iv] Walsh, David C. "Know Thine Enemy ." *Defense Technology International*, November 1, 2009, 39.

[v] "Ghost in the machine; A cyber-warfare mystery. (A cyber-attack on America)*The Economist* (2009), http://www.economist.com/displaystory.cfm?story_id=14011859. (accessed December 2, 2009).

[vi] *JP 1-02, Deparment of Defense Military and Associated Terms, supra* note 17 at 141.

[vii] *JP 1-02, Deparment of Defense Military and Associated Terms, supra* note at 113.

[viii] U.S. Dep't of Air Force Policy Dir. 10-7, Information Operations 19 (6 Sept. 2006) http://www.fas.org/irp/doddir/usaf/afpd10-7.pdf

[ix] U.S. Dep't of Air Force Policy Dir. 10-7, Information Operations 19 (6 Sept. 2006) http://www.fas.org/irp/doddir/usaf/afpd10-7.pdf

[x] Schapp, Arie J.. "Cyber Warfare Operations: Development and Use Under International Law." *Air Force Law review* 64, no. (2009):

[xi] Sunzi, Sunzi, Tzu, Sun, & Griffith, Samuel. (1971). *Art of war 0195014766.* Oxford University Press, USA.

[xii] Clausewitz, Carl, Howard, Michael, Paret, Peter, Howard, Michael, Paret, Peter, & West, Rosalie. (1984). *Carl von clausewitz.* Princeton Univ Pr.

[xiii] Scott Applegate. "Cyber warfare – Addressing New threats in the Information Age" March 29, 2009

[xiv] Tony Cappacio. "GAO Says joint Strike Fighter Cost is Rising." *Washington Post.* March 12, 2008 http://www.washingtonpost.com/wp-dyn/content/article/2008/03/11/AR2008031102796.html

[xv] Tony Cappacio. "GAO Says joint Strike Fighter Cost is Rising." *Washington Post.* March 12, 2008 http://www.washingtonpost.com/wp-dyn/content/article/2008/03/11/AR2008031102796.html

[xvi] Angela Moscaritolo. "Report: Cyberattacks against the U.S. "Rising Sharply"" http://www.scmagazineus.com/report-cyberattacks-against-the-us-rising-sharply/article/158236/ November 20, 2009

[xvii] Brian Mazanec. "The Art of (Cyber) War" *The Journal of International Security Affairs.* No. 16 (2009) http://www.securityaffairs.org/issues/2009/16/mazanec.php

Bibliography

Janczewski, Lech, and Andrew Colarik. *Cyber warfare and cyber terrorism*. Idea Group Reference, 2008. Print.

Ventre, Daniel. *Information Warfare*. Wiley-ISTE, 2009. Print.