The Evolution Of U.S. CYBERPOWER

ABSTRACT

How has the United States dealt with cyber attacks in the past? How should we deal with cyber attacks in the future? This paper will analyze the cyber events that took place during four kinetic conflicts to answer these questions: the Desert Storm campaign, the Allied Force operation, the Unified Protector conflict, and finally, the Global War on Terror.

During the research, it was discovered that, for the purposes of this paper, no satisfactory definition of cyberspace existed, so as a first step a new definition was created. The case studies analyzed revealed several important lessons. Desert Storm demonstrates that quick responses and the sharing of information between institutions are critical. The Operation Allied Force case reveals that every kinetic conflict will likely have cyber elements. Operation Unified Protector illustrates that it only takes a small cyberforce to have major influence in a conflict. Finally, since the advent of War on Terror there has been an increase in the number and sophistication of cyber attacks.

The recommendations proposed in this paper are drawn directly from the case studies themselves. The key recommendations being that a separate military service is necessary for cyber supremacy, cyber warfare should be dealt with as guerrilla warfare, and non-conventional tactics may be the most effective.

Table of Contents

Introduction 1

Purpose 1

Definitions 1

History 7

Case Studies 11

Desert Storm 1990 11

Allied Force 1999 18

Unified Protector 2011 23

Global War on Terror 2001-Present 27

Conclusion 33

Summary 33

Recommendations 34

Final Thoughts 37

Bibliography 38

Introduction

PURPOSE

The Evolution of U.S. Cyberpower

The twofold purpose of this paper is to provide a systematic framework for analyzing the history of the cyber security domain, and to examine certain weaknesses in cyber security practices. As a foundation for understanding cyber security issues, the Desert Storm (1990), Operation Allied Force (1999), Operation Unified Protector (2011), and the Global War on Terror (2001-present) case studies will be scrutinized. By providing a clear, concise picture of the events that transpired in each of these case studies, and by drawing logical conclusions from them, we glean important strategic lessons. The cumulative results will be used to formulate recommendations for future strategies and tactics in cyberspace security.

DEFINITIONS

"Imprecision in terminology hampers serious discussion of these issues."

James A. Lewis, Center for Strategic and International Studies[1]

Defining Cyberspace

Before introducing any case studies, it is important to clearly define the term "cyberspace." The modern interpretation of the word "cyber" and its use as a prefix is a fairly recent phenomenon; however, despite the relative infancy of the term, it has been

[1] James Andrew Lewis, *Thresholds for Cyberwar*, ed. Center for Strategic and International Studies, page 1, accessed June 4, 2012, http://csis.org/publication/thresholds-cyberwar.

accepted industry-wide as a way of indicating anything electronic or computer related. The term "cyberspace" has also become synonymous with the concept of a digital virtual domain, especially the Internet.

As the cyber domain has become an increasingly critical component in modern life, several leading organizations have attempted to establish a definition for the word "cyberspace," including the CIA, the NSA, the Russian-American Cyber Security Summit, and the oft-cited U.S. Department of Defense. However, the novelty and rapidly changing nature of the domain have hampered consensus. Definitions within the various organizations continue to evolve over time to better fit the developing concept of cyberspace. The following are two recent definitions for cyberspace, put forward by leading sources, illustrating the challenge of clear definition:

U.S. Department of Defense:

> *"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."*[2]

Russian-American Cyber Security Summit:

> *"An electronic medium through which information is created, transmitted, received, stored, processed, and deleted."*[3]

---

[2] *Department of Defense Dictionary of Military and Associated Terms*, joint publication 1-02 ed. (2010), page 83, by Office of the Joint Chiefs of Staff, accessed June 4, 2012, last modified March 15, 2012, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[3] East West Institute and Information Security Institute of Moscow State University, *The Russia - U.S. Bilateral on Cybersecurity - Critical Terminology Foundations*, ed. Karl F. Rauscher and Valery Yaschenko, Issue 1

While these are excellent definitions, and each captures many elements associated with cyberspace, neither is complete. This paper will attempt to present a new, more comprehensive definition. The primary challenge is to follow a logical and realistic framework of thought, while avoiding the trap of attempting to include every small element of the cyber domain. It is necessary to be simultaneously thorough and concise, to avoid a definition so wordy as to render it useless.

The pursuit of a definition for cyberspace in this paper will be based primarily on an examination of vulnerabilities in the cyber domain. These vulnerabilities, by their very nature, tend to illuminate critical, observable, and definable aspects of the cyber world.

Therefore, as a first step in constructing a definition for cyberspace, it is useful to describe the types of attacks to which the cyber domain is vulnerable. The Government Accountability Office (GAO) presents a fairly comprehensive list and description of vulnerabilities in their Congressional report, *CYBERSPACE - United States Faces Challenges in Addressing Global Cybersecurity and Governance.*[4] The descriptions from the GAO congressional report are given in Table 1.1.

(2011), page 1, accessed June 4, 2012, http://cybersummit2011.com/component/content/article/32.

[4] Government Accountability Office, *Report to Congressional Requesters: CYBERSPACE - United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606, page 5, accessed June 4, 2012, http://gao.gov/products/GAO-10-606.

Table 1.1 GAO List of Cyber Attacks

Name	Description
Denial of service	A method of attack from a single source that denies system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.
Distributed denial of service	A variant of the denial of service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bombs	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.
Phishing	The creation and use of e-mails and Web sites—designed to look like those of well-known legitimate businesses, financial institutions, and government agencies—in order to deceive Internet users into disclosing their personal data, such as bank and financial account information and passwords. The phishers then use that information for criminal purposes, such as identity theft and fraud.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	A program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.

Vishing	A method of phishing based on voice-over-Internet-Protocol technology and open-source call center software that have made it inexpensive for scammers to set up phony call centers and criminals to send e-mail or text messages to potential victims, saying there has been a security problem, and they need to call their bank to reactivate a credit or debit card, or send text messages to cell phones, instructing potential victims to contact fake online banks to renew their accounts.
War driving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adapter that involves patrolling locations to gain unauthorized access.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	A cyber threat taking advantage of a security vulnerability on the same day that the vulnerability becomes known to the general public and for which there are no available fixes.

In total, the GAO presents twelve types of attacks. Upon closer examination, a pattern emerges which allows the twelve attacks to be simplified further by grouping them into fewer but broader categories. The twelve types of attacks resolve into three categories, based upon the nature of the vulnerability. Table 1.2 illustrates the pattern.

Table 1.2 The Three Categories of Cyber Attacks

Attacks Targeting Hardware (Kinetic)	**Attacks Targeting Software (Hacking)**	**Attacks Targeting Humans (Espionage)**
Denial of Service (DOS) Distributed DOS	Exploit Tools Logic Bombs Sniffer Trojan Virus Worm Zero-Day	Phishing Trojan Vishing

Based on Table 1.2, cyberspace consists of three elements, hardware, software, and humans, each of which is vulnerable to attack. Some might immediately insist a key element is missing from this description -- information -- that is, the content exchanged between each of the three elements. However, as defined in this paper, information is regarded as the commodity moving THROUGH the system, rather than as an element of the system itself. In this framework, manipulation of information is seen as the PURPOSE of cyberspace, not an element of it. This key distinction allows us to isolate the non-virtual and defensible infrastructure from the incorporeal and indefensible commodity within the system.

