KENNETH GEERS

STRATEGIC CYBER SECURITY

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Publisher:
CCD COE Publication
Filtri tee 12, 10132 Tallinn, Estonia
Tel: +372 717 6800
Fax: +372 717 6308
E-mail: ccdcoe@ccdcoe.org
www.ccdcoe.org

Print: OÜ Greif Trükikoda
Design & Layout: Marko Söönurm

ISBN 978-9949-9040-5-1 (print)
ISBN 978-9949-9040-6-8 (epub)
ISBN 978-9949-9040-7-5 (pdf)

KENNETH GEERS

STRATEGIC CYBER SECURITY

NATO Cooperative Cyber Defence Centre of Excellence

Abstract

This book argues that computer security has evolved from a technical discipline to a strategic concept. The world's growing dependence on a powerful but vulnerable Internet – combined with the disruptive capabilities of cyber attackers – now threatens national and international security.

Strategic challenges require strategic solutions. The author examines four nation-state approaches to cyber attack mitigation.

- Internet Protocol version 6 (IPv6)
- Sun Tzu's *Art of War*
- Cyber attack deterrence
- Cyber arms control

The four threat mitigation strategies fall into several categories. IPv6 is a technical solution. Art of War is military. The third and fourth strategies are hybrid: deterrence is a mix of military and political considerations; arms control is a political/technical approach.

The Decision Making Trial and Evaluation Laboratory (DEMATEL) is used to place the key research concepts into an influence matrix. DEMATEL analysis demonstrates that IPv6 is currently the most likely of the four examined strategies to improve a nation's cyber defense posture.

There are two primary reasons why IPv6 scores well in this research. First, as a technology, IPv6 is more resistant to outside influence than the other proposed strategies, particularly deterrence and arms control, which should make it a more reliable investment. Second, IPv6 addresses the most significant advantage of cyber attackers today – anonymity.

About the Author

Kenneth Geers, PhD, CISSP, Naval Criminal Investigative Service (NCIS), is a Scientist and the U.S. Representative to the North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in Tallinn, Estonia.

To Jeanne

CONTENTS

Acknowledgements

I would like to thank faith, hope, love, family, friends, NCIS, CCD CoE, TUT, my PhD advisor Professor emeritus Leo Võhandu, and Vana Tallinn.

I. INTRODUCTION

1. CYBER SECURITY AND NATIONAL SECURITY

Cyber security has quickly evolved from a technical discipline to a strategic concept. Globalization and the Internet have given individuals, organizations, and nations incredible new power, based on constantly developing networking technology. For everyone – students, soldiers, spies, propagandists, hackers, and terrorists – information gathering, communications, fund-raising, and public relations have been digitized and revolutionized.

As a consequence, all political and military conflicts now have a cyber dimension, the size and impact of which are difficult to predict, and the battles fought in cyberspace can be more important than events taking place on the ground. As with terrorism, hackers have found success in pure media hype. As with Weapons of Mass Destruction (WMD), it is difficult to retaliate against an asymmetric attack.

The astonishing achievements of cyber espionage serve to demonstrate the high return on investment to be found in computer hacking. The start-up cost is low, and traditional forms of espionage, such as human intelligence, are more dangerous. Computer hacking yields free research and development data and access to sensitive communications. National leaders, who frequently address cyber espionage on the world stage, are worried.[1]

The use and abuse of computers, databases, and the networks that connect them to achieve military objectives was known in the early 1980s in the Soviet Union as the Military Technological Revolution (MTR). After the 1991 Gulf War, the Pentagon's Revolution in Military Affairs was almost a household term.[2] A cyber attack is not an end in itself, but a powerful means to a wide variety of ends, from propaganda to espionage, from denial of service to the destruction of critical infrastructure. The nature of a national security threat has not changed, but the Internet has provided a new delivery mechanism that can increase the speed, scale, and power of an attack.

Dozens of real world examples, from the U.S. to Russia, from the Middle East to the Far East, prove that the ubiquity and vulnerability of the Internet have tangible political and military ramifications. As the Internet becomes more powerful and as our dependence upon it grows, cyber attacks may evolve from a corollary of real-world disputes to play a lead role in future conflicts.

1 *Spiegel*, 2007; Cody, 2007.

2 Mishra, 2003.

In 1948, Hans Morgenthau wrote that national security depends on the integrity of a nation's borders and its institutions.[3] In 2011, military invasion and terrorist attack remain the most certain way to threaten the security of an adversary. However, as national critical infrastructures, including everything from elections to electricity, are computerized and connected to the Internet, national security planners will also have to worry about cyber attacks.

It is a fact that large, complex infrastructures are easier to manage with computers and common operating systems, applications, and network protocols. But this convenience comes at a price. Connectivity is currently well ahead of security, and this makes the Internet, and Internet users, vulnerable to attack. There are not only more devices connected to the Internet every day, but there are dozens of additions to the Common Vulnerabilities and Exposures (CVE) database each month.[4] These combine to create what hackers call the expanding "attack surface." Hackers tend to be creative people, and they are able to exploit such complexity to find ways to read, delete, and/or modify information without proper authorization.

One paradox of the cyber battlefield is that both big and small players have advantages. Nations robust in IT exploit superior computing power and bandwidth; small countries and even lone hackers exploit the amplifying power of the Internet to attack a stronger conventional foe. Furthermore, Internet-dependent nations are a tempting target because they have more to lose when the network goes down.

In cyber conflict, the terrestrial distance between adversaries can be irrelevant because everyone is a next-door neighbor in cyberspace. Hardware, software, and bandwidth form the landscape, not mountains, valleys, or waterways. The most powerful weapons are not based on strength, but logic and innovation.

It is also true that cyber attacks are constrained by the limited terrain of cyberspace. There are many skeptics of cyber warfare. Basically, tactical victories amount to a successful reshuffling of the bits – the ones and zeros – inside a computer. Then the attacker must wait to see if anything happens in the real world. There is no guarantee of success. Network reconfiguration, software updates, and human decision-making change cyber terrain without warning, and even a well-planned attack can fall flat.[5]

In fact, the dynamic nature of the Internet offers benefits to both an attacker and a defender. Many cyber battles will be won by the side that uses cutting-edge technologies to greater advantage. Although an attacker has more targets to strike and

3 Morgenthau, 1948.

4 CVE, 2011.

5 Parks & Duggan, 2001.

more ways to hit them, a defender has the means to design an ever-increasing level of network redundancy and survivability.[6]

In 2011, an attacker's most important advantage remains a degree of anonymity. Smart hackers hide within the international, maze-like architecture of the Internet. They route attacks through countries with which a victim's government has poor diplomatic relations or no law enforcement cooperation. In theory, even a major cyber conflict could be fought against an unknown adversary.

Law enforcement and counterintelligence investigations suffer from the fact that the Internet is an international entity, and jurisdiction ends every time a telecommunications cable crosses a border. In the case of a state-sponsored cyber attack, international cooperation is naturally non-existent.

The anonymity or "attribution" problem is serious enough that it increases the odds that damaging cyber attacks on national critical infrastructures will take place in the absence of any traditional, real-world warning, during times of nominal peace.

Cyber defense suffers from the fact that traditional security skills are of marginal help in defending computer networks, and it is difficult to retain personnel with marketable technical expertise. Talented computer scientists prefer more exciting, higher-paying positions elsewhere.

As a consequence, at the technical level, it can be difficult even knowing whether one is under cyber attack. At the political level, the intangible nature of cyberspace can make the calculation of victory, defeat, and battle damage a highly subjective undertaking. And with cyber law, there is still not enough expertise to keep pace with the threat.

Finally, cyber defense suffers from the fact that there is little moral inhibition to computer hacking, which relates primarily to the use and abuse of computer code. So far, there is little perceived human suffering.

All things considered, the current balance of cyber power favors the attacker. This stands in contrast to our historical understanding of warfare, in which the defender has traditionally enjoyed a home field advantage.

Therefore, many governments may conclude that, for the foreseeable future, the best cyber defense is a good offense. First, cyber attacks may be required to defend the homeland; second, they are a powerful and sometimes deniable way to project national power.

6 Lewis, 2002.

Can a cyber attack pose a serious threat to national security? Decision makers are still unsure. Case studies are few in number, much information lies outside the public domain, there have been no wars between two first-class militaries in the Internet era, and most organizations are still unsure about the state of their own cyber security.

Conducting an "information operation" of strategic significance is not easy, but neither is it impossible. During World War II, the Allies took advantage of having broken the Enigma cipher to feed false information to Adolf Hitler, signaling that the D-Day invasion would take place at Pas-de-Calais and not Normandy. This gave Allied forces critical time to establish a foothold on the continent and change the course of history.[7]

What military officers call the "battlespace" grows more difficult to define – and to defend – over time. Advances in technology are normally evolutionary, but they can be revolutionary – artillery reached over the front lines of battle; rockets and airplanes crossed national boundaries; today cyber attacks can target political leadership, military systems, and average citizens anywhere in the world, during peacetime or war, with the added benefit of attacker anonymity.

Narrowly defined, the Internet is just a collection of networked computers. But the importance of "cyberspace" as a concept grows every day. The perceived threat is such that the new U.S. Cyber Command has declared cyberspace to be a new domain of warfare,[8] and the top three priorities at the U.S. Federal Bureau of Investigation (FBI) are preventing terrorism, espionage, and cyber attacks.[9]

Cyber warfare is unlike traditional warfare, but it shares some characteristics with the historical role of aerial bombardment, submarine warfare, special operations forces, and even assassins. Specifically, it can inflict painful, asymmetric damage on an adversary from a distance or by exploiting the element of surprise.[10]

The post-World War II U.S. Strategic Bombing Survey (USSBS) may hold some lessons for cyber war planners. The USSBS concluded that air power did not permanently destroy any indispensable adversary industry during the war, and that "persistent re-attack" was always necessary. Nonetheless, the report left no doubt about its ultimate conclusion:

7 Kelly, 2011.

8 "Cyber Command's strategy..." 2011.

9 From the FBI website: www.fbi.gov.

10 Parks & Duggan, 2001.

> ... Allied air power was decisive in the war in Western Europe ... In the air, its victory was complete. At sea, its contribution ... brought an end to the enemy's greatest naval threat – the U-boat; on land, it helped turn the tide overwhelmingly in favor of Allied ground forces.[11]

Cyber attacks are unlikely to have the lethality of a strategic bomber, at least for the foreseeable future. But in the end, the success of military operations is effects-based. If both a ballistic missile and a computer worm can destroy or disable a target, the natural choice will be the worm.

In May 2009, President Obama made a dramatic announcement: "Cyber intruders have probed our electrical grid ... in other countries, cyber attacks have plunged entire cities into darkness."[12] Investigative journalists subsequently concluded that these attacks took place in Brazil, affecting millions of civilians in 2005 and 2007, and that the source of the attacks is still unknown.[13] National security planners should consider that electricity has no substitute, and all other infrastructures, including computer networks, depend on it.[14]

In 2010, the Stuxnet computer worm may have accomplished what five years of United Nations Security Council resolutions could not: disrupt Iran's pursuit of a nuclear bomb.[15] If true, a half-megabyte of computer code quietly substituted for air strikes by the Israeli Air Force. Moreover, Stuxnet may have been more effective than a conventional military attack and may have avoided a major international crisis over collateral damage. To some degree, the vulnerability of the Internet to such spectacular attacks will provide a strong temptation for nation-states to take advantage of computer hacking's perceived high return-on-investment before it goes away.

If cyber attacks play a lead role in future wars, and the fight is largely over ownership of IT infrastructure, it is possible that international conflicts will be shorter and cost fewer lives. A cyber-only victory could facilitate post-war diplomacy, economic recovery, and reconciliation. Such a war would please history's most famous military strategist, Sun Tzu, who argued that the best leaders can attain victory before combat is necessary.[16]

It may be unlikely, however, that an example like Stuxnet will occur frequently. Modern critical infrastructures present complex, diverse, and distributed targets. They

11 United States *Strategic* Bombing Survey, 1945.

12 "Remarks by the President..." 2009.

13 "Cyber War..." 2009.

14 Divis, 2005.

15 Falkenrath, 2011.

16 Sawyer, 1994.

comprise not one system, technology, or procedure, but many and are designed to survive human failings and even natural disasters. Engineers on-site may see the start of an attack and neutralize it before it becomes a serious threat. In short, computer vulnerabilities should not be confused with vulnerabilities in whole infrastructures.[17]

Cyber attacks may rise to the level of a national security threat only when an adversary has invested a significant amount of time and effort into a creative and well-timed strike on a critical infrastructure target such as an electrical grid, financial system, air traffic control, etc.

Air defense is an example of a system that plays a strategic role in national security and international relations. It may also represent a particular cyber vulnerability in the context of a traditional military attack. In 2007, for example, it was reported that a cyber attack preceded the Israeli air force's destruction of an alleged Syrian nuclear reactor.[18]

Military leaders, by virtue of their profession, should expect to receive Denial of Service (DoS) attacks against their network infrastructure. As early as the 1999 Kosovo war, unknown hackers attempted to disrupt NATO military operations via the Internet and claimed minor victories.[19] In future conflicts, DoS attacks may encompass common network "flooding" techniques, the physical destruction of computer hardware, the use of electromagnetic interference,[20] and more.

Terrorists do not possess the unqualified nation-state backing that militaries enjoy. As a consequence, they may still believe that the Internet poses more of a danger than an opportunity.

Forensic examination of captured hard drives proves that terrorists have studied computer hacking,[21] and Western economies are a logical target. For example, tension in the Middle East is now always accompanied by cyber attacks. During the 2006 war between Israel and Gaza, pro-Palestinian hackers successfully denied service to around 700 Israeli Internet domains.[22]

But a long-term, economic threat from cyber terrorists may be illogical. In a globalized, interconnected world, a cooperative nation-state would only seem to be hurting itself, and a terrorist group may crave a higher level of shock and media atten-

17 Lewis, 2002.

18 Fulghum et al, 2007.

19 Verton, 1999; "Yugoslavia..." 1999.

20 Designed to destroy electronics via current or voltage surges.

21 "Terrorists..." 2006.

22 Stoil & Goldstein, 2006.

tion than a cyber attack could create.[23] Former U.S. Director of National Intelligence (DNI) Mike McConnell has argued that a possible exception could be a cyber attack on the public's confidence in the financial system itself, specifically in the security and supply of money.[24]

All things considered, cyber attacks appear capable of having strategic consequences; therefore, they must be taken seriously by national security leadership. At the national and organizational levels, a good starting point is methodical risk management, including objective threat evaluation and careful resource allocation. The goal is not perfection, but the application of due diligence and common sense.

The pertinent questions include:

- What is our critical infrastructure?
- Is it dependent on information technology?
- Is it connected to the Internet?
- Would its loss constitute a national security threat?
- Can we secure it or, failing that, take it off-line?

Objectivity is key. Cyber attacks receive enormous media hype, in part because they involve the use of arcane tools and tactics that can be difficult to understand for those without a formal education in computer science or information technology.

As dependence on IT and the Internet grow, governments should make proportional investments in network security, incident response, technical training, and international collaboration.

However, because cyber security has evolved from a technical discipline to a strategic concept, and because cyber attacks can affect national security at the strategic level, world leaders must look beyond the tactical arena. The quest for strategic cyber security involves marshaling all of the resources of a nation-state.

Therefore, the goal of this research is to evaluate nation-state cyber attack mitigation strategies. To support its arguments and conclusions, the author employs the Decision Making Trial and Evaluation Laboratory (DEMATEL).

23 Lewis, 2010. CSIS's Lewis recently stated: "It remains intriguing and suggestive that [terrorists] have not launched a cyber attack. This may reflect a lack of capability, a decision that cyber weapons do not produce the violent results terrorists crave, or a preoccupation with other activities. Eventually terrorists will use cyber attacks, as they become easier to launch..."

24 "Cyber War..." 2009.

The Nature and Scope of this Book

Today, world leaders fear that cyber terrorism and cyber warfare pose a new and perhaps serious threat to national security – the Internet is a powerful resource, modern society is increasingly dependent upon it, and cyber attackers have demonstrated the capability to manipulate and disrupt the Internet for a wide variety of political and military purposes.

There is a clear need for national security planners to prepare cyber defenses at both the tactical and strategic levels. The goal of this research is to help decision makers with the latter – to choose the most efficient courses of action to take at the strategic level in order to defend their national interests in cyberspace.

Beyond its Introduction and Conclusion, this book has three primary parts. First, it explores the changing nature of cyber security, tracing its evolution from a technical discipline to a strategic concept. Second, it evaluates four approaches to improving the cyber security posture of a nation-state – Internet Protocol version 6 (IPv6), the application of Sun Tzu's *Art of War* to cyber conflict, cyber attack deterrence, and cyber arms control. Third, it employs the Decision Making Trial and Evaluation Laboratory (DEMATEL) to analyze the key concepts covered and to prioritize the four cyber security strategies.

The four cyber attack mitigation strategies – IPv6, *Art of War*, deterrence and arms control – fall into several categories. IPv6 is a technical solution. *Art of War* is military. The third and fourth strategies are hybrid: deterrence is a mix of military and political considerations; arms control is a political/technical approach.

There are significant limitations to this research. Cyberspace is complex, dynamic, and constantly evolving. National security planning involves a wide array of fallible human perceptions and at times irrational decision-making at both the national and international levels. At a minimum, strategic cyber security demands a holistic investigation, subject to the particular context of different nations. These complexities serve to limit the aspiration of this research to an initial policy evaluation that addresses the needs of a theoretical nation-state.

Data collection for this research consisted primarily of peer-reviewed scientific literature and the author's direct observation of events such as the 2010 Cooperative Cyber Defence Centre of Excellence/Swedish National Defence College cyber defense exercise (CDX), "Baltic Cyber Shield." Data analysis is almost exclusively that of the author,[25] whose personal experience as a cyber security analyst spans over a decade.

25 Three chapters were co-written by colleagues with a very strong technical background.

The validation of this research rests on peer-review, to which every chapter has been subjected. It encompasses fourteen articles related to strategic cyber security, eleven written solely by the author, six of which are listed in the Thomson Reuters ISI Web of Knowledge.

The author is ideally placed to conduct this research. Since 2007, he has been a Scientist at the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.[26] Previously, he was the Division Chief for Cyber Analysis at the Naval Criminal Investigative Service (NCIS) in Washington, DC.

Research Outline

This book seeks to help nation-states mitigate strategic-level cyber attacks. It has five parts.

I. Introduction: Cyber Security and National Security

II. Birth of a Concept: Strategic Cyber Security

III. Nation-State Cyber Attack Mitigation Strategies

IV. Data Analysis and Research Results

V. Conclusion: Research Contributions

Part II explores the concept of "strategic" cyber security, moving beyond its tactical, technical aspects – such as how to configure a firewall or monitor an intrusion detection system – to defending the cyberspace of a nation-state. It provides the foundation and rationale for Parts III and IV, and has three chapters.

2. Cyber Security: A Short History

3. Cyber Security: A Technical Primer

4. Cyber Security: Real World Impact

Part III of this book asks four research questions, which highlight four likely strategic approaches that nations will adopt to mitigate the cyber attack threat and to improve their national cyber security posture.

5. The Next-Generation Internet: can Internet Protocol version 6 (IPv6) increase strategic cyber security?

26 The Centre's vision is to be NATO's primary source of expertise in the field of cooperative cyber defense research. As of mid-2011, the Centre employed cyber defense specialists from nine different Sponsoring Nations.

6. Sun Tzu's *Art of War*: can the world's best military doctrine encompass cyber warfare?
7. Cyber attack deterrence: is it possible to prevent cyber attacks?
8. Cyber arms control: can we limit cyber weapons?

Part IV employs the Decision Making Trial and Evaluation Laboratory (DEMATEL) to analyze the key concepts covered in this book and to prioritize the four proposed cyber attack mitigation strategies addressed in Part III. Its goal is to help decision makers choose the most efficient ways to address the challenge of improving cyber security at the strategic level.

9. DEMATEL and Strategic Analysis
10. Key Findings

Part V, the Conclusion, summarizes the contributions of this book and provides suggestions for future research.

II. BIRTH OF A CONCEPT: STRATEGIC CYBER SECURITY

2. CYBER SECURITY: A SHORT HISTORY

Human history is often marked by revolutions in science and technology. During the Industrial Revolution, for example, the steam engine worked miracles for our muscles. Standardization and mass production dramatically lowered the cost of manufactured goods by decreasing the amount of human energy required to make them.

We are now in the middle of the Information Revolution. The computer is in effect a steam engine for our brains. It dramatically facilitates the acquisition and validation of knowledge. The primary goal of building the first computers was simple – to create a machine that could process calculations faster than a human could by hand. In due course, scientists were able to accomplish that and much, much more.

Chapter 2 of this book outlines the primary historical events that have transformed cyber security from a technical discipline to a strategic concept.

The Power of Computers

In 1837, Cambridge University Professor Charles Babbage designed the "Analytical Engine," a surprisingly modern mechanical computer that was never built because it was about 100 years ahead of its time.

Historically, national security considerations have been the prevailing wind behind the development of Information Technology (IT).[27] In 1943, the U.S. military commissioned the world's first general-purpose electronic computer, the Electronic Numerical Integrator and Computer (ENIAC). This collection of 18,000 vacuum tubes was designed to compute ballistic trajectories at 100,000 "pulses" per second, or 100 times faster than a human with a mechanical calculator. ENIAC smashed all expectations, calculating at speeds up to 300,000 times faster than a human.

After WWII, cutting-edge computers began to demonstrate their value outside the military realm. UNIVAC I,[28] the first commercial computer produced in the United

27 Commercially, companies such as International Business Machines (IBM) had found success in marketing electro-mechanical devices by 1900.

28 The Universal Automatic Computer I had a clock speed of 2.5 MHz, a central memory of 1,000 91-bit words, and a peak rate of 1,000 FLOPS, or about 1/1,000,000th the speed of a CRAY-2.

States, correctly predicted the results of the 1952 Presidential election based on a sample of just 1%.

But the Information Revolution had only just begun. The arrival of the personal computer (PC) left a much deeper impact on the Earth. The invention of the microprocessor, random-access storage, and software of infinite variety allowed anyone to own a "personal mainframe" with demonstrable scientific and engineering capabilities.[29]

Information Technology (IT) now pervades our lives. In 1965, Gordon Moore correctly predicted that the number of transistors on a computer chip would double every two years.[30] There has been similar growth in almost all aspects of information technology (IT), including the availability of practical encryption, user-friendly hacker tools, and Web-enabled open source intelligence (OSINT).

The physical limits of desktop computing are approaching. For example, electronic circuitry may be reaching its minimum physical size, and the maximum rate at which information can move through any computer system may be limited by the finite speed of light.

However, the simultaneous rise of "cyberspace" solves this problem. In 2010, there were nearly one billion computers connected directly to the Internet, and over 1.5 billion Internet users on Earth.[31] Today, a reliable connection to the Internet is more important than the power of one's computer and provides infinitely greater utility to the user.

The Rise of Malicious Code

Together, computers and computer networks offer individuals, organizations, and governments the ability to acquire and exploit information at unprecedented speed. In business, diplomacy, and military might, this translates into a competitive advantage, suggesting that brains will beat brawn with increasing frequency over time and that computer resources will play a central role in future human conflict.

The original meaning of the term "hacker" was quite positive. It meant a very clever user of technology, specifically someone who modified hardware or software in order to stretch its limits, especially to take it beyond where its inventors had intended

29 Miller, 1989.

30 "Moore's Law..." www.intel.com.

31 These figures are from *The World Factbook*, published by the Central Intelligence Agency: "Internet hosts" are defined as a computer connected directly to the Internet, either from a hard-wired terminal, or by modem/telephone/satellite, etc.

it to go. Over time, however, the criminalization of hacking has led to a decay of the word's original meaning.

Regardless of a hacker's intentions, there are three basic forms of cyber attack[32] that national security planners should keep in mind.

The first type of attack targets the *confidentiality* of data. It encompasses any unauthorized acquisition of information, including via "traffic analysis," in which an attacker infers communication content merely by observing communication patterns. Because global network connectivity is currently well ahead of global and local network security, it can be easy for hackers to steal enormous amounts of sensitive information.

For example, in 2009 a Canadian research group called *Information Warfare Monitor* revealed the existence of "GhostNet," a cyber espionage network of over 1,000 compromised computers in 103 countries that targeted diplomatic, political, economic, and military information.[33]

The second type of attack targets the *integrity* of information. This includes the "sabotage" of data for criminal, political, or military purposes. Cyber criminals have been known to encrypt the data on a victim's hard drive and then demand a ransom payment in exchange for the decryption key. Some countries with poor human rights records have been accused of editing the email and blog entries of their citizens.[34]

The third type of attack targets the *availability* of computers or information resources. The goal here is to prevent authorized users from gaining access to the systems or data they require to perform certain tasks. This is commonly referred to as a denial-of-service (DoS) and encompasses a wide range of malware, network traffic, or physical attacks on computers, databases, and the networks that connect them.

In 2001, "MafiaBoy," a 15 year-old student from Montreal, conducted a successful DoS attack against some of the world's biggest online companies, likely causing over $1 billion in financial damage.[35] In 2007, Syrian air defense was reportedly disabled by a cyber attack moments before the Israeli air force demolished an alleged nuclear reactor.[36] And the Burmese government, during a government crackdown on political protestors, completely severed its Internet connection to the outside world.[37]

32 The term "cyber" is used generically to describe computers, networks, and digital information.

33 "Tracking GhostNet..." 2009.

34 Geers, 2007a.

35 Verton, 2002.

36 Fulghum et al, 2007.

37 Tran, 2007.

If computer users were isolated from one another, computer security management would be straightforward and rely primarily on personnel background checks and padlocks. But the benefits of networking are too great to ignore. Modern organizations require Internet connectivity.

The trick is to find the right balance between functionality, performance, and security. It is impossible to optimize the equilibrium with respect to all attacks. Before a military operation, if every soldier knew every detail of the plan, morale and readiness might improve, but it would be far easier for the enemy to become witting as well. On the other hand, when too few soldiers are in the know, the odds of success are lower.[38]

As during WW II, the national security community continued to lead the way. By 1967, the U.S. military had configured an IBM System/360 network with discrete levels of clearance, compartments, need-to-know, and centralized authority control. In the civilian world, however, system administrators could not prevent users from reading the data of another user until 1970. And even then, the administrative goal was to prevent accidental data corruption, not to protect users from one another.[39]

As Internet connectivity grew, malicious users and computer hackers were able to conduct increasingly asymmetric attacks. In theory, an attacker can target all Internet-connected computers simultaneously, with an attack that travels at near light-speed. The strength of the Internet – an accessible, collaborative framework based on common technologies and protocols – unfortunately makes it vulnerable to novel attacks and susceptible to swift and massive damage.

The notion of a computer worm or virus dates to 1949, when the mathematician John von Neumann proposed "self-replicating automata." However, such malware remained in an experimental stage[40] until the early 1990s.[41] Hackers wrote viral programs such as the Creeper worm, which infected ARPANET[42] in 1971 and a 1988 Internet virus that exploited weak passwords in SUN and VAX computers. However, these programs did not yet attempt to steal or destroy data.[43]

38 Saydjari, 2004.

39 Saltzer & Schroeder, 1975.

40 These were primarily boot-sector viruses that targeted MS DOS.

41 Chen & Robert, 2004.

42 The U.S. Advanced Research Projects Agency Network.

43 Eichin & Rochlis, 1989.

During the 1990s, as the number of Internet users grew exponentially, there was an explosion of malware, in both quantity and quality. In 2003, a DARPA[44]-funded study[45] categorized the known Internet worms[46] by attacker motivation:

- experimental curiosity (Morris/ILoveYou),
- non-existent or non-functional payload (Morris/Slammer),
- backdoor creation for remote control (Code Red II),
- HTML proxy, spam relay, phishing (Sobig),
- DoS (Code Red/Yaha),
- Distributed DoS (Stacheldraht),
- criminal data collection, espionage (SirCam),
- data damage (Chernobyl/Klez), and
- political protest (Yaha).

