Strategy Research Project

PROACTIVE SELF DEFENSE IN CYBERSPACE

BY

LIEUTENANT COLONEL BRUCE D. CAULKINS
United States Army

USAWC CLASS OF 2009

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

Prudens Futuri

U.S. Army War College, Carlisle Barracks, PA 17013-5050

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **30 MAR 2009**	2. REPORT TYPE	3. DATES COVERED	
4. TITLE AND SUBTITLE **Proactive Self Defense in Cyberspace**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) **Bruce Caulkins**		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220**		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 unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see attached

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**30**	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 23-02-2009	**2. REPORT TYPE** Strategy Research Project	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE

Proactive Self Defense in Cyberspace

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LTC Bruce D. Caulkins

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
COL Blane R. Clark
Department of Military Strategy, Planning, and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The most prevalent form of warfare in the 21st Century will occur in cyberspace. Cyberwarfare can take on many forms and levels of volatility and the persistent environment of cyberwarfare will force network and systems security specialists to continue improving upon their tools of the trade. Most of these tools are reactive in nature. The U.S. Department of Defense (DoD) and other government agencies need to develop a blend of reactive and proactive tools and standards to properly secure and defend the Global Information Grid (GIG) from cyber attacks.

This paper will discuss the strategic requirements for enacting a proactive self-defense mechanism in cyberspace. It starts by providing a background on the cyber issues, vulnerabilities, and threats that face us today. Then it discusses the future cyber threats and how a proactive cyber defense will combat these threats. Supporting technologies like modeling and simulation and the Disruption Tolerant Network (DTN) are addressed as well. The paper then concludes with strategic recommendations for establishing a proactive self-defense in cyberspace to properly secure the GIG while maintaining superiority in the cyber domain.

15. SUBJECT TERMS
Cyberwarfare, Information Assurance, Anomaly Detection, Disruption Tolerant Networks, Modeling, Simulation

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	30	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC STRATEGY RESEARCH PROJECT

PROACTIVE SELF DEFENSE IN CYBERSPACE

by

Lieutenant Colonel Bruce D. Caulkins
United States Army

Colonel Blane R. Clark
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR:	Lieutenant Colonel Bruce D. Caulkins
TITLE:	Proactive Self Defense in Cyberspace
FORMAT:	Strategy Research Project
DATE:	17 February 2009 WORD COUNT: 5,802 PAGES: 30
KEY TERMS:	Cyberwarfare, Information Assurance, Anomaly Detection, Disruption Tolerant Networks, Modeling, Simulation
CLASSIFICATION:	Unclassified

The most prevalent form of warfare in the 21st Century will occur in cyberspace. Cyberwarfare can take on many forms and levels of volatility and the persistent environment of cyberwarfare will force network and systems security specialists to continue improving upon their tools of the trade. Most of these tools are reactive in nature. The U.S. Department of Defense (DoD) and other government agencies need to develop a blend of reactive and proactive tools and standards to properly secure and defend the Global Information Grid (GIG) from cyber attacks.

This paper will discuss the strategic requirements for enacting a proactive self-defense mechanism in cyberspace. It starts by providing a background on the cyber issues, vulnerabilities, and threats that face us today. Then it discusses the future cyber threats and how a proactive cyber defense will combat these threats. Supporting technologies like modeling and simulation and the Disruption Tolerant Network (DTN) are addressed as well. The paper then concludes with strategic recommendations for establishing a proactive self-defense in cyberspace to properly secure the GIG while maintaining superiority in the cyber domain.

PROACTIVE SELF DEFENSE IN CYBERSPACE

> For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill. Thus, what is of supreme importance in war is to attack the enemy's strategy.
>
> --Sun Tzu
> The Art of War[1]

Current Cyberwar

Sun Tzu wrote the words above more than 2,500 years ago. His statement above centered on the strategic tools that can be used in defeating an opponent without actually fighting that opponent on the battlefield. He was contemporaneously referring to the existing diplomatic or economic means available at that time. Sun Tzu later hinted that an adversary who has to make defensive preparations in all areas was not really prepared to properly conduct a battle.[2] Sun Tzu pointedly noted that this type of adversary had many weaknesses to exploit in the long run.[3]

In a similar vein, Sun Tzu's comments apply to today's cyber fight and underscore the inherent vulnerabilities within most modern networks and systems. An opponent can be defeated or crippled from attacks in cyberspace. These attacks could precede or preclude attacks on an actual battlefield. Further, an opponent who prepares defenses in one or two areas may leave other critical avenues of approach vulnerable. An opponent who prepares everywhere in cyberspace may feel more secure about his security measures. He may feel, in fact, *too* secure. However, preparing cyber defenses that react to attacks addresses only half of the defensive problem facing today's cyber security specialists. Cyber defense must be holistic in nature and address both proactive measures and the legacy reactive defensive measures taken through the employment of firewalls, intrusion detection devices, anti-virus programs, and other software programs and hardware devices.