The following definition for cyberspace emerges in this framework:

Cyberspace
A virtual domain created by the union of three non-virtual agents: hardware, software, and humans – for the purpose of manipulating information.

HISTORY

Having defined a framework for the discussion of cyber security issues, it is useful to review a general history of cyberspace before moving on to specific case studies. Decade by decade, we briefly recount the evolution of major milestones in cyberspace history, focusing primarily on events in the United States.

1920's

- Arguably, the first instance of "cyberspace" usage (according to the definition above) was in 1926, when the German Navy began using the Enigma Machine, invented by German engineer, Arthur Scherbius. The Enigma Machine was an electro-mechanical encryption device, which combined hardware and software (crude by today's standards, but nevertheless, they were algorithms in the form of rotors), with human operators for the purpose of manipulating information.[5]

1930's

- Interestingly, in the United States, the Navy was also the first military branch to adopt a device similar to the Enigma Machine, dubbed SIGABA, in the late 1930's. By the end of World War II, cipher machines were in widespread use.[6]
- Also in the late 1930's, another German inventor, by the name of Konrad Zuse, designed the first freely programmable mechanical computer, called the Z1.[7]

---

[5] Tony Sale, "The Breaking of German Naval Enigma ," Naval Enigma Index, accessed June 4, 2012, http://www.codesandciphers.org.uk/virtualbp/navenigma/navenig1.htm.

[6] Richard Pekelney, "What Is The SIGABA-ECM Mark II and Why It Was Important?" Crypto Machines, accessed June 4, 2012, last modified April 30, 2012, http://www.jproc.ca/crypto/ecm2.html.

1940's

- The first electronic digital computer, the Atanasoff-Berry Computer (ABC), pioneered several crucial components of modern computing; including electronic switch features and the ability to do binary arithmetic.[8]
- Probably the single most important development in computing, the transistor, was designed in AT&T's Bell Labs, in 1947 by John Bardeen and Walter Brattain.[9]

1950's

- IBM drafted the first "high level" computer language, FORTRAN, in 1954-1957, with a team of assembly language programmers, headed by John W. Backus.[10]
- Another historic cyber milestone reached in the 1950's was the development of the integrated circuit chip. The development of the IC chip had several notable contributors; including, Geoffrey Dummer and then later Jack Kilby, ultimately culminating in the development of the silicon chip by Robert Noyce in 1959.[11]

---

[7] *Complete Dictionary of Scientific Biography* (Encyclopedia.com, 2008), s.v. "Zuse, Conrad," accessed June 4, 2012, http://www.encyclopedia.com/doc/1G2-2830906236.html.

[8] *Encyclopedia of World Biography* (Encyclopedia.com), s.v. "John Atanasoff," accessed June 4, 2012, last modified 2004, http://www.encyclopedia.com/doc/1G2-3404707524.html.

[9] *Complete Dictionary of Scientific Biography* (Encyclopedia.com), s.v. "Bardeen, John," accessed June 4, 2012, last modified 2008, http://www.encyclopedia.com/topic/John_Bardeen.aspx.

[10] Ian Chivers and Jane Sleightholme, *Fortran History and Development*, page 1, accessed June 4, 2012, http://www.fortranplus.co.uk/resources/Fortran_history_and_development.pdf.

[11] *Encyclopedia of World Biography* (Encyclopedia.com), s.v. "Robert Noyce," accessed June 4, 2012, last modified 2004, http://www.encyclopedia.com/doc/1G2-3404704801.html.

1960's

- Developed as a defense project by the Advance Research Projects Agency, the ARPAnet was the first computer network to use a technique called packet switching, a type of information transfer that allowed more than one communication exchange to occur on the same phone line at the same time. BBN Technologies was awarded a contract to build the first network in 1969. This network was the direct ancestor of the modern Internet.[12]

1970's

- In 1975, the first commercial packet-switching network available to the general public went into service: Telenet.[13]
- ARPAnet also began merging with other networks in the mid 1970's. This merging of networks was referred to as the internetwork, which was replaced by the shortened and more familiar term, the Internet.[14]

1980's

- DoD declared the TCP/IP protocol to be the official military network standard in 1982.[15]

---

[12] *Gale Encyclopedia of E-Commerce* (Encyclopedia.com), s.v. "ARPAnet," accessed June 4, 2012, last modified 2002, http://www.encyclopedia.com/topic/ARPANET.aspx.

[13] Janet Abbate, "Government, Business, and the Making of the Internet," *Business History Review* 75, no. 1 (Spring 2001): 164.

[14] Ibid, 165.

[15] *Computer Sciences* (Encyclopedia.com), s.v. "TCP/IP," by William J. Yurcik, accessed June 4, 2012, last modified 2002, http://www.encyclopedia.com/doc/1G2-3401200604.html.

- In 1983, the DoD split the ARPAnet into two networks: ARPAnet and MILnet.[16]
- The first .com domain name was registered on March 15, 1985 by Symbolics Inc. Symbolics.com is the first and oldest registered commercial domain name on the Internet.[17]
- In 1988, the first Internet wide virus, known as the Morris Worm, took advantage of a simple security flaw, and wreaked significant havoc.[18]

1990's

- ARPAnet is officially decommissioned in 1990.[19]
- The World Wide Web protocol, developed by Tim Bernes-Lee is release in 1991.[20]
- Two Stanford students, Larry Page and Sergey Brin, registered Google.com on September 15, 1997, to host their new search engine.

---

[16] Janet Abbate, *Inventing the Internet* (Cambridge, Massachusetts: MIT Press, 2000), 185.

[17] Robin Wauters, "25 Years Later, First Registered Domain Name Changes Hands," AOL Tech, accessed June 4, 2012, last modified August 27, 2009, http://techcrunch.com/2009/08/27/25-years-later-first-registered-domain-name-changes-hands/.

[18] United States of America v. Robert Tappan Morris, No. 90-1336 (2d Cir. March 7, 1991), accessed June 4, 2012, http://www.loundy.com/CASES/US_v_Morris2.html.

[19] *Gale Encyclopedia of E-Commerce* , 2002.

[20] *Encyclopedia of World Biography* (Encyclopedia.com), s.v. "Tim Berners-Lee," accessed June 4, 2012, last modified 2004, http://www.encyclopedia.com/doc/1G2-3404707535.html.

Case Studies

DESERT STORM 1990

"Nothing is more important in war than unity in command."

Napoleon Bonaparte[21]

In the history of cyber attacks against the United States, the incidents that occurred in 1990 in conjunction with the events of the Desert Storm campaign stand out as particularly dramatic and severe. The case bears all the hallmarks of a highly successful attack, and had Saddam Hussein been slightly more cyber-savvy, he could well have altered the outcome of the Desert Storm/Desert Shield conflict.

To fully appreciate the nature of the 1990 cyber attack, it is necessary to place the specific events of the attack within the broader context of the progress of cyber evolution at the time. One of the main challenges of the very early Internet era, in the 1980's, was compatibility between network elements. At the time, industry views on the economic viability of networking varied, and by extension, so did the practical applications. There were multiple companies and universities simultaneously building computers and networks, and each organization had its own protocol for interconnecting network elements.[22] To resolve the issue of incompatibility, gateway computers were

---

[21] National Defense University, editorial, *Joint Force Quarterly*, April 2005, page Inside Cover, accessed June 4, 2012, http://www.ndu.edu/press/lib/pdf/jfq-37/JFQ-37.pdf.