Clearly, the goal of computer hacking is limited only by the attacker's imagination. The DARPA study speculated that future worms could facilitate human surveillance, commercial advantage, the management of distributed malware, terrorist reconnaissance, and even the manipulation of critical infrastructures in support of cyber war objectives.

Why are hackers so successful, and are we improving our defenses against them?

Fortunately, an enormous amount of attention has been drawn to cyber security. For example, in 2002, Microsoft advertised its Trustworthy Computing Initiative, declaring that security would henceforth be at the forefront of Window's development.

44 The U.S. Defense Advanced Research Projects Agency.

45 Five worm characteristics were analyzed: target discovery, method of transmission, code activation, payload, and attacker motivation. Motivation is normally learned by studying the payload, or the non-propagation code, of malware.

46 A computer worm is a program that self-propagates across a network, exploiting security or policy flaws in widely-used services. Viruses typically infect non-mobile files and normally require some user action to move them across a network. Thus the propagation rate of a worm is typically much faster than with a virus.

Unfortunately, many common computer vulnerabilities are of a persistent nature.[47] These include:

- the high cost of producing quality software,[48]
- technical challenges associated with software patch deployment,
- susceptibility of the commonly-used C/C++ languages to buffer overflows and code-injection,[49]
- use of administrator rights by common system and user programs,[50] and
- the prevalence of "monoculture" computing environments.[51]

The computer security problem space is both broad and deep. In terms of quantity, in the single month of May 2009, Kaspersky Lab identified 42,520 unique samples of possible malware on its clients' computers.

In terms of quality, the cyber defense community is currently analyzing the most sophisticated piece of malware yet found – Stuxnet.[52] This worm targeted national critical infrastructures, specifically the SCADA[53] systems used to manage major industrial installations such as power grids and the Programmable Logic Controllers (PLCs) used to control devices such as pumps and valves.

Stuxnet's propagation strategy is a wonder to behold. It exploits at least four zero-day[54] vulnerabilities and employs two stolen digital certificates.[55] It targets "air-gapped"[56] networks via removable USB drives and is smart enough to attempt its exploits only when connected to a SCADA environment. Finally, in 2010, most of the

47 Weaver et al, 2003.

48 Unfortunately, even the most robust and scrutinized software, such as OpenSSH, OpenSSL and Apache, have been shown to contain major security vulnerabilities.

49 These refer to attacks that target ostensibly inaccessible computer memory space and the exploitation of flaws in a computer program to insert unauthorized hacker code.

50 Hackers take advantage of the fact that malicious code normally runs at the level of the user who executes it. This is why one should never surf the Web from an Administrator account.

51 The Windows operating system, for example, commands about 90% of the desktop market share.

52 Stuxnet was discovered by a Belarusian anti-virus firm in June 2010, but the worm had been active on the Internet, undetected, for at least one year.

53 Supervisory Command and Data Acquisition.

54 Zero-day vulnerabilities are computer weaknesses that are unknown to the cyber defense community, which a witting attacker may exploit at will.

55 Digital certificates contain sensitive and hard-to-acquire cryptographic information that is used to verify identities via the Internet.

56 Air-gapped networks are not physically connected to the Internet.

infected machines were located in a country of high interest to intelligence agencies around the world – Iran.[57]

A strategic challenge for cyber defense is that the Internet evolves so quickly it is impossible for any organization to master all of the latest developments. Over time, attackers have subverted an ever-increasing number of operating systems, applications, and communications protocols. Defenders simply have too much technical ground to cover, which is to a hacker's advantage and places a premium on defensive creativity, good intelligence, and some level of automated attack detection and response.

Lone Hacker to Cyber Army

Information operations are surely as old as warfare itself. A well-known example from the 20th century is the spectacular effort by the Allies to convince the German military leadership that the D-Day invasion would take place at Pas-de-Calais instead of Normandy.[58]

The first mention of a forthcoming "information war" in cyberspace is attributed to Thomas Rona, the author of a 1976 Boeing Corporation research paper entitled "Weapon Systems and Information War."[59] Rona perceived that computer networks were both an asset and a liability for any organization. Once a mission came to rely on the proper functioning of IT for success, computer systems would be among the first targets in war. Rona argued that all information flows within any command-and-control system are vulnerable to jamming, overloading, or spoofing by an adversary.[60]

In 1993, a widely-cited U.S. Naval Postgraduate School (NPS) article examined the historical aspects of "cyberwar." Its authors argued that the Information Revolution would change not only how wars are fought, but even why wars are fought. IT offered the world such increased organizational efficiency and improved decision-making that traditional hierarchies and political systems would be forced to evolve or die, and even international borders would have to be redrawn.

For militaries, IT-enhanced situational awareness was compared to the 13th century Mongol army's use of "arrow riders" on horseback to keep national leadership informed of distant battlefield developments with astonishing speed and to the advantage a chess player would have over a blindfolded opponent. Cyberwar could be

57 "Stuxnet..." 2010.
58 Churchman, 2005.
59 Rona, 1976.
60 Van Creveld, 1987.

to the 21st century what *blitzkrieg* or "lightning war" was to the 20th century, and a standard military goal will be to turn the balance of information control in one's favor, especially if the balance of conventional forces is not.

The NPS professors envisioned two levels of Internet conflict: a "netwar" of diplomacy and propaganda, and "cyberwar," which would encompass all military operations designed to attack an adversary's critical IT systems.[61]

In 2001, computer scientists from the Carnegie Mellon University Computer Emergency Response Team (CERT) wrote an article for the *NATO Review*, "Countering Cyber War," which argued that cyber attacks would play an increasingly strategic role in warfare and that NATO must immediately begin to plan for the defense of cyberspace.

The CERT team described three levels of cyber warfare. The first is a simple adjunct to traditional military operations to gain information superiority, such as by targeting an air defense system. However, because military functions such as early warning have an intrinsic strategic value to a nation, a successful cyber attack against air defense could lead to strategic losses.

The second level is "limited" cyber war. Here, civilian Internet infrastructure becomes part of the battleground, and the target list includes some civilian enterprises.

The third and most serious level is "unrestricted" cyber war. Here, an adversary seeks to cause maximum damage to civilian infrastructure in order to rupture the "social fabric" of a nation. Air-traffic control, stock exchange, emergency services, and power generation systems[62] could be targets. The goal is as much physical damage and as many civilian casualties as possible.[63]

In 2001, James Adams revealed in the pages of *Foreign Affairs* that the U.S. Department of Defense had in fact put cyber war theories to a real-world test in a classified 1997 Red Team exercise codenamed "Eligible Receiver." Thirty-five U.S. National Security Agency (NSA) personnel, simulating North Korean hackers, used a variety of cyber and information warfare (IW) tools and tactics, including the transmission of fabricated military orders and news reports, to attack the U.S. Navy's Pacific Command from cyberspace. The Red Team was so successful that the Navy's "human command-and-control system" was paralyzed by mistrust, and "nobody ... from the president on down, could believe anything."[64]

61 Arquilla & Ronfeldt, 1993.

62 Successful attacks on electricity grids have subsequent, unforeseeable effects on an economy because most infrastructures, including computer systems, rely on electricity to function.

63 Shimeall et al, 2001.

64 Adams, 2001.

Nonetheless, two important IW thinkers remained dubious. Georgetown University Professor Dorothy Denning agreed that "hacktivism"[65] had begun to influence political discourse, but argued that there had not been a single verifiable case of cyber terrorism, and believed that no cyber attack had yet caused a human casualty.[66]

Furthermore, James Lewis of the Center for Strategic and International Studies (CSIS) opined that cyber attacks were easy to hype because cyber security is an arcane discipline that is difficult for non-experts to understand. He argued that vulnerabilities in computers did not equate to vulnerabilities in critical infrastructures, and that terrorists would continue to prefer traditional physical attacks because the likelihood of real-world damage was much higher. While cyber attacks were a growing business problem, they did not yet pose a threat to national security.[67]

One decade later, it is possible that some militaries have crossed that threshold. A 2009 report on the cyber warfare capabilities of the People's Republic of China (PRC) described a highly-networked force that can now communicate with ease across military services and through chains of command. Furthermore, each military unit has a clear, offensive cyber mission in times of both war and peace. In peacetime, strategic intelligence is gathered via cyber espionage to help win future wars.[68] In war, a broad array of computer network operations (CNO), electronic warfare (EW), and kinetic strikes will be used to achieve information superiority over an adversary,[69] especially during the early or preemptive-strike phases of a conflict.[70]

Is cyber espionage alone capable of changing the balance of power among nations?

By 1999, the U.S. Energy Department had discovered hundreds of attacks on its computer systems from outside the United States and determined that Chinese hacking in particular posed an "acute" intelligence threat to U.S. nuclear weapons laboratories.[71]

The U.S. Joint Strike Fighter (JSF) is the most expensive weapons program in world history. Unknown hackers have stolen terabytes of JSF design and electronics data[72]

65 Hacktivism is a combination of hacking and political activism.

66 Denning, 2002.

67 Lewis, 2002.

68 As evidence of state-sponsorship, the report cites sophisticated hacking techniques and the collection of military and China-specific policy information that is of little commercial value.

69 One goal would be to create exploitable "blind spots" in an adversary's decision cycle that could, for example, lead to the delay of adversary military deployments.

70 Krekel, 2009.

71 Gerth & Risen, 1999.

72 Officials believed that the jet's most closely-held secrets, which pertained to flight controls and sensors, were safe because they had been stored on computers not connected to the Internet.

in a mammoth case of cyber espionage that has revealed a government's vulnerability to the security posture of its civilian contractors and the exasperating task of conducting a cyber battle damage assessment.[73] Based on the IP addresses used and other known digital fingerprints, the JSF attacks were believed with a high level of certainty to come from the Chinese military.[74]

From a strategic perspective, the cyber threat that hits closest to home and may eventually spur international agreements to mitigate the hacker threat relates to critical infrastructure protection (CIP). The potential target list seems endless: air traffic,[75] financial sector,[76] national elections,[77] water,[78] even electricity.[79] Trends suggest that all of the above are increasingly connected to the Internet, and that custom IT systems are over time replaced with less expensive Windows and UNIX systems that are not only easier to use, but easier to hack.[80]

Have real-world attacks on national critical infrastructures already taken place?

In May 2009, President Obama made a dramatic announcement: "Cyber attacks have plunged entire cities into darkness."[81] Investigative journalists subsequently concluded that the attacks took place in Brazil in 2005 and 2007, affected millions of civilians, and that the source of the attacks is still unknown.[82]

National Security Planning

Scientists began to warn the world about the danger of computer hacking shortly after WW II. Technical precautions, at least within the national security community, were implemented by the 1960s.

73 The hackers encrypted the JSF data they found before removing it from the network, so it was nearly impossible for investigators to determine exactly what had been stolen. JSF electronics run over seven million lines of computer code, more than triple currently used in the top Air Force fighter, so the attackers have potentially found many vulnerabilities to exploit in the future.

74 Gorman et al, 2009.

75 Gorman, 2009a.

76 Wagner, 2010. After the Dow Jones surprisingly plunged almost 1,000 points, White House adviser John Brennan stated that officials had considered but found no evidence of a malicious cyber attack.

77 Orr, 2007. In 2007, California held a hearing on the security of its touch-screen voting machines, in which a Red Team leader testified that the voting system was vulnerable to attack.

78 Preimesberger, 2006. In 2006, the Sandia National Laboratories Red Team conducted a network vulnerability assessment of U.S. water distribution plants.

79 Meserve, 2007. Department of Homeland Security (DHS) officials briefed CNN that Idaho National Laboratory (INL) researchers had hacked into a replica of a power plant's control system and changed the operating cycle of a generator, causing it to self-destruct.

80 Preimesberger, 2006.

81 "Remarks by the President..." 2009.

82 "Cyber War..." 2009.

As the size and importance of the Internet grew, however, there was a need for computer security to move from a tactical to a strategic level. And the driving force for national policy was the realization that a combination of persistent computer vulnerabilities and worldwide connectivity had placed national critical infrastructures at risk.

In 1997, Bill Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP). Its final report, *Critical Foundations: Protecting America's Infrastructures*, identified eight sectors of the U.S. economy that held strategic security value: telecommunications, electric power, gas and oil, water, transportation, banking and finance, emergency services, and government continuity.

PCCIP recognized not only the nation's dependence on its critical infrastructure (CI), but also the dependence of modern CI on IT systems. Further, it cited "pervasive" vulnerabilities that were open to attack by a "wide spectrum" of potential threats and adversaries.

Because the cyber attack threat to CI is strategic in scope, the national response must be equal to the task: public awareness, investment in education, scientific research, the development of cyber law, and international cooperation. New agencies and economic "sector coordinators" were also created,[83] but PCCIP emphasized that no single individual or organization could be responsible for CIP because critical infrastructures are collective assets that the government and private sector must manage together.[84]

On December 4, 1998, Russia sponsored United Nations (UN) General Assembly Resolution 53/70, "Developments in the field of information and telecommunications in the context of international security." It stated that science and technology play an important role in international security, and that while modern information and communication technology (ICT) offers civilization the "broadest positive opportunities," ICT was nonetheless vulnerable to misuse by criminals and terrorists. UN member states were therefore requested to inform the Secretary-General of their concerns regarding ICT misuse and offer proposals to enhance its security in the future. The UN adopted Resolution 53/70 on January 4, 1999.[85]

The most successful international cyber security agreement to date – the Council of Europe Convention on Cybercrime – opened for signature in 2001. This treaty takes

83 PCCIP led to many developments relative to cyber security, including Presidential Decision Directive 63 (PDD-63), National Infrastructure Protection Center (NIPC), Critical Infrastructure Assurance Office (CIAO), National Infrastructure Assurance Council (NIAC), Information Sharing and Assessment Centers (ISACs), and DoD Joint Task Force—Computer Network Defense (JTF-CND).

84 Neumann, 1998.

85 "53/70..." 1999.

aim at copyright infringement, fraud, child pornography and violations of network security policy. It offers guidelines to law enforcement regarding data interception and the search of computer networks. Its ultimate goal is a common policy on cyber crime worldwide via national legislation and international cooperation. Currently, the Convention has forty-seven national signatories, thirty ratifications, and is the primary legal instrument available to nation-states with respect to cyber security.[86]

At the level of national security, the most visible changes in cyber defense strategy have taken place within the U.S. military. A turning point occurred in 2008, when unknown hackers successfully compromised classified military systems in the "most significant breach" of U.S. military computers ever.

U.S. Deputy Secretary of Defense William J. Lynn wrote in *Foreign Affairs* that adversaries now have the power to disrupt critical U.S. information infrastructure, and that the asymmetric nature of hacking means that a "dozen" computer programmers can pose a national security threat. Over the long term, Lynn believed that computer hacking can lead to the loss of enough intellectual property to deprive a nation of its economic vitality.

The most tangible U.S. response has been the creation of its military Cyber Command in 2010. USCYBERCOM has three primary missions: computer network defense, the coordination of national cyber warfare resources, and cyber security liaison with domestic and foreign partners. Its first mission, defense, relies on a combination of traditional best practices in computer security and classified intelligence threat information, to create a unique, "active" U.S. cyber defense posture.[87]

The quest for strategic cyber defense took its most recent step forward in Lisbon, Portugal, in November 2010, where twenty-eight national leaders from the world's foremost political and military alliance published a new "Strategic Concept" for the North Atlantic Treaty Organization (NATO).

This document clearly illustrates the rapid rise in the perceived connection between computer security and national security. The previous Strategic Concept, written in 1999, did not contain a single mention of computers, networks, or hackers. The new document, entitled "Active Engagement, Modern Defence," describes cyber attacks as "frequent, organized, and costly," and having now reached a threshold where they threaten "national and Euro-Atlantic prosperity, security and stability."

If NATO hopes to defend the cyber domain, it must improve its ability to prevent, detect, counter and recover from cyber attacks. At a minimum, this requires placing

86 From the Council of Europe Convention on Cybercrime website: http://conventions.coe.int/.

87 Lynn, 2010.

all NATO bodies under centralized cyber protection, upgrading member state cyber defense capabilities, and coordinating the efforts of national and organizational cyber security resources.[88]

In fact, NATO may be the best place to begin answering the national security challenge posed by cyber attacks. The Internet is now an international asset. As such, threats to it require an international response. As a large group of affluent nations with a shared political and military agenda,[89] it is possible that NATO today could deal a significant blow to one of a hacker's greatest advantages – anonymity.[90]

More Questions than Answers

Although the first modern computer was designed at Cambridge in 1837, in many ways the Information Revolution has just begun. The World Wide Web, for example, is just twenty years old.[91]

As our use of and dependence on the Internet have grown, however, computer security has quickly evolved from a purely technical discipline to a geopolitical strategic concept. At the 2010 NATO Summit in Lisbon, twenty-eight world leaders declared that cyber attacks now threaten international prosperity, security, and stability.

Moreover, in the future the consequences of a cyber attack may rise because the threat will affect national critical infrastructures of every kind. In our homes, the use of "smart grid" networks is proliferating. And in our militaries, the production of IP-enabled munitions, such as unmanned aircraft, is outpacing that of their manned counterparts, meaning that even warfare is now managed remotely via the Internet.[92]

As national security thinkers attempt to defend their interests in cyberspace, a key to success will be to bridge the gap between cyber strategy and cyber tactics. Goals such as the security of national critical infrastructures and strategies like military deterrence and arms control demand a greater appreciation for the capabilities and challenges of computer scientists, who fight their battles on the front lines of cryptography, intrusion detection, reverse engineering, and other highly technical disciplines.

88 "Active Engagement..." 2010.

89 NATO is much larger than its 28 Member Countries. It also encompasses 22 members of the Euro-Atlantic Partnership Council, 7 Mediterranean Dialogue, 4 Istanbul Cooperation Initiative, and 4 Contact Countries.

90 Three areas of obvious collaboration could be in network security, law enforcement and counterintelligence.

91 The Web was conceived at the European Organization for Nuclear Research (CERN) in 1990.

92 Orton, 2009.

The quest for strategic cyber security began in Cambridge and paused most recently in Lisbon, but for emerging policies to reflect technical realities, policymakers must return to Cambridge.

3. CYBER SECURITY: A TECHNICAL PRIMER

Chapter 2 demonstrated that cyber security has evolved from a purely technical discipline to a strategic, geopolitical concept that can directly impact national security. Nonetheless, at the tactical level cyber security remains a highly technical discipline that is difficult to understand for those without a formal education in computer science or information technology.

Therefore, before this research examines the real-world impact of cyber attacks and explores strategic threat mitigation strategies, Chapter 3 will introduce the reader to the basics of cyber security analysis, macro-scale hacking, the case-study of Saudi Arabia, and cyber defense exercises. Hopefully, a greater appreciation for the challenges of computer science will help policy makers to bridge the gap between tactical and strategic cyber security thinking.

Cyber Security Analysis

To introduce the reader to the topic of cyber security analysis, the author will briefly analyze his own personal firewall log.[93]

Almost everyone today has a personal or "host" firewall installed on his or her computer. It protects both the computer and its user from unwanted network activity. Technically speaking, it accepts or rejects incoming data "packets." Professional computer security analysts examine the log files, or recorded events, of firewalls and other computing devices for signs of suspicious activity.

Most of the recorded network traffic is non-malicious even if it may be unsolicited and unwanted. For example, an Internet Service Provider (ISP) may "scan" its clients' computers for policy violations such as hosting an unauthorized Web server. Businesses go to extraordinary and sometimes unethical lengths to gather in-depth information about computers and their users, such as which operating system they use and what type of movies they prefer, for advertising purposes.

Firewall logs can be viewed in many different ways. A security analyst can sort them by country, for example, to identify blocked traffic by world geography.[94]

93 This analysis is of a Zone Alarm personal firewall log that contains 12,700 record entries from 31 DEC 2000 to 23 JAN 2003.

94 My firewall had blocked traffic from over 70 foreign countries.

COUNTRY	FAILED ACCESS
Canada	121
Brazil	115
France	93
Taiwan	46
Poland	21

Countries robust in international network infrastructure, such as Canada and Taiwan, will always appear in network traffic. Connections to or from more isolated countries, especially when no logical business relationship can be identified, require close scrutiny.

For a more detailed view, IP addresses can be associated with a specific network.

IP ADDRESS	FAIL	OWNER
141.76.XX.XX	25	Tech Univ Informatik, Dresden, Germany
203.241.XX.XX	18	Samsung Networks Inc., Seoul, Korea
212.19.XX.XX	12	Tribute MultiMedia, Amsterdam, Netherlands
61.172.XX.XX	8	CHINANET Shanghai province network
192.58.XX.XX	5	University of California, Berkeley

Unfortunately for the analyst, most computer network logs contain many potential threats to investigate.

The IP addresses listed in a log file are not always the true source of network traffic. Obtaining reliable "attribution" is one of the most frustrating aspects of cyber attacks, as hackers often forge or "spoof" the IP address of an unwitting, third party network. This is possible because Internet routers, for the sake of efficiency, normally only use a data packet's destination address to forward it across the Internet and disregard the source address.

How to improve attribution is one of the hottest topics in cyber defense research. At a minimum, security analysts must use a combination of technical databases such as WHOIS,[95] non-technical Web tools such as a good Internet search engine, and common sense, which helps to verify whether the discovered network traffic corresponds logically to real life activity.

95 WHOIS can tell you the owner of an Internet Protocol (IP) address.

Firewalls are designed to block many types of suspicious traffic automatically, and often they will prohibit everything that a user does not specifically allow. For example, there are over 65,000 computer "ports," or points of entry, into an operating system. By default, my firewall blocked access to the following notorious ports that are associated with "trojans," or hacker programs that allow illicit remote access to a victim computer.

PORT	TROJAN
1243	SubSeven
1524	Trinoo
3128	RingZero
27374	Ramen
31337	Back Orifice

Blocking known malicious traffic seems easy enough, but hackers are adept at subverting whatever connections are allowed onto your computer. For example, the Internet Control Message Protocol (ICMP), commonly used for network management, is fairly simple in design and would seem amenable to security observation. However, hackers routinely use it for target reconnaissance, Denial of Service (DoS) attacks, and even as a covert channel for communications.

Analyzing outbound traffic is just as important as inbound traffic, if not more so. To begin, a security analyst should sort outbound firewall log data by the names of the programs installed on the computer. He or she should verify that legitimate programs are only contacting legitimate IP addresses, e.g., Microsoft Word should only contact Microsoft.

All unrecognizable programs should be examined closely. Often, quick Internet searches will suffice. However, if there is no proper (and reassuring) description for it on the Web, the program should be disallowed from contacting the Internet, if not uninstalled from the computer altogether.

My firewall log showed that one unidentifiable program, ISA v 1.0, had tried to contact a remote computer in both China and France. I could not find any information about the program on the Web, so deleted it from the system.

PROG	IP ADDRESS	DESTINATION	DATE
ISA 1.0	61.140.X.X	Chinanet Guangdong province	7/30/2001
ISA 1.0	193.54.X.X	Universite Paris, France	8/10/2001

Another program, WINSIP32.EXE, had tried three times to connect to a U.S. government agency, the General Services Administration (GSA).[96] A further red flag was that the name of the program was suspiciously close to WINZIP, a common program used to minimize file size for transmission via the Internet. I tried unsuccessfully to discuss the issue with a GSA system administrator, who almost certainly managed a hacked network.

DATE	TIME	PROGRAM	REMOTE IP ADDRESS
2/18/2002	20:17:06	WINSIP32.EXE	159.142.XX.XX
3/15/2002	07:06:17	WINSIP32.EXE	159.142.XX.XX
3/20/2002	14:54:39	WINSIP32.EXE	159.142.XX.XX

The level of technical expertise and experience required to thoroughly evaluate computer network security is high. An analyst must understand hardware and software, as well as Internet protocols, standards, and services. Security is an art as well as a science that involves common sense, original research, risk management, and a willingness to pick up the phone and speak with unknown system administrators.

In fact, the problem of attribution is the most complicating factor in cyber threat analysis. If the attacker is careless and leaves a large digital footprint (e.g., his home IP address), law enforcement may be able to take quick action. If the cyber attacker is smart and covers his digital tracks, then deterrence, evidence collection, and prosecution become major challenges.

In almost all cases, computer log files alone do not suffice. Unmasking a cyber attacker requires the fusion of cyber and non-cyber data points. Investigators must enter the real world if they want to arrest a computer hacker. There will always be clues. If the goal is extortion, where is the money to be paid, and is there a point-of-contact? If the threat is Denial of Service, the target could ask for a proof of capability. The point is to generate a level of interactivity with the cyber threat actor that might be used against it. Further, cross-checking suspect information against trusted sources is always one of the best defenses.

In this chapter, the author has tried to make clear that catching a computer hacker is not a simple chore. Cyber attackers are often able to hide in network traffic and remain anonymous to their victims. Still, this does not mean that cyber attacks can easily rise to the level of a strategic threat; but it does mean that, when they do, national security leaders can be in the awkward position of not knowing who is attacking them.

This is the topic of the next chapter.

96 GSA supports the basic functioning of other federal agencies.

Macro-Scale Hacking

If one successfully attacked computer can pose a security threat, what if an adversary could secretly command thousands or even millions of computers at once? At what point does a tactical cyber attack become a strategic cyber attack?

In fact, these are no longer academic questions. The Conficker worm is now estimated to have compromised at least seven million computers worldwide,[97] leaving an unknown cyber attacker, in theory, in control of their aggregated computer processing power.

"Botnets" are networks of hacker-controlled computers that are organized within a common Command and Control (C2) infrastructure.[98] Hackers often use botnets to send spam, spread malicious code, steal data, and conduct Denial of Service (DoS) attacks against other computers and networks around the world.

In the future, botnets may be used to conduct more complex and far-reaching attacks, some of which could have national security ramifications. One scenario, demonstrated in 2009 by the author and Roelof Temmingh,[99] envisioned a "semantic botnet," composed of a virtual army of randomly-generated and/or stolen human identities,[100] which could be used to support any personal, political, military, or terrorist agenda.[101]

Such a cyber attack is possible because humans now communicate via ubiquitous software that is by nature impersonal and non-interactive. A botnet made up of thousands or millions of computers could be used to post a wide range of information, opinions, arguments, or threats across the Internet. These could target a person, an organization, or a nation-state and promote any political or criminal cause. The amplification power of the Internet guarantees that not every victim must fall for the scam; a certain percentage will suffice.

Most of the information found on the Internet is open to theft and/or abuse. Hackers can steal any type of file, text, or graphics and alter it for nefarious purposes. Although effective authentication technologies such as digital signatures exist, they are rarely used for common communications.

97 Piscitello, 2010.

98 Freiling et al, 2005.

99 Temmingh is the founder of Sensepost and Paterva. Their 2009 paper was presented at the CCD CoE Conference on Cyber Warfare.

100 Ramaswamy, 2006. In 2006, identity theft was already the fastest-growing crime in the United States, affecting almost 20,000 persons per day. Acoca, 2008. Nearly a third of all adults in the U.S. reported that security fears had compelled them to shop online less or not at all.