Background Issues. In the 2003 *National Strategy to Secure Cyberspace,* the potential for cyber disaster is clear. The document says that our "economy and national security are fully dependent upon information technology and information infrastructure. At the core of the information infrastructure upon which we depend is the Internet, a system originally designed to share unclassified research among scientists."[4] This salient point cannot be stressed nor repeated enough: the Internet's underlying technologies, especially the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, were created in order to ensure message delivery, not ensure message security, non-repudiation, or any other security concept.

IP is a connectionless, "fire and forget" protocol that packetizes messages and does not rely directly on establishing connections between hosts. TCP, on the other hand, is a connection-oriented standard that provides the reliability function for the IP layer between two communicating hosts.[5] In other words, IP first chops up the message into packets from the sending host in preparation to send the packets to the receiving host computer. Then, TCP delivers those packets to the desired computer host at the destination. TCP further ensures that the received packets are reorganized in proper order. However, little consideration is given to the possibility of packet integrity or integrity of the sending host's IP address, leading to possible security issues like IP spoofing or TCP session hijacking.

TCP session hijacking, IP spoofing, and synchronization (SYN) flooding are just three examples of simple yet effective attacks against TCP/IP-based networking. TCP session hijacking, in particular, can be difficult to detect properly as the Media Access Control (MAC) address of the sending location changes while the corresponding IP address appears to be the same. An automated security system like an intrusion detection system may notice a change in the MAC address of a message and give a false negative reading since the change in the MAC address is only a possible indicator of TCP hijacking. Attack examples like these against the TCP standard are commonplace. The original authors of TCP worried more about getting the message through the network than security of the message. But when you consider the context of that time, this position made sense.

Networks, and in particular the Internet, run on widely-used standards and protocols. The Internet Society (ISOC) is a not-for-profit organization that pursues the creation of newer and better Internet standards and policy. ISOC's Internet Engineering Task Force (IETF) produces "high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better. These documents include protocol standards, best current practices, and informational documents of various kinds."[6] To meet their mission's goals, the IETF sponsors and supports the production of Request For Comments (RFC) documents. These RFC documents spell out the proposed future protocols for the Internet itself.

In RFC 675, the authors of the TCP standard describe "the functions to be performed by the internetwork Transmission Control Program [TCP] and its interface to programs or users that require its services."[7] Very little attention was given to computer or network security. The authors wrote RFC 675 in 1973 and successfully transmitting a simple message from one host computer to another was a great accomplishment and not much thought was given to computer or network security. In fact, the TCP authors briefly mentioned security only twice in the entire RFC document.

Today's computer and network security facts remain the same: when you add more and more security measures, you inevitably get a reduction in speed and responsiveness in your networks and systems. The challenge for 21st Century cyber defense specialists is to correctly balance their organization's network security needs against the speed, usage and bandwidth requirements of their organization's users.

As an example, the need to balance security with user needs when an attack occurs against a computer's port 80 on the organization's web servers. This type of attack can be easily stopped by eliminating access to port 80 from the server itself to all users, even legitimate website users. Unfortunately, port 80 is the world-wide default for web services and disabling port 80 would drastically reduce the number of legitimate users on the organization's web site, as those users would not readily know that port 80 was not available for their legitimate use.

These types of trade-offs are common in the cybersecurity realm. Information Assurance, and by extension cyber defense, are "in a trade-off with other critical properties such as system functionality and performance… [security specialists] need to be able to intelligently adjust this trade-off during system operation to offer up the best defense."[8] Security engineers and administrators who do not balance properly their security needs with the performance requirements are bound to fail in the long run.

Cyber Vulnerabilities. In the commercial world, vulnerabilities are primarily:

> Design or implementation errors in information systems that can result in a compromise of the confidentiality, integrity, or availability of information stored upon or transmitted over the affected system. They are most often found in software, although they exist in all layers of information systems, from design or protocol specifications to physical hardware implementations.[9]

Network vulnerabilities may also be compromised intentionally by malicious users or automated malicious code. The eventual discovery and disclosure of a single vulnerability in a critical system or network "can seriously undermine the security posture of an organization."[10]

The U.S. Defense Department defines the term *vulnerability* as the susceptibility to attack or "a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system."[11] The key term here is *weakness.* Weaknesses in any system or network can and should be prevented. However, a weakness in a system or network implies that a solution is known and reasonably implementable.