[22] Abbate,(Spring 2001): 164.

developed that could interface with all of these networks. These gateways were placed between each network to interpret and relay signals.[23]

Eventually, endeavoring to keep the gateway computers compatible with every existing and developing network became too complicated to maintain. To remedy the situation, the Defense Advanced Research Projects Agency (DARPA) created a new network transmission method that nested specific network protocols into a single common protocol. This new protocol became known as TCP/IP. It was named after the Transmission Control Protocol (TCP) and the Internet Protocol (IP), and it transferred the responsibility for reliable compatibility to each end/host node, and away from the central network. It was officially adopted as the military network standard in 1982. This new system allowed ARPAnet to effectively connect with practically any industry network, regardless of the protocol, and revolutionized cyber connectivity. However, this increased connectivity introduced an inherent security breach, due to the large number of nodes brought together into a single network.[24]

In 1983, the DoD separated the military portion of its network from the public ARPAnet, and the new network was called MILnet.[25] MILnet was intended to be more secure than its civilian counterpart, but the DoD didn't want complete separation. To achieve security of MILnet without complete separation, the DoD installed highly secure gateway computers between ARPAnet and MILnet, believing this would prevent

---

[23] Janet Abbate, (2000), 128.

[24] Mukundan Venkataraman, Kartik Muralidharan, and Puneet Gupta, *Designing new Architectures and Protocols for Wireless Sensor Networks: A Perspective*, ed. IEEE Communications Society, page 38, accessed June 4, 2012, http://www.cs.ucf.edu/~mukundan/secon05.pdf.

[25] Abbate, (2000), 128.

hackers from gaining a quick access point into the different networks. This turned out to be a simplistic view of network security, and unwittingly exposed MILnet to a kind of "springboard effect" security flaw created by the adoption of the TCP/IP.

Hackers learned how to gain outside control of individual computers fairly early, and as single computers began to be connected through networks and gateway computers, they found ways to take advantage. Four security flaws, which by today's standards are relatively archaic, were exploited in 1988 by the first "internet-wide" worm, the infamous Morris Worm, a program written by a Cornell University student, Robert Tappan Morris. The Morris Worm exploited vulnerabilities in SEND MAIL, Finger, "trusted host" privileges, as well as password guessing.[26]

Using these simple security loopholes to gain control of a host computer, the Morris Worm would then send itself to other computers on the same network. The gateway computers had security measures in place to prevent someone from gaining unauthorized access; however, they didn't necessarily regulate the information being passed through. Therefore, if the worm controlled a host on one network, it could simply springboard to the next network without overcoming any defensive measures on the gateway computers. Due to the Morris Worm's self-propagating nature, it caused considerable strain on computers, and essentially became the first distributed denial of service (DDOS) attack on any network, causing widespread server failure. The introduction of TCP/IP technology provided even broader opportunities to these existing security flaws.

---

[26] United States of America v. Robert Tappan Morris, No. 90-1336 (2d Cir. March 7, 1991), accessed June 4, 2012, http://www.loundy.com/CASES/US_v_Morris2.html.

These historical events lead us directly into the Desert Storm case study and the incidents that unfolded in 1990. Two years after the Morris Worm incident, the same security loopholes still existed, with very few updates to defense mechanisms, and cyber attackers again exploited precisely the same vulnerabilities. These loopholes were compounded by the increased connectivity of TCP/IP and allowed a group of hackers based out of the Netherlands to gain control of server hosts in the ARPAnet, and then to use those hosts as a springboard into the MILnet. Security expert, Andrew Landsman describes the attacks very well.

> *The first indications of the widespread break-ins into MILnet hosts were from log entries in Department of Energy (DoE) machines. The attackers broke into DoE machines using what now seems like very rudimentary attack methods, including password guessing (or sometimes even using null passwords), exploiting a VMS vulnerability in the SYSMAN utility, exploiting trust relationships between hosts, and a few others. Once they gained access to a host, they often already had super-user privileges, but if they did not, they exploited other vulnerabilities to take complete control of the victim systems. They then installed back doors. By breaking into hosts at DoE sites such as Los Alamos National Laboratory, Lawrence Livermore National Lab, Fermi National Lab, Sandia National Lab, and Brookhaven National Lab, the attackers had more than enough springboards from which they could launch attacks against MILnet hosts at military centers such as US Navy Headquarters, the Pacific Fleet Command, Rome Air Force Base, Kelly Air Force Base, the Pentagon, and many more, which they did successfully day after day for well over a year.*

> *Once the attackers broke into DoD hosts, they used commands such as grep in Unix systems to discover files that contained the information they desired: information about military equipment, weapons systems, troop and warship movements (especially in connection with Operations Desert Storm and Desert Shield) and much more—they often even searched for "nuclear." The attackers stole so much information that they quickly filled the hard drives of their own machines. They then resorted to downloading huge amounts of information onto systems at the University of Chicago and Bowling Green University.*[27]

The worst part of the fiasco was that the DoE's Computer Incident Advisory Capability (CAIC) noticed and reported the attacks to the DoD; in fact, CERT/CC also received similar reports. Landsman explains, "At one point the DoD, DoE, U.S. Navy's incident response team, the National Security Agency, the US State Department, the National Institute of Standards and Technology (NIST), the Central Intelligence Agency, the Air Force Office of Special Investigations, Army Intelligence, the Federal Bureau of Investigation, CIAC and CERT/CC were involved. Cooperation and coordination were extremely difficult to obtain, but despite many obstacles (most of them political and bureaucratic in nature), these entities managed to conduct reasonably successful investigation efforts."[28] In all fairness, organizing and executing an effective approach to dealing with cyber security breaches was a relatively new operation.

---

[27] Andrew Landsman, "A Short and Shortsighted History of Hacks: Part 1 – The Desert Storm/Desert Shield Attacks," *Network Security Consulting Blog*, May 12, 2009, accessed June 4, 2012, http://blog.emagined.com/2009/05/12/a-short-and-shortsighted-history-of-hacks-part-1-%E2%80%93-the-desert-stormdesert-shield-attacks/.

[28] Ibid.

Fortunately, the criminals were not politically motivated. Instead the hackers tried to sell the information to Saddam Hussein for one million dollars. Hussein, for whatever reason, never took them up on the offer, possibly thinking it a hoax. Needless to say, had he done so, the Desert Storm conflict may have taken a drastically different course.[29]

A New York Times article published in 1991, which cited computer experts who reconstructed the 1990 attacks using key logs of the hackers' activities, drew this conclusion: "The tactics of the group are of particular interest to computer security experts because members have repeatedly used security loopholes demonstrated by a program written by Robert Tappan Morris, a Cornell University student, more than two years ago."[30] The reconstructed attacks provide ample evidence of the correlation between the Morris Worm attack of 1988 and the cyber-attacks during Desert Storm in 1990. The two attacks were so similar that one expert stated, "It looked like (the attacker) had a cookbook sitting next to him telling him what to do next at each step."[31]

The Gulf War cyber attack incident illustrates a central difficulty facing institutions and governments with regard to cybersecurity management. Experience indicates that "lessons learned" must be implemented rapidly in the cyber arena. If not, enemies will

---

[29] Nelly Favis Villafuerte, "The Reality of Cyber Terrorism," Manila Bulletin Publishing Corporation, accessed June 4, 2012, last modified March 25, 2011, http://www.mb.com.ph/articles/311407/the-reality-cyber-terrorism.