101 Geers & Temmingh, 2009.

The calculated, political manipulation of information, which is today most often found in the form of computer data, is not uncommon. In 2006, *Reuters* news service, prior to publishing a photo, darkened the sky over Beirut to make an Israeli air raid appear more dramatic;[102] in 2008, newspapers published a photo of an Iranian missile test in which an extra missile had been added;[103] and in 2010, *Al-Ahram* newspaper in Cairo printed a photo after it had switched the places of Presidents Obama and Mubarak at the White House.[104] Without some kind of technical means of verification, it can be difficult even for writers and photographers to know that their own work has not been modified.

Distinguishing fact from fiction – and humans from robots – is difficult online, especially in a timely and accurate way. Hackers will exploit the maze-like architecture of the Internet, and the anonymity it offers, to make threat evaluation slow and labor-intensive. In short, there is no quick way to determine whether a virtual person really exists. Over time, a fraudulent virtual identity would even come to have a "life" of its own as it posts a variety of information to the Web.

Historically, computers have had great difficulty impersonating a human being. In 1950, Alan Turing wrote that even the "dullest" human could outperform a computer in a conversation with another human, and that a machine could not provide a "meaningful answer" to a truly wide variety of questions. The celebrated Turing Test was born.[105]

However, Internet communications are increasingly impersonal conversations. This creates an *attack space* for a hacker because there is normally insufficient content and interactivity to evaluate whether a particular message was posted by a human or a machine.

The average computer programmer could never pass the Turing Test, but he or she could write a program to update the world via Twitter on how a fraudulent Web user is spending her day, or what she thinks about a political leader.

Every day, email is losing ground to new media such as YouTube, Facebook, and Twitter. Although the opportunity to cross-examine someone by email is limited, it does exist; email is typically interactive, one-to-one correspondence.[106] The new communication models are not one-to-one, but one-to-many or many-to-one. Users feel empowered as they quickly become a prolific producer of digital information;

102 Montagne, 2006.

103 Nizza & Lyons, 2008.

104 "Doctoring photos..." 2010.

105 Oppy & Dowe, 2008.

106 Internet Relay Chat (IRC) is also interactive, but it was never a mainstream form of communication.

however, much of the output is trivial, and there is a loss of intimacy and interactivity. This benefits a cyber attacker, who can push information to the Web that would not be subject to serious cross-examination.

Due to the speed of modern communications, humans do not have much time to analyze what they read on the Web. Was a message posted by a human or a machine? It will be hard to know when even highly idiomatic language can be stolen and repackaged by a hacker. And Natural Language Processing, or the computer analysis of human languages, is still unproven technology that requires significant human oversight to be effective.[107]

It is increasingly difficult to separate cyberspace from what we think of as the real world; human beings respond to stimuli from both. If a botnet were used to promote a political or military goal, once a certain momentum toward the desired goal were attained – that is, if real people began to follow the robots – the attacker could then begin to scale back the Artificial Intelligence (AI) and reprogram the botnet for its next assignment.

It may not matter if the botnet campaign could eventually be discovered and discredited. In time-sensitive contexts such as an election it might be too late. The attacker may desire to sway public opinion only for a short period of time. In the week before an election, what if both left and right-wing blogs were seeded with false but credible information about one of the candidates? It could tip the balance in a close race to determine the winner. Consider the enormous impact of the 2004 Madrid train bombings on Spain's national elections, which took place three days later.[108]

Roelof Temmingh, who is a brilliant programmer, wrote a complex, copy-and-paste algorithm to collect biographical information and facial images from various websites and used them to construct skeletons of randomized, artificial personalities. Personal profiles, including categories such "favorite movie," were added based on details from popular news sites. In future versions of the software, these fraudulent identities would begin to interact with the Web. This is the most difficult step, but far from impossible to implement. Over time, each new identity would assume a virtual "life" of its own.

Phishing attacks are successful even though they normally employ only one layer of deceit – the website itself. Intelligent attackers can weave a much more intricate web of deception than that; an entire organization could successfully be faked if the time were taken to invest in enough third-party references.

107 Author interview with Temmingh, 2009.

108 "Europe..." 2004.

One of the primary reasons that such a cyber attack could succeed is the growing power of Web-enabled Open Source Intelligence (OSINT). The average Web user today has access to a staggering amount of information. Beginning with only a name, a good OSINT researcher can quickly obtain date-of-birth, address, education, medical records, and much more. Via social networking sites, the attacker may even discover intimate details of a person's life, including where he or she might physically be at any given moment. Eventually, a web of connections to other people, places, and things can be constructed.

Computer hackers are not only able to conduct OSINT via the Web, but also exploit the technical vulnerabilities of the Web to target their victims. Hackers "enumerate," or conduct in-depth technical reconnaissance, against cyber targets, for information such as an IP address, a timestamp, or other "metadata" that can be exploited in the real world.

A semantic botnet could enhance the credibility of any agenda. For example, if the target were an international energy corporation, OSINT might reveal a wide range of attack vectors: disgruntled employees, friction with indigenous populations, whistleblowers, or ongoing lawsuits. The botnet army could be used to target all of the above, via blogs, posting comments to news articles, sending targeted email, etc. (The corporation, of course, could hire its own botnet army in retaliation.) The challenge for the attacker would be to make the communications as realistic as possible while making identity verification a complex and time-consuming challenge.

Given the size of cyberspace and the speed at which data packets travel, one of the primary ways to combat a macro-scale cyber threat is by statistical analysis. A security analyst must use advanced mathematics to identify and counter cyber threats.

In an election, humans typically vote in a "bell curve." Some people are extremists, but most tend to vote for a party somewhere in the middle of the political spectrum. If a botnet controller does not simulate this tendency, statistical analysis of network traffic and internal databases can quickly reveal divergences that could suggest a tainted vote. These include a randomized voting preference (i.e., too many votes on the extremes), demographic anomalies, or strange patterns such as too many votes during normal human working hours.

Technical data should not conflict with a security analyst's common sense. IP addresses must be scattered realistically within the voting space. Internet browsers should manage website visits as a human would, pausing for images to load and allowing time for a user to read important information. Automated computer programs may move too quickly and "mechanically" from one data request to the next. A security analyst should investigate anomalies for other non-human properties.

The primary challenge to a statistical cyber defense strategy is a mathematically-gifted attacker. In theory, it is possible to give a botnet army a range of dynamic characteristics that are based on real-time analysis of current news and entertainment media. However, this is not easy to program, and an attacker can never be completely sure what a security analyst is looking for. An attack always requires some guesswork and miscalculation.

Over time, this is a game of cat-and-mouse. A security analyst can write a sophisticated algorithm that correlates many factors, such as name, vote, geography, education, income, and IP address, to known or expected baselines. However, a botnet controller can do the same.

One pitfall for the attacker is that, if the bots vote too realistically, or if there are too few bots involved in the attack, there should be a correspondingly small impact on the election. Moreover, in order to mirror real Internet traffic patterns, a botnet needs to be both large and sophisticated.

Of course, there are some purely technical investments to be made, including the increased use of Public Key Infrastructure (PKI), biometrics and Internet Protocol version 6 (IPv6). Neural networks, for example, have played a considerable role in reducing credit card fraud.[109] For important business transactions, the simple use of a live video feed is beneficial.

Unfortunately, the use of good cyber defense tactics and technologies is rare. Most system administrators do not have the time, expertise, or staff to undertake a sophisticated analysis of their own networks and data. For the foreseeable future, much of the burden is on individual web users to recognize threats emanating from cyberspace and take action (or inaction) to counter them.

This chapter has tried to argue that macro-scale cyber attack threats are serious, but most, such as the theoretical botnet army described in this chapter, do not yet pose a threat to national security. It is possible to create one fraudulent web identity, so millions of them could already exist. However, what makes many categories of cyber attack easy – the ubiquity, vulnerability, and anonymity of the web – can also lessen the credibility of a cyber threat. Good OSINT can lead to a significant bluff.

To a large extent, the most dangerous threat actors are those with the ability to bridge the gap between the virtual and physical worlds. Thus, there are two important categories of cyber attacker: those who have "reach" into the real world, and those whose threats are limited to cyberspace. The trouble from a strategic, national

109 Rowland, 2002.

security perspective is that foreign intelligence services and militaries possess that kind of reach, which obviously can make a cyber attack much more serious.

All things considered, cyber attacks have the potential to rise to the level of a strategic threat. Therefore, they must be addressed by national security planners. The next chapter will examine how one nation-state, Saudi Arabia, has attempted to mitigate this threat at the national level.

Case Study: Saudi Arabia

Every country has a unique perspective on security, especially a country as tradition-bound as Saudi Arabia. But at the technical level, the quest for strategic cyber security mostly comprises the exact same elements: computer hardware, software, legal authority, system administrators, and cyber security experts. Therefore, Saudi Arabia, where there is a strong perception of a close connection between computer security and national security, provides an instructive example.

The Saudi government censors a wide range of information based on a mix of morality, security, and politics. It has built a national firewall designed to keep "inappropriate" web content out of the country, inaccessible from anywhere within its borders, at any time, in public or private spaces. However, from both a semantic and a technical perspective, it is difficult, especially in authoritarian countries, to balance the public's need and desire for information with the government's need and desire to maintain information control.

Myriad technologies exist that can circumvent or even punch a hole straight through the Saudi national firewall. These include international telephone calls to foreign Internet Service Providers (ISPs), hacking Internet protocols, pseudonymous email accounts and remailers, direct-to-satellite access, peer-to-peer networking, anonymous proxy servers, encryption, steganography, and more. As censorship circumvention tools, all have strengths and weaknesses, and none of them is perfect.

Specific software applications are not prohibited in the Kingdom per se. For example, the King Abdul-Aziz City for Science and Technology (KACST) explained that Internet chat programs are allowed unless the software in question is specifically linked to the distribution of pornography.[110]

Content-filtering on a national scale is a monumental task. The Saudi government built a national proxy server[111] at KACST to surveil the nation's Internet traffic for

110 "The Internet..." Human Rights Watch.

111 Or a single, centralized connection between Saudi Arabia and the outside world, capable of censoring undesirable information.

"appropriateness" according to Muslim values, traditions, and culture.[112] Internet Service Providers must conform to these rules in order to obtain an operating license.[113]

Such laws are easier to enforce in some countries than others. In Saudi Arabia, the effort is greatly facilitated by the fact that the entire telecommunications network, including international gateways, are owned and operated by the government.[114]

Saudi Arabia is home to some of the most educated citizens in the Arab world. Furthermore, Saudis routinely communicate with each other and with the outside world on a modern and sophisticated telecommunications infrastructure.[115] The Kingdom has been connected to the Internet since 1994, but until 1999 access was restricted to state, academic, medical, and research facilities.[116] Today, home accounts are widespread, and there are hundreds of cyber cafes in the country. Men and women are both active Web surfers, and their average daily time online is over three hours.[117]

The amount of data processed by KACST every day is so great that the national firewall took two years to build. Due to the sensitive nature of its mission, the entire project is housed under one roof. Technicians are imported from places like the USA and Scandinavia,[118] but the censors handing out directives regarding what Web content to block are exclusively Saudi Arabian.[119]

KACST is analogous to a national post office through which all domestic and international correspondence must travel. There are now dozens of private ISPs in Saudi Arabia.[120] However, KACST is the country's only officially sanctioned link to the Internet, and all ISPs must route their traffic through its gateway.[121] Electronic data is unlike traditional mail in that it is broken into small packets to increase the speed with which it travels through cyberspace, but these packets are reassembled at KACST for inspection.[122]

From the beginning, KACST's goals were ambitious. Its president, Saleh Abdulrahman al-'Adhel, said that, before his organization would turn on the switch to the

112 Whitaker, 2000.
113 "Saudi Arabian Response..." Virginia Tech.
114 "Cybercensorship..." Human Rights Watch.
115 Dobbs, 2001.
116 Gavi, 1999 and 2002.
117 "Saudi Arabia to double..." 2001.
118 Gardner, 2000.
119 "SafeWeb..." 2000.
120 "The Internet..." Human Rights Watch.
121 "Losing..." 2001.
122 "How Users..." Human Rights Watch.

Internet, KACST would try to eliminate all of the Internet's negative aspects.[123] However, KACST technicians knew that they could not accomplish these goals without strictly regulating the behavior of individual users. Therefore, they forbade the sending or receiving of encrypted information as well as the sharing of usernames and passwords.[124]

Saudi Arabia's first line of defense is a list of banned URLs that are explicitly denied when requested by a user from a browser window.[125] Many websites commonly accessed outside Saudi Arabia are forbidden.

For those websites that are allowed through the filter, Web users access "cached" copies of Internet sites on government-controlled web servers physically located in the country.

When a user attempts to visit a website that has not been evaluated by KACST censors, a second stage of the content-filtering system is activated. Software automatically examines the site's content for prohibited words before the request is granted. One of the first is the presence of a "stop word" on the homepage.[126] A list of banned topics stops the request from getting through the KACST proxy server. There are at least thirty categories of prohibited information,[127] and the number of banned sites goes well into the hundreds of thousands.[128]

When access to a site is denied, either because its URL is already on the banned list or it is found to contain objectionable material, a pop-up warning window appears on the screen. It informs the user in both Arabic and English, "Access to the requested URL is not allowed!"[129] It also informs the user that all Web requests are logged.[130] The second warning is important, because law enforcement can, with an IP address, find the computer terminal in question and possibly also locate the end user. This is why in many countries publicly available Internet terminals that allow for easy, anonymous web surfing, are scarce.[131]

The two-stage system described above is the one advertised by the Saudi government. However, there are more stifling approaches to censorship, such as the use of a "whitelist," of which the Saudi government has been accused. Blacklists ban

123 "Saudi Arabian Response..." Virginia Tech.
124 "The Internet..." Human Rights Watch.
125 "The Internet..." Human Rights Watch.
126 "Government-Imposed..."
127 "Losing..." 2001.
128 "Saudi Arabia to double..." 2001.
129 Lee, 2001.
130 Gavi, 1999 and 2002.
131 "How Users..." Human Rights Watch.

material based on the fact that it has been officially reviewed and deemed to contain inappropriate content.[132] Whitelisting, a far stricter policy, takes a dramatically different approach, banning everything that is not explicitly allowed.[133] In other words, there is no need for a two-stage system. When a user tries to visit an unfamiliar webpage, there is simply no response. The only accessible websites have been pre-approved by the government. Some reporting has quoted "industry insiders" as stating that an internal KACST committee officially sanctions a list of "desirable" sites, and all others have been banned by default.[134]

With such power over Saudi networks, KACST has the ability to do far more than simple website content filtering. In theory, KACST network administrators can read, block, delete, or alter network traffic based on email address, IP address, or keywords in the message. For example, if "royal family" and "corrupt" were found to exist in the same sentence, such a message could be flagged for closer inspection, perhaps by law enforcement authorities.[135]

Technical support for such a large system requires an enormous effort. At least ten companies from four foreign countries have played a role in its administration, including Secure Computing, Symantec, Websense, Surf Control, and N2H2.[136]

Secure Computing's software is called SmartFilter. Saudi Arabia began using it as soon as the country was officially connected to the Internet in February 1999. SmartFilter ships with default content categories like pornography and gambling, but it was selected by KACST due to its overall ease of customization.

An example of widely-used, open source censorship software is DansGuardian, which is advertised as sophisticated, free Internet surveillance, to create "a cleaner, safer, place for you and your children." Its settings can be configured from "unobstructive" to "draconian," and it can filter data by technical specifications such

132 Such as the words "government" and "corrupt" appearing in the same sentence. From a censor's perspective, the problem with blacklisting is that it can be easy to fool the system, for example by simply misspelling those words: i.e. "govrment" and "korrupt."

133 "Government-Imposed..."

134 "The Internet..." Human Rights Watch.

135 "How Users..." Human Rights Watch.

136 There are many content filtering software products to choose from, including 8e6, CensorNet, Content Keeper, Cyber Patrol, Cyber Sentinel, DansGuardian, Fortinet, Internet Sheriff, K9, N2H2, Naomi, Net Nanny, SmartFilter, squidGuard, Surf Control, We-Blocker, Websense, and more. Each can be configured for a single schoolroom or an entire nation-state.

as URL, IP, domain, user, content, file extension, and POST. There are many more advanced features to choose from.[137]

Privacy advocates criticize the software companies that create such tools, but industry representatives counter that their products are politically neutral. According to an executive at Secure Computing, "We can't enforce how they use it."[138]

Pornography is the first topic Saudi authorities mention when asked about Internet censorship. And KACST claims that the battle against pornography has been successful.[139] But according to human rights groups, Saudi Arabia also disallows many political sites.[140]

A case in point is the website of a London-based dissident group called the Movement for Islamic Reform in Arabia (MIRA) (**www.islah.org**). MIRA's IP address was on KACST's list of banned sites, which was apparent in MIRA's computer log files. MIRA decided to change its IP address, and immediately the site was available again inside Saudi Arabia. (MIRA did not know why the second stage of KACST's system was not able to block the website based on content.) Eventually, the new IP address was discovered by KACST technicians, who blocked it again. This process repeated itself many times over; on average, MIRA was able to stay ahead of the government for about a week at a time. Its challenge was to make interested Saudi citizens aware of its new address before the block was in place again.[141]

MIRA was not satisfied with this protracted game of hide-and-seek, so its webmasters developed better solutions. First, the site randomized its port numbers, adding more than 60,000 possible Web addresses (equal to the number of available ports on a computer) to each new IP address. This change made it more difficult for KACST to do its detective work, since the Web requests leaving Saudi Arabia for MIRA were not necessarily headed for port 80, which normally hosts websites.[142]

Next, MIRA developed a novel way to let its followers know the new address. Its email server, **islah@islah.org**, would respond to a blank email with an automatic reply, containing the IP and port number. From Saudi Arabia, the blank emails were sent from webmail accounts such as Hotmail, whose secure, web application login

137 Advanced features include PICS labeling, MIME type, regular expressions, https, adverts, compressed HTML, intelligent algorithm matches for phrases in mixed HTML/whitespace, and phrase-weighting, which is intended to reduce over- and under-blocking. Furthermore, there is a whitelist mode and stealth mode, where access is granted to the user but an alert is nonetheless sent to administrators.

138 Lee, 2001.

139 Gardner, 2000.

140 "The Internet..." Human Rights Watch.

141 "Losing..." 2001.

142 Dobbs, 2001.

process made it impossible for KACST to see where the emails were going or what information they contained.

MIRA's head, Dr. Saad Fagih, said that following these changes, the number of Saudi visits to his site rose to 75,000 per day, and that before long KACST abandoned its efforts to block the site. [143]

From a technical perspective, it is a challenge even to begin to censor the Internet. But to evaluate frequently changing websites for their moral and political content is a monumental task. Computer software can recognize individual words, but understanding how they are used by an author in a given sentence or article is much more difficult. Words such as "breast" can be used to block sexual references to women, but the system may also block recipes for cooking chicken breasts. Likewise, it is difficult to avoid sexual references when offering medical advice related to sexually-transmitted diseases (STDs).[144]

Critics say that the decision to censor information at all leads to over-censorship.[145] For example, in practice it is convenient to block an offensive website by IP address. However, this means that any other website sharing the same IP will also be blocked.[146] An attacker can exploit this – and conduct a denial-of-service attack against a target website – simply by "poisoning" its webserver with prohibited material. Ideally, all censored information should be double-checked by real people to make sure that the system is working properly, but that may not always be practical or even possible.

OpenNet Initiative researchers claim that blocked sites include material related to religion, health, education, humor, entertainment, general reference works, computer hacking, and political activism. But Saudi authorities argue that their system has safeguards against both over- and under-censorship. KACST provides forms for users to request additions to and removals from the blacklist, and they say hundreds of requests are received each day asking for new sites to be banned, of which about half are subsequently blacklisted. Thus, based on user feedback, around 7,000 sites a month are added to the list. Over 100 requests to unblock sites also arrive each day, many based on a belief that the system has mischaracterized certain web content, but no statistics were offered regarding how many are unblocked.[147]

143 "Losing..." 2001.
144 "Government-Imposed..."
145 Whitaker, 2000.
146 "Government-Imposed..."
147 Lee, 2001.

On balance, pornography is easier to censor than politics. Vulgar words can simply be removed from network traffic, but software cannot readily determine whether political keywords are used in a positive or negative way by an author. Furthermore, foreign computer technicians are also of little help since the author's intention may have been positive feedback, constructive criticism, humor, irony, sarcasm, or satire. A proper evaluation requires subject matter experts who are fluent in the local language, a naturally expensive and time-consuming undertaking.

The problem for censors is that users who are intent on obtaining forbidden information often find a way to get it. And Saudi citizens are no different. Some access the Internet simply by finding computer terminals they assume are not being monitored.[148] Others make expensive telephone calls to unrestricted foreign ISPs.[149] Increasingly, Saudi citizens have acquired direct-to-satellite Internet access, with dishes small enough to fit discreetly on a balcony or rooftop.[150]

Blocked websites "mirror" their content on known accessible sites, or users forward the forbidden content by email as an attached file.[151]

There are many ways to send email that offer an increased level of security, and all of them have been used in Saudi Arabia. Many webmail services are free and do not require users to register with a real name.[152] "Remail" services attempt to remove all identifying user information, try not to keep log files of their activity, and route their encrypted email through other remailers before reaching its destination. A government censor typically only knows that a user has visited a remailer site, but cannot obtain a copy of the message or know its recipient.[153]

Cutting edge peer-to-peer networking presents another major challenge to Internet censors. It employs virtual private networking (VPN) technology in an attempt to make file-sharing between computer users invisible to firewalls and content-filtering systems such as that used in Saudi Arabia.[154]

Saudi Web surfers have often made use of anonymous proxy servers,[155] which make web requests on a user's behalf, by substituting their own IP for that of the user. Unwanted tracking software, such as a browser "cookie," is also disabled in the pro-

148 "How Users..." Human Rights Watch.
149 Whitaker, 2000.
150 "How Users..." Human Rights Watch.
151 ""The Internet..." Human Rights Watch.
152 "How Users..." Human Rights Watch.
153 "How Users..." Human Rights Watch.
154 Lee, 2001.
155 Dobbs, 2001.

cess. APS IPs are of course blocked by KACST,[156] but such services try to make such blocking as difficult as possible.[157]

Today, strong encryption, such as Pretty Good Privacy (PGP), is both reliable and cheap. PGP's design, which couples a sophisticated encryption algorithm with a secret passphrase, works so well that it has come to play an important role in providing privacy to individual web users around the world. As a result, many countries, including Saudi Arabia, disallow its use.[158]

Information on computer hacking, which can give ordinary citizens an upper hand in figuring out how to beat censorship, is often banned.[159] But no specific tools can be recommended because none of them is perfect.[160]

New software tools are frequently released, some of which are specifically designed to support anti-censorship movements. Psiphon, for example, is easy to use and difficult for governments to discover. It works like this: a computer user in an uncensored country installs Psiphon on his or her computer and then allows a user in a censored country to open an encrypted connection through their computer to the Internet. Connection information, including a username and password, is passed by telephone, posted mail, or human contact.

In summary, network communications are highly vulnerable to surveillance, especially when all traffic flows through one state-owned system. The Saudi national firewall has been successful in keeping ordinary users from visiting many anti-Muslim or anti-Saudi websites. However, it is extremely difficult for any government to prevent those who are willing to accept the risk of arrest from conducting prohibited activities.

In the long run, large-scale Internet control may be doomed to failure. Censorship tends to inhibit economic development, and governments are often simply too far behind the technology curve. New websites appear every minute, and any one of them – or all of them – are potentially hostile. Saudi officials publicly acknowledge that it is hard to keep up.[161]

This chapter sought to demonstrate that managing Internet security is highly problematic, even for a willing and well-resourced government. But from a strategic security perspective, there are concerns that lie above and beyond political criticism and

156 "SafeWeb..." 2000.
157 "SafeWeb..." 2000.
158 "How Users..." Human Rights Watch.
159 Gavi, 1999 and 2002.
160 "How Users..." Human Rights Watch.
161 Gardner, 2000.

pornography: to wit, the protection of national critical infrastructures. Are they safe from cyber attack? This is the topic of the next chapter, which examines a hypothetical cyber terrorist attack against an electricity plant.

Modeling Cyber Attack and Defense in a Laboratory

Many national security thinkers fear that the age of cyber terrorism and cyber warfare is coming soon. And the target list seems to grow by the day: electricity,[162] water, air traffic control, stock exchange,[163] national elections,[164] and more. However, the extent to which cyber attacks pose a true threat to national security is unclear. Expert opinions range from dismissive[165] to apocalyptic.[166]

We do know that there are worrisome trends in information technology (IT). National critical infrastructures are increasingly connected to the Internet. At the same time, their custom IT systems, some created in the 1950s and 1960s, are now being replaced with less expensive, off-the-shelf and Internet-enabled Windows and UNIX systems that are not only easier to use but easier to hack. The older systems were relatively more secure because they were not well-understood by outsiders and because they had minimal network contact with other computer systems.[167]

National security planners require a better understanding of the threat posed by cyber attacks as soon as possible. Some real-world case studies exist.[168] However, much information lies outside the public domain. Furthermore, there have been no wars yet between two Internet-enabled militaries, and the ignorance of many organizations regarding the state of their own cyber security is alarming. Looking toward the future, military planners must be able to simulate cyber attacks and test cyber

162 "Remarks by the President..." 2009; "Cyber War..." 2009: The threat to electricity encompasses everything that relies on electricity to function, including computer systems. In May 2009, President Obama stated that "cyber attacks have plunged entire cities into darkness," reportedly referencing large scale, anonymous attacks in Brazil.

163 Wagner, 2010: In May 2010, after the Dow Jones surprisingly plunged almost 1,000 points, White House adviser John Brennan stated that officials had considered but found no evidence of a malicious cyber attack.

164 Orr, 2007: In 2007, California held a hearing for election officials on the subject of whether hackers could subvert the integrity of the state's touch-screen voting machines. While the system manufacturer disputed the validity of the tests, the Red Team leader testified that the voting system was vulnerable to numerous attacks that could be carried out quickly.

165 Persuasive cyber war skeptics include Cambridge University Professor Ross Anderson, *Wired* "Threat Level" Editor Kevin Poulsen, and *Foreign Policy* editor Evgeny Morozov.

166 Bliss, 2010: In early 2010, former U.S. Director of National Intelligence Michael McConnell testified that the U.S. would "lose" a cyber war today, and that it will probably take a "catastrophic event" before needed security measures are undertaken to secure the Internet.

167 Preimesberger, 2006.

168 Geers, 2008: This author has highlighted the cases of Chechnya, Kosovo, Israel, China, and Estonia.

defenses within the bounds of a safe laboratory environment, without threatening the integrity of operational networks.[169]

The need for cyber defense exercises (CDX) is clear. But the complex and ever-changing nature of IT and computer hacking makes conducting a realistic CDX an enormous challenge and may render its conclusions valid only for a short period of time. The world is experiencing a rapid proliferation of computing devices, processing power, user-friendly hacker tools, practical encryption, and Web-enabled intelligence collection.[170] At the same time, a CDX requires the simulation of not only adversary and friendly forces, but even the battlefield itself.

Of course, the military is no stranger to computers. Software is now used to train tank drivers and pilots; it is also used to simulate battles, campaigns, and even complex geopolitical scenarios. But it remains controversial how closely a computer simulation can model the complexity of the real world. Myriad factors can contribute to failure – poor intelligence, incorrect assumptions, miscalculations, a flawed scoring system, and even political considerations. In 2002, the U.S. military spent $250 million on a war game called Millennium Challenge, which was designed to model an invasion of Iraq. In the middle of the exercise, the Red Team (RT) leader, Marine Corps Lt. Gen. Paul Van Riper, quit the game on the grounds that it had been rigged to ensure a Blue Team (BT) victory.[171]

This chapter covers the origin and evolution of CDXs, and it describes the design, goals, and lessons learned from a recent "live-fire" international CDX, the May 2010 Baltic Cyber Shield (BCS). BCS was managed at the Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn, Estonia. Its virtual battlefield was designed and hosted by the Swedish Defence Research Agency (FOI) in Linköping, Sweden with the support of the Swedish National Defence College (SNDC).[172] Over 100 participants hailed from across northern Europe.