Dozens of system and network vulnerability analyzers are available, to include the Automated Vulnerability Detection System (AVDS) and Tiger. Both AVDS and Tiger look at the known vulnerabilities that exist based on previously-identified attack vectors. Cyber attack vectors are the identifiable pathways that a particular attack can take against a given target or set of targets. AVDS also uses simulated attacks on a network to fully analyze the network's cyber posture and has a low false positive rate.[12] Other similar tools used by cyber specialists are the Security Administrator's Integrated Network Tool (SAINT) and Network Mapper (nmap). SAINT and nmap are network-based vulnerability assessment tools that are fast and reliable.[13] Hackers also use nmap due to its portability and ease of use. Nmap has versions for Linux, UNIX and Microsoft Windows platforms and can easily scan huge networks containing hundreds of thousands of systems and servers.[14] Both SAINT and nmap scan the network for vulnerable ports and/or services and obviously can be used for malicious and non-malicious reasons.[15] Novel attacks or attack vectors “fly under the radar” of most vulnerability assessment tools as their strengths lie in the well-known nature of attack signatures and locations.

A quick vulnerability check on any network server can yield a potential problem if, for example, port 21 is active on any server. Port 21 is the default port for file transfer protocol (FTP) processes that run in the background. The legacy FTP program provided no data encryption and no strong user authentication and in this situation it would be relatively easy to steal data in transit due to no data encryption. Another problem can possibly arise as a hacker could spoof a system easily into thinking he was a legitimate user of the FTP server when he should not have access due to no strong user authentication. One answer to these vulnerabilities is to employ an encryption technologies secure-shell (SSH) FTP, or SFTP. SSH provides data integrity and confidentiality over the Internet through its encryption scheme. SFTP uses SSH over a reliable data connection to allow remote and secure transfer of files. This protocol uses port 22 by default and allows the system administrator to disable the legacy FTP server and thus eliminate the need to use port 21. Amazingly, a few administrators mistakenly forget to disable FTP when they are running SFTP, thereby creating a potential back door for hackers to exploit.

Vulnerability assessment tools are a two-way street. While they provide a much-needed capability for administrators to assess their system's and network's statuses, these tools also provide a scanning ability for malicious hackers to abuse. Any port scanning tool can remotely probe a network server and determine which ports are open and available to the outside world. The hacker then can see if any of these open ports are easily exploitable.

Cyber Threats. Cyber threats "refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway."[16] Security specialists look at known and, more importantly, *more-probable* attack vectors to conduct a risk assessment of sorts to better protect their systems and networks. Sun Tzu's quote at the beginning of this paper comes into play here: a network security specialist that works and plans for every known contingency is doomed for disaster. After all, not all contingencies can really be addressed as new and new attack methodologies are created every day.

Stephen Northcutt, the President of the SysAdmin, Audit, Network, Security (SANS) Technology Institute, detailed a list of primary threat vectors for networks and systems: outsider attack from network; outsider attack from telephone; insider attack from local network; insider attack from local system; and, attack from malicious code.[17] These vectors allow a cyber security specialist to properly analyze the available assets and vulnerabilities of those assets, based on the most-likely threat they would encounter on the organization's network or system.

As with vulnerability analysis, however, looking at the potential threats only covers the well-known exploits and attack vectors. Any thought of protecting the network against never-seen-before attacks must come from a different source and perspective. Cyber security specialists must use proactive cyber defense to combat these new attacks.

Current Tools, Standards, and Techniques. Routers, firewalls, intrusion detection systems (IDS's), and antivirus programs like McAfee VirusScan or Symantec AntiVirus provide most of the security capabilities in today's ongoing cyber war, particularly at the desktop level of security. A brief summary of each device's capabilities and characteristics follows.

Routers forward network packets between two networks and provide filtering mechanisms on known traffic locations that present potential cyber security problems. If the router's default setting is *deny all*, then an access control list must be implemented to allow network traffic that is acceptable. On the other hand, if the router's default setting is *permit all,* then the access control list must be implemented to figure out what traffic should be denied. In the purest sense, the former scheme is too restrictive and inefficient while the latter is too permissive and unsecure. Most modern network engineers use the latter paradigm as the major router manufacturers like Cisco Systems have introduced advanced security features in their products that enhance the router's ability to protect the internal network while not significantly slowing down legitimate network traffic.

Firewalls work closely with routers and filter incoming and outgoing traffic but also implement a pre-defined ruleset that determines which incoming or outgoing packets are allowed or discarded. The firewall's internal program checks packets against its ruleset and allows or denies the packet. A faulty or outdated ruleset renders a firewall less useful. Further, the firewall generally is not able to detect novel attacks that are not known and not in the ruleset database. Firewalls can be hardware or software or a combination of both. The firewall device needs to reside physically near the network gateway to ensure proper analysis of packets is conducted. A helpful analogy is to consider a firewall like the security guard that checks the credentials of any and all visitors that go in and out of a building. Using a solid set of criteria that determines a person's eligibility to enter the building, a building's security guard knows who to let into the building and who he needs to prevent from entering the building. Like the security guard, today's firewall determines which network packets are allowable and which are not allowed based on a set of rules in its database.