[30] John Markoff, "Dutch Computer Rogues Infiltrate American Systems With Impunity," *New York TImes*, April 21, 1991, accessed June 4, 2012, http://www.nytimes.com/1991/04/21/us/dutch-computer-rogues-infiltrate-american-systems-with-impunity.html?pagewanted=all&src=pm.

[31] Ibid.

have the opportunity to exploit vulnerabilities. As stated in the New York Times article at the time: "The fact that the same security flaws can be used to illicitly enter computers several years after they were widely publicized indicates that many professional computer managers are still paying only minimal attention to protecting the security of the information contained on the computers they oversee."[32]

If cyber incidents had become less frequent today than in the early 1990s, one might have hope. However, attacks today are only more complex and more frequent, while the pace of institutional responses continues to lag the accelerating rate of the problem. Large institutions continue to have inherently slow decision-making processes, with responsibility for implementing change divided across many competing, internal power centers.

[32] Ibid.

OPERATION ALLIED FORCE 1999

"The conventional army loses if it does not win. The guerrilla wins if he does not lose."

Henry A. Kissinger[33]

In 1999, Slobodan Milošević entered into a cunning political battle with NATO, and particularly with the Unites States. Two warring factions vied for dominance of the Kosovo countryside: the Albanians and the Serbians. Milošević led the Serbian faction, and he attempted to carry out a brutal ethnic cleansing program to eliminate all Albanians from Kosovo. He was soon pressured by international outrage to stop his hideous acts. NATO threatened drastic actions if he didn't withdraw his troops from Kosovo, but Milošević would not comply. An extended period of NATO-directed bombing ensued, initiating a prolonged battle of wills. Who would outlast the other? Milošević counted on being able to maintain popular support in his own country while waiting out the disciplinary measures, hoping the international community would grow tired of the conflict first, and lose popular support in their own countries. It was an asymmetric conflict, a political guerrilla war. Milošević had to survive politically until he had the advantage, and so he would seize upon and trumpet whatever small victories

[33] Henry Kissinger, "The Vietnam Negotiations," *Foreign Affairs*, January 1969, page 214.

he could find. He was determined that he and his countrymen would not despair first in this battle of wills.[34]

As a part of the effort, the Serbians initiated several cyber attacks on the West during the Kosovo conflict. These attacks were relatively mild compared with the Desert Storm events. Although attacks were spread across several sites within NATO, the U.S., and the UK, the impact of the attacks was relatively insignificant. In the U.S., the White House website was defaced, the UK admitted to having lost at least some database information, and the NATO headquarters' public affairs website was "virtually inoperable for several days," due to DDOS attacks.[35]

However, there was a complicating factor that contributed to the conflict. Serbians weren't the only ones initiating the cyber attacks; in fact, the attacks were coming from all over the world.[36] These attacks included sympathizers in major countries such as China, although whether the Chinese government was involved is questionable.[37]

Some classic elements of guerrilla warfare emerge in the analysis of this incident. It is evident non-state actors attempted to disrupt military operations through hacking, and

---

[34] *Kosovo: War in Europe - The Road to War*, "FRONTLINE," PBS, June 4, 2012 (originally aired February 22, 2000), YouTube, accessed June 4, 2012, http://www.youtube.com/watch?v=__kbfuyYIiA&feature=related.

[35] Kenneth Greers, *Cyberspace and the Changing Nature of Warfare,* accessed June 4, 2012, http://www.carlisle.army.mil/DIME/documents/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf.

[36] Dan Verton, "Serbs launch cyberattack on NATO," *Federal Computer Week*, April 4, 1999, accessed June 4, 2012, http://fcw.com/articles/1999/04/04/

[37] Bob Brewin, "General: Cyberattacks against NATO traced to China," *Federal Computer Week*, August 31, 1999, accessed June 4, 2012, http://fcw.com/articles/1999/08/31/general-cyberattacks-against-nato-traced-to-china.aspx?sc_lang=en.

were able to claim minor victories. According to Marine Corps authors Peter Paret and John Shy, disruption is often all that is necessary for the guerrilla warrior to succeed. "The weakness of the guerrilla himself and his consequent need to gain and maintain strength among the civilian population largely determine his techniques and objectives. Unable to destroy his opponent physically by direct, military action, he fights psychologically by indirect, political means. Never attacking unless overwhelmingly superior, and never fighting long enough to be caught by a counterattack, the guerrilla leader uses combat itself as a psychological weapon. With an unbroken string of victories, however insignificant many of them may be, he creates confidence in ultimate success among his supporters. At the same time, he fosters a growing despair among his opponents."[38]

Interestingly, cyberspace is often thought of as a physical "space." Metaphorically, cyberspace would resemble a jungle, where the thoughts of millions of individuals intertwine, mingle, and grow. This virtual jungle is precisely the type of terrain that guerrilla warriors thrive in. It allows the fighter to hide until the most opportune moment arrives to strike. The environment is friendly and provides him with resources and information to fight his enemy. The environment is difficult to navigate off the beaten path, unless one is familiar with the terrain, making tracing the actions of someone difficult. Every advantage is given to the attacker, allowing him to strike at his own

---

[38] Peter Paret and John Shy, *U.S. Marine Corps - FMFRP 12-25: The Guerilla and How to Fight Him*, Guerilla Warfare and U.S. Military Policy: A Study (Washington, D.C.: U.S. Marine Corps, 1990), accessed June 4, 2012, http://www.scribd.com/doc/3605861/US-Marine-Corps-FMFRP-1225-The-Guerilla-and-How-to-Fight-Him#outer_page_53.

convenience and advantage. He strikes only when he is guaranteed success, fading into the cyber-jungle whenever he is confronted. In this new cyber-guerrilla warfare, it only takes one skilled individual to wreak havoc on the unified efforts of several world superpowers. This amplifying effect is dishearteningly alarming in its potential impact.

In Kosovo, small victories were key. Therefore, seemingly insignificant cyber events, such as the defacing of the White House website were actually symbols of success and hope for the Serbians, ultimately prolonging the conflict. Regarding the DDOS attacks against NATO, Greers states that, “the cyber attacks became a propaganda victory for the hackers.”[39] Actually, this victory was twofold: not only was the incident a propaganda success for the hackers, but their attack also blocked NATO from releasing their side of the story. The implications provided by the Kosovo conflict are far reaching. Greers further states: "Above all, the Internet is vulnerable to attack. Further, its amplifying power means that future victories in cyberspace could translate into victories on the ground. Both state and non-state actors enjoy a high return on investment in cyber tactics, which range from the placement of carefully crafted propaganda to the manipulation of an adversary's critical infrastructure."[40]

The Kosovo incident illustrates several critical lessons regarding cyber security. First of all, the cyber components necessary for cyber conflict reached a meaningful maturity in the mid 1980’s; since then, continuing an emerging pattern, nearly every kinetic

---

[39] Kenneth Greers, *Cyberspace and the Changing Nature of Warfare.*

[40] Ibid.

conflict has had a cyber element associated with it.[41] Though the effects of the Kosovo cyber attacks were restricted to psychological effects, cyber effects can just as surely expand into direct kinetic impacts on weapons systems and critical infrastructure, causing much more immediate and obvious effects. Secondly, in an isolated conflict, non-affiliated parties can participate via cyber warfare, creating a global cyber conflict, even while the kinetic conflict remains regionally isolated. And finally, it only takes a small cyberforce to have major influence in a conflict. A shrewd warrior can wield this tool with devastating effect.