A robust CDX requires a team-oriented approach. There are friendly forces (Blue), hostile forces (Red), technical infrastructure (Green), and game management (White). The RT and BTs are the CDX combatants. The Green Team (GT) and White Team (WT) are non-combatants; RT attacks against either in most CDXs are strictly prohibited.

169 Occasionally, "penetration tests" are conducted against operational networks, but extreme care is always taken to avoid a real-life denial-of-service and/or the loss of sensitive data.

170 In the Internet age, Open Source Intelligence (OSINT) collection, against both people and organizations, is easier and more powerful than ever.

171 Gomes, 2003.

172 Estonian Cyber Defence League, Finnish Clarified Networks, NATO Computer Incident Response Capability-Technical Centre (NCIRC-TC), Swedish Civil Contingencies Agency (MSB) and National Defence Radio Establishment (FRA) also participated in the CDX.

BT personnel are normally real-life system administrators and computer security specialists. Their goal is to defend the confidentiality, integrity, and availability (CIA) of their computer networks against hostile RT attacks. In BCS 2010, the BTs were the primary targets for instruction; their progress was tracked by automated and manual scoring systems.

The RT plays the role of a cyber attacker, or in this CDX, a "cyber terrorist." The RT attempts to undermine the CIA of BT networks, using a variety of hacker tools and tactics.[173] In a "white box" test, RTs may be given detailed, prior knowledge of the BT networks; a "black box" test requires the RT to gather this information on its own.[174] Either way, RTs – just like real-life hackers – have an enormous advantage over their BT counterparts because they can often methodically work their way through various cyber attacks until they succeed in hacking the network.[175]

The WT manages and referees the CDX. Normally, it writes the game's scenario, rules, and scoring system. The WT will make in-game adjustments in an effort to ensure that all participants are gainfully employed throughout the CDX. It also seeks to prevent cheating. For example, if a particular firewall rule appeared to be detrimental to the game and/or unrealistic in real-life, the WT may disallow it. Finally, the WT often declares a CDX "winner."

The GT is responsible for designing and hosting the CDX network infrastructure. It is the in-game "Internet Service Provider" (ISP). To allow for post-game analysis, the GT should attempt to record all CDX network traffic. With the aid of virtual machine technology, it is technically possible to carry out a CDX on a handful of computers. However, to simulate a powerful adversary, significant resources are required, and a time- and labor-intensive CDX is unavoidable. (The RT, for example, should have a plan that indicates the availability of significant money and manpower.) With Virtual Private Network (VPN) technology, the RT, BTs, and WT can be located anywhere in the world and remotely connect to the CDX environment. All automatic scoring in the CDX is implemented by the GT.

Cyber warfare is very different from traditional warfare. Tactical victories amount to a reshuffling of the electronic bits of data – also known as ones and zeros – inside

173 Preimesberger, 2006: In the U.S., Sandia National Laboratories have developed eight "natural categories" of Red Teaming: design assurance, hypothesis testing, benchmarking, behavioral Red Teaming, gaming, operational Red Teaming, penetration testing, and analytic Red Teaming.

174 A black box is often considered more realistic because real-world hackers normally find themselves in this position. However, given strict time limits, white box CDXs are the norm. In BCS 2010, the RT had access to the initial BT network for three weeks prior to the CDX.

175 Geers, 2010: In a CDX, this depends in part on the complexity of the network the BTs have to defend and the amount of time the RT has to attack it. In the real world, hackers can often remain anonymous in cyberspace, so deterring cyber attacks is difficult. Attackers may be able to keep trying to crack a network until they succeed, and there is normally no penalty for the failed attempts.

a computer. At that point, an attacker must wait to see if any intended real-world effects actually occur. A cyber attack is best understood not as an end in itself, but as an extraordinary means to a wide variety of ends: espionage,[176] denial of service,[177] identity theft,[178] propaganda,[179] and even the destruction of critical infrastructure.[180]

The primary goal of a CDX is to credibly simulate the attack and defense of a computer network. At the tactical level, the RT has the same goals as any real-world hacker – to gain unauthorized access to the target network.[181] If "administrator" or "root" access is obtained, the intruder may be able to install malicious software and erase incriminating evidence at will. Further actions, possibly aimed to support some political or military goal, could range in impact from a minor annoyance to a national security crisis.

The CDX "scenario" is helpful in determining the overall strategic significance of an exercise. A well-written scenario should estimate the required resources and projected cost of a theoretical attack. This in turn helps national security planners to determine whether a person, group, or nation could attempt it. For example, it still remains difficult to imagine a lone hacker posing a threat to a nation-state.[182] However, future cyber attacks might change that perception.

It is almost impossible for a limited-duration CDX to simulate the threat posed by a nation-state. Military and intelligence agencies are "full-scope" actors that do not rely solely on computer hacking to achieve an important objective. Governments draw from a deep well of expertise in many IT disciplines, including cryptogra-

176 "Tracking GhostNet...," 2009: The most famous case to date is "GhostNet," investigated by *Information Warfare Monitor*, in which a cyber espionage network of over 1,000 compromised computers in 103 countries targeted diplomatic, political, economic, and military information.

177 Keizer, 2009: During a time of domestic political crisis, hackers were able to make matters worse by knocking the entire nation-state of Kyrgyzstan offline.

178 Gorman, 2009b: American identities and software were reportedly used to attack Georgian government websites during its 2008 war with Russia.

179 Goble, 1999: Since the earliest days of the Web, Chechen guerilla fighters have demonstrated the power of Internet-enabled propaganda. "'USA Today' Website Hacked..." 2002: On a lighter note, a hacker placed a series of fake articles on the USA Today website. One read, "Today, George W. Bush has proposed ... a Cabinet Minister for Propoganda and Popular Englightenment [sic].... If approved, Bush would appoint Dr. Joseph Goebbels to the post."

180 Meserve, 2007: Department of Homeland Security (DHS) officials briefed CNN that Idaho National Laboratory (INL) researchers had hacked into a replica of a power plant's control system and changed the operating cycle of a generator, causing it to self-destruct.

181 There are exceptions, such as a denial-of-service attack in which the main goal is to overload the system with superfluous data.

182 Verton, 2002: Nonetheless, it is astonishing what some lone hackers have been able to accomplish. In 2001, "MafiaBoy," a 15 year-old from Montreal, was able to deny Internet service to some of the world's biggest online companies, causing an estimated $1.7 billion in damage.

phy, programming, debugging, vulnerability discovery, agent-based systems, etc.[183] Those skill sets are in turn supported by experts in the natural sciences, physical security, supply chain operations, continuity of business, social engineering,[184] and many more.

The Sandia National Laboratories RT, based in New Mexico, provides a robust model. Sandia has a long track record of successfully hacking its clients, which include military installations, oil companies, banks, electric utilities, and e-commerce firms. Its RT takes pride in finding hidden vulnerabilities in complex environments,[185] including obscure infrastructure interdependencies in highly specialized domains.[186] A former Sandia RT leader put it best: "Our general method is to ask system owners: 'What's your worst nightmare?' and then we set about to make that happen."[187]

Every CDX is unique. There are simply too many variables in cyberspace, and IT continues to evolve at an astonishing rate. Some CDXs are conducted only in a laboratory, while others take place on real networks in the real world. For the latter, cyber defenders may be warned about the CDX before it starts, or the RT attack may come as a complete surprise.

In 1997, an RT of thirty-five U.S. National Security Agency (NSA) personnel, playing the role of North Korean hackers, targeted the U.S. Pacific Command from cyberspace. The CDX, code-named Eligible Receiver, was an enormous success. James Adams wrote in *Foreign Affairs* that the RT was able to infect the "human command-and-control system" with a "paralyzing level of mistrust," and that "nobody in the chain of command, from the president on down, could believe anything."[188] Furthermore, Eligible Receiver was credited with revealing that a wide variety of national critical infrastructures was equally vulnerable to common hacker tools and techniques.[189]

Many CDXs involve a proof-of-concept. In 2006, the U.S. Environmental Protection Agency asked the Sandia RT to conduct a vulnerability assessment of every water

183 Lam et al, 2003.

184 Lawlor, 2004: Social engineering takes advantage of human weaknesses in security. Experience shows that malicious or co-opted insiders, due to the physical access they have to IT systems, can do more damage to an organization than a malicious outsider. This type of attack can be surprisingly easy to conduct against a large organization, where one does not personally know everyone in the organization.

185 For example, the production of energy – as well as the ability to attack an energy plant – can require a knowledge of systems and computer languages that is truly unique to that environment.

186 Lawlor, 2004.

187 Gibbs, 2000.

188 Adams, 2001.

189 Verton, 2003.

distribution plant serving at least 100,000 people. The fear was that a malicious hacker might be able to change the chemical composition of water enough to poison it. When the RT discovered that there were 350 such facilities in the country – far too many to examine each one – Sandia decided to conduct a thorough analysis of five sites and then construct the Risk Assessment Methodology for Water (RAM-W), which could then be used for self-assessment.[190]

Today, an important trend in CDXs is to encompass international partners. Because the architecture of the Internet is international in scope, Internet security is by definition an international responsibility.

In 2006, the U.S. Department of Homeland Security (DHS) began a bi-annual, international CDX called Cyber Storm. This event specifically seeks to assess how well government agencies and the private sector can work together to thwart a cyber attack.[191] The 2006 scenario simulated an attack by non-state, politically-motivated "hacktivists."[192] The 2008 Cyber Storm II[193] simulated a nation-state actor that conducted both cyber and physical attacks on communications, chemical, railroad, and pipeline infrastructure.[194] In 2010, Cyber Storm III added the compromise of trusted Internet transactions and relationships and included cyber attacks that led to the loss of life.

The testing of cyber defenses is not confined to the First World. In 2009, the U.S. sponsored an international CDX in remote and mountainous Tajikistan, which included participants from Kazakhstan, Kyrgyzstan and Afghanistan.[195]

Baltic Cyber Shield (BCS), held on May 10-11, 2010 in numerous countries across northern Europe, was a "live-fire" CDX. A twenty-person international RT and six national BTs took part in an unscripted battle in which the use of malicious code – within the confines of a virtual battlefield[196] – was both authorized and encouraged.

190 Preimesberger, 2006.

191 Verton, 2003: Market forces, deregulation, and outsourcing mean that myriad important computer networks and critical infrastructures now lie in private hands. This, combined with the reluctance of many businesses to disclose cyber attacks for fear of embarrassment, make it difficult for government to help protect the private sector.

192 Chan, 2006.

193 This CDX included eighteen federal agencies, nine U.S. states, three dozen private companies, and four foreign governments: Australia, Canada, New Zealand, and the UK. These were the same countries that took part in 2006. It is worth noting that these governments are members of a joint 1947 intelligence-sharing accord that makes it possible for them to share classified information.

194 Waterman, 2008: The RT also targeted the media in an effort to undermine public trust in government.

195 "International cyber exercise..." 2009.

196 The entire CDX took place within the bounds of a safe laboratory environment.

BCS 2010 was similar in nature to the annual CDXs that pit U.S. military services against one another[197] and for which the Pentagon now sponsors a national competition at the high school level.[198] Other CDXs that inspired aspects of BCS 2010 included the Pentagon's International Cyber Defense Workshop (ICDW), the UCSB International Capture the Flag (iCTF), and the U.S. National Collegiate Cyber Defense Competition.

The game scenario described a volatile geopolitical environment in which a hired-gun, Rapid Response Team of network security personnel defended the computer networks of a power supply company against increasingly sophisticated cyber attacks sponsored by a non-state, terrorist group.[199]

BCS 2010 had three primary goals. First, the BTs should receive hands-on experience in defending computer networks containing Critical Information Infrastructure (CII) and elements of Supervisory Command and Data Acquisition (SCADA).[200] Second, the CDX scenario sought to highlight the international nature of cyberspace, to include the political, institutional, and legal obstacles to improved cyber defense cooperation. Third, participating teams were meant to gain a better understanding of how to conduct CDXs in the future.

The WT was based primarily at SNDC in Stockholm, Sweden, with a smaller contingent at CCD CoE in Tallinn, Estonia. The WT's scoring criteria were designed to gauge the BTs' ability to maintain the CIA of their virtual networks, including office infrastructure and external services.[201] In the event of compromise, the number of points lost depended on the criticality of the system, service, or penetration. For example, if the RT gained Admin/Root-level access to a computer or compromised a SCADA Programmable Logic Controller (PLC), the BT was significantly penalized. On the other hand, BTs won positive points for thwarted attacks, for successfully

197 Caterinicchia, 2003.

198 *Defense & Aerospace,* 2010: In March 2010, "Team Doolittle" from Clearfield High School in Utah won the CyberPatriot II Championships, sponsored by the U.S. Air Force Air Warfare Symposium in Orlando, Florida.

199 Lewis, 2010: James Lewis of CSIS recently stated: "It remains intriguing and suggestive that [terrorists] have not launched a cyber attack. This may reflect a lack of capability, a decision that cyber weapons do not produce the violent results terrorists crave, or a preoccupation with other activities. Eventually terrorists will use cyber attacks, as they become easier to launch..."

200 SCADA systems can be used to support the management of national critical infrastructures such as the provision of electricity, water, natural gas and manufacturing. The disruption or other misuse of such systems could potentially become a national security issue.

201 Both automated and manual means were used to verify CIA. The latter, for example, could entail the WT simulating the actions of ordinary users. They may periodically request a BT webpage to see that it is reachable and not defaced.

completing in-game "business requests,"[202] and for the implementation of innovative cyber defense strategies and tactics.

The six BTs consisted of 6-10 personnel each, and hailed from various northern European governments, military, private sector, and academic institutions. All were provided an identical, pre-built, and somewhat insecure computer network composed of 20 physical PC servers running a total of 28 virtual machines.[203] These were further divided into four VLAN segments – DMZ, INTERNAL, HMI,[204] and PLC. The BT networks were further connected to various in-game servers that provided additional business functionality to their fictitious users.

The BCS 2010 scenario called for the inclusion of SCADA software in order to simulate a power generation company's production, management, and distribution capabilities. These comprised GE PLCs, Simplicity HMI terminals, Historian databases, and two physically-separated model factories per BT network.

Because of the "rapid response" nature of the BCS 2010 scenario, the BTs were given access to the CDX environment – including somewhat outdated network documentation – only on day one of the CDX. They were allowed to harden their networks,[205] but a minimum number and type of applications and services had to be maintained.[206] The BTs were allowed to install new software and/or modify existing software. However, offensive BT cyber attacks, either against the RT or against other BTs, were strictly prohibited.[207]

202 This aspect of the game was intended to raise the stress level of BT participants. It simulated the real-world challenge of handling both security threats and ordinary business processes at the same time. For example, a CEO may call while on a business trip, needing immediate remote access, and the BT must provide a timely solution. Alternatively, a BT member might become "ill" and have to spend one hour on "sick leave" in a break room.

203 The BTs accessed the game environment by VMWare Console from a browser or over SMB, RPC, SSH, VNC, or RDP. The power company's network included both Windows and Linux operating systems. Unfortunately, the Console access of the free version of VMWare Server proved to be too slow and unstable for such a large event.

204 Human Machine Interface: these workstations ran the control software for the PLCs, providing the communication link between the Supervisor node and the remote factories.

205 In the real world too, new IT hires cannot assume that legacy systems are secure or even properly installed. They are likely to find some vulnerable, unpatched, redundant, etc systems. Further, existing documentation may be dated or incomplete. Once given access to the infrastructure, the BTs were allowed to disable, patch, and/or replace applications and services as long as the final configuration met CDX parameters.

206 These included HTTP, HTTPS, SMTP, DNS, FTP, IMAP/POP3, SSH, and NTP.

207 As a starting point, the BTs must stay within their countries' legal frameworks.

The BCS RT consisted of twenty volunteers[208] from throughout northern Europe.[209] The RT was given access to the game environment two weeks prior to the CDX in order to simulate a degree of prior reconnaissance. To maximize the CDX's value to all participants, the WT directed the RT to begin its attacks slowly, and to progressively increase the scale and sophistication of its attacks throughout the game. Beyond that, there was no limit on the type of hacker tools and techniques that the RT could use.[210] However, the RT was strictly prohibited from attacking the CDX infrastructure,[211] and all attacks were confined to the virtual game environment. Internally, the RT divided itself into four sub-teams, depending on the hackers' attack specialization: "client-side," "fuzzing," "web app," and "remote."

The GT, based at the Swedish Defence Research Agency (FOI) in Linköping, Sweden, hosted most of the BCS 2010 infrastructure. The BT networks were designed collaboratively by the GT and the WT. The FOI laboratory consisted of nine racks, with twenty physical servers in each rack.[212] The game infrastructure included twelve, twenty centimeter tall physical models of factories, each with its own PLC, SCADA software, and "Ice Fountain" fireworks that the RT could turn on as "proof" of a successful attack. The GT provided the RT and BTs access to the game environment via OpenVPN.

Finally, the WT had access to a robust visualization environment[213] that displayed all network topography, network traffic flows, observer reports, chat channels, team workspaces, scoreboard, and a terrestrial map of the CDX environment.[214]

BCS 2010 formally began when the BTs and the RT logged into the CDX environment. But the most anticipated moment arrived when the RT began its cyber attack on the BT networks.

208 The BCS 2010 RT was mostly volunteer-based. However, it is worth noting that one contractor bid to provide an RT came in at $500,000.

209 The Estonian Cyber Defence League built and managed the RT.

210 However, it is helpful if many easily-accessible, Internet-available attack tools are used, because the BTs will see these often in the real world.

211 Including the game scoring system ☺.

212 The servers had 2 Xeon 2.2 GHz processors, 2 GB RAM, 80 GB HDD, VMware Server 2.0.2 on Gentoo Linux, 2x Ethernet interfaces, and 2 switches, one for management and one for the game network.

213 This was provided by the Finnish company Clarified Networks.

214 In the BCS 2010 scenario, two BTs were theoretically based in South America, two in Africa, and two in Asia; the RT was in Iceland (in reality, all teams were located in northern European countries).

The RT campaign was divided into four phases:

- Declaration of war
- Breaching the castle wall
- Owning the infrastructure
- Wanton destruction

The first objective, declaration of war, required the RT to "deface" the six BT public websites and to give each power company an ultimatum. In a posted statement, the "cyber warfare division" of an extremist environmental organization called "K3" demanded that the power company publicly announce its intention to convert to alternative, greener power ... or face a crippling cyber attack. The RT succeeded in defacing five of the six sites within 30 minutes.

During phase one, the RT was allowed to compromise only one server in each BT DMZ and only one internal workstation in each BT network. Even with these constraints, however, the RT succeeded in creating such a steady stream of incident reports that the WT had trouble translating all of them into negative points for the BTs. For example, within an hour the RT had established a live audio and video connection into one BT network; in other words, the game had barely begun and a digital spy was already working inside one of the power companies.

In the past, a major challenge inherent in CDXs is that it has been difficult for the RT to maintain balanced and sustained pressure on all BTs throughout the game. At different stages in a CDX, some BTs could be quite busy, while others had nothing to do. To help avoid this, the WT instructed the RT that, for each vulnerability discovered on a BT network, the RT must systematically check all other BT systems for the same vulnerability and exploit it if possible.

Phase two of the K3 attack campaign called for the RT to compromise as many DMZ[215] systems as possible. At the end of day one, the RT had successfully attacked 42 computers, including web and email servers. The RT leader was more than pleased with his team's progress.

Phase three called for the RT to steal the BT networks' "crown jewels." In BCS 2010, these were the internal network computers that served as the HMI for power generation and management, i.e., its SCADA infrastructure. Although the RT was quite successful in the CDX overall, it claimed only limited victories in phase three. Of the

215 The DMZ, or demilitarized zone, is a physical or logical subnetwork that is exposed to untrusted networks, such as the Internet.

twelve model factories, the RT succeeded in setting only one of them on fire, and it is still unclear whether this RT success was intentional or accidental.[216]

The fourth and final phase of BCS 2010, "wanton destruction," allowed the RT to attack and destroy any BT system in the CDX. The goal was to simulate a desperate attempt by K3 to cause maximum disruption to the power companies' operations. Unfortunately, RT successes in this phase often denied service to the same computers it had previously compromised, and it prevented the WT from scoring the game properly. In other words, a poorly-designed DoS attack can bring down large sections of network infrastructure and nearly ruin the game. In this CDX, for example, the RT used a custom-configured Cisco router to simulate traffic; at one point, it created such a high volume of data that the RT denied itself access to the gamenet for 15 minutes.

The RT successfully attacked several publicly-known vulnerabilities during BCS 2010, including MS03-026, MS08-067, MS10-025, and flaws in VNC, Icecast, ClamAV, and SQUID3. It hacked web applications such as Joomla and Wordpress and also employed SQL injection, local and remote file inclusion, path traversal, and cross-site scripting against Linux, Apache, Mysql, and PHP. Other tactics included account cracking, online brute-forcing, DoS with fuzzing tools, obtaining password hashdumps of compromised systems, and using the "pass-the-hash" technique to hack into more machines. The RT installed Poison Ivy, netcat, and custom made code as backdoors. Metasploit was used to deploy reverse backdoors. The RT modified compromised systems in various ways, such as altering the victim's crontab file to continuously drop firewall rules. Last but not least, the RT possessed a zero-day client-side exploit for virtually every browser in existence today.

Although the BCS 2010 scoring system applied only to the BTs, when the game was over, the RT leader smiled as if his team had won the game. When the CDX ended, there were over 80 BT computers that were confirmed compromised.

However, the BTs did adopt some successful defensive strategies. The most successful BT – which was also declared the winner of BCS 2010 – quickly moved essential network services, such as NTP, DNS, SMTP and WebMail, to its own custom-built, higher-security virtual machine. IPsec filtering rules were used for communications with the Domain Controller. This BT had also requested the use of an "out-of-band" communication channel for its discussions with the WT, i.e., not the in-game email system, which it assumed might be compromised. Finally, the winning BT was successful in finding and disabling preexisting GT-installed malware.[217]

216 The RT may have gotten lucky while examining the SCADA Modbus protocol with their fuzzing tools.

217 Preexisting malware can simulate what a Rapid Response Team would likely find on any computer network.

BCS 2010 also highlighted the value of numerous current OS-hardening tools and techniques. For Linux computers, these included AppArmor, Samhain, and custom short shell scripts; for Windows, Active Directory (AD) group policies, the CIS SE46 Computer Integrity System, Kernel Guard, and the central collection of event logs. For all OSs, the white/black-listing and blocking/black hole-routing of offending IP addresses, on a case-by-case basis, proved invaluable.

The Cooperative Cyber Defence Centre of Excellence (CCD CoE), the Swedish National Defence College (SNDC) and the Swedish Defence Research Agency (FOI) believe that BCS 2010 accomplished its three primary goals.

First, the GT network infrastructure provided a sufficiently robust environment for a rare "live fire" CDX that offered six professional BTs the opportunity to defend CII and SCADA-enabled computer networks against a highly-motivated, capable RT. All teams were fully occupied throughout the two-day exercise, and very little downtime was reported. Further, the BCS 2010 scenario described a "cyber terrorist" threat that may already endanger the national security of governments around the world.[218]

Second, BCS 2010 was a truly international exercise. Because cyber attacks can be launched from anywhere in the world and are likely to traverse third-party countries en route to a target, it is critical to develop cross-border relationships before an international crisis occurs. In BCS 2010, over 100 personnel from seven countries participated. Numerous international partnerships were either established or strengthened during the course of this project.

Third, BCS 2010 conducted a post-exercise participant survey with a view toward providing a list of lessons learned to future CDXs around the world.[219] Here are the highlights:

- There should be at least one WT member per BT and two WT members on the RT to allow for sufficient observation, communication, adjudication, and clarification on scoring.
- The WT should include a cyber-savvy lawyer to shed light on the legality of unscripted attack and defense scenarios.
- Each BT must have at least one full-time WT-appointed "dumb user" active on the virtual network to make client-side attacks possible.[220] In BCS 2010, the

218 "Remarks..." 2009; Cyber War..." 2009.

219 The author gave a BCS 2010 presentation at DEF CON 18: www.defcon.org/html/links/dc-archives/dc-18-archive.html#Geers.

220 This cannot be an integral BT member due to the obvious conflict of interest.

RT did not have the chance to use a powerful "zero-day" browser exploit with which they had intended to target the virtual power company employees.

- Prior to a "live-fire" CDX, all participants should devote one full day to testing connectivity, bandwidth, passwords, cryptographic keys, etc., and for clarification on rules and scoring.
- The VMWare Server Console was too slow for the high demands BCS 2010 placed upon it, and it cannot be recommended to other CDXs.
- The WT/GT should grant the BTs some network administration rights over their physical machines in the CDX environment. Otherwise, installing and patching software can be too time-consuming.
- A "wanton destruction" phase (i.e., one without a clearly defined purpose and certain limits on the RT) will likely destroy the game itself and so for most CDX scenarios cannot be recommended.
- In a project this big, some egos and agendas are bound to clash. It is important to designate diplomatic yet authoritative personalities, who can meet team-oriented deadlines, from the beginning.

Finally, one of the lessons of BCS 2010 is that many of the challenges inherent in conducting a robust CDX mirror the challenges of managing both IT and cyber security in the real world. Cyberspace is complicated, polymorphic, dynamic, and evolving quickly. Cyber defenders may never see the same attack twice. Furthermore, the intangible nature of cyberspace can make the calculation of victory, defeat, and battle damage a highly subjective undertaking. Therefore, believe it or not, both in the laboratory and in the real world, even knowing *whether* one is under cyber attack can be a challenge.

Chapter 3 has introduced the reader to the highly technical nature of cyber security at the tactical level. Chapter 4 will show how cyber attacks have impacted the real world, even at the strategic level.

4. CYBER SECURITY: REAL-WORLD IMPACT

Chapter 3 described a wide range of technical challenges to securing the Internet and revealed that even our national critical infrastructures are at risk. But it is always important to correlate theoretical discussion with real-world events. Have cyber attacks truly had an influence at the highest levels of government? To what extent have they impacted national security?

Cyber Security and Internal Political Security[221]

National security begins at home. No government can worry about foreign threats or adventures before it feels secure within its own borders.

In terms of domestic security, a major consideration for many governments is information management, if not information control. The most famous example comes from fiction. In 1949, in his novel *Nineteen Eighty-Four* George Orwell imagined a government that waged full-time information warfare against its own citizens, with the aid of two-way Internet-like "telescreens."[222]

Unfortunately, in 2011 some countries are not far from Orwell's vision, and media carry only stories that are carefully crafted by government censors. For example, in North Korea, the world's most repressive and isolated country, the perceived threat to stability from unrestricted access to the Internet is prohibitively high. Television and radio carry only government channels, and there is an Orwellian "national intercom" wired into residences and workplaces throughout the country through which the government provides information to its citizens.

North Korea's aging leader, Kim Jong-il, is said to be fascinated with the IT revolution. In 2000, he gave visiting U.S. Secretary of State Madeleine Albright his personal email address. However, computers are unavailable to ordinary North Korean citizens, and it is believed that only a small circle of North Korean leadership have free access to the Internet.