IDS machines monitor, report, and respond to possible intrusions to a network or to a host system.[18] Multiple sensors—small computer applications located in various places on the network that report back to the main IDS server—are the eyes and ears of the IDS methodology. If a firewall can be looked at as a building's security guard, then the IDS can be seen as a set of security video cameras that scan the foot traffic that goes in and out of the building and also at various key points throughout the building. In this case, however, this set of "video cameras" can trigger immediate alarms and cause an active response to a perceived event. The IDS's strength, like the firewall, lies in its knowledge base (KB). A defective or outdated KB gives the administrator a false sense of security as attacks can slip by the IDS unnoticed due to the outdated KB being used by the system.

Antivirus (AV) programs are the last piece of the security system discussed. AV programs reside on the hard drives of desktop computers and servers. These software programs scan and clean hard drives, incoming emails, and other system-based objects to ensure no malicious software, or malware, gets access to the system itself. Like firewalls and IDS programs, the AV program is only as good as its most-recent AV signature update. Hackers create new viruses daily and a strong AV program must be kept up-to-date constantly to allow the system to recognize the newest attacks via their well-known digital signatures. Unfortunately, a digital signature can be changed very easily and since hackers usually publish their attack codes to fellow hackers, variants of well-known viruses come into being very quickly and frequently.

As with most of the current cyber defense technologies and methodologies, a solid understanding of current attacks and attack vectors is necessary. This requirement for understanding will not change for the foreseeable future. What is required in the future is a complementary strategy that employs proactive cyber defense mechanisms along with an anomaly-based modeling and simulation paradigm. That is, instead of waiting for any attack to commence, security administrators must proactively defend the network perimeter by creating new and innovative processes.

These new processes are needed to "stimulate research and to promote development of research information assurance and survivability technologies. Current processes insure that innovators and developers are always playing catch-up to the adversaries."[19] It is time to stop "playing catch-up" and start to proactively engage the cyber enemy before he strikes at our cyber infrastructure.

Future Cyberwar

Future Threats. In the Joint Operating Environment (JOE) document for 2008, the Joint Forces Command (JFCOM) describes the next twenty plus years of activity that we can expect in the cyber domain:

> Key to understanding information technology in the 2030s is the fact that the pace of technological change is accelerating almost exponentially. Because most individuals tend to view change in a linear fashion, they tend to overestimate what is achievable by technology in the short term, while dramatically underestimating and discounting the power of scientific and technological advances in the long term.[20]

JFCOM further explains that the JOE "maintains a longer term view and avoids a preclusive vision of future war. Any enemy worth his salt will adapt to target our perceived weaknesses, so the implications contained in this study cannot be rank ordered."[21] Only a truly proactive self defense in cyberspace, coupled with the traditional reactive regime, can defeat these new threats.

In the current cyber fight, several interwoven themes are emerging that will last for a decade or more. These themes will persist and continue to occur if our cyber defense posture remains static and reactive in nature.

The first theme actually encompasses a security corollary to the so-called "shiny object syndrome" (SOS). SOS can be best described as a headlong rush into the latest fad for no good business reason. Karyn Greenstreet described it further: "it's not quite ADD/ADHD. It's more that a new idea captures your imagination and attention in such a way that you get distracted from the bigger picture and go off in tangents instead of remaining focused on the goal."[22] Senior executives in the military or commercial business can waste a lot of time and resources by chasing the next computer fad. The so-called security corollary of the SOS pertains to the rush to acquire the latest electronic gizmo without taking the inherent risks into account. The BlackBerry phenomenon is a perfect example of the security corollary. Most executives today use a BlackBerry-type device in some official capacity, and this situation has expanded greatly over the last few years. When these devices first came on the scene, little thought was given towards properly securing and encrypting these devices. The BlackBerries themselves were too useful and too convenient even though the data the BlackBerries sent were not encrypted. Over time, however, most organizations discovered the inherent security flaws to these wireless devices and began to force the use of encryption and other security measures.

A second theme is the continued expansion of cyber crime. Profit is the motivation for these cyber criminals and many of these lawbreakers are very successful unfortunately. In fact, experts in the computer and network security fields see that in the future, the cyber criminals "will become increasingly organized and profit-driven."[23] Money will continue to flow and motivate hackers to develop newer and more clandestine means of stealing corporate and military secrets. After all, it is much less expensive to electronically steal the plans for a new fighter plane than it is to develop and build the plane on your own.