---

[41] Jason Healey and Karl Grindal, "Lessons from the First Cyber Commanders," New Atlanticist, accessed June 4, 2012, last modified March 14, 2012, http://www.acus.org/new_atlanticist/lessons-first-cyber-commanders.

OPERATION UNIFIED PROTECTOR 2011

"No longer is diplomacy conducted purely government to government or government to people. It is now conducted people to people and people to government."

U.S. Department of State[42]

In many respects, the conflict in Libya in 2011 mirrored the events in Kosovo more than a dozen years earlier. Libya's autocratic ruler, Muammar Gaddafi, used military force to kill his own citizens in an effort to retain power and control. NATO responded by threatening military action if Gaddafi did not stop the killing. Gaddafi refused to comply, and NATO forces began bombing strategic targets and enforcing a No Fly Zone. There were also key differences regarding NATO's approach to the operation in Libya that set it apart from the Kosovo conflict. This time, NATO was careful to garner significant international support before taking action. This reduced political propaganda leverage against NATO. Additionally, NATO had previously bolstered their cyber defenses preventing the predictable onslaught of cyber attacks from having any appreciable effect on the course of events.[43]

---

[42] U.S. Department of State, "21st Century Statecraft," U.S. Department of State - Diplomacy in Action, accessed June 4, 2012, http://www.state.gov/statecraft/overview/index.htm.

[43] Joshua McGee, "NATO and Cyber Defense: A Brief Overview and Recent Events," Center for Strategic and International Studies, accessed June 4, 2012, last modified July 8, 2011, http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events.

However, in a fascinating twist of cyber warfare dynamics, a cyber battle was being fought inside of Libya, between Gaddafi and his own citizens. “The anti-Gaddafi movement uploaded videos of the dictator’s fighter jet attacks on his own people – not only to rally the crowds at home but also to put pressure on the international community.”[44] The asymmetrical power of the cyber world was clearly evidenced by the fact that a single individual uploading a video to the Internet could influence the outcome of a kinetic conflict.

Gaddafi recognized the potential impact of this cyber activity and took drastic measures to limit its influence. Spencer Ackerman described Gaddafi’s response to the events as they were unfolding: “[Gaddafi] attempted to shut down the Internet in order to limit the outside world’s ability to learn about his crackdown. But the shutdown isn’t absolute, and graphic images… have proliferated online.”[45]

The pattern that emerges from these events is telling. Despite the fact that he controlled the levers of power in the central government, Gaddafi’s efforts in the cyber domain did not yield the traditional advantage to the greater power. In fact, the threat of a crack down was not only ineffective, it had the opposite effect: the larger the threat, the greater the cyber resistance became.

---

[44] Tobias Franke, "Social media: the frontline of cyberdefence?" NATO Review, accessed June 4, 2012, http://www.nato.int/docu/review/2011/Social_Medias/cyber-defense-social-media/EN/index.htm.

[45] Spencer Ackerman, "Desperate Gaddafi bombs protesters, blocks internet," *Wired.co.uk*, February 22, 2011, accessed June 4, 2012, http://www.wired.co.uk/news/archive/2011-02/22/libya-gaddafi-bombs-protestors.

The inability of Gaddafi to threaten his opponents in the cyber domain is not surprising. In general, people demonstrate a lack of concern for consequences in their cyber activity. John Suler, in his work entitled *The Psychology of Cyberspace*, calls this lack of concern for consequences the "disinhibition effect." He attributes this to the fact that the cyber domain offers anonymity, distance between actors, worldwide reach, instant gratification, and empowerment via access to a wealth of information. All these elements combined create an environment where the individual feels free from traditional consequences. Suler describes some of the practical outcomes resulting from this environment.

> *It's well known that people say and do things in cyberspace that they wouldn't ordinarily say or do in the face-to-face world. They loosen up, feel more uninhibited, and express themselves more openly. Researchers call this the "disinhibition effect." It's a double-edged sword. Sometimes people share very personal things about themselves. They reveal secret emotions, fears, wishes. Or they show unusual acts of kindness and generosity. We may call this benign disinhibition.*
>
> *On the other hand, the disinhibition effect may not be so benign. Out spills rude language and harsh criticisms, anger, hatred, even threats. Or people explore the dark underworld of the internet, places of pornography and violence, places they would never visit in the real world. We might call this toxic disinhibition.*[46]

---

[46] John Suler, "The Online Disinhibition Effect," Rider University: The Psychology of Cyberspace, accessed June 4, 2012, last modified August 4, 2004, http://users.rider.edu/~suler/psycyber/disinhibit.html.

Anyone who has used the Internet has likely experienced this disinhibition effect to some degree. On a daily basis, ordinary individuals post unbelievably frank and sometimes personal content in YouTube videos, inputs to blogs, forum posts, email, etc. Thus, it is not surprising that during a life and death conflict against a despot, Libyans would feel empowered to strike back in the cyber domain.

The unique psychology attached to human behavior in the cyber domain suggests something significant about effective cyber warfare strategies. It seems likely the best defensive strategies for maintaining peace and security in this realm are proactive communication messaging and good diplomacy. Nevertheless, as John Suler states, the disinhibition effect is a double-edged sword. Every element that makes the cyber domain useful for initiating a positive message, also empowers guerrilla warriors to use it is a tool to propagate their message in an uninhibited fashion. Fighting cyber wars must take into account the psychology of the domain, and a politically savvy actor will find a way to rob the guerrilla warrior of legitimacy. An effective military strategy always requires more than just defensive measures.

GLOBAL WAR ON TERROR 2001-PRESENT

"Today, terrorists have not used the Internet to launch a full-scale cyberattack, but we cannot underestimate their intent."

Robert Mueller FBI Director, March 2012[47]

Though the FBI cannot confirm a terror group has ever carried out a cyber attack against the United States, there have been many high-level cyber incidents since the beginning of the global war on terror. Some of the more ominous examples include the Slammer Worm infection of an Ohio nuclear power plant in 2004,[48] and the coordinated cyber attacks against Estonia in 2007.[49] In fact, there have been so many cyber attacks, that a congressional report on cyberterrorism made the following statement:

> *"Whenever a cyberattack against computers or networks [occurs it] is reported to CERT/CC … However, as of 2004, CERT/CC has abandoned this practice for keeping a record of cyberattacks. This is because the widespread use of automated cyberattack tools has escalated the number of network attacks to such a high level,*

---

[47] Robert S. Mueller III, "Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies" (Speech, RSA Cyber Security Conference, San Francisco, March 1, 2012), Federal Bureau of Investigation, accessed June 4, 2012, http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[48] Kevin Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Network," Security Focus, accessed June 4, 2012, last modified August 19, 2003, http://www.securityfocus.com/news/6767.

[49] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 16, 2007, U.S. edition, accessed June 4, 2012, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

that their organization has stated that a count of security incidents has become meaningless as a metric for assessing the scope and effects of attacks against Internet-connected systems."[50]

The extremely high number of cyber attacks is a critical issue in and of itself. As an additional feature in the asymmetrical nature of cyberspace, the sheer number of attacks makes even a small percentage of successful attacks problematic. If terrorists decide to engage in large-scale attacks, they need only succeed once. Alternately stated, security measures need only fail once. Using this large-number, statistical threat framework as a starting point for analysis, an important question arises: in an age of global terror, how can the large-number-of-attacks-small-percentage-of-failures asymmetrical nature of the cyber domain be leveraged in favor of the U.S. military?

In an attempt to answer this question, this paper will consult an unusual and rather unlikely set of cases for inspiration. These cases are drawn from the world of public health, and the fight against communicable diseases among animals and humans.

In the Libyan Arab Jamahiriya, severe cases of myiasis - an infestation of animal wounds - were found in livestock, in early 1988.[51] The larvae causing the myiasis cases were soon identified as the New World Screwworm, Chochliomyia hominivorax. Only a few people, who had previous experience with the Screwworm Fly, were concerned and

---

[50] Clay Wilson, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report for Congress, page 14, accessed June 4, 2012, http://www.history.navy.mil/library/online/computerattack.htm.

[51] D. A. Lindquist and M. Abusowa, "Eradicating the New World Screwworm from the Libyan Arab Jamahiriya," *IAEA Bulletin*, April 1992, page 19, accessed June 4, 2012, http://www.iaea.org/Publications/Magazines/Bulletin/Bull344/34402081724.pdf.

foresaw the enormous potential threat it posed to livestock, humans, and trade. The screwworm is capable of killing its host within ten days of infestation, and understandably trade is blocked with any country suspected of screwworm contamination.

The following is an excerpt from the text: *Eradication of the New World Screwworm from the Libyan Arab Jamahiriya*:

> *"Sometimes called "the worm of death," the New World Screwworm historically has been one of the most destructive and costly insect pests of warm-blooded animals in the western hemisphere. Its discovery in Libya in 1988 presented grave health and economic risks for the country and surrounding regions.*
>
> *The fly itself is harmless. Its reputation as a deadly parasite comes instead from its larvae, which are totally dependent on the living tissue of the host animals for survival. The wound they cause is known as myiasis, the presence of dipterous larvae in the tissues of animals or humans.*
>
> *The cost of living with the NWS … is enormous. Even when an infected animal does not die, it is more susceptible to other diseases, and milk and meat production can be seriously affected. Damage to hides and the cost of inspection and treatment amount to significant economic losses to livestock owners. Based on an annual cost … for inspection and treatment against NWS, it was estimated that living with the pest would cost Libya more than US $28 million annually. The five countries in the North African region, with 70 million head of livestock, would incur a combined cost of US $280 million annually."*[52]

---

[52] Ibid

The discovery of the New World Screwworm posed a threat not only to Libya, but to all of the surrounding countries as well. By September of 1990, nearly 3,000 cases of screwworm had been confirmed in Libya.[53]

In a striking parallel with terrorism and asymmetric warfare, time and chance are on the side of the screwworm fly. All the fly needs is a single wound and it can lay its eggs, and millions of new flies can appear. On the flip side, the scientists, farmers, and doctors, must spend inordinate amounts of time trying to find, kill, eradicate, avoid, prevent, and overcome every single fly. Obviously, standard "kinetic kill' tactics are very hard to employ against flies. The flies use common "guerrilla tactics": speed, agility, familiarity with terrain, and small, repeated strikes that only cumulatively and over time hurt the larger organism.

To fight the infestation, a control method known as the Sterile Insect Technique was enacted. This technique, developed by Raymond Bushland and Edward Knipling in the 1950's, is analogous to the concept of using fire to fight fire.[54] Millions of screwworm flies are bred in captivity, and then the male flies are sterilized using radiation. These sterilized flies are then released by airdrop over the infested area. The goal is to release enough flies so that for every wild male fly there are at least ten sterile males

---

[53] Bakri A., *The Area-Wide Sterile Insect Technique for Screwworm (Diptera: Calliphoridae) Eradication*, page 2, accessed June 4, 2012, http://www-iswam.iaea.org/drd/refs_files/195_The-Area-wide-SIT-Screwworm.pdf.

[54] The World Food Prize Foundation, "1992: Knipling and Bushland," The World Food Prize, accessed June 4, 2012, http://www.worldfoodprize.org/en/laureates/19871999_laureates/1992_knipling_and_bushland/.

competing for a mate. Because these insects mate only once per life cycle, the technique is extremely effective. In the case of the Libyan infestation, six months after the program was started, the screwworm fly was literally eradicated from an area of over forty thousand square kilometers. By March 1991, there were no new cases of screwworms.[55]

In another similar story, scientists studying Tanzanian lions in the Ngorongoro Crater became alarmed as the lions suddenly started dying off. The cause: stomoxys flies, a type of blood-sucking fly, were literally pestering the lions to death. So miserable were the king of beasts under the barrage of guerrilla attacks from the flies, the lions stopped eating and drinking and simply looked for a place to hide from the flies. Attracted to the scent of blood, it only took one small scratch for the flies to swarm a lion. Accomplishing what few other animals were capable of, the little flies killed six lions. In an apt model of asymmetric warfare, the lion's teeth and claws were completely ineffective against the onslaught of flies.[56]

Once again, this incident has direct metaphorical parallels with U.S. cyberspace. America is the lion, and the flies the cyber terrorist constantly probing for a weakness. Nothing can compare to the teeth and claws of the American military. However, these tools are almost entirely useless against tiny pests. Therefore, it is necessary to fight the asymmetric enemy in an asymmetric fashion. Instead of fighting the enemy head

---

[55] Bakri A., page 2.

[56] Dar Es Salaam, "Deadly Flies Kill Six Lions," *News24*, March 13, 2001, accessed June 4, 2012, http://www.news24.com/xArchive/Archive/Deadly-flies-kill-six-lions-20010312.

on, trying to completely eliminate each potential individual direct attack, this paper proposes a new technique, which we call the Sterile Information Technique.

The logic behind this method is to flood the cyber domain with useless information on a single subject (species) of information, such as “how to hack the Pentagon.” Taking advantage of the anonymity of the internet, the DoD could flood the internet with websites full of misleading instructions on how to go about attempting said endeavor. The websites might even provide downloadable “hacking” software, that in reality is government bugged software that does nothing damaging at all except give the DoD the permission and capability to monitor/control the would-be-hacker’s computer. The average fourteen year-old in his basement is unlikely to determine the authenticity of any given website. If the number of such websites with “sterile” information outnumbers the number of websites with real information at a ratio of say 100 to 1, the odds are now suddenly in favor of the DoD.

There would be additional advantages to this strategy. As the number of “fourteen year-old hackers” (i.e. inexperienced hackers attempting to follow useless DoD hack “cookbooks") disappears, statistically speaking, the remaining attacks would tend to come from well-trained individuals. High-end hacking techniques are trackable. Cyber investigations could focus more on the incidents where teeth and claws are very useful.

Conclusion

SUMMARY

There are several important conclusions to be drawn from the four case studies examined in this paper. First, the Desert Storm incident reveals that institutions and bureaucracies find it extremely difficult to adapt defensive measures to match the pace of change in the cyber domain. The difficulty arises because the cyber domain creates networks that bring together not just hardware and software, but agencies and human beings. These multiple agencies have great difficulty adapting to changing circumstances and coordinating cyber-incident responses, due to the sheer number of people involved and the corresponding bureaucracy.

From the Operation Allied Force case in Kosovo, we're reminded that all future conflicts will likely have cyber elements, in both the psychological and direct kinetic realms. We also see that even isolated conflicts can attract the participation of non-affiliated parties, in which the cyber conflict can be global, even while the kinetic conflict remains regionally isolated.

Operation Unified Protector in Libya illustrates that cyber warfare is often manifested as guerrilla warfare. It only takes a small cyberforce to have major influence in a conflict. Because tremendous power can be wielded by individuals and small groups, a shrewd warrior can use this tool with devastating effect, resulting in an asymmetric advantage for the guerilla against a much greater power. At the same time, the proactive use of cyber can yield significant benefits in diplomacy and soft power projection, at great savings compared to kinetic power projection.

Finally, though there are not yet any FBI-confirmed cyberterror attacks against the United States, it is nonetheless true that since the advent of War on Terror there has been an explosion in the number and sophistication of cyber attacks in general. In the same way that concerns about the nexus of terror and weapons of mass destruction creates a new and unique security threat, so the nexus of cyber attacks and ideologically driven terror attacks – cyberterror -- looms as one of the defining security challenge of our Information Age. However, ironically, the explosion in the number of cyber attacks can be used to our advantage, but only if viewed through the lens of statistical strategy. Effective cyber security will likely come about through implementation of asymmetric techniques, such as Sterile Information Techniques, rather than via old-fashioned, hunt-and-kill kinetic operations.

RECOMMENDATIONS

Based on case study lessons learned, three major recommendations emerge:

First, create a “Cyber Security Agency” as a separate government security agency. This is necessary to maximize the focus on, legitimacy of, and political clout of cyber security efforts within the broader national security community. The Cyber Force agents in this agency would constitute an independent service from all other existing military or law enforcement branches, lending it an autonomy that could not otherwise be achieved. This separation would help unify and clarify actions taken in the cyber domain. Currently every security agency and each branch of the military has its own distinct cyber division. This structure has certain advantages. However, to reduce

political and bureaucratic obstacles to progress, and to legitimize unified action, a separate service for cyber supremacy may prove necessary.

During operational cyber incidents, the Cyber Security Agency should be given operational command. This presents several advantages. First of all, it would provide a centralized "go to" point for anyone in the U.S. suffering a cyber attack. In the Desert Storm case study, multiple incident response teams received reports of the same incident; however, due to bureaucracy, information sharing was limited. Just as a kidnapping or money forging crime is expected to be reported to the FBI, similarly, cyber attacks would be expected to be reported to the Cyber Force. This centralized control would facilitate quick and skilled responses, vital institutional attributes in a domain where millions of computers can be infected in seconds. Most importantly, it would help unify the efforts of all of the cyber services participating in any incident.

Other advantages of this concept relate to the necessity of maturing cyber laws. A dedicated Cyber Security Agency would facilitate improved development of cyber laws, enabling Congress to keep up this rapidly evolving and increasingly vital area of public good. Similar to the FDA, the CSA could also take on an enforcement role, helping inspect industry cyber infrastructure in accordance with new regulatory standards. This would help protect the American public from unscrupulous businesses who cut costs by reducing cyber security, potentially exposing their customers' private data to attack.

The second recommendation is to officially classify cyber warfare as an element within guerilla warfare military doctrine. This facilitates the development of effective strategies relating to the asymmetric nature of cyberspace, as well as an element of official diplomacy. Due to the unique nature of cyberspace, the individual has a

powerful asymmetric tool to wield against a much greater power. Because the cyber domain puts tremendous power in the hands of the individual, and because the disinhibition effect defines the psychology of the domain, people are willing to use power in new and different ways than in the past. No longer are insurgents easily threatened by kinetic or legal consequences. (Copyright laws are another good example of the disinhibition effect.) From the defensive side, military and security training must include cyber warfare training among classic guerilla war studies. Nearly every conflict in the future is likely to include global cyberwar activity. Similarly, from the proactive, diplomatic standpoint, it is essential to recognize the opportunity for using cyber diplomacy directly to individuals. Diplomats can expect to be capable of wielding this new tool to their advantage. Just as the individual on the street can attempt to use the cyber domain to influence political outcomes, diplomats can use the same techniques to influence political outcomes as well.

The final recommendation of this paper is to adopt an unconventional method for combating cyber attacks called the Sterile Information Technique. The basic premises of the technique is to flood the internet, the highway of information, with so much useless and "sterile" information on a certain topic, that it becomes impossible to discern the truth. Since it is virtually impossible to completely eradicate any type of information on the Internet, this counter-intuitive approach can be successfully employed.

Currently, any curious teenager can do an online search for hacking tools, tips, forums, etc. and find something to experiment with. However, if the Internet were inundated with "sterilized" websites on the subject of hacking, the odds that a teenager

will actually find something useful drops significantly. In an ironic twist of potential, the anonymity of the Internet now becomes an advantage to the cyber crime fighters. The average fourteen year old won't know that the website he just visited is a government created website, or that the software he downloaded is useless.

If this surge in sterile information were complimented with an agreement with Internet giants, such as Google, it would make it even more likely to download sterile information. Further, if the downloaded software pinged a tracking signal to a cyber security monitoring agency, then in game theory terms, the cost/benefit ratio would suddenly fall in favor of NOT downloading the hacking software. The chance of downloading government bugged software, and getting caught suddenly becomes a very possible outcome. This would significantly reduce the number of attacks from "curious" fourteen year-olds in their parents basement, isolating the remaining attacks as sophisticated attacks done by individuals who know what they are doing and probably have a purpose.

FINAL THOUGHTS

History offers a wealth of lessons learned. But no matter what course the United States ultimately chooses, the crucial factor is the nation must act quickly. With each passing day, cyberspace becomes ever more integrated into our nation’s infrastructure and security processes, and more central to the vital interests of the United States. If nothing else, these case studies offer a dim preview of what could happen if action is not taken with alacrity.

BIBLIOGRAPHY

A., Bakri. *The Area-Wide Sterile Insect Technique for Screwworm (Diptera: Calliphoridae) Eradication*. Accessed June 4, 2012. http://www-iswam.iaea.org/drd/refs_files/195_The-Area-wide-SIT-Screwworm.pdf.

Abbate, Janet. "Government, Business, and the Making of the Internet." *Business History Review* 75, no. 1 (Spring 2001): 164.

Abbate, Janet. *Inventing the Internet*. Cambridge, Massachusetts: MIT Press, 2000.

Ackerman, Spencer. "Desperate Gaddafi bombs protesters, blocks internet." *Wired.co.uk*, February 22, 2011. Accessed June 4, 2012. http://www.wired.co.uk/news/archive/2011-02/22/libya-gaddafi-bombs-protestors.

Barnett, Thomas P.M., and Henry H. Gaffney, Jr. "The Global Transaction Strategy." *Transformation Trends* (December 2002). Accessed June 4, 2012. http://www.au.af.mil/au/awc/awcgate/transformation/trends_169_transformation_trends_16december02_issue.pdf.