221 This chapter consists of an updated section from a 2007 paper, "Greetz from Room 101," written and presented by the author at *DEF CON 15* and *Black Hat*. It contains material from Reporters without Borders (www.rsf.org), OpenNet Initiative (www.opennet.net), Freedom House (www.freedomhouse.org), Electronic Frontier Foundation (www.eff.org), ITU Digital Access Index (www.itu.int), and Central Intelligence Agency (www.cia.gov). For example, RSF assessments are based on a combination of "murders, imprisonment or harassment of cyber-dissidents or journalists, censorship of news sites, existence of independent news sites, existence of independent ISPs, and deliberately high connection charges."

222 Orwell, 2003 (originally written in 1949).

Each year, one hundred male students as young as 8 years old are chosen to attend the Kumsong computer school, where the curriculum consists of computer programming and English. The students are not allowed to play games or access the Internet, but they do have an instant messaging system within the school.

According to the South Korean Chief of Military Intelligence, some top graduates from the Kim Il-Sung Military Academy have been selected for an elite, state-sponsored hacker unit, where they develop "cyber-terror" operations.

International Internet connections run from North Korea to the rest of the world via Moscow and Beijing. They are managed at the Korea Computer Centre (KCC), established in 1990. Reports suggest that KCC downloads officially-approved research and development data, which it offers to a very short list of clients.

North Korea's official stance on Internet connectivity is that the government cannot tolerate the "spiritual pollution" of its country. However, South Korea determined that North Korea was operating a state-run cyber casino on a South Korean IP address. Since that time, South Korean companies have been barred from registering North Korean sites without government approval.

According to recent statistics, North Korea is 48th in the world in population at 24.5 million. However, the country possesses only three computers which are directly connected to the Internet, so it sits at number 227 in the world in that category.[223]

North Korea is not alone in fearing the power of the Internet to undermine its domestic security. In Turkmenistan, President-for-Life Saparmurat Niyazov – the *Turkmenbashi*, or Father of All – died in late 2006, but his personality cult and the tightly-controlled media he left behind have had a lasting impact on the country.

Information and communication technology is woefully underdeveloped. The Turkmentelekom monopoly has allowed almost no Internet access, either from home or via cyber café. A few Turkmen organizations have been allowed to access just a handful of officially-approved websites. In 2001, of all the countries of the former Soviet Union, Turkmenistan had the fewest number of IT-certified personnel – fifty-eight.

In addition, the CIA reported in 2005 that there were only 36,000 Internet users, out of a population of 5 million. In 2006, a Turkmen journalist who had worked with Radio Free Europe died in prison, only three months after being jailed. Despite repeated European Union (EU) demands, there has been no investigation into the incident.

223 CIA *World Factbook*, 9 March, 2011.

Foreign embassies and non-governmental organizations furnish their own Internet access. In the past they have offered access to ordinary Turkmen, but it was too dangerous for the average citizen to accept the offer.

Following Niyazov's death, Gurbanguli Berdymukhamedov was elected president[224] with a campaign promise to allow unrestricted access to the Internet. And within days, two cyber cafés opened in the capital. A visiting AP journalist reported easy access to international news sites, including those belonging to Turkmen political opposition groups. However, the price per hour was $4, exorbitant in a country where monthly income is under $100.

Today, Turkmenistan has a population of 5 million. Unfortunately, under 100,000, or under 2%, are believed to have Internet access.[225] On the bright side, computer hardware is available in Turkmenistan, and computer gaming is popular. Also, the use of satellite TV is on the rise, which could be used to improve Internet connectivity in the future.

The world's largest and most sophisticated Internet surveillance belongs to the People's Republic of China (PRC), which employs an army of public and private[226] cyber security personnel to keep watch over its citizens. The PRC has strict controls on access to the World Wide Web, and policemen are stationed at cyber cafés, which track patrons' usage for 60 days.

The "Great Firewall" is designed specifically to prevent the free flow of information in and out of the country, including content related to politics, human rights, religion, and pornography. Some sites, such as Google and BBC, have been completely blocked for a period of time. Search results are believed to be filtered by keyword at the national gateway and not by web browsers in China.

The high level of sophistication in Chinese Internet surveillance is evident by the fact that some URLs have been blocked, even while corresponding top level domains (TLD) are accessible and webpage content appears consistent across the domain. This suggests active human participation in state censorship (i.e., the system is not completely automated). At the extreme end, some blog entries appear to have been edited by censors and reposted to the Web.

224 This election was not monitored by international observers.

225 CIA World Factbook, 9 March, 2011.

226 Some Western companies have been accused of too much cooperation with China on cyber control issues: Google, Yahoo, and Microsoft have all collaborated in government prosecutions.

Comprehensive laws authorize government control of the media, while individual privacy statutes are unclear, in short supply, and perhaps even inapplicable in terms of information and communications technology (ICT).[227]

In 2007, Chinese President Hu Jintao called for a "purification" of the Internet, suggesting that Beijing intended to tighten its control over computer networks even further. According to Hu, new technologies such as blogging and webcasting had allowed Chinese citizens to circumvent state controls, which had negatively affected the "development of socialist culture," the "security of information," and the "stability of the state."

Today, China is on the cutting edge of Internet technology research. In particular, it has invested heavily in Internet Protocol version 6 (IPv6), which could be used to support a long-term strategy of user control. PRC Internet Society chairwoman Hu Qiheng has stated that China's goal is to achieve a state of "no anonymity" in cyberspace.

China's fear of Internet freedom is shared by Cuba, whose highly educated population lacks regular access to the web. Special authorization is required to buy computer hardware, and Internet connection codes must be obtained from the government. This has led to a healthy cyber black market; for example, students have been expelled from school for trading in connection codes. Some Cubans have connected to the Internet from the homes of expatriates, who have in turn been threatened by the police with expulsion from the country.

Cuban Decree-Law 209, written in 1996, states that "access from the Republic of Cuba to the Global Computer Network" may not violate "moral principles" or "jeopardize national security." Illegal network connections can earn a prison sentence of five years, posting a counter-revolutionary article, 20 years. At least two dozen journalists are now serving up to 27 years in prison.

As governments grow more familiar with censorship technology, they are capable of more complex decision-making. For example, at a 2006 Non-Aligned Movement summit in Havana, conference attendees had no problem connecting to the web. However, in the same year, when a human rights activist in the small village of Viñales tried to open an email from Reporters Without Borders containing the names

227 However, in Asia, it is generally accepted that there is less privacy in one's daily life, and the general populace is more comfortable with government oversight than in the West.

of Cuban dissidents, a pop-up window announced: "This programme will close down in a few seconds for state security reasons."[228]

Recent statistics indicate that around 15% of Cuba's population of 11 million is now online. However, there are only about 3,000 Internet-connected computers on the island, which is an extremely low number for 1.5 million users.[229] Obviously, such a narrow funnel would make it easier for the government to monitor web communications.

Burma presents another extreme example of Internet paranoia. Out of a population of 50 million, only 78,000, or 0.6% of citizens, now use the web. The number of Internet-connected host computers in the country is just 42. A few cyber cafés exist, but they require name, identification number, address, and frequent screenshots of user activity to log in. Thus, online privacy is non-existent.

In Burma, average citizens access not the Internet per se, but the "Myanmar Internet," which hosts only a small number of officially-sanctioned business websites. Furthermore, only state-sponsored email accounts are allowed; commercial webmail is prohibited.

One of the most common ways to deny Internet access is to make it prohibitively expensive. The Burmese average annual income is $225. A broadband connection is $1,300. Dial-up, the most common form of access, is $6 for 10 hours; outside the cities of Rangoon and Mandalay, long distance fees are also required. Entrance to a cyber café is $1.50.

According to the 1996 Computer Science Development Law, all network-ready computers must be registered with the government. Failure to do so or sharing an Internet connection with another person carries penalties of up to 15 years in prison.

Burma's State Peace and Development Council (SPDC) prohibits "writings related to politics," "incorrect ideas," "criticism of a non-constructive type," and anything "detrimental to the ideology of the state" or "detrimental to the current policies and secret security affairs of the government."

Some international groups, such as Free Burma Coalition and BurmaNet, have campaigned for greater Internet freedom since 1996. But there is little resistance to Internet governance within Burma itself, due to its high level of political repression.

228 Voeux, 2006: The reporter stated that the names of the dissidents had asterisks and other punctuation marks between the letters of their names in an effort to make them illegible to government censorship software, but that "this precaution turned out to be insufficient." However, it could be that the system was triggered by the source IP or email address of the Reporter Without Borders' author of the email.

229 CIA World Factbook, 9 March, 2011.

Although Burma now has a population of 54 million, only around 110,000 of its citizens can connect to the web – around 0.2% - through a funnel of roughly 170 Internet-connected computers.[230]

In Africa, Eritrea has played an infamous role as the last country to go online and the first to go offline. In November 2000, Eritrea opened its first national gateway to the Internet, with a capacity of 512 Kbps.[231] Within five years, about 70,000 people had accessed the web, mostly from a "walk-in" ISP.

There was no initial censorship of the web, but in 2001, human rights in Eritrea began to deteriorate. In 2004, all cyber cafés were physically transferred to government "educational and research" centers. The official reason was to control pornography, but international diplomats are skeptical of this explanation.

Historically, oral traditions in Africa have played a powerful role in fostering national solidarity. Radio and clandestine radio stations in the Horn of Africa are skillfully employed by both government and anti-government forces. One transmitter in the Sudan, for example, has hosted three separate anti-Eritrean radio stations simultaneously.

Given the low level of Internet usage in Africa, political battles are slow to shift from the radio spectrum to cyberspace. However, via the web even the most parochial factions are able to appeal to the entire world, thereby creating international political and economic support for their cause. Sites such as Pan-African News and Eritrea Online offer a growing amount of information and analysis, and their influence will only grow over time. Today, Eritrea has a population of around 6 million, of which only about 200,000 connect to the web.[232]

Two thousand miles to the south, the government of Zimbabwe is engaged in a deadly game of information warfare against its own citizens.

In October 2006, President Robert Mugabe reportedly met with his Central Intelligence Organisation (CIO) for the purpose of infiltrating Zim Internet service providers (ISP). Operatives were to "flush out" journalists using the Internet to send "negative" information to international media. The police worked as cyber café attendants and posed as web surfers. A police spokesman confirmed that the government would do "all it can" to prevent citizens from writing "falsehoods against the government." Jail terms were up to 20 years in length.

230 CIA World Factbook, 9 March, 2011.

231 Kilobits per second.

232 CIA World Factbook, 9 March, 2011.

The Zim Interception of Communications Bill (ICB) forced ISPs to purchase special hardware and monitoring software from the government. No court challenges to government intercepts are allowed. Some ISPs threatened to shut down in protest.

In terms of national telecommunications infrastructure, Zimbabwe has followed a similar path as other authoritarian governments, giving monopoly control to a state-controlled firm.[233] The reason is simple – if one entity controls all gateways in and out of the country, surveillance is much easier, and the government can charge whatever price it desires.

In many countries, a major challenge for the government is the speed with which millions of its citizens have connected to the web. In 2001, there were just 1 million Internet users in Iran; today that number has increased to over 8 million.[234]

Former president Ali Mohammad Khatami stated that the Iranian government has tried to have the "minimum necessary" control over the Internet. Moreover, while Muslim values are emphasized, only sites that are "truly insulting" towards Islam are censored, and political opposition sites are accessible.

However, the OpenNet Initiative estimates that about one-third of all Internet sites, most often relating to politics, pornography, translation, and anonymizing software, are blocked by the Iranian government. Websites are more likely to be blocked if they are in Farsi than in English. In fact, in Iran it is technically illegal to access "non-Islamic" websites, and the maximum penalties for doing so include severe punishments. In addition, Iranian ISPs are required to install web- and email-filtering tools.

Human rights groups, such as Reporters Without Borders, argue that since 2006 all Iranian websites have had to register with the authorities to demonstrate that they do not contain prohibited content. And many popular international sites, such as photo-sharing FlickR and video-sharing YouTube, are inaccessible for reasons of "immorality."[235] Iranian media publications are not legally allowed to contradict government goals. Media receive a list of banned subjects each week, and there is a dedicated press court.

On March 14, 2011, UN secretary-general Ban Ki-moon stated that he was "deeply troubled by reports of increased executions, amputations, arbitrary arrests, unfair trials, and possible torture and ill-treatment of human rights activists, lawyers, journalists, and opposition activists" in Iran. No UN human rights investigators have been allowed to visit the country since 2005. Since June 12, 2009, about 20 foreign

233 The state-owned provider in Zimbabwe is Tel*One.

234 Iran has a population of almost 80 million, 18th on the world list, but it has just 120,000 Internet-connected computers, good for 75th in the world (CIA World Factbook, 9 March, 2011).

235 *Handbook...*, 2008.

journalists and correspondents have been expelled from Iran. A dozen were stripped of their press cards following a demonstration in February 2011 that was organized to support the revolution in Egypt. Abdolreza Tajik, the 2010 RSF-FNAC press freedom prize recipient, was given a six-year jail term.[236]

During the early-2011 unrest across the Middle East, Iranian authorities increased surveillance in cyberspace. In order to obstruct anti-government protests in February 2011, independent and pro-opposition websites, including www.fararu.com and sahamnews.org, were blocked. Prior to anti-regime demonstrations, broadband speed has slowed down enormously. Mobile phone and text-message traffic was disrupted. Satellite TV broadcasts, especially relating to news about the revolution in Egypt, were jammed. Finally, in an effort to reduce the number of calls for protest, the name of the Persian month "bahman" (roughly corresponding to February 2011) was censored.[237]

Iranian citizens are Internet savvy, and this should hinder government attempts to control Iranian cyberspace in the future. Since 2000, blogging has become both a mainstream and an alternative form of communication, and even President Mahmud Ahmadinejad has his own blog. In August 2004, when a number of reformist news sites were blocked, their content was quickly mirrored on other domains. An anonymous system administrator posted an alleged official blacklist of banned sites. And reformist Iranian legislators have openly complained about censorship, even posting their criticisms online.

In the Internet age, the power of communications within civil society to overwhelm government stability has risen to new heights. In a classic coup d'état, the national television, radio station and printing press were among the first paramilitary objectives. But the Internet has changed the rules of the game. Now anyone who owns a personal computer and a connection to the Internet possesses both a printing press and a radio transmitter in their own home. Furthermore, the entire world is potentially their audience.

Authoritarian governments, within their borders, will attempt to pare down the Internet to a manageable size, both in terms of physical infrastructure (e.g., no unmonitored Internet cafes) and information content (censorship). Common laws gov-

236 "Human rights investigators..." 2011.

237 "Regime steps up censorship..." 2011.

erning information and communications technology (ICT) are likely to include the following:

- all Internet accounts must be officially registered with the state,
- all Internet activity must be directly attributable to individual accounts,
- users may not share or sell Internet connections, and
- users may not encrypt their communications.

Clearly the Internet is a powerful tool in the hands of a despot. Through a monopoly of state-owned and operated telecommunications, the government can conduct country-wide and international ICT surveillance,[238] including information manipulation, even with some plausible deniability. Further, the government has an effective means to deliver political messages directly to its citizens, while at the same time denying that opportunity to rival political factions. Thus, network security designed for law enforcement purposes can be used not only to catch criminals but also to target political adversaries.

A challenge for any government – including those run by dictators – is to find a balance between too much and too little freedom of information. Although governments must be given appropriate law enforcement powers, there may be temptations to abuse them, and risks will follow.

Governments like those in North Korea are doomed to fail eventually. The Internet – and human beings – thrive on the open exchange of information. If civil society is not given sufficient freedom to flourish, the regime will die. In the Internet era, choking online freedom likely also entails choking long-term economic prospects, which will in turn threaten political stability.

In the next chapter, the author has translated a first-person account, written in Russian by a Belarusian computer expert, which examines the ongoing battle in cyberspace between government authorities and civil society in Belarus.

238 For the international communications that do not begin or end on its national territory, but still need to traverse it.

Case Study: Belarus[239]

Foreword by Kenneth Geers[240]

Life in Belarus has not changed much since the Cold War. In 2001, U.S. Secretary of State Colin Powell called its autocratic President, Alexander Lukashenko, Europe's "lone outlaw."[241]

The Belarusian Presidential Administration directly controls nearly all media within the country.[242] There are fewer than 10 professional quality printing presses outside of state control.[243] Television and radio stations try to avoid news programming altogether – for fear of losing their license – and even Russian TV is heavily censored.[244] In 2005, Freedom House ranked only Turkmenistan lower than Belarus in terms of democracy among the countries of the former Soviet Union.[245]

The state-owned Beltelecom monopoly is the sole provider of telephone and Internet connectivity, although about 30 national ISPs connect *through* Beltelecom. The only reported independent Internet link is via the government's academic and research network, BasNet. Strict government controls are enforced on all telecommunications technologies; for example, transceiver satellite antennas and IP telephony are prohibited. Beltelecom has been accused of "persecution by permit" and of requiring a demonstration of political loyalty to access its services. At least one Belarusian journalist is reported to have "disappeared."[246]

As in Zimbabwe, the Beltelecom monopoly status is intended not only for government oversight, but also to maximize financial gain. It is the primary source of revenue for the Ministry of Communications (MIC).[247]

The State Center for Information Security (GCBI), in charge of domestic signals intelligence (SIGINT), controls the ".by" Top Level Domain (TLD) and thus manages both the national Domain Name Service (DNS) and website access in general. Formerly

239 Following the Foreword, this chapter is a translation by the author of a Russian language paper written by Fedor Pavluchenko of www.charter97.org, entitled "Belarus in the Context of European Cyber Security," which was presented at the 2009 Cooperative Cyber Defence Centre of Excellence Conference on Cyber Warfare.

240 This chapter Foreword is taken from: Geers, 2007a.

241 Kennicott, 2005.

242 Usher, 2006.

243 Kennicott, 2005.

244 "The Internet and Elections...," 2006.

245 Kennicott, 2005.

246 "The Internet and Elections...," 2006.

247 *Ibid.*

part of the Belarusian KGB, GCBI reports directly to President Lukashenko.[248] Department "K" (for Кибер or Cyber), within the Ministry of Interior, has the lead in pursuing cyber crime. A common media offense in Belarus is defaming the "honor and dignity" of state officials[249].

Belarus already has a significant history of political battles in cyberspace. In 2001, 2003, 2004, and 2005, Internet access problems were experienced by websites that were critical of the President, state referenda, and/or national elections. While the government announced that website availability problems were the result of access "overload," the opposition countered that the sites were inaccessible altogether, and that the regime was deliberately blocking access. One of the affected sites had been characterized by the Ministry of Foreign Affairs as "political pornography".[250]

The biggest cyber showdown took place during the March 2006 Belarusian presidential elections, during which the opposition tried to use its youth and computer savvy to organize in cyberspace. The sitting government attempted the same, but because its supporters consisted of many rural and elderly voters who were still unconnected or new to the Internet, its efforts were uphill at best.[251]

Election Day 2006 provided the world an infamous example of modern-day cyber politics. As Belarusians went to the polls on March 19, thirty-seven opposition media websites were inaccessible from Beltelecom.[252] "Odd" DNS (Internet address) errors were reported, and the website of the main opposition candidate, Aleksandr Milinkevich, was "dead."

President Lukashenko won the election by a wide margin. A week later, as anti-government protestors clashed with riot police, the Internet was inaccessible from Minsk telephone numbers. A month later, when an opposition "flash-mob" was organized over the Internet, arriving participants were promptly arrested by waiting policemen.[253]

Similar to Iran, a primary lesson from Belarus is that Internet filtering and government surveillance do not have to be comprehensive to be effective. Selective targeting of known adversaries and increased computer network operations at critical points in time, such as during elections, can be very useful to a sitting government.

248 *Ibid.*

249 Kennicott, 2005.; and "Press Reference: Belarus."

250 "The Internet and Elections...," 2006.

251 *Ibid.*

252 The OpenNet Initiative confirmed that 37 of 197 tested websites were inaccessible from the Beltelecom network, but were still accessible from other computer networks.

253 *Ibid.*

"Belarus in the Context of European Cyber Security"

Written in Russian by Fedor Pavluchenko (**www.charter97.org**)

Translated to English by Kenneth Geers

During the first decade of the 21st century, Internet censorship in Belarus has become a government tool used to combat political dissent. This ongoing cyber conflict between state and non-state actors is similar to the struggle between the Russian government and its domestic adversaries in cyberspace.

State-sponsored, politically-motivated Denial of Service (DDoS) attacks against civil society are unacceptable. In Belarus, this violation of freedom of expression has become a national crisis. But the problem is not confined within these borders; it threatens the integrity of Internet resources in other European countries as well.

Modern technology offers the world significantly improved communications, but it also creates novel threats. Governments can abuse their power over state-controlled infrastructures. This not only violates human rights, but it engenders long-term political instability. Democratic states in Europe should work to strengthen independent Internet institutions and extend the rule of law to the whole of European cyberspace.

Alexander Lukashenko has governed Belarus as an autocrat since a disputed political referendum in 1996. His government has suppressed freedom of speech, and for over a decade there has been virtually no independent media in Belarus. The popular newspapers of the 1990s have ceased to exist or have seen their circulation greatly reduced, and independent radio stations have been closed. Sadly, there has never been an independent Belarusian television channel.

The Internet, despite its high cost in Belarus, has unsurprisingly become the only source of objective information for the majority of the citizens. The number of web users has now grown to nearly one-quarter of the country's population.

The Charter '97 website has been a leading Belarusian venue for public policy discussion for over a decade. However, because Charter '97 is known for siding with Belarusian political dissidents, the site has been the target of myriad state-sponsored Internet information-blocking strategies.

September 9, 2001: Belarusian Internet users discovered the power of a government to wage cyber warfare against its own citizens on the day of its own national presidential elections. At 1200, Beltelecom blocked access to many popular political websites. Although the prohibited sites remained accessible outside Belarus, no one in Belarus could view them until the following afternoon at 1600, when the Internet "filtering" stopped.

From a technical perspective, this type of Internet censorship is easy for a telecommunications monopoly to perform. The data packets can be filtered at a government Internet Service Provider's (ISP) network router, based solely on the Internet Protocol (IP) address of the websites in question.

However, it can be equally simple for an Internet user or the censored website to understand exactly what is happening. For example, the "traceroute" computer network utility, which measures the paths and transit times of packets across networks, can be used to spot the exact point of network interruption.

Some of the prohibited sites were hosted on servers in Belarus, within the ".by" Top Level Domain (TLD). These sites were disabled by altering their Domain Name Service (DNS) records to make them inaccessible. This is possible because ".by" is administered by the Operations and Analysis Center, a special state agency that falls under the direct control of the Belarusian President. On September 9, 2001, the following domains were unreachable on the Belarusian web: home.by, minsk.by, org.by, unibel.by, nsys.by, and bdg.by.

Numerous websites, including www.charter97.org, responded by creating "mirrors" or copies of their content at other web addresses in an effort to stay online. All such mirrors were promptly blocked by the government. Furthermore, websites that specialize in obscuring the source and destination of web searches, such as "anonymizers" and "proxy" servers, were also blocked. In all, over 100 websites were inaccessible.

It is important to note that within Belarusian law there were no legal grounds to perform censorship of political content on the web. What happened in 2001 directly violated the constitution. Beltelekom and the Belarus Ministry of Communications both announced that the outage stemmed from too many Belarusians trying to access the affected sites at the same time, and that this led to a self-inflicted Denial of Service. But this story is easy to disprove via simple technical analysis.

For its part, Belarusian government leadership had no comment, even though Internet censorship and computer sabotage are an offense under Belarusian law. Furthermore, there was never any official investigation into the facts of this case.

October 24, 2001: The Charter '97 website was completely deleted from its web server by an unidentified computer hacker. A few days after the attack, under pressure from the Belarusian secret services, our hosting company broke the terms of our contract. www.charter97.org was no longer allowed space on its server.

January 20, 2004: For the first time, Charter '97 was the target of a Distributed Denial of Service (DDoS) attack. The DDoS followed our publication of a journalistic investigation into a possible connection between high-ranking officials from the Be-

larusian Interior Ministry – which is responsible for investigating computer crimes – and the trading of online child pornography.

The DDoS attack lasted more than three weeks and was supported by a botnet that comprised more than 55,000 active IP addresses. This network of infected computers spanned the globe and included machines in Latin America, the United States, South-East Asia, China, and India. The source IPs and intensity of the attack changed several times, which indicated an active command and control (C2) over the activity.

Of course, it is impossible to prove that the DDoS attack was politically motivated, but external simultaneous factors corroborate this theory. On state television, a campaign of harassment targeted the employees of Charter '97. Among other things, the employees themselves were accused of trading in online pornography. In addition, Natalya Kolyada, a human rights activist working with the site, was convicted on misdemeanor charges.

July 14-21, 2004: On July 14, for 2 hours, a cyber attack paralyzed the server that hosted the Charter '97 website. It is believed that this event was a "test" to facilitate what happened one week later.

On July 21, there were mass protests in Minsk to demonstrate against the 10th anniversary of the Lukashenko government. Charter '97 had planned to host a webcast in support of the protests. For the second time, the website came under a DDoS-attack, which began at 1400 – 4 hours before the demonstrations began – and lasted until the political protests were over. This DDoS bore strong similarities to the first attack in January of 2004.

October 10, 2004: The next large-scale attempt to block Charter '97 and other independent websites occurred during parliamentary elections and a simultaneous referendum on whether to lift presidential term limits in Belarus.

On the day before the election, news correspondents were not only unable to access the website, but they could not telephone Charter '97 by mobile or landline phone. In addition, other political opposition websites were again blocked by a filter on Beltelekom's primary router. However, many Belarusian web users were better prepared for this attack and immediately switched to Internet proxies and anonymizers.

Unfortunately, the government had a new, effective cyber weapon in its arsenal: the artificial stricture – or "shaping" – of Internet bandwidth. The use of this tactic meant that, in principle, forbidden sites were still available, but it took anywhere from 5-10 minutes for their pages to load in a browser. Thus, web users were simply unable to gain full access to Charter '97 and other targeted sites. Non-political Internet resources were accessible as normal.

Neither the Ministry of Communications nor Beltelekom made any announcement regarding this incident, and no official investigation was undertaken.

March 19, 2006: The next time that Belarusian websites were blocked was during the 2006 presidential elections. Anticipating the government's strategy, Charter '97 well before the election took place offered its visitors numerous ways to circumvent censorship in an initiative called "Free Internet." Due in part to those efforts, Beltelekom's IP-filtering failed. However, its network "shaping," or the selective starvation of specific streams of bandwidth, was again successfully employed.

On March 18, the day before the election, a censorship "test" was conducted from 1600-1630. On election day, the sites of opposition presidential candidates, political parties, leading independent news sources, and the international blogging site www.livejournal.com, which is very popular with Belarusians, were all successfully blocked. Beltelekom announced that the service interruptions were caused by too many users trying to connect to the affected sites, but no formal investigation was undertaken.

April 25-26, 2008: On the eve of massive street protests in Minsk, which Charter '97 had intended to broadcast via live webcast, the website suffered a DDoS-attack that paralyzed its server. This was another "test," which lasted 30 minutes.[254]

On April 26 – the day of the planned demonstration – the real DDoS attack began, five hours before the start of the protest. The hosting company, www.theplanet.com, was overwhelmed. Its hardware was designed to carry up to 700 Mbit/s of network traffic, but the DDoS surpassed 1 Gbit/s.[255] There was no alternative but to turn off the website and simply wait for the attack to end (on the following day).

Other independent online media were targeted simultaneously, including the Belarusian-language version of "Radio Liberty." A server hosting the opposition site, "Belarusian Partisan," for several days came under the control of unknown hackers, who used it as a platform to publish fabricated, scandalous news stories which Belarusian Partisan editors were forced to refute on other websites. The high level of expertise required for this attack strongly suggested the involvement of Belarusian intelligence agencies.