The third theme is the threat to cyber control systems in the infrastructure arena. In the National Infrastructure Advisory Council's (NIAC's) final report on the convergence of physical and cyber technologies and the associated challenges, the working group determined that while "there are no commonly known examples of infrastructure failures that can be tied to a cyber attack, the potential for such an event exists and the consequences could be catastrophic."[24] One of the main reasons for this potential threat derives from the fact that companies that run and operate the control systems facilities often have a very limited grasp of the enormity of the cyber threat itself. While most companies deal with novice hackers and other low-level actors on the cyber scene, control system companies deal with cyber threats from "organized crime, rogue corporations, terrorist organizations, and nation states."[25] These hackers are not only resourced well, but they are also more motivated and determined to be successful when attacking a control system's cyber infrastructure. The U.S. Department of Homeland Security's Control Systems Security Program addresses many of these concerns through a coordination of activities world-wide "to reduce the likelihood of success and severity of impact of a cyber attack against critical infrastructure control systems through risk-mitigation activities."[26]

The fourth theme that we will encounter in the future will be the polymorphic nature of attacks themselves. *Polymorphism* is the ability of an object to change the very nature or outward appearance of that object. A polymorphic computer virus, for example, changes its code each time it is copied and infected in a new file. This action allows the new version of the virus to stealthily slip by IDS and AV detectors as its digital signature is new and virtually unknown to the detectors' data engines.[27] Uses of malware, like polymorphic viruses, will continue to increase in frequency due to the successful and stealthy nature of these attacks.

Supporting the polymorphic threats will continue to be the explosion of the presence and use of botnets.[28] A *botnet* is the acronym for Internet robot network. When used for malicious means, these botnets are formed secretly over a series of hijacked computers, also known as *zombie* computers, which perform a clandestine set of functions in accordance with the hacker's desires. Hackers often use botnets to launch Distributed Denial of Service (DDoS) attacks against various target systems.[29] Botnets can provide an ideal foothold into a distributed set of computers, providing a launching platform for polymorphic attacks. Cyber security specialists use software devices like honeypots to lure an unsuspecting hacker into a safe enclave where the hacker can do no harm and his movement can be controlled and monitored. Honeypots are technological means to counteract any botnet-based attack[30], but these honeypot devices provide only a partial answer to the problem. Symantec noted in its Internet Security Threat Report for the second half of 2007 that there were over five million distinct bot-infected computers during that time period.[31] The cyber attacks in Estonia in 2007 provided a startling instance of botnets attacking servers from many sides, mostly from over a million unsuspecting zombie computers.[32] Symantec further noted that attackers favor bot-infected computers as an attack platform because those infected computers can effectively perform many malicious functions and they are easy and inexpensive to propagate and exploit. Symantec also said that these bot-infected computers are "difficult to disable with a decentralized command-and-control model, and most importantly, can be used for substantial financial gain."[33]

The final theme, which hits close to home for the U.S. military, is the more-persistent and more-open nature of military cyberwarfare.[34] Russian cyber operations in Estonia[35] and Georgia[36] underscore this new, emerging theme. The DDoS cyber attacks in Georgia eerily show similarities to conventional use of field artillery fires to precede an attack by pounding the enemy into submission, making the likelihood of success in a conventional attack more likely. Now, the "cyber artillery shells" of the 21st

Century provide a new way to shock one's opponent prior to an attack. By some accounts, Russia used its cyber artillery weeks before invading Georgia[37] and continued to utilize its cyber operations during its occupation of parts of Georgia to support its strategic and operational objectives.[38] In addition to the DDoS attacks, Russia reportedly used various cyber attacks like route hijacking and data theft to accomplish its cyber goals in Georgia.[39]

Cyber attacks in the past were virtually unseen by most of the public. Now, the ubiquitous nature of the Internet itself enables events like defacing the website of the Georgian President to become front-page news.[40] These five emerging themes will continue to persist and only through proactive cyber defense can we defeat these new threats.

Proactive Cyber Defense. In the executive summary of the *National Strategy to Secure Cyberspace,* the Bush Administration notes that privacy and civil liberties need to be better protected in the cyber domain. They add that because "no cybersecurity plan can be impervious to concerted and intelligent attack, information systems must be able to operate while under attack and have the resilience to restore full operations quickly."[41] This strategy represents a dramatic turn away from the static, legacy cybersecurity mechanisms of the 1990s. The administration recognizes the fact that no cyber defense plan can cover all of our needs.[42] However, our cyber defense strategy needs to be dynamic and polymorphic in nature. Our strategy needs to be grounded in sound theory but flexible and adaptive as well.

In the Quadrennial Defense Review Report (QDR) of 2006, the U.S. Department of Defense stated that the DOD "will maintain a deterrent posture to persuade potential aggressors that their objectives in attacking would be denied and that any attack on U.S. territory, people, critical infrastructure (including through cyberspace) or forces could result in an overwhelming response."[43] While many DOD officials still question the legal aspects of proactive and reactive defense strategies,[44] the proposals in this paper focus on the technical, not legal, ramifications of developing a more active cyber defense posture.

A truly proactive cyber defense needs to concentrate on the five emerging themes described earlier in this paper. Current cyber defense postures alone cannot defeat these emerging themes. Vulnerabilities (SOS corollary theme) must be better addressed while motivating factors (Cyber Crime theme) must be eradicated altogether. Valuable cyber targets (Control Systems theme) must be hardened against newer attacks (Polymorphic Attack theme). Finally, these four themes together will culminate into the final theme: the state of persistent military cyberwar. Proactive cyber defense standards and mechanisms will enable cyber security specialists to defeat or at least counteract these themes.