Brewin, Bob. "General: Cyberattacks against NATO traced to China." *Federal Computer Week*, August 31, 1999. Accessed June 4, 2012. http://fcw.com/articles/1999/08/31/general-cyberattacks-against-nato-traced-to-china.aspx?sc_lang=en.

Chivers, Ian, and Jane Sleightholme. *Fortran History and Development*. Accessed June 4, 2012. http://www.fortranplus.co.uk/resources/Fortran_history_and_development.pdf.

Complete Dictionary of Scientific Biography. Encyclopedia.com, 2008. Accessed June 4, 2012. http://www.encyclopedia.com/doc/1G2-2830906236.html.

Computer Sciences. Encyclopedia.com. Accessed June 4, 2012. Last modified 2002. http://www.encyclopedia.com/doc/1G2-3401200604.html.

Department of Defense Dictionary of Military and Associated Terms. Joint Publication 1-02 ed. 2010. Accessed June 4, 2012. Last modified March 15, 2012. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

East West Institute, and Information Security Institute of Moscow State University. *The Russia - U.S. Bilateral on Cybersecurity - Critical Terminology Foundations* . Edited by Karl F. Rauscher and Valery Yaschenko. Issue 1. 2011. Accessed June 4, 2012. http://cybersummit2011.com/component/content/article/32.

Franke, Tobias. "Social media: the frontline of cyberdefence?" NATO Review. Accessed June 4, 2012. http://www.nato.int/docu/review/2011/Social_Medias/cyber-defense-social-media/EN/index.htm.

Gale Encyclopedia of E-Commerce. Encyclopedia.com. Accessed June 4, 2012. Last modified 2002. http://www.encyclopedia.com/topic/ARPANET.aspx.

Government Accountability Office. *Report to Congressional Requesters: CYBERSPACE United States Faces Challenges in Addressing Global Cybersecurity and Governance*. GAO-10-606. Accessed June 4, 2012. http://gao.gov/products/GAO-10-606.

Greers, Kenneth. *Cyberspace and the Changing Nature of Warfare* . Accessed June 4, 2012. http://www.carlisle.army.mil/DIME/documents/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf.

Healey, Jason, and Karl Grindal. "Lessons from the First Cyber Commanders." New Atlanticist. Accessed June 4, 2012. Last modified March 14, 2012. http://www.acus.org/new_atlanticist/lessons-first-cyber-commanders.

Kissinger, Henry. "The Vietnam Negotiations." *Foreign Affairs*, January 1969, 214. Vol. 48, No.2

Kosovo: War in Europe - The Road to War. "FRONTLINE." PBS. June 4, 2012 (originally aired February 22, 2000). YouTube. Accessed June 4, 2012. http://www.youtube.com/watch?v=__kbfuyYliA&feature=related.

Lewis, James Andrew. *Thresholds for Cyberwar*. Edited by Center for Strategic and International Studies. Accessed June 4, 2012. http://csis.org/publication/thresholds-cyberwar.

Lindquist, D. A., and M. Abusowa. "Eradicating the New World Screwworm from the Libyan Arab Jamahiriya." *IAEA Bulletin*, April 1992, 17-24. Accessed June 4, 2012. http://www.iaea.org/Publications/Magazines/Bulletin/Bull344/34402081724.pdf.

Markoff, John. "Dutch Computer Rogues Infiltrate American Systems With Impunity." *New York TImes*, April 21, 1991. Accessed June 4, 2012. http://www.nytimes.com/1991/04/21/us/ dutch-computer-rogues-infiltrate-american-systems-with-impunity.html?pagewanted=all&src=pm.

McGee, Joshua. "NATO and Cyber Defense: A Brief Overview and Recent Events." Center for Strategic and International Studies. Accessed June 4, 2012. Last modified July 8, 2011. http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events.

Mueller, Robert S., III. "Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies." Speech, RSA Cyber Security Conference, San Francisco, March 1, 2012. Federal Bureau of Investigation. Accessed June 4, 2012. http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

National Defense University. Editorial, *Joint Force Quarterly*, April 2005, Inside Cover. Accessed June 4, 2012. http://www.ndu.edu/press/lib/pdf/jfq-37/JFQ-37.pdf.

Network Security Consulting Blog. http://blog.emagined.com/.

Paret, Peter, and John Shy. *U.S. Marine Corps - FMFRP 12-25: The Guerilla and How to Fight Him*. Guerilla Warfare and U.S. Military Policy: A Study. Washington, D.C.: U.S. Marine Corps, 1990. Accessed June 4, 2012. http://www.scribd.com/doc/3605861/US-Marine-Corps-FMFRP-1225-The-Guerilla-and-How-to-Fight-Him#outer_page_53.

Pekelney, Richard. "What Is The SIGABA-ECM Mark II and Why It Was Important?" Crypto Machines. Accessed June 4, 2012. Last modified April 30, 2012. http://www.jproc.ca/crypto/ecm2.html.

Poulsen, Kevin. "Slammer Worm Crashed Ohio Nuke Plant Network." Security Focus. Accessed June 4, 2012. Last modified August 19, 2003. http://www.securityfocus.com/news/6767.

Salaam, Dar Es. "Deadly Flies Kill Six Lions." *News24*, March 13, 2001. Accessed June 4, 2012. http://www.news24.com/xArchive/Archive/Deadly-flies-kill-six-lions-20010312.

Sale, Tony. "The Breaking of German Naval Enigma ." Naval Enigma Index. Accessed June 4, 2012. http://www.codesandciphers.org.uk/virtualbp/navenigma/navenig1.htm.

Suler, John. "The Online Disinhibition Effect." Rider University: The Psychology of Cyberspace. Accessed June 4, 2012. Last modified August 4, 2004. http://users.rider.edu/~suler/psycyber/disinhibit.html.

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian*, May 16, 2007, U.S. edition. Accessed June 4, 2012. http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

U.S. Department of State. "21st Century Statecraft." U.S. Department of State – Diplomacy in Action. Accessed June 4, 2012. http://www.state.gov/statecraft/overview/index.htm.

Venkataraman, Mukundan, Kartik Muralidharan, and Puneet Gupta. *Designing new Architectures and Protocols for Wireless Sensor Networks: A Perspective*. Edited by IEEE Communications Society. Accessed June 4, 2012. http://www.cs.ucf.edu/~mukundan/secon05.pdf.

Verton, Dan. "Serbs launch cyberattack on NATO." *Federal Computer Week*, April 4, 1999. Accessed June 4, 2012. http://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx.

Villafuerte, Nelly Favis. "The Reality of Cyber Terrorism." Manila Bulletin Publishing Corporation. Accessed June 4, 2012. Last modified March 25, 2011. http://www.mb.com.ph/articles/311407/the-reality-cyber-terrorism.

Wauters, Robin. "25 Years Later, First Registered Domain Name Changes Hands." AOL Tech. Accessed June 4, 2012. Last modified August 27, 2009. http://techcrunch.com/2009/08/27/ 25-years-later-first-registered-domain

Wilson, Clay. *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. CRS Report for Congress. Accessed June 4, 2012. http://www.history.navy.mil/library/online/computerattack.htm.

World Food Prize Foundation. "1992: Knipling and Bushland." The World Food Prize. Accessed June 4, 2012. http://www.worldfoodprize.org/en/laureates/19871999_laureates/1992_knipling_and_bushland/.