The technical defense capabilities of the Radio Liberty server – home to its Belarusian, Albanian, Azerbaijani, Tajik, and Russian services – were sufficient to withstand the attack for more than 3 days. The site remained accessible, but was nonetheless

254 For about 10 minutes, the site was difficult to access, but normal traffic was restored before the attack ended. The following IP addresses were used in the attack: 89.211.3.3, 122.169.49.85, 84.228.92.1, 80.230.222.107, 212.34.43.10, 81.225.38.110, 62.215.154.167, and 62.215.117.15.

255 Megabits per second/gigabits per second.

difficult to reach, and this caused a minor diplomatic scandal. The U.S. mission to the Organization for Security and Cooperation in Europe (OSCE) issued a statement condemning the cyber attack. The Belarusian Ministry of Foreign Affairs denied any involvement.

June 8, 2009: The most recent example of a politically-motivated DDoS attack on Charter '97 occurred during a political row between the governments of Russia and Belarus, which resulted in the imposition of Russian economic sanctions against Belarus and a worsening of the political situation inside Belarus itself.

The cyber attack lasted more than a week, and for a while it paralyzed the site completely. The strength of the DDoS in this case was not particularly high; only around five thousand IP addresses took part in it. In cooperation with our ISP, the Charter '97 technical support staff was able to neutralize the attack.

Countermeasures and their effectiveness: Charter '97 is constantly looking for ways to counter government censorship, but there is no foolproof solution. The situation in Belarus is best described as an effort to outmaneuver an opponent who has vastly more resources than they do.

Over time, Charter '97 has found some answers in technology and in cyber security expertise. They moved their site to a relatively powerful, hardened server,[256] built an intrusion detection system, and constantly monitor vulnerabilities. They use encryption to access both the server and the site's content management system. They have multi-tiered levels of access to both the server and the site, and they are able to quickly replace all passwords in the event administrators and/or journalists are arrested. They have a distributed system for creating server data backups. Moreover, they have endeavored to master simple, open-source technologies such as UNIX, PHP, and MySQL.[257] All told, these efforts go a long way toward preventing the compromise of the web server.

Charter '97 also launched the "Free Internet" project, which provides recommendations to visitors in case the site becomes unavailable. It explains how to use an Internet proxy, anonymizers, Virtual Private Networks (VPN), and software such as Tor.[258] This information is rebroadcast via RSS[259] and mirror websites, and visitors are encouraged to disseminate it through their own blogs, chat rooms, social networking, etc. These measures are sufficient to overcome simple IP blocking, but there is still no solid countermeasure to DDoS, especially with limited resources.

256 Firewall and caching technologies are sufficient to repulse DDoS-attacks of average strength.

257 This helps with site mobility (i.e. the rapid transfer of our site to another hosting platform).

258 The Onion Router or the Tor anonymity network.

259 Really Simple Syndication.

Charter '97 believes that the government's most effective methods of censorship are DoS attacks and various kinds of information manipulation. For the latter, intelligence operatives can insert themselves into ongoing discussions on the web in order to monitor or even "guide" conversations. If and when the political dialogue rises above a certain threshold, especially during politically sensitive points in time, the authorities can take action.

Government power, cyber crime, and the future: The current Belarusian government suppresses political dissent on the Internet and flagrantly violates its own constitution. There is no legal basis for Internet censorship at all, much less for state-sponsored computer hacking and DoS attacks. Furthermore, such attacks could be used to block any kind of information. The result is the absence of the rule of law within the Belarusian Internet space, and a situation in which organized, state-sponsored cyber crime could flourish, not only in Belarus but also beyond its borders.

There is active cooperation between Belarusian and Russian intelligence agencies in cyberspace, as specified in the Agreement on Cooperation of the Commonwealth of Independent States (CIS) in Combating Cybercrime, signed in 2000. And there are strong similarities between attacks on Estonia, Georgia, and the websites of human rights organizations in Belarus and Russia. These Internet crimes share common characteristics and appear to have common roots.

Civil society is threatened throughout Eastern Europe: in Belarus, Ukraine, Russia, Georgia, Armenia, and Azerbaijan, governments have likely used DoS attacks as a tool for suppressing political dissent.

In response, a multinational, collaborative approach is required. A good start would be the creation of an international web hosting platform designed to support freedom of speech throughout Europe. It should be built by a team of international experts, who could improve defenses and investigate attacks based on aggregate data. Privacy must of course be balanced with legitimate law enforcement powers, but the mere creation of an international platform would enhance cyber security and freedom of expression in Europe, especially during important events such as national elections.

International Conflict in Cyberspace

Chapter 4 has demonstrated that many governments already perceive a clear connection between cyber security and internal political security. But what about international conflict? To what extent can nation-states threaten their peers, and even defeat their rivals, in cyberspace?

In fact, all international political and military conflicts now have a cyber dimension, the size and impact of which are difficult to predict. Today, practically everything that happens in the "real world" is mirrored in cyberspace, and for national security planners this includes propaganda, espionage, and – to an unknown but increasing extent – warfare itself.

The Internet's ubiquitous and unpredictable characteristics can make the battles fought in cyberspace just as important, if not more so, than events taking place on the ground. A brief analysis of current events proves that international cyber conflict is already commonplace.

Here are five illustrative examples that suggest it is no longer a question of whether computer hackers will take world leaders by surprise, but when and under what circumstances.

Chechnya 1990s: Propaganda

In the Internet era, unedited news from a war front can arrive in real-time. As a result, Internet users worldwide play an important role in international conflicts simply by posting information, in either text or image format, to a website.

Since the earliest days of the World Wide Web, Chechen guerilla fighters, armed not only with rifles but with digital cameras and HTML, have clearly demonstrated the power of Internet-enabled propaganda.

Since the earliest days of the World Wide Web, pro-Chechen and pro-Russian forces have waged a virtual war on the Internet, simultaneous with their conflict on the ground. The Chechen separatist movement in particular is considered a pioneer in the use of the Web as a tool for delivering powerful public relations messages. The skillful placement of propaganda and other information, such as the number to a war funds bank account in Sacramento, California, helped to unite the Chechen diaspora.[260]

260 Thomas, 2002.

The most effective information, however, was not pro-Chechen, but anti-Russian. Digital images of bloody corpses served to turn public opinion against perceived Russian military excesses. In 1999, just as Kremlin officials were denying an incident in which a Chechen bus was attacked and many passengers killed, images of the incident appeared on the Web.[261] As technology progressed, Internet surfers watched streaming videos of favorable Chechen military activity, such as ambushes on Russian military convoys.[262]

The Russian government admitted the need to improve its tactics in cyberspace. In 1999, Vladimir Putin, then Russia's Prime Minister, stated that "we surrendered this terrain some time ago ... but now we are entering the game again." Moscow sought the help of the West in shutting down the important pro-Chechen **kavkaz.org** website, and "the introduction of centralized military censorship regarding the war in the North Caucasus" was announced.[263]

During the second Chechen war (1999-2000), Russian officials were accused of escalating the cyber conflict by hacking into Chechen websites. The timing and sophistication of at least some of the attacks suggested nation-state involvement. For example, **kavkaz.org** (hosted in the U.S.) was reportedly knocked offline simultaneously with the storming by Russian special forces of a Moscow theater under siege by Chechen terrorists.[264]

Kosovo 1999: Hacking the Military

In globalized, Internet-era conflicts, anyone with a computer and a connection to the Internet is a potential combatant. NATO's first major military engagement followed the explosive growth of the Web during the 1990s. Just as Vietnam was the world's first TV war, Kosovo was its first broad-scale Internet war.

As NATO planes began to bomb Serbia, numerous pro-Serbian (or anti-Western) hacker groups, such as the "Black Hand," began to attack NATO Internet infrastructure. It is unknown whether any of the hackers worked directly for the Yugoslav military. Regardless, their stated goal was to disrupt NATO's military operations.[265]

The Black Hand, which borrowed its name from the Pan-Slavic secret society that helped to start World War I, claimed it could enumerate NATO's "most important" computers, and that through hacking it would attempt to "delete all the data" on

261 Goble, 1999.
262 Thomas, 2002.
263 Goble, 1999.
264 Bullough, 2002.
265 "Yugoslavia..." 1999.

them. The group claimed success on at least one U.S. Navy computer, and stated that it was subsequently taken off-line.[266]

NATO, U.S., and UK computers were all attacked during the war, via Denial-of-Service and virus-infected email (twenty-five different strains of viruses were detected).[267] In the U.S., the White House website was defaced, and a Secret Service investigation ensued. While the U.S. claimed to have suffered "no impact" on the overall war effort, the UK admitted to having lost at least some database information.[268]

At NATO Headquarters in Belgium, the attacks became a propaganda victory for the hackers. The NATO public affairs website for the war in Kosovo, where the organization sought to portray its side of the conflict via briefings and news updates, was "virtually inoperable for several days." NATO spokesman Jamie Shea blamed "line saturation" on "hackers in Belgrade." A simultaneous flood of email successfully choked NATO's email server. As the organization endeavored to upgrade nearly all of its computer servers, the network attacks, which initially started in Belgrade, began to emanate from all over the world.[269]

Middle East 2000: Targeting the Economy

During the Cold War, the Middle East often served as a proving ground for military weapons and tactics. In the Internet era, it has done the same for cyber warfare.

In October 2000, following the abduction of three Israeli soldiers in Lebanon, blue and white flags as well as a sound file playing the Israeli national anthem were planted on a hacked *Hizballah* website. Subsequent pro-Israeli attacks targeted the official websites of military and political organizations perceived hostile to Israel, including the Palestinian National Authority, *Hamas*, and Iran.[270]

Retaliation from Pro-Palestinian hackers was quick and much more diverse in scope. Israeli political, military, telecommunications, media, and universities were all hit. The attackers specifically targeted sites of pure economic value, including the Bank of Israel, e-commerce, and the Tel Aviv Stock Exchange. At the time, Israel was more wired to the Internet than all of its neighbors combined, so there was no shortage of targets. The ".il" country domain provided a well-defined list that pro-Palestinian hackers worked through methodically.

266 *Ibid.*

267 "Evidence..." 1999.

268 Geers, 2005.

269 Verton, 1999.

270 For example, the Zone-H website lists 67 such defacements from pro-Israeli hacker m0sad during this time period.

Wars often showcase new tools and tactics. During this conflict, the "Defend" DoS program was used to great effect by both sides, demonstrating in part that software can be copied more quickly than a tank or a rifle. Defend's innovation was to continually revise the date and time of its mock Web requests; this served to defeat the Web-caching security mechanisms at the time.[271]

The Middle East cyber war demonstrated that Internet-era political conflicts can quickly become internationalized. For example, the Pakistan Hackerz Club penetrated the U.S.-based pro-Israel lobby AIPAC and published sensitive emails, credit card numbers, and contact information for some of its members.[272] The telecommunications firm AT&T – clearly an international critical infrastructure service provider to all sectors of the world economy – was targeted for providing technical support to the Israeli government during the crisis.[273]

Since 2000, the Middle East cyber war has generally followed the conflict on the ground. In 2006, as tensions rose on the border between Israel and Gaza, pro-Palestinian hackers shut down around 700 Israeli Internet domains, including those of Bank Hapoalim, Bank Otsar Ha-Hayal, BMW Israel, Subaru Israel, and McDonalds Israel.[274]

U.S. and China 2001: Patriotic Hacking

On April 26, 2001, the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center (NIPC) released Advisory 01-009:

"Citing recent events between the United States and the People's Republic of China (PRC), malicious hackers have escalated web page defacements over the Internet. This communication is to advise network administrators of the potential for increased hacker activity directed at U.S. systems .... Chinese hackers have publicly discussed increasing their activity during this period, which coincides with dates of historic significance in the PRC...."[275]

Tensions had risen sharply between the two countries following the U.S. bombing of the Chinese embassy in Belgrade in 1999, the mid-air collision of a U.S. Navy plane with a Chinese fighter jet over the South China Sea in 2001, and the prolonged detainment of the American crew in the PRC.

271 Geers & Feaver, 2004.
272 "Israel..." 2000.
273 Page, 2000.
274 Stoil & Goldstein, 2006.
275 "Advisory 01-009..." 2001.

Hackers on both sides of the Pacific, such as China Eagle Alliance and PoizonB0x, began wide-scale website defacement and built hacker portals with titles such as "USA Kill" and "China Killer." When the cyber skirmishes were over, both sides claimed defacements and DoSs in the thousands.[276]

The FBI investigated a Honker Union of China (HUC), 17-day hack of a California electric power grid test network that began on April 25th.[277] The case was widely dismissed as media hype at the time, but the CIA informed industry leaders in 2007 that not only is a tangible hacker threat to such critical infrastructure possible, it in fact has already happened.[278]

On the anniversary of this cyber war, as businesses were bracing for another round of hacking, the Chinese government is said to have successfully called for a stand-down at the last minute, suggesting that Chinese hackers may share a greater degree of coordination than their American counterparts.[279]

Estonia 2007: Targeting a Nation-State

On April 26, 2007, the Estonian government moved a Soviet World War II memorial from the center of its capital to a military cemetery. The move inflamed public opinion both in Russia and among Estonia's Russian minority population. Beginning on April 27, Estonian government, law enforcement, banking, media, and Internet infrastructure endured three weeks of cyber attacks, whose impact still generates immense interest from governments around the world.

Estonians conduct over 98% of their banking via electronic means. Therefore, the impact of multiple Distributed Denial-of-Service (DDoS) attacks, which severed all communications to the Web presence of the country's two largest banks for up to two hours and rendered international services partially unavailable for days at a time, is obvious.

Less widely discussed, but likely of greater consequence – both to national security planners and to computer network defense personnel – were the Internet infrastructure (router) attacks on one of the Estonian government's ISPs, which disrupted government communications for a "short" period of time.[280]

276 Wagstaff, 2001; Allen & Demchek, 2003.

277 Weisman, 2001.

278 Nakashima & Mufson, 2008.

279 Hess, 2002.

280 This case-study relies on some data available exclusively to CCD-CoE.

On the propaganda front, a hacker defaced the Estonian Prime Minister's political party website, changing the homepage text to a fabricated government apology for having moved the statue, along with a promise to move it back to its original location.

Diplomatic interest in the Estonia case was high, in part due to the possible reinterpretation of NATO's Article 5, which states that "an armed attack against one [Alliance member]... shall be considered an attack against them all."[281] Article 5 has been invoked only once, following the terrorist attacks of September 11, 2001. Potentially, it could one day be interpreted to encompass cyber attacks as well.

For many observers, the 2007 denial-of-service attacks in Estonia demonstrated a clear "business case" cyber attack model against an IT-dependent country. The crisis significantly influenced the 2010 debate over NATO's new Strategic Concept, when cyber security assumed a much higher level of visibility in international security dialogue, ranking alongside terrorism and ballistic missiles as a primary threat to the Alliance.[282]

To summarize Part II of this book, the world has witnessed the transformation of cyber security from a technical discipline to a strategic concept. The growing power of the Internet, the rapid development of hacker tools and tactics, and clear-cut examples from current events suggest that cyber attacks will play an increasingly important, and perhaps a lead role, in future international conflicts.

Since the Estonia crisis in 2007, this trend shows no sign of slowing down:

- in 2007, the Israeli military is reported to have conducted a cyber attack against Syrian air defense prior to its destruction of an alleged nuclear reactor;[283]
- in 2008, many analysts argued that the Russo-Georgian war demonstrated that there will be a close relationship between cyber and conventional operations in all future military campaigns;[284]
- in 2009, during a time of domestic political crisis, hackers knocked the entire nation-state of Kyrgyzstan offline;[285] and
- in 2010, the Stuxnet worm was believed to be the most sophisticated piece of malware yet examined by public researchers and is widely assumed to have been written by a state sponsor.[286]

281 "*The North Atlantic Treaty*," 1949.

282 "NATO 2020..." 2010.

283 Fulghum et al, 2007.

284 "Overview..." 2009.

285 Keizer, 2009.

286 "Stuxnet..." 2010.

Therefore, national security leadership has no choice but to dramatically increase its level of understanding of the technology, law, and ethics related to cyber attack and defense so that it can competently factor cyber conflict, terrorism and warfare into all stages of national security planning.

Part III of this book will examine four strategies that nation-states are likely to adopt as they seek to mitigate the threat of cyber attacks and attempt to improve their national cyber defense posture.

III. NATION-STATE CYBER ATTACK MITIGATION STRATEGIES

Part II of this book examined the advent of cyber security as a strategic concept. Part III will evaluate four likely strategies that governments will employ to mitigate the cyber attack threat: the "next-generation" Internet Protocol version 6 (IPv6), an application of the world's best military doctrine (Sun Tzu's *Art of War*) to cyber warfare, cyber attack deterrence, and cyber arms control.

5. NEXT GENERATION INTERNET: IS IPV6 THE ANSWER?[287]

First and foremost, governments will seek to reach a higher level of strategic cyber security through improved technology. And the most likely candidate to have an effect at the strategic level is a sleeping giant – the new "language" of networks, Internet Protocol version 6 (IPv6).

In fact, due to its stellar number of viable computer addresses and its enhanced security features, many nations view IPv6 as crucial to their national security plans for the future. However, its high learning curve has led myriad government agencies and large businesses to miss deadlines for IPv6 compliance.

A different perspective is offered by some human rights organizations, which fear that the "next-generation" Internet will have adverse effects on individual privacy and online anonymity.

Regarding IPv6 security, a key point to understand is that, during the long transition period from IPv4 to IPv6, hackers will be able to exploit vulnerabilities in both languages at once.

IPv6 Address Space

IPv4, the current language of the Internet, will run out of available IP addresses – or "space" from which one can connect to the Internet – in 2011. The address shortage is especially acute in the developing world, which connected to the Internet after most IP addresses had already been allocated or bought.[288]

287 This chapter was co-authored with Alexander Eisen.

288 Grossetete et al, 2008.

IPv6 decisively answers the need for more IP addresses. IPv4 has around four billion, which seemed like a lot when the protocol was written in the early 1980s, but is insufficient today. IPv6, developed in the late 1990s, has 128-bit addresses, which create 340 undecillion IPs,[289] or 50 octillion for every human on Earth.[290]

As an added bonus, IPv6 employs much more powerful IP "headers," or internal management data, which allow for more advanced features and customization than with IPv4. IPv6 headers will be used to support "telematics," the integrated use of telecommunications and informatics. Since IPv6 will allow practically everything, including common household appliances, to be connected to the Internet, its advocates argue that telematics will provide more convenient, economical, and entertaining lifestyles.[291]

Improved Security?

But the most important aspect of IPv6 for this research is that it was designed to provide better security than IPv4.[292] The goal was to build security into the protocol itself. Thirty years ago, IPv4 defeated more feature-rich rivals precisely because IP was a "dumb" protocol. It lacked sophistication, but was simple, resilient, and easy to implement and maintain. The problem was that IPv4's lack of intrinsic security left it open to misuse.

Today, a better network protocol is needed, both for size and for security. IPv6 offers clear security upgrades over IPv4. First, IPv6 is much more cryptography-friendly. A mechanism called IP Security (IPSec) is built directly into the protocol's "code stack." IPSec should reduce Internet users' vulnerability to spoofing,[293] illicit traffic sniffing[294] and Man-in-the-Middle (MITM) attacks.[295]

IPv6 also offers end-to-end connectivity, which is afforded by the incredibly high number of IP addresses available. Since it is possible, in theory, to give anything an IP address, any two points on the Internet may communicate directly with each other.

289 Or 340,282,366,920,938,463,463,374,607,431,768,211,456 possible addresses.

290 An IPv4 address looks like this: 207.46.19.60. IPv6 is much longer: 2001:0db8:0000:0000:0000:0000:1428:57ab (or, for short, 2001:0db8::1428:57ab).

291 Godara, 2010: The term telematics often refers to automation in automobiles, such as GPS navigation, hands-free cell phones, and automatic driving assistance systems.

292 Hagen, 2002.

293 Spoofing means impersonating another computer user or program.

294 Passively collecting network data, with or without appropriate approval.

295 This is when an attacker secretly controls both sides of a conversation. The victims think they are speaking with one another directly, for example, by email, when in fact they are not.

These upgrades should have numerous follow-on benefits. For example, the astronomical number of IP addresses may mean that attackers will no longer be able to randomly "scan" the Internet to find their victims. In addition, the Internet should be more resistant to self-propagating worms.[296]

To improve strategic cyber security across the Internet, any successor to IPv4 should have a greater focus on structure and logic (e.g., Internet navigation, data packet routing, IP address allocation). Fortunately, with IPv6, this is the case. The Internet Engineering Task Force (IETF) created the first IPv6 Forum in 1999; today there are IPv6-specific Task Forces worldwide, which still have the opportunity to make tangible improvements in the next-generation protocol as it evolves.

IPv6 Answers Some Questions, Creates Others

In spite of these promising characteristics, it is unlikely that IPv6 will end cyber attacks in the future. Hackers have already demonstrated that IPv6 is not invulnerable to many traditional, IPv4 attack methods, including DoS,[297] packet crafting,[298] and MITM attacks.[299] Vulnerabilities in software (operating systems, network services, web applications) will continue to exist, no matter which protocol they use.[300] And perhaps most crucially, although IPSec is available, it is not required.[301]

As an analogy, the history of Public Key Infrastructure (PKI)[302] does not bode well for IPv6. The high cost and resource-intensive nature of PKI pose challenges to most organizations, and in the future, the same dynamic could hamper the large-scale deployment of IPSec in IPv6.

False identities are often assumed by stealing or creating fraudulent ID cards or other documents. Via the Internet, attackers will still attempt to use hacked computers as "proxies" for nefarious activity, even in the IPv6 era. The case of Stuxnet has

296 Popoviciu et al, 2006.

297 E.g., Smurf6, Rsmurf6, Redir6, connection flooding, and stealing all available addresses.

298 This refers to manually creating network data packets instead of using default or existing network traffic characteristics.

299 Or "man-in-the-middle" attacks, e.g., Parasite6, Fake_router6.

300 In fact, the majority of attacks today may not involve eavesdropping on or manipulating the traffic on a network wire. A compromised application, for example, could exfiltrate stolen information equally well via either the IPv4 or the IPv6 code stack.

301 It is also important to note that the improved IP header still does not travel across the Internet encrypted, but in the clear.

302 This refers to the management of digital certificates. PKI uses asymmetric cryptography to create an electronic identity. Internet services are increasingly using it, and this should lower the risk of identity theft, but Stuxnet has shown that PKI is not a silver bullet.

shown that, even with PKI safeguards, it is possible to steal digital identities that allow a hacker to run computer code as if it were installed by a trustworthy company.

And of course, the next-generation Internet will spawn next-generation attacks. For example, if IPv6 precludes network vulnerability scanning, hackers may increasingly target Certificate Authorities (CA) and Domain Name Servers (DNS). In fact, a successful compromise of a DNS server may be required for an attacker to acquire detailed knowledge of a target Local Area Network (LAN).[303]

The necessarily long transition period will provide its own set of challenges. The most important is that, as the world uses both IP languages at once, hackers will have an increased "attack surface." There will simply be a higher number of vulnerabilities to exploit as computer security personnel are forced to defend a larger network space within their enterprise.

The level of complexity will rise as system administrators manage more devices per enterprise, more network interface cards (NIC) per device, and more code "stacks" or data structures per NIC. Furthermore, some network data will be "native" or IPv6-only, but other IPv6 traffic will be "tunneled" or shuttled across the Internet within IPv4 carrier packets.

Such a new and complex environment may allow some cyber attacks to slip through myriad cracks in cyber defense architecture. In fact, this may already be the case on countless networks, given that modern devices and operating systems are often IPv6-enabled by default.

The opposite is true for computer network defense. For example, even in the latest version of the world's most popular intrusion detection software, called "Snort," IPv6 awareness is not enabled by default, but must be specifically turned on by a security analyst.[304] The likely result is a serious blind spot in global network traffic analysis.

Consider the "auto-configuration" aspect of IPv6. Its intended function is to ease and increase mobility through enhanced, ad hoc network associations. This appears to be an exciting part of the world's future networking paradigm. However, auto-configuration would also seem to greatly complicate the task of tracking network-enabled devices that enter and leave enterprise boundaries.

303 If DNS attacks are successful in the IPv6 era, the overall trend toward client-side exploits – those which target the end user – should continue.

304 "SNORT Users Manual..." 2011.

Privacy Concerns

From a law enforcement and national security perspective, there is worldwide interest in the implications of IPv6 for online privacy and anonymity, which will have a tangible impact on relations between government and civil society.

IPv6 security, specifically in the form of IPsec, contains a potential paradox. Users gain end-to-end connectivity with peers and acquire strong encryption to obscure the content of their communications, but the loss of Network Address Translation (NAT) means that it is easier for third parties to see who is communicating with whom. Even if an eavesdropper is not able to read encrypted content, "traffic analysis" – or the deduction of information content by analyzing communication patterns – should be easier than with IPv4.

NAT allows multiple users to connect to the Internet from one IP address. It almost single-handedly saved IPv4 from address depletion for many years.[305] Further, NAT provides Internet users with some "security through obscurity" by making IP addresses temporary and not permanently associated with a human user. This characteristic offers a small but tangible amount of Internet privacy.

Critics of NAT claim that it is labor-intensive, expensive, and unnecessary, but others worry that its loss will come at the expense of privacy. For example, Chinese Internet Society chairwoman Hu Qiheng told the *New York Times* in 2006 that "there is now anonymity for criminals on the Internet in China ... with the China Next Generation Internet project, we will give everyone a unique identity on the Internet."[306]

The simple reasoning behind Qiheng's thinking is that IPv6 could facilitate the direct association of a permanent IP address to a particular Internet user. For law enforcement, end-to-end connectivity may help to solve the vexing "attribution" problem of cyber attacks, in which hackers are able to remain anonymous. But human rights groups fear that governments will use this new power to quash political dissent.

This open question is serious enough that, in the future, various national IPv6 implementations may be incongruous or even incompatible with one another, as different network configurations are used for different purposes.

IPv6 "privacy extensions" were designed to address this problem by making it possible for a user to acquire somewhat random, temporary IP addresses in order to surf the web with greater privacy and security. Only time will tell whether IPv6 privacy extensions work in practice. Since IPv6 is just now being broadly deployed,

305 IPv4's lifespan was also extended by coding other aspects of IPv6, such as IPSec, into IPv4.

306 Crampton, 2006.

many of its advanced features have not been subjected to sufficient testing or security analysis.[307]

In 2011, it is still unknown whether the IPv6 era will favor attackers or defenders in cyberspace. In the long-run, it is possible that the new protocol's benefits will be good for overall Internet security. However, it is a near certainty that the long transition phase from IPv4 to IPv6 will be characterized by increased security risks.

Uneven Worldwide Deployment

Many governments are not waiting for this debate to be settled. In a network-centric world, future Internet technologies such as IPv6 cannot be ignored. A government's ability to conduct national security-related operations may depend on them one day. Nations and businesses risk falling behind peers, competitors, and enemies. Thus, numerous governments have set deadlines for various levels of IPv6 compliance.

In the United States, the Executive Branch Office of Management and Budget (OMB) mandated that U.S. government agencies be "IPv6 compliant" by June 30, 2008. However, compliance in this case had very limited goals.[308] Furthermore, the OMB mandate was almost immediately contradicted by a U.S. Department of Commerce report advising that premature transition to IPv6 could lead to higher overall transition costs and even reduced security.