Any *proactive* defense posture needs to anticipate future attacks. Additionally, cyber security specialists need to have the tools and knowhow to be able to prevent or respond to any and all attacks to the network or any part of their internal computer system. Cyber training and education must be expanded by the Department of Defense to improve the knowledge base for cyber security specialists and administrators. Training must also continue to occur for military leaders at all levels to indoctrinate them on the importance of cyber security and what they can do to better assist their cyber experts to properly secure and defend their networks and systems.

As noted by Wood, et.al., "[w]e must think about attack strategy and defensive counter-strategies as an evolution in time and project forward several moves ahead, as in chess playing, to find the most effective next move, whether that move be in system design, operation, or even research itself."[45] Current cyber defense strategies rely almost exclusively on *reacting* and defending. The United States government must proactively defend our network's perimeter while predicting the type, time and location of the next cyber attack. Then we can successfully respond to the attack in an appropriate and timely manner instead of constantly trying to catch up with our adversaries. To achieve these goals we must produce a robust modeling and simulation paradigm for our networks and systems in conjunction with an enhanced use of new technologies like Disruption Tolerant Networks (DTNs).

Supporting Technologies

Modeling and Simulation Paradigm for Proactive Cyber Defense. In 2005 a series of research papers were written that were centered on the paradigm for modeling systems and networks for anomaly-based detectors for cyber defense. These papers were accepted in publications for the Association of Computing Machinery (ACM)[46] as well as the Institute of Electrical and Electronics Engineers (IEEE)[47]. These publications continued the network modeling work of several scientists, most notably Dr. Matt Mahoney, who also used data mining concepts within a programming interface to detect anomalous network traffic with a high degree of success.[48]

The network models that were created along with those models created by Mahoney show a different side of the cyber defense paradigm. This research concentrated on modeling *what* the network should look like; therefore, any zero-day—

or never seen before—virus or attack will not pass by unnoticed. This research in modeling and simulation also used decision-tree based data mining techniques in conjunction with concepts like bootstrapping the data in order to provide a sounder model. To bootstrap the testing data, a random packet of the data was repeatedly removed for every thousand packets in order to re-validate the model continuously. Bootstrapping is an extremely computational-intensive process but it is necessary to create a better model to apply against the zero-day attacks.[49]

A cyber defense system with anomaly detectors will immediately notice any irregular traffic and report its findings to the large-scale defense system. A truly sound security prototype will employ anomaly-based detectors alongside signature-based detectors, as neither type of detector, by itself, is foolproof. However, utilizing both systems together properly and in serial will drastically improve a network's security posture.[50]

Disruption Tolerant Network (DTN). DTN is another innovative approach that can dramatically alter the cyber defense landscape. DTN is a set of protocols designed to be a replacement of sorts for the legacy TCP/IP suite. DTN-enabled networks provide an enhanced level of reliability in disrupted environments while using a flexible node addressing scheme in lieu of the traditional IP naming conventions.

DTN architecture revolves around a data-centric model, not a network-centric model. DTN addresses major concerns with the legacy IP networks that are nearly impossible to fully secure. Additionally, the performance within IP networks can be very poor for mobile ad-hoc networks seen in the military/tactical domain. DTN uses a unique, new naming convention for routing the data bundles—not packets—throughout the network. Data is protected while at rest and can be stored along the network path to the destination if the network is not stable.

Recently, the National Aeronautics and Space Administration's (NASA's) Jet Propulsion Laboratory (JPL) used DTN software in a test with a satellite orbiting the Earth by sending dozens of images between the satellite and the NASA ground station. Technologies like DTN are important for space communications since glitches "can happen when a spacecraft moves behind a planet, or when solar storms and long communication delays occur. The delay in sending or receiving data from Mars takes between three-and-a-half to 20 minutes at the speed of light."[51] The test proved immensely successful. NASA experienced that in the DTN design itself, "if a destination path can't be found, the data packets are not discarded. Instead, each network node keeps custody of the information as long as necessary until it can safely communicate with another node."[52]

DTN is also a burgeoning project within the Defense Advanced Research Projects Agency (DARPA) and DARPA scientists are working on DTN this fiscal year. Promising tests at Fort AP Hill, Virginia and at other locations have shown that DTN provides a truly reliable and robust networking schema for disruption-laden network environments like those seen in space and especially in the tactical realm of military operations.

Recommendations

Cyber defense has challenged the DoD for years. A continual reliance on reactive defensive postures will not improve our cyber defenses in the long term. To ensure that a proactive self defensive bearing in cyberspace is taken, the United States government should enact the recommendations listed below.

First, the Congress must enact cyber-related legislation similar to the Goldwater-Nichols Act of 1986. This legislation should streamline the cyber defense structure in the government while increasing cyber cooperation and information sharing between military and non-military agencies in the government. The various computer emergency response teams spread out over the military and governmental agencies would report directly to the senior response team in the Department of Homeland Security. The intelligence agencies would also synthesize, analyze, and most importantly report intrusions to the governmental agencies in a timelier manner. This increase in information sharing will need to be tightly controlled and secured. This legislation will provide the solid foundation for enacting the proactive cyber defense measures discussed throughout this paper.

Second, the military needs to develop a robust modeling and simulation architecture for proactive cyber security. Traditional methods of reacting to known cyber attacks are becoming obsolete. Newer, more proactive measures of understanding the current network and system architecture through proper modeling of the underlying network traffic would produce substantial benefits in our cyber defense posture.

Third, we must begin to dislodge ourselves of the legacy TCP/IP architecture. TCP/IP was designed decades ago to move data from one point to the next with little or no thought to security whatsoever. TCP/IP has proven to be a successful protocol suite but it is time to move away from this standard. This change would be a huge undertaking and would take many years to accomplish. Advanced technologies like DTN provide a window on how we can leverage software and hardware tools to proactively enhance our cyber security while maintaining a healthy level of capabilities and throughput throughout the enterprise.

Fourth, we must expand our training and education in the cyber realm. Each military service conducts various levels of cyber training to meet its needs and requirements. Most, if not all, of the cyber training and education has been directed towards a reactive defensive posture. Training for lower-level administrators should continue to be reactive. Most of the proactive education needs to occur in the upper levels of systems and network administration and engineering. These proactive cyber defense specialists would need to have the education as well as the tools to conduct proper cyber defensive activities at the correct time.

Finally, we must fund these activities. Education, research, manning, and operations for a more proactive self defense in cyberspace take time and money. We must fund these activities now to prevent a disaster in the future.

Conclusions

A state of constant cyberwarfare is upon us[53] and this persistent environment propels cyber security specialists to continue improving their cyber defense tools and devising new methodologies to combat the new and emerging threats. Most of these tools are reactive in nature, forcing the guiding rules and mechanisms to be reactive as well. However, a blend of reactive and proactive tools and standards need to be developed by the U.S. Department of Defense (DoD) in order to properly secure and defend the Global Information Grid (GIG) from attacks originating from home and abroad. Proactive tools like network modeling for anomaly detection and the establishment of ad hoc DTN architectures will enhance cyber security in DoD as well as for our coalition partners.

Endnotes

[1] Sun Tzu, *The Art of War,* trans. Samuel B. Griffith (Oxford: Oxford University Press, 1963), 77.

[2] Ibid., 99.

[3] Ibid.

[4] George W. Bush, *The National Security Strategy to Secure Cyberspace* (Washington, D.C.: The White House, February 2003), viii.

[5] Stephen Northcutt, *Network Intrusion Detection: An Analyst's Handbook* (Indianapolis, IN: New Riders Publishing, 1999), 9.

[6] Internet Engineering Task Force (IETF), "A Mission Statement for the IETF (RFC 3935)," http://www.ietf.org/rfc/rfc3935.txt (accessed December 17, 2008).

[7] Vinton Cerf, Yogen Dalal, and Carl Sunshine, "RFC 675: Specification of Transmission Control Program," http://tools.ietf.org/html/rfc675 (accessed December 5, 2008).

[8] Bradley J. Wood, O. Sami Saydjari, and Victoria Stavridou, *A Proactive Holistic Approach to Strategic Cyber Defense*, (Menlo Park, CA: SRI International, 2000), 2, http://www.cyberdefenseagency.com/publications/A_Proactive_Holistic_Approach_to_Strategic_Cyber_Defense.pdf (accessed November 3, 2008).

[9] Dean Turner, ed., *Symantec Global Internet Security Threat Report: Trends for July–December 07* (Cupertino, CA: Symantec Corporation, 2008), 24.

[10] Ibid.

[11] U.S. Department of Defense, *DOD Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: U.S. Department of Defense, October 17, 2001), 587.

[12] Beyond Security, "Automated Scanning Server - Overview," http://www.beyondsecurity.com/automatedscanningserver_overview.html (accessed December 18, 2008).

[13] Northcutt, *Network Intrusion Detection: An Analyst's Handbook*, 183.

[14] Insecure.org, "Network Mapper Tool," http://nmap.org (accessed December 18, 2008).

[15] Northcutt, *Network Intrusion Detection: An Analyst's Handbook*, 231.

[16] U.S. Department of Homeland Security—U.S. Computer Emergency Readiness Team, "Cyber Threat Source Descriptions," http://www.us-cert.gov/control_systems/csthreats.html (accessed December 6, 2008).

[17] Northcutt, *Network Intrusion Detection: An Analyst's Handbook*, 229.

[18] Edward Amoroso, *Intrusion Detection* (Sparta, NJ: Intrusion.Net Books, 1999), 20.

[19] Wood, Saydjari, and Stavridou, *A Proactive Holistic Approach to Strategic Cyber Defense*, 2.

[20] J.N. Mattis, *The Joint Operating Environment 2008* (Suffolk, VA: Joint Forces Command, November 25, 2008), 22-23.

[21] Ibid., iv.

[22] Karyn Greenstreet, "Eeek! Shiny Object Syndrome!" http://ezinearticles.com/?Eeek!-Shiny-Object-Syndrome!&id=685223 (accessed December 7, 2008).

[23] Georgia Tech Information Security Center (GTISC), "Emerging Cyber Threats Report for 2009," (Atlanta, GA: Georgia Institute of Technology, 2008), 6, http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf (accessed December 7, 2008).

[24] Margaret E. Grayson, *The NIAC Convergence of Physical and Cyber Technologies and Related Security Management Challenges Working Group: Final Report and Recommendations by the Council* (Washington, D.C.: U.S. Department of Homeland Security, January 16, 2007), 12.

[25] Ibid.

[26] U.S. Department of Homeland Security—U.S. Computer Emergency Readiness Team, "Control Systems Security Program (CSSP)," http://www.us-cert.gov/control_systems/ (accessed December 7, 2008).

[27] PC Magazine, "Polymorphic Virus Definition," http://www.pcmag.com/encyclopedia_term/0,2542,t=polymorphic+virus&i=49482,00.asp (accessed December 7, 2008).

[28] Georgia Tech Information Security Center (GTISC), "Emerging Cyber Threats Report for 2009," 2.

[29] Paul Bächer, et al., "Know your Enemy: Tracking Botnets," http://www.honeynet.org/papers/bots (accessed December 20, 2008).

[30] Ibid.

[31] Turner, *Symantec Global Internet Security Threat Report: Trends for July–December 07,* 21.

[32] Adrian Blomfield, “Russia accused over Estonian 'cyber-terrorism',” http://www.telegraph.co.uk/news/worldnews/1551850/Russia-accused-over-Estonian-'cyber-terrorism'.html (accessed December 13, 2008).

[33] Turner, *Symantec Global Internet Security Threat Report: Trends for July–December 07,* 21.

[34] Georgia Tech Information Security Center (GTISC), “Emerging Cyber Threats Report for 2009,” 3.

[35] Blomfield, “Russia accused over Estonian 'cyber-terrorism'.”

[36] Dancho Danchev, “Coordinated Russia vs Georgia cyber attack in progress,” http://blogs.zdnet.com/security/?p=1670 (accessed December 13, 2008).

[37] John Markoff, “Before the Gunfire, Cyberattacks,” http://www.nytimes.com/2008/08/13/ technology/13cyber.html?_r=1&em&oref=slogin (accessed December 13, 2008).

[38] Ibid.

[39] Georgia Tech Information Security Center (GTISC), “Emerging Cyber Threats Report for 2009,” 3.

[40] Markoff, “Before the Gunfire, Cyberattacks.”

[41] Bush, *The National Security Strategy to Secure Cyberspace*, x.

[42] Ibid.

[43] Donald H. Rumsfeld, *Quadrennial Defense Review Report* (Washington, D.C.: Department of Defense, February 6, 2006), 25.

[44] Clay Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues* (Washington, D.C.: Library of Congress, Congressional Research Service, March 20, 2007), 5.

[45] Wood, Saydjari, and Stavridou, *A Proactive Holistic Approach to Strategic Cyber Defense*, 2.

[46] Bruce D. Caulkins, Joohan Lee, and Morgan Wang, “A Dynamic Data Mining Technique for Intrusion Detection Systems,” ACM SouthEast Conference (ACMSE), March 2005.

[47] Bruce D. Caulkins, Joohan Lee, and Morgan Wang, "Packet- Vs. Session-Based Modeling for Intrusion Detection Systems,” IEEE International Conference on Information Technology (ITCC), Las Vegas, April 2005.

[48] Matt Mahoney, *A Machine Learning Approach to Detecting Attacks by Identifying Anomalies in Network Traffic*, Ph.D. Dissertation (Melbourne, FL: Florida Institute of Technology, 2003), 123.

[49] Robert D. Small and Herbert A. Edelstein, “Scalable Data Mining,” http://www.twocrows.com/ whitep.htm (accessed December 14, 2008).

[50] Caulkins, Lee, and Wang, “A Dynamic Data Mining Technique for Intrusion Detection Systems,” 2.

[51] National Aeronautics and Space Administration, “NASA Tests First Deep-Space Internet,” http://www.nasa.gov/topics/technology/features/internet-20081118.html (accessed January 3, 2008).

[52] Ibid.

[53] Georgia Tech Information Security Center (GTISC), “Emerging Cyber Threats Report for 2009,” 3.