More recently, the first U.S. Chief Information Officer (CIO), Vivek Kundra, provided a more detailed government directive – public Internet services such as webmail and DNS must operationalize "native" or IPv6-only traffic by October 2012. Internal networks must do the same by 2014.[309]

Most American businesses feel no direct pressure to migrate to IPv6. The reason is that the U.S. is the original home of the Internet, so most American firms possess enough IP addresses to satisfy their needs. However, the largest software companies, such as Microsoft, support IPv6 because it should reduce or even eliminate the costs associated with NAT, which can be significant for online gaming, instant messaging, file sharing, etc.[310] Indeed, Microsoft made IPv6 the default Internet protocol for its Vista operating system, which was released in January 2007.

307 Barrera, 2010.

308 This referred only to the capability of an agency's core computer networks to forward IPv6 traffic to its intended destination.

309 Montalbano, 2010.

310 Golding, 2006.

China has made the most determined effort of any nation to transition to IPv6. Above all, the size of China's population demands a huge increase in its number of IP addresses since China has only one IPv4 address for every four of its citizens. At the same time, China has held the world's biggest single IPv6 demonstration to date. During the 2008 Summer Olympics in Beijing, everything from live television and data feeds to security and traffic control was streamed over one vast IPv6 network.[311] The cutting edge nature of IPv6 gives China a good way to development its Intellectual Property (IP) base. The China Next Generation Internet (CNGI) and the China Education and Research Network (CERNET) are huge IPv6 projects that will influence the evolution of the Internet for years to come. However, the slow pace of popular IPv6 application development, which has helped to keep worldwide transition sluggish, has disappointed Chinese Internet officials.[312]

Within the European Union (EU), an IPv6 Task Force has stated that the importance of the next-generation Internet "cannot be overestimated." In 2008, the European Commission advised private companies and the public sector to make the switch by 2010 and committed €90 million to IPv6 research.[313] But near the end of 2009, a survey found that less than 20% had done so and that a majority of respondents feared its immediate financial costs.[314] On the bright side, numerous European companies have made commercial contributions to IPv6 development. Ericsson built the world's first IPv6 router in 1995, and an IPv6 concept car was jointly developed by Cisco and Renault. Nonetheless, European companies have complained that further incentives from Brussels are needed to ensure a smooth transition.[315]

In Japan, the need for increased address space is similar to China's, but the reason is not population size. It stems from the desire to connect billions of electronic gadgets to the Internet. The Japanese government has assured its country a leadership role in IPv6 deployment by offering tax breaks to companies that switch to IPv6. Its importance is emphasized in political speeches at the highest level of government[316] and by initiatives such as "eJapan 2005," in which IPv6 was given prominent status. NTT, the largest telecommunications provider in Japan, has offered commercial IPv6 services since 2001, and the University of Tokyo has held both the IPv4 and IPv6 "World Speed" records simultaneously. As in China, however, both the public

311 "Renumbering..." 2011.
312 Geers & Eisen, 2007.
313 Meller, 2008.
314 Kirk, 2009.
315 Geers & Eisen, 2007.
316 Essex, 2008.

and private sectors are still waiting for more IPv6 applications, even while they are attempting to future-proof their infrastructure.[317]

Differences of Opinion Remain

While there are obvious business opportunities in IPv6, governments are also keenly interested in the strategic cyber security ramifications of the next-generation Internet. The loss of NAT will lower the cost of Internet connectivity and provide the foundation for improved communications worldwide, but it may also allow governments to monitor their Internet space – at least via traffic analysis – with much greater ease.

As an international project, IPv6 will both benefit and suffer from significant differences of approach and opinion. In Asia, citizens are more comfortable with government oversight than in the West. In Europe, Internet users are highly motivated to protect online anonymity. However, the U.S. is somewhere in the middle – personal information is jealously guarded, but the public is sympathetic to the needs of law enforcement.

In order to make the IPv6 era fairer than with IPv4, the Internet Assigned Numbers Authority (IANA) has published these guidelines:

- every address should be unique;
- every address should be in an accessible registry database;
- distribution should be aggregated, efficient, and hierarchical;
- there should be no "stockpiling" of unused addresses; and
- all potential members of the Internet community should have equal access.

Another factor is the "IPv6 Ready Logo," which is awarded to software and hardware that meets internationally-recognized technical standards. However, this initiative has already revealed the politically charged atmosphere surrounding IPv6. For example, China successfully argued against the direct inclusion of IPSec in the Logo award criteria, a seemingly small victory that could have enormous implications for privacy, anonymity, and security on the web for years to come. It remains an open question whether the U.S. and the EU should have pushed China harder during these negotiations. However, like China they must worry that IPsec will make life too hard for law enforcement.[318]

317 Geers & Eisen, 2007.

318 Geers & Eisen, 2007.

6. SUN TZU: CAN OUR BEST MILITARY DOCTRINE ENCOMPASS CYBER WAR?

Cyberspace is a new warfare domain. Computers and the information they contain are prizes to be won during any military conflict. But the intangible nature of cyberspace can make victory, defeat, and battle damage difficult to calculate. Military leaders today are looking for a way to understand and manage this new threat to national security. The most influential military treatise in history is Sun Tzu's *Art of War*. Its recommendations are flexible and have been adapted to new circumstances for over 2,500 years. This chapter examines whether *Art of War* is flexible enough to encompass cyber warfare. It concludes that Sun Tzu provides a useful but far from perfect framework for the management of cyber war and urges modern military strategists to consider the distinctive aspects of the cyber battlefield.

What is Cyber Warfare?

The Internet, in a technical sense, is merely a large collection of networked computers. Humans, however, have grown dependent on "cyberspace" – the flow of information and ideas that they receive from the Internet on a continual basis and immediately incorporate into their lives. As our dependence upon the Internet grows, what hackers think of as their potential "attack surface" expands. The governance of national security and international conflict is no different: political and military adversaries now routinely use and abuse computers in support of strategic and tactical objectives. In the early 1980s, Soviet thinkers referred to this as the Military Technological Revolution (MTR); following the 1991 Gulf War, the Pentagon's Revolution in Military Affairs (RMA) was practically a household term.[319]

Cyber attacks first and foremost exploit the power and reach of the Internet. For example, since the earliest days of the Web, Chechen rebels have demonstrated the power of Internet-enabled propaganda.[320] Second, cyber attacks exploit the Internet's vulnerability. In 2007, Syrian air defense was reportedly disabled by a cyber attack moments before the Israeli Air Force demolished an alleged Syrian nuclear reactor.[321] Third, cyber attackers benefit from a degree of anonymity. During the 1999 war over Kosovo, unknown hackers tried to disrupt NATO military operations and were able to claim minor victories.[322] Fourth, even a nation-state can be targeted. In 2009, the whole of Kyrgyzstan was knocked offline during a time of domestic politi-

319 Mishra, 2003.
320 Goble, 1999.
321 Fulghum et al, 2007.
322 Geers, 2008.

cal crisis.[323] This list could be lengthened to include cyber warfare's high return on investment, an attacker's plausible deniability, the immaturity of cyber defense as a discipline, the increased importance of non-state actors in the Internet era, and more.

Cyber attacks are best understood as an extraordinary means to a wide variety of ends: espionage, financial damage, and even the manipulation of national critical infrastructures. They can influence the course of conflict between governments, between citizens, and between government and civil society.

What is *Art of War?*

Modern military doctrine draws from a deep well of philosophy that spans political, economic, and scientific revolutions. The oldest and most profound treatise is Sun Tzu's *Military Strategy*, known as *Art of War* (孫子兵法). Much of our current understanding of military concepts such as grand strategy, center of gravity, decisive point, and commander's intent can be traced to this book.[324]

According to Chinese tradition, *Art of War* was written by Sun Wu (now Tzu) in the 6th century B.C. and is one of China's *Seven Military Classics*. Some scholars argue that gaps in logic and anachronisms in the text point to multiple authors, and they further contend that *Art of War* is a compilation of different texts that were brought together over time. Nonetheless, the book has an internal consistency that implies it is the product of one school of military thought. *Art of War* was translated for the West by a French missionary in 1782 and may have had an influence on the battlefield victories of Napoleon, who was likely familiar with its contents.[325]

Art of War has survived for 2,500 years because its advice is not only compelling, but concise, easy to understand, and flexible. Sun Tzu does not give military leaders a concrete plan of action, but a series of recommendations that can be adapted to new circumstances. Sun Tzu's concepts have been successfully applied to disciplines other than warfare, including sports, social relationships, and business.[326]

There are thirteen chapters in *Art of War*, each dedicated to a particular facet of warfare. This chapter highlights at least one topical passage from each chapter and will argue that Sun Tzu provides a workable but not a perfect framework for the management of cyber war.

323 Keizer, 2009.

324 Van Riper, 2006.

325 Ralph D. Sawyer, *Sun Tzu: Art of War* (Oxford: Westview Press, 1994) 79, 127.

326 *Ibid*, 15.

Strategic Thinking

Art of War opens with a warning:

> The Art of War is of vital importance to the State. It is a matter of life and death, a road either to safety or to ruin. Hence it is a subject of inquiry which can on no account be neglected. *AoW: I. Laying Plans*[327]

At the strategic level, a leader must take the steps necessary to prevent political coercion by a foreign power and to prevent a surprise military attack.[328] Regarding offensive military operations, *Art of War* states that they are justified only in response to a direct threat to the nation; economic considerations, for example, are insufficient.[329]

Cyberspace is such a new arena of conflict that basic defense and attack strategies are still unclear. There have been no major wars (yet) between modern, cyber-capable adversaries. Further, cyber warfare tactics are highly technical by nature, often accessible only to subject matter experts. As with terrorism, hackers have found success in pure media hype. As with Weapons of Mass Destruction (WMD), it is challenging to retaliate against an asymmetric threat. Attack attribution is the most vexing question of all – if the attacker can remain anonymous, defense strategies appear doomed from the start. Finally, the sensitive nature of cyber warfare capabilities and methods has inhibited international discussion on the subject and greatly increased the amount of guesswork required by national security planners.

The grace period for uncertainty may be running out. Modern militaries, like the governments and economies they protect, are increasingly reliant on IT infrastructure. In 2010, the United States Air Force procured more unmanned than manned aircraft for the first time.[330] IT investment on this scale necessarily means an increased mission dependence on IT. As adversaries look for their opponent's Achilles heel, IT systems will be attractive targets. It is likely that the ground fighting of future wars will be accompanied by a parallel, mostly invisible battle of wits between state-sponsored hackers over the IT infrastructure that is required to wage war at all.

Celebrated Red Team exercises, such as the U.S. Department of Defense's Eligible Receiver in 1997, suggest that cyber attacks are potentially powerful weapons. Dur-

327 All Sun Tzu quotes are from Sun Tzu, *Art of War* (Project Gutenberg eBook, 1994, translated by Lionel Giles, 1910).

328 Sawyer, 1994.

329 *Ibid.*

330 Orton, 2009.

ing the exercise, simulated North Korean hackers, using a variety of hacker and information warfare tactics including the transmission of fabricated military orders and news reports, "managed to infect the human command-and-control system with a paralyzing level of mistrust .... As a result, nobody in the chain of command, from the president on down, could believe anything."[331]

Because cyber warfare is unconventional and asymmetric warfare, nations weak in conventional military power are likely to invest in it as a way to offset conventional disadvantages. Good hacker software is easier to obtain than a tank or a rifle. Intelligence officials such as former CIA Director James Woolsey warn that even terrorist groups will possess cyber weapons of strategic significance in the next few years.[332]

Some analysts argue persuasively that the threat from cyber warfare is overstated.[333] However, national security planners cannot afford to underestimate its potential. A general rule could be that, as dependence on IT and the Internet grows, governments should make proportional investments in network security, incident response, technical training, and international collaboration.

In the near term, international security dialogue must update familiar vocabulary, such as attack, defense, deterrence and escalation, to encompass post-IT Revolution realities. The process that began nearly thirty years ago with MTR and RMA continues with the NATO Network Enabled Capability (NNEC), China's *Unrestricted Warfare*, and the creation of U.S. Cyber Command. However, the word cyber still does not appear in NATO's current Strategic Concept (1999), so there remains much work to be done. A major challenge with IT technology is that it changes so quickly it is difficult to follow – let alone master – all of the latest developments.

From a historical perspective, it is tempting to think cyber warfare could have a positive impact on human conflict. For example, Sun Tzu advised military commanders to avoid unnecessary destruction of adversary infrastructure.

> In the practical *Art of War*, the best thing of all is to take the enemy's country whole and intact; to shatter and destroy it is not so good. So, too, it is better to recapture an army entire than to destroy it, to capture a regiment, a detachment or a company entire than to destroy them. *AoW: III. Attack by Stratagem*

If cyber attacks play a lead role in future wars, and the nature of the fight is largely over IT infrastructure, it is conceivable that international conflicts will be shorter

331 Adams, 2001.

332 Aitoro, 2009.

333 Two are Cambridge University Professor Ross Anderson and *Wired* Threat Level Editor Kevin Poulsen.

and cost fewer lives. A cyber-only victory could facilitate economic recovery and post-war diplomacy. Such an achievement would please Sun Tzu, who argued that the best leaders can attain victory before combat is even necessary.[334]

> Hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting. *AoW: III. Attack by Stratagem*

But there is no guarantee that the increased use of cyber warfare will lead to less human suffering during international conflicts. If national critical infrastructures, such as water or electricity, are damaged for any period of time, what caused the outage will make little difference to those affected. Military leaders are specifically worried that cyber attacks could have unforeseen "cascading" effects that would inadvertently lead to civilian casualties, violate the Geneva Convention and bring war crimes charges.[335] The anonymous nature of cyber attacks also leads to the disturbing possibility of unknown and therefore undeterred hackers targeting critical infrastructures during a time of peace for purely terrorist purposes.

Cultivating Success

Due to the remarkable achievements of cyber crime and cyber espionage,[336] as well as plenty of media hype, cyber warfare will be viewed by military commanders as both a threat and an opportunity. But the most eloquent passages from *Art of War* relate to building a solid defense, and this is where a cyber commander must begin.

> The *Art of War* teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable. *AoW: VIII. Variation in Tactics*

Sun Tzu advises commanders not to rely on the good intentions of others or to count on best-case scenarios.[337] In cyberspace, this is sound advice; computers are attacked from the moment they connect to the Internet.[338] Cyber attackers currently have numerous advantages over defenders, including worldwide connectivity, vul-

334 Sawyer, 1994.
335 Graham, 1999.
336 "Espionage Report..." 2007; Cody, 2007.
337 Sawyer, 1994.
338 Skoudis, 2006.

nerable network infrastructure, poor attacker attribution, and the ability to choose their time and place of attack.

Defenders are not without resources. They own what should be the most powerful asset in the battle – home-field advantage, and they must begin to use it more wisely. Defenders have indigenous "super-user" rights throughout the network, and they can change hardware and software configurations at will. They can build redundancy into their operations and implement out-of-band cross-checking of important information. Such tactics are essential because cyber attack methods evolve so quickly that static, predictable defenses are doomed to fail. A primary goal should be to create a unique environment that an attacker has never seen before. This will require imagination, creativity, and the use of deception.

> Hence that general is skillful in attack whose opponent does not know what to defend; and he is skillful in defense whose opponent does not know what to attack. *AoW: VI. Weak Points and Strong*

Adversary cyber reconnaissance should be made as difficult as possible. Adversaries must have to work hard for their intelligence, and they should doubt that the information they were able to steal is accurate. Attackers should be forced to lose time, wander into digital traps, and betray information regarding their identity and intentions.

> Thus one who is skillful at keeping the enemy on the move maintains deceitful appearances, according to which the enemy will act. He sacrifices something that the enemy may snatch at it. By holding out baits, he keeps him on the march; then with a body of picked men he lies in wait for him. *AoW: V. Energy*

As in athletics, cyber warfare tactics are often related to leverage. In an effort to gain the upper hand, both attackers and defenders attempt to dive deeper than their opponent into files, applications, operating systems, compilers, and hardware. Strategic attacks even target future technologies at their source – the research and development networks of software companies or personnel working in the defense industry.

> The general who is skilled in defense hides in the most secret recesses of the earth... *AoW: IV. Tactical Dispositions*

In fact, professional hacker tools and tactics are stealthy enough that a wise system administrator should presume some level of system breach at all times. Defenses should be designed on the assumption that there is always a digital spy somewhere in the camp.

One of the first challenges in cyber warfare is simply to know if you are under attack. Therefore, a good short-term cyber defense goal is to improve an organization's ability to collect, evaluate, and transmit digital evidence.

> If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle. *AoW: III. Attack by Stratagem*

In the late 1990s, Moonlight Maze, the "largest cyber-intelligence investigation ever," uncovered wide-ranging attacks targeting U.S. technical research, government contracts, encryption techniques, and war-planning data. Despite years of effort, law enforcement was able to find "disturbingly few clues" to help determine attribution.[339] And because cyber warfare is a new phenomenon that changes so quickly, it is difficult even for law enforcement officers to be sure they are operating within the constraints of the law.

A long-term national objective should be the creation of a Distant Early Warning Line for cyber war. National security threats, such as propaganda, espionage, and attacks on critical infrastructure, have not changed, but they are now Internet-enabled. Adversaries have a new delivery mechanism that can increase the speed, diffusion, and even the power of an attack.

> Thus, what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge. *AoW: XIII. The Use of Spies*

Because IT security is a highly technical discipline, a broader organizational support structure must be built around it. To understand the capabilities and intentions of potential adversaries, such an effort must incorporate the analysis of both cyber and non-cyber data points. Geopolitical knowledge is critical. Whenever international tension is high, cyber defenders must now take their posts. In today's Middle East, it is safe to assume that cyber attacks will always accompany the conflict on the ground. For example, in 2006 as fighting broke out between Israel and Gaza, pro-Palestinian hackers denied service to around 700 Israeli Internet domains.[340]

Information collection and evaluation were so important to Sun Tzu that the entire final chapter of *Art of War* is devoted to espionage. Spies are called the "sovereign's

339 Adams, 2001: Russian telephone numbers were eventually associated with the hacks, but the U.S. was unable to gain further attribution.

340 Stoil & Goldstein, 2006.

most precious faculty" and espionage a "divine manipulation of the threads." The cost of spying, when compared to combat operations, is said to be so low that it is the "height of inhumanity" to ignore it. Such a commander is "no leader of men, no present help to his sovereign, no master of victory."[341]

In the wars of the future, brains will beat brawn with increasing frequency. Following the IT Revolution, the need for investment in human capital has risen dramatically. However, cyber defense is still an immature discipline, and it is difficult to retain personnel with highly marketable training. To gain a long-term competitive advantage, a nation must invest in science and technology as a national priority.[342]

Objective Calculations

Sun Tzu warns that a commander must exhaustively and dispassionately analyze all available information. Offensive operations in particular should wait until a decisive victory is expected. If objective calculations yield an unfavorable result, the inferior party must assume a defensive posture until circumstances have changed in its favor.[343]

> Now the general who wins a battle makes many calculations in his temple ere the battle is fought. The general who loses a battle makes but few calculations beforehand. Thus do many calculations lead to victory, and few calculations to defeat: how much more no calculation at all! It is by attention to this point that I can foresee who is likely to win or lose. *AoW: I. Laying Plans*

In any conflict, there are prevailing environmental and situational factors over which the combatants have little control. *Art of War* lists over three dozen such factors to evaluate, including offense/defense, orthodox/unorthodox, rested/exhausted, dry/wet, and confident/afraid.[344] Most of these will have direct or indirect parallels in cyberspace.

In cyberspace, reliable calculations are extremely difficult to perform. First and foremost, cyber attackers possess enough advantages over defenders that there is an enormous gap in Return-on-Investment (RoI) between them. The cost of conducting a cyber attack is cheap, and there is little penalty for failure. Network reconnaissance can be conducted, without fear of retaliation, until a suitable vulnerability is found. Once an adversary system is compromised and exploited, there are often im-

341 Sun Tzu, *Art of War*. "XIII. The Use of Spies."

342 Rarick, 1996.

343 Sawyer, 1994.

344 *Ibid.*

mediate rewards. By comparison, cyber defense is expensive and challenging, and there is no tangible RoI.

Another aspect of cyberspace that makes calculation difficult is its constantly changing nature. The Internet is a purely artificial construct that is modified continually from across the globe. Cyber reconnaissance and intelligence collection are of reliable valuable to a military commander only for a short period of time. The geography of cyberspace changes without warning, and software updates and network reconfiguration create an environment where insurmountable obstacles and golden opportunities can appear and disappear as if by magic. The terrestrial equivalent could only be a catastrophic event such as an earthquake or an unexpected snowstorm.

Art of War describes six types of battlefield terrain, ranging from "accessible," which can be freely traversed by both sides, to "narrow passes," which must either be strongly garrisoned or avoided altogether (unless the adversary has failed to fortify them).[345] Although they will change over time, cyber equivalents for each *Art of War* terrain type are easily found in Internet, intranet, firewall, etc.

> The natural formation of the country is the soldier's best ally; but a power of estimating the adversary, of controlling the forces of victory, and of shrewdly calculating difficulties, dangers and distances, constitutes the test of a great general. *AoW: X. Terrain*

Cyberspace possesses characteristics that the *Art of War* framework does not encompass. For example, in cyberspace the terrestrial distance between adversaries can be completely irrelevant. If "connectivity" exists between two computers, attacks can be launched at any time from anywhere in the world, and they can strike their targets instantly. There is no easily defined "front line;" civilian and military zones on the Internet often share the same space, and military networks typically rely on civilian infrastructure to operate. With such amazing access to an adversary, never before in history has superior logic – not physical size or strength – more often determined the victor in conflict.

Similar to cyber geography, cyber weapons also have unreliable characteristics. Some attacks that hackers expect to succeed fail, and vice versa. Exploits may work on one, but not another, apparently similar target. Exploits that work in one instance may never work again. Thus, it can be impossible to know if a planned cyber attack will succeed until the moment it is launched. Cyber weapons should be considered single-use weapons because defenders can reverse-engineer them to defend their

345 Sun Tzu, *Art of War*: "X. Terrain."

networks or try to use them for their own offensive purposes. These limitations make meticulous pre-operational cyber attack planning and timing critical.[346][347]

Last but not least, one of the major challenges confronting any military commander is to keep track of the location and constitution of adversary forces. However, cyber defenses such as passive network monitoring devices can be nearly impossible to find.

> If in the neighborhood of your camp there should be any hilly country, ponds surrounded by aquatic grass, hollow basins filled with reeds, or woods with thick undergrowth, they must be carefully routed out and searched; for these are places where men in ambush or insidious spies are likely to be lurking. *AoW: IX. The Army on the March*

Cyber commanders are wise to assume, especially if they are conducting an offensive operation on adversary terrain, that the defenses and traps they can see are more powerful than they appear, and that there are some defenses in place that they will never find. Adversary sensors could even lie on the open Internet, such as on a commercial Internet Service Provider (ISP), outside of the cyber terrain that the adversary immediately controls.

Time to Fight

Once the decision to go to war has been made (or forced), Sun Tzu offers plenty of battlefield advice to a military commander. *Art of War* operations emphasize speed, surprise, economy of force, and asymmetry. These characteristics happen to be synonymous with cyber warfare.

> Rapidity is the essence of war: take advantage of the enemy's unreadiness, make your way by unexpected routes, and attack unguarded spots. *AoW: XI. The Nine Situations*

> If you set a fully equipped army in march in order to snatch an advantage, the chances are that you will be too late. On the other hand, to detach a flying column for the purpose involves the sacrifice of its baggage and stores. *AoW: VII. Maneuvering*

The potential role of computer network operations in military conflict has been compared to strategic bombing, submarine warfare, special operations forces, and

346 Parks & Duggan, 2001.

347 Lewis, 2002.

assassins.[348] The goal of such unorthodox, asymmetric attacks is to inflict painful damage on an adversary from a safe distance or from close quarters with the element of surprise.

> By discovering the enemy's dispositions and remaining invisible ourselves, we can keep our forces concentrated, while the enemy's must be divided.... Hence there will be a whole pitted against separate parts of a whole, which means that we shall be many to the enemy's few. *AoW: VI. Weak Points and Strong*

In theory, a cyber attack can accomplish the same objectives as a special forces raid, with the added benefit of no human casualties on either side. If cyber attacks were to achieve that level of success, they could come to redefine elegance in warfare.

A cyber attack is best understood not as an end in itself, but as an extraordinary means to accomplish almost any objective. Cyber propaganda can reach the entire world in seconds via online news media. Cyber espionage can be used to steal even nuclear weapons technology.[349] Moreover, a successful cyber attack on an electrical grid could bring down myriad other infrastructures that have no other source of power.[350] In fact, in 2008 and 2009, hackers were able to force entire nation-states offline.[351]

Attacking a nation's critical infrastructure is an old idea. Militaries seek to win not just individual battles, but wars. Toward that end, they must reduce an adversary's long-term ability to fight. And the employment of a universal tool to attack an adversary in creative ways is not new. Witness Sun Tzu's advice from *Art of War* on the use of fire:

> There are five ways of attacking with fire. The first is to burn soldiers in their camp; the second is to burn stores; the third is to burn baggage trains; the fourth is to burn arsenals and magazines; the fifth is to hurl dropping fire amongst the enemy. *AoW: XII. The Attack by Fire*

Sun Tzu did not know that baggage trains would one day need functioning computers and uncompromised computer code to deliver their supplies on time.

Specific tactical advice from *Art of War* provides a clear example. As in the Syrian air defense attack cited above, Sun Tzu instructs military commanders to accomplish

348 Parks & Duggan, 2001.
349 Gerth & Risen, 1999.
350 Divis, 2005.
351 Keizer, 2008; Keizer, 2009.

something for which digital denial-of-service (DoS) appears ideal – to sever communications between adversary military forces.

> Those who were called skillful leaders of old knew how to drive a wedge between the enemy's front and rear; to prevent co-operation between his large and small divisions; to hinder the good troops from rescuing the bad, the officers from rallying their men. *AoW: XI. The Nine Situations*

If modern military forces use the Internet as their primary means of communication, what happens when the Internet is down? Thus it is likely that cyber attacks will play their most critical role when launched in concert with a conventional military (or terrorist) attack.

Sun Tzu warns that surprise attacks may come when a defender's level of alert is lowest:

> Now a soldier's spirit is keenest in the morning; by noonday it has begun to flag; and in the evening, his mind is bent only on returning to camp. A clever general, therefore, avoids an army when its spirit is keen, but attacks it when it is sluggish and inclined to return. This is the art of studying moods. *AoW: VII. Maneuvering*

Cyber criminals already operate according to this rule. They know the work schedules of network security personnel and often launch attacks in the evening, on weekends, or on holidays when cyber defenders are at home. Unfortunately, given the current challenges facing cyber defense, it may be possible simply to tie up computer security specialists with diversionary attacks while the critical maneuvers take place elsewhere.

If an invasion is successful, Sun Tzu advises military commanders to survive as much as possible on the adversary's own resources.

> Hence a wise general makes a point of foraging on the enemy. One cartload of the enemy's provisions is equivalent to twenty of one's own, and likewise a single picul of his provender is equivalent to twenty from one's own store. *AoW: II. Waging War*

In this sense, *Art of War* and cyber warfare correspond perfectly. In computer hacking, attackers typically steal the credentials and privileges of an authorized user, after which they effectively become an insider in the adversary's (virtual) uniform. At that point, inflicting further damage on the network – and thus on the people using that network and their mission – through DoS or espionage is far easier. Such attacks could include poisoned pen correspondence and/or critical data modification. Even

if the compromise is discovered and contained, adversary leadership may lose its trust in the computer network and cease to use it voluntarily.

Finally, cyber warfare is no different from other military disciplines in that the success of an attack will depend on keeping its mission details a secret.

> Divine art of subtlety and secrecy! Through you we learn to be invisible, through you inaudible; and hence we can hold the enemy's fate in our hands. *AoW: VI. Weak Points and Strong*

In military jargon, this is called operational security (OPSEC). However, the characteristics that make cyber warfare possible – the ubiquity and interconnected nature of the Internet – ironically make good OPSEC more difficult than ever to achieve. Open source intelligence (OSINT) and computer hacking can benefit cyber defense as much as cyber offense.

The Ideal Commander

Decision-making in a national security context carries significant responsibilities because lives are often at stake. Thus, on a personal level, *Art of War* leadership requirements are high.

> The Commander stands for the virtues of wisdom, sincerity, benevolence, courage and strictness. *AoW: I. Laying Plans*

Good leaders not only exploit flawed plans, but flawed adversaries.[352] Discipline and self-control are encouraged; emotion and personal desire are discouraged.[353] Sun Tzu states that to avoid a superior adversary is not cowardice, but wisdom.[354] Moreover, due to the painstaking nature of objective calculations, patience is a virtue.

> Thus it is that in war the victorious strategist only seeks battle after the victory has been won, whereas he who is destined to defeat first fights and afterwards looks for victory. *AoW: IV. Tactical Dispositions*

Commanding a cyber corps will require a healthy mix of these admirable qualities. As a battleground, cyberspace offers political and military leaders almost limitless possibilities for success – and failure. Behind its façade of global connectivity and influence, the Internet has a complicated and vulnerable architecture that is an ideal

352 Parks & Duggan, 2001.

353 Sun Tzu, *Art of War*. "VIII. Variation in Tactics."

354 Sawyer, 1994.

environment in which to conduct asymmetric and often anonymous military operations. Imagination and creativity are required skill sets. Cyber warfare also involves an enormous amount of uncertainty; even knowing *whether* one is under attack can be an immense challenge. And the high tempo of Internet operations may lead to a high burn-out rate throughout the ranks.

A cyber commander must have a minimum level of subject matter expertise in IT. The core concepts of computing, networking, and data security should be thoroughly understood before employing them in support of a national security agenda. Any leader must be able to articulate the mission so that everyone in the organization understands and believes in it;[355] a further challenge in cyber warfare will be communicating with highly technical personalities, who have vastly different personal needs than the soldiers of a traditional military element.

In all future wars, military leadership will have the challenge of coordinating and deconflicting the cyber and non-cyber elements of a battle plan. Sun Tzu gives high praise for a great tactician:

> Having collected an army and concentrated his forces, he must blend and harmonize the different elements thereof before pitching his camp. After that, comes tactical maneuvering, than which there is nothing more difficult. The difficulty of tactical maneuvering consists in turning the devious into the direct, and misfortune into gain. *AoW: VII. Maneuvering*

As circumstances change throughout the course of a conflict, both tactics and strategy must be reevaluated and modified to fit the new environment.[356]

> He who can modify his tactics in relation to his opponent and thereby succeed in winning, may be called a heaven-born captain. *AoW: VI. Weak Points and Strong*

The dynamic nature of the Internet and the speed of computer network operations guarantee that traditional military challenges such as seizing the initiative and maintaining momentum will require faster decision cycles than a traditional chain-of-command can manage. A cyber commander must have the ability and the trust of his or her superiors to act quickly, creatively, and decisively.

355 Rarick, 1996.

356 *Ibid.*

Art of Cyber War: Elements of a New Framework

Art of War is the most influential military treatise in human history. The book has survived over 2,500 years in part because its guidance is highly flexible. Strategists and tacticians have adapted *Art of War* to new circumstances across many scientific revolutions, and Sun Tzu's insight has never lost much of its resonance.

This chapter argues that in the future cyber warfare practitioners should also use *Art of War* as an essential guide to military strategy. However, cyberspace possesses many characteristics that are unlike anything Sun Tzu could have imagined in ancient China. There are at least ten distinctive aspects of the cyber battlefield.

1. The Internet is an artificial environment that can be shaped in part according to national security requirements.
2. The rapid proliferation of Internet technologies, including hacker tools and tactics, makes it impossible for any organization to be familiar with all of them.
3. The physical proximity of adversaries loses much of its relevance as cyber attacks are launched without regard to terrestrial geography.
4. Frequent software updates and network reconfiguration change Internet geography unpredictably and without warning.
5. In a reversal of our historical understanding of warfare, the asymmetric nature of cyber attacks strongly favors the attacker.
6. Cyber attacks are more flexible than any weapon the world has seen. They can be used for propaganda, espionage, and the destruction of critical infrastructure.
7. Cyber attacks can be conducted with such a high degree of anonymity that defense strategies such as deterrence and retaliation are not credible.
8. It is possible that a lengthy and costly cyber war could take place without anyone but the direct participants knowing about it.[357]
9. The intangible nature of cyberspace can make the calculation of victory, defeat, and battle damage a highly subjective undertaking.
10. There are few moral inhibitions to cyber warfare because it relates primarily to the use and exploitation of information in the form of computer code and data packets; so far, there is little perceived human suffering.

357 Libicki, 2009.

None of these characteristics of cyberspace or cyber conflict fits easily into Sun Tzu's paradigm. As national security thinkers and military strategists begin to write concepts, strategies, and doctrine for cyber warfare with the *Art of War* model in mind, they should be aware of these differences.

7. DETERRENCE: CAN WE PREVENT CYBER ATTACKS?

National security planners have begun to look beyond reactive, tactical cyber defense to proactive, strategic cyber defense, which may include international military deterrence. The incredible power of nuclear weapons gave birth to deterrence, a military strategy in which the purpose of armies shifted from winning wars to preventing them. Although cyber attacks per se do not compare to a nuclear explosion, they do pose a serious and increasing threat to international security. Real-world examples suggest that cyber warfare will play a lead role in future international conflicts. This chapter examines the two deterrence strategies available to nation-states (denial and punishment) and their three basic requirements (capability, communication, and credibility) in light of cyber warfare. It also explores whether the two most challenging aspects of cyber attacks – attribution and asymmetry – will make cyber attack deterrence an impossible task.

Cyber Attacks and Deterrence Theory

The advent of nuclear weapons disrupted the historical logic of war completely. Deterrence theory emerged after the United States and the Soviet Union created enough military firepower to destroy human civilization on our planet. From that point forward, according to the American military strategist Bernard Brodie,[358] the purpose of armies shifted from winning wars to preventing them.

Nothing compares to the destructive power of a nuclear blast. But cyber attacks loom on the horizon as a threat that is best understood as an extraordinary means to a wide variety of political and military ends, many of which can have serious national security ramifications. For example, computer hacking can be used to steal offensive weapons technology (including technology for weapons of mass destruction) or to render an adversary's defenses inoperable during a conventional military attack.[359] In that light, attempting proactively to deter cyber attacks may become an essential part of national military strategies. This chapter examines whether it is possible to apply deterrence theory to cyber attacks.

What military officers call the "battlespace" grows more difficult to define – and to defend – over time. In 1965, Gordon Moore correctly predicted that the number of transistors on a computer chip would double every two years. There has been similar growth in almost all aspects of information technology (IT), including practical

358 Brodie, 1946.

359 Fulghum et al., 2007.

encryption, user-friendly hacker tools, and Web-enabled open source intelligence (OSINT). Even the basic services of a modern society, such as water, electricity and telecommunications, are now computerized and often connected to the Internet.[360]

Advances in technology are normally evolutionary, but they can be revolutionary – artillery reached over the front lines of battle, and rockets and airplanes crossed national boundaries. Today, cyber attacks can target political leadership, military systems, and average citizens anywhere in the world, during peacetime or war, with the added benefit of attacker anonymity. Political and military strategists now use and abuse computers, databases, and the networks that connect them to achieve their objectives. In the early 1980s, this concept was already known in the Soviet Union as the Military Technological Revolution (MTR); after the 1991 Gulf War, the Pentagon's Revolution in Military Affairs was almost a household term.[361]

However, the real-world impact of cyber conflict is still difficult to appreciate, in part because there have been no wars between modern cyber-capable militaries. But an examination of international affairs over the past two decades suggests that cyber battles of increasing consequence are easy to find. Since the earliest days of the World Wide Web, Chechen guerilla fighters, armed not only with rifles but with digital cameras and HTML, have demonstrated the power of Internet-enabled propaganda.[362] In 2001, tensions between the United States and China spilled over into a non-state, "patriotic" hacker war, with uncertain consequences for national security leadership.[363] In 2007, Syrian air defense was reportedly disabled by a cyber attack moments before the Israeli air force demolished an alleged Syrian nuclear reactor.[364] In 2009, the entire nation-state of Kyrgyzstan was knocked offline during a time of domestic political crisis,[365] and Iranian voters, in "open war" with state security forces, used peer-to-peer social networking websites to avoid government restrictions on dialogue with the outside world.[366] Such a rapid development in the use of cyber tools and tactics suggests that they will play a lead role in future international conflicts.

While the Internet has on balance been hugely beneficial to society, law enforcement, and counterintelligence, personnel struggle to keep pace with its security

360 Geers, 2009.

361 Mishra, 2003.

362 Goble, 1999.

363 On April 26, 2001, the Federal Bureau of Investigation (FBI) National Infrastructure Protection Center (NIPC) released Advisory 01-009, "Increased Internet Attacks against U.S. Web Sites and Mail Servers Possible in Early May."

364 Fulghum et al, 2007.

365 Keizer, 2009.

366 Stöcker et al., 2009.

implications. The ubiquity of the Internet makes cyber warfare a strategic weapon since adversaries can exchange blows at will, regardless of the physical distance between them. By contrast, cyber defense is a tedious process, and cyber attack investigations are typically inconclusive. The astonishing achievements of cyber crime and cyber espionage should hint at the potential damage of a true nation-state-sponsored cyber attack. Intelligence officials such as former CIA director James Woolsey fear that even terrorist groups will possess cyber weapons of strategic significance in the next few years.

Military leaders have begun to look beyond reactive, tactical cyber defense[367] to the formulation of a proactive, strategic cyber defense policy, which may include international military deterrence.[368] However, two challenging aspects of cyber attacks – attribution and asymmetry – will be difficult to overcome.

In theory, nation-states have two primary deterrence strategies – denial and punishment. Both strategies have three basic requirements – capability, communication, and credibility.[369]

This chapter will examine each concept in turn and explore whether it is possible to deter cyber attacks at the nation-state level.

Cyber Attack Deterrence by Denial

Deterrence by denial is a strategy in which an adversary is physically prevented from acquiring a threatening technology. This is the preferred option in the nuclear sphere because there is no practical defense against a nuclear explosion. Its heat alone is comparable to the interior of the sun, and its blast can demolish reinforced concrete buildings three kilometers away.[370] The abhorrent nature of nuclear warfare makes even a theoretical victory difficult to imagine. Deterrence by denial is a philosophy embodied in the Non-Proliferation Treaty (NPT) and one reason behind current international tension with North Korea and Iran.[371]

367 E.g., how to configure a network or an intrusion detection system.

368 In May, 2009, the head of the U.S. Strategic Command, Air Force Gen. Kevin Chilton, stated that retaliation for a cyber attack would not necessarily be limited to cyberspace.

369 These deterrence strategies and requirements I took from a personal interview with Prof. Peter D. Feaver, Alexander F. Hehmeyer Professor of Political Science and Public Policy at Duke University and Director of the Triangle Institute for Security Studies (TISS).

370 Sartori, 1983.

371 Shultz et al., 2007.

Denial: Capability

Despite the diplomatic efforts of NPT, the well-funded inspection regime of the International Atomic Energy Agency (IAEA)[372] and unilateral military operations such as Israel's destruction of nuclear facilities in Iraq in 1981 and in Syria in 2007, the size of the world's nuclear club is growing. In addition to the five permanent members of the United Nations Security Council,[373] de facto members now include India, Israel, Pakistan, and North Korea.[374]

Cyber attack tools and techniques are not nearly as dangerous as their nuclear counterparts, but they are by comparison simple to acquire, deploy, and hide. Hacker training and conferences are abundant; over the past 17 years, almost 1,000 how-to presentations have been given at DEF CON. More sensitive hacker information can be kept secret, physically transported on a miniscule hard drive, or sent encrypted across the Internet. A nuclear weapons program is difficult to hide;[375] a cyber weapons program is not. Cyber attacks can be tested discretely in a laboratory environment[376] or live on the Internet, anonymously. Further, it appears increasingly common to outsource the illegal business of hacking to a commercial or criminal third party.[377]

A major challenge to cyber attack tool anti-proliferation is how to define malicious code. A legitimate path for remote system administration can also be used by a masquerading hacker to steal national secrets. Even published operating system and application code is difficult for experts to understand thoroughly, as there are simply too many lines of code to analyze.[378] The dynamic and fast-evolving nature of cyber attack technology contrasts sharply with the fundamental design of nuclear warheads, which, with the exception of the neutron bomb, has not changed much since the late 1950s.[379] In the single month of May 2009, Kaspersky Anti-Virus Lab

372 The IAEA is the world's nuclear inspectorate, with more than four decades of verification experience. Inspectors work to verify that safeguarded nuclear material and activities are not used for military purposes. The annual budget of IAEA is almost $500 million USD.

373 China, France, Russia, United Kingdom and United States.

374 Huntley, 2009.

375 Milhollin & Lincy, 2009.

376 With nuclear weapons, a hard-to-conceal test is required to prove that a capability exists. If the goal were cyber attack tool anti-proliferation, it would seem difficult to know if or when success had been achieved.

377 Jolly, 2009: In 2009, the French Interior Ministry investigated the collection of "strategic intelligence" by a former intelligence agent and a for-hire computer hacker on behalf of some of France's biggest companies.

378 Cole, 2002.

379 There have, however, been many design modifications relating to safety, security, and reliability.

reported that it had found 42,520 unique, suspicious programs on its clients' computers.

Finally, in nuclear warfare one of the most important considerations is the retention of a second-strike capability. Following a surprise attack, is it still possible for the victim to fight back? In nuclear and conventional warfare, this is a constant worry among strategic planners. In contrast, a unique characteristic of cyber attacks is their ability to be launched from anywhere in the world, at any time. During the cyber attacks on Estonia in 2007, most of the compromised and attacking computers were located in the United States.[380] Cyber attacks can be set to launch under predetermined conditions or on a certain date in the future. Discovered attack tools can also be difficult to remove from a computer network completely, even by forensic experts. With cyber attack technology, it seems impossible to know for sure that all adversary attack options have been eliminated.

Denial: Communication

Cyber attacks now have the attention of the world's national security planners. In the U.S., enhancing cyber security was one of the six "mission objectives" of the 2009 Director of National Intelligence (ODNI) National Intelligence Strategy,[381] and counteracting the cyber threat is currently the third-highest priority of the Federal Bureau of Investigation (FBI), after preventing terrorist attacks and thwarting foreign intelligence operations.

However, cyber warfare is a new phenomenon; national and international norms have yet to be established. Different approaches are under consideration. One is to broaden international law enforcement coordination, specifically via the Council of Europe Convention on Cybercrime. Objections to this strategy include the possible infringement of national sovereignty by foreign law enforcement agencies. Another approach is to prohibit the development of cyber weapons via international treaty, such as that negotiated for chemical weapons. Articles to such a treaty might ban supply chain attacks and the disruption of non-combatant networks, as well as increase international management of the Internet. One objection to the second approach is that it does little to improve cyber attack attribution.[382]

380 As computer incident response teams began to block hostile network packets, the source of the attack moved to countries with less mature and/or helpful network management practices.

381 The other five objectives were Combat Violent Extremism, Counter WMD Proliferation, Provide Strategic Intelligence and Warning, Integrate Counterintelligence Capabilities, and Support Current Operations.

382 Markoff & Kramer, 2009b.

The Convention on Cybercrime is the first such international treaty. It describes law enforcement powers and procedures related to data interception and the search of computer networks. In 2009, forty-six nations were signatories, and twenty-six had ratified the treaty.[383] Its main objective, set out in the Preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially via national legislation and international cooperation. Deterrence is specifically mentioned as a goal: "the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems."

The continued success of the Convention on Cybercrime requires addressing myriad national and international data security and privacy concerns, including the respect for national sovereignty. A non-governmental organization in Thailand, for example, has claimed that similar legislation there has been used by the government more to threaten Thai citizens than to protect them.[384] A proposed international treaty banning the development and use of hacker tools would be no less challenging to sign and enforce, because many hacker tools can properly be called dual-use technology.[385]

The Council of Europe's protocol on criminalizing racist and xenophobic statements on the Web may offer a partial solution. Because countries have wildly varying laws regarding what constitutes free speech, universally-accessible websites can create international legal headaches.[386] This protocol recommends a nationally-tailored approach to regulation that allows for implementation at the local ISP and end-user levels. In this way, signatories are able to project their norms of free speech onto the Internet, without extending liability beyond national borders.[387][388]

Denial: Credibility

Deterrence theory states that capability and communication alone are insufficient. The threatened party must believe that the threat of retaliation – or of a preemptive strike – is real. This third requirement of deterrence is the most difficult for national

383 The U.S. acceded to the Council of Europe Convention on Cybercrime on January 1, 2007.

384 Anonymous, 2009.

385 System administrators often use hacker tools such as a password cracker to audit their own networks. Cyber defense studies in academia require hacker tools for laboratory purposes.

386 For example, a French judge found a U.S. ISP criminally liable for hosting an auction of Nazi paraphernalia, the sale of which is illegal in France.

387 Oberdorfer Nyberg, 2004.

388 The named methods of implementing the protocol are self-regulation of content by ISPs, government regulation of specific content, government regulation of end-users, and government regulation of local ISPs.

security leadership to assess because it involves evaluating human psychology, rationality, the odds of miscalculation, and foreign political-military affairs.

At the beginning of the year 2011, it was still not likely that nation-states would sacrifice much to prevent the proliferation of cyber attack tools and techniques. Although it is indisputable that cyber attacks cause enormous financial damage, that world leaders increasingly complain of cyber espionage, and that Internet-connected critical infrastructures are now at risk, deterrence theory was created for nuclear weapons. In terms of their destructive power, nukes are in a class by themselves. Cyber attacks per se do not cause explosions, deadly heat, radiation, an electromagnetic pulse (EMP), or human casualties.[389]

However, a future cyber attack, if it caused any of the above effects, could change this perception. Worldwide technological convergence, as described by Dawson,[390] is constantly expanding what hackers call the "attack surface." In theory, the successful conquest of an adversary's Internet space could equate to assuming command and control of the adversary's military forces, and firing their own weapons against their own cities. But for now, this scenario still lies in the realm of science fiction.

Cyber Attack Deterrence by Punishment

Deterrence by punishment is a strategy of last resort. It signifies that deterrence by denial was not possible or has failed, and that Country X possesses the technology it needs to threaten Country Y or its government. The goal of deterrence by punishment is to prevent aggression by threatening greater aggression in the form of painful and perhaps fatal retaliation. For the strategy to work, Country X must be convinced that victory is not possible, even given the option of using its new technology.

Two key aspects of cyber attacks present challenges to national security planners who would seek to deter them by punishment: attribution and asymmetry. The first challenge undermines a state's capability to respond to a cyber attack, and the second undermines its credibility.

Punishment: Capability

All nations with robust military, law enforcement, and/or diplomatic might theoretically have the power to punish a cyber attacker in some way, either in cyberspace

389 Persuasive cyber war skeptics include Cambridge University Professor Ross Anderson and *Wired* "Threat Level" Editor Kevin Poulsen.

390 Dawson, 2003.

or in the real world. And if a known attacker is beyond the reach of physical pursuit, the victim could at least present incriminating evidence in an international forum. But in practice, for punishment to be a viable option, the victim must know for sure who the attacker is and be able to prove it.

In cyber warfare, the attacker enjoys a formidable advantage: anonymity. Proof in cyberspace is hard to come by. Smart hackers hide within the maze-like architecture of the Internet. They route attacks through countries with which the target's government has poor diplomatic relations or no law enforcement cooperation, and exploit unwitting third-party networks. Cyber investigations typically end at a hacked, abandoned computer, where the trail goes cold. Plausible deniability is also a concern. Because hackers obscure the true origin of an attack by hopping through a series of compromised computers to reach their target, the real attacker could always claim that her computer had merely been hacked and used in someone else's operation. This aspect of cyber attacks also makes "false flagging," or intentionally trying to pin the blame on a third party, an attractive option.

Even in the event that cyber attack attribution is positively determined, deterrence by punishment is still inherently less credible than deterrence by denial. It requires decision-makers to make more difficult choices. A proactive law enforcement strategy is easier to justify than the use of military force, which can cause physical destruction, human casualties, or other collateral damage. At the very least, there will be serious diplomatic consequences.

One important decision facing decision-makers in the aftermath of a cyber attack would be whether to retaliate in kind or to employ more conventional weapons. It may seem logical to keep the conflict within cyberspace, but a cyber-only response does not guarantee proportionality, and a cyber counterattack may lack the required precision. A misfire in cyberspace might adversely affect critical national infrastructure, such as a hospital, which could result in a violation of the Geneva Convention and even bring war crimes charges against national authorities.[391] The Law of Armed Conflict states that the means and methods of warfare are not unlimited:[392] commanders may use "only that degree and kind of force ... required in order to achieve the legitimate purpose of the conflict ... with the minimum expenditure of life and resources."[393]

391 Graham, 1999.

392 See "Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land." The Hague, 18 October 1907, International Committee of the Red Cross.

393 This quote is from *The Manual of the Law of Armed Conflict*, Section 2.2 (Military Necessity). United Kingdom: Ministry of Defence. Oxford: OUP. (2004).

Punishment: Communication

Whereas deterrence by denial relies on a criminal law framework for support, the foundation of deterrence by punishment lies in military doctrine. When bombs begin to fall on adversary targets, diplomatic and law enforcement options have normally run their course. Military doctrine serves at least two important purposes: to prepare a nation's military forces for conflict, and to warn potential foes of the consequences of war.

It should not be surprising that the advent of an open and ubiquitous communications medium like the Internet demands a reassessment of military strategy, tactics, and doctrine. In 2006, a secret Israeli government report argued for a "sea change" in military thinking because the national security paradigm of army versus army was under assault by suicide bombers, Katyusha rockets and computer hackers, none of whom has to have direct ties to government or even be susceptible to political pressure.[394] In China, the potential impact of computer network operations on the nature of warfare is thought to be strong enough even to have transformed 2,500 years of military wisdom; the Chinese military has almost certainly quit the defensive depth of the Chinese countryside to conquer international cyberspace.[395] In Washington, one of the first reports that incoming President Obama found on his desk was "Securing Cyberspace for the 44th Presidency," which argued that the U.S. must have a credible military presence in cyberspace to act as a deterrent against operations by its adversaries in that domain.[396]

Cyber doctrine must address how military and civilian authorities will collaborate to protect private sector critical information infrastructure. Even cyber attacks that strike purely military sites are likely to traverse civilian networks before reaching their target. In fact, the destruction of civilian infrastructure may be the cyber attacker's only goal. A further challenge is that private sector enterprises such as banks have been reluctant to disclose successful cyber attacks against them for fear of an impact on their bottom line. This dynamic could make it difficult for national security leadership even to know that an attack on its national territory – in violation of its national sovereignty – has occurred. Thus, proactive cyber attack deterrence by government to defend civilian infrastructure will be difficult to achieve, and any national response may be too little, too late.

The dynamic nature of cyber attacks could ensure that defenders never see the same attack twice. Therefore, decision makers will need a range of diplomatic and military options to consider for a punitive response. In terms of military doctrine,

394 Fulghum, 2006.

395 Rose, 1999.

396 Lewis, 2008.

one possibility might be the delineation of red lines in cyberspace. Propaganda and low-level computer network exploitation (CNE) may trigger the first line of passive cyber defense, while the manipulation of code in an operational weapons system could be grounds for real-world retaliation. Finally, to support a deterrence strategy, cyber doctrine must be clearly written. An adversary should have no doubt what the consequences will be if the red lines are crossed.

Punishment: Credibility

As we have seen, the credibility of cyber attack deterrence by denial is low. The political will and even the capability to attempt such a denial are lacking. Therefore, a strategy of cyber attack deterrence by punishment is a more likely scenario.

The trouble with a punishment strategy, however, is that governments are always reluctant to authorize the use of military force (for good reason). Deterrence by punishment is a simple strategy, but one that demands a high burden of proof: a serious crime must have been committed, and the culprit positively identified. The challenge of cyber attack attribution, as described above, means that decision-makers will likely not have enough information on an adversary's cyber capabilities, intentions, and operations to respond in a timely fashion.

However, there is another characteristic of cyber attacks that undermines the credibility of deterrence by punishment even more: asymmetry. At the nation-state level, some countries are more dependent upon the Internet than others. Some governments possess sophisticated computer network attack programs, while others have none at all. Non-state actors such as a lone hacker or a terrorist group may not possess any computer network or other identifiable infrastructure against which to retaliate.

The asymmetric nature of information technology and cyber warfare manifests itself in countless ways. From a technical perspective, the Smurf attack is a classic example. A hacker sitting at computer X pretends to be coming from computer Y, then requests data from hundreds of other computers at once. Myriad responses easily overwhelm computer Y, creating a denial-of-service condition.[397] From a human perspective, the case of Briton Gary McKinnon is illuminating. According to McKinnon, he is a "bumbling hacker" who was merely looking for UFO data on unsecured Pentagon networks. But the U.S. prosecutor seeking his extradition describes McKinnon's

397 See "Smurf IP Denial-of-Service Attacks," CERT Advisory CA-1998-01.

exploits as "the biggest military computer hack of all time."[398][399] In terms of financial damages, "MafiaBoy" – a 15 year-old kid from Montreal – in 2001 was able to deny Internet service to some of the world's biggest online companies, causing an estimated $1.7 billion in damage.[400]

Mutually Assured Disruption (MAD)

There is a growing relationship between computer security and national security. Military leaders, fearing the potential impact of cyber warfare as well as the start of a cyber arms race, are now considering whether it is possible proactively to deter cyber attacks.

At the nation-state level, there are two possible deterrence strategies: denial and punishment. In cyberspace, both suffer from a lack of credibility. Denial is unlikely due to the ease with which cyber attack technology can be acquired, the immaturity of international legal frameworks, the absence of an inspection regime, and the perception that cyber attacks are not dangerous enough to merit deterrence in the first place. Punishment is the only real option, but this deterrence strategy lacks credibility due to the daunting challenges of cyber attack attribution and asymmetry.

At a minimum, attribution must improve before a cyber attacker may feel deterred. This will take time. In the short term, organizations must improve their ability to collect and transmit digital evidence, especially to international partners. In the long term, national security planners should try to create a Distant Early Warning Line (DEWL) for cyber war and the capability to select from a range of rapid response tactics.

To pave the way forward, a legal foundation for cyber attack, defense, and deterrence strategies is needed as soon as possible. Because information technology changes so quickly – no one can predict what the next cyber attack will look like – it may be necessary to adopt an effects-based approach. If a cyber attack results in a level of human suffering or economic destruction equivalent to a conventional military attack, then it could be considered an act of war, and it should be subject to the existing laws of war. Consequently, national security planners have no time to waste in reevaluating, and updating, if necessary, the Geneva, Hague, and Human Rights conventions, as well as the Just War theory, and more.

398 Lee, 2006.

399 Glendinning, 2006: The press has speculated whether one reason for prosecuting McKinnon is for the deterrent effect it could have on other cyber attackers.

400 Verton, 2002.

Back to the Cold War. By the year 1968, Soviet mastery of nuclear technology had made one-sided nuclear deterrence meaningless.[401] The U.S. and the USSR were forced into a position of mutual deterrence or Mutually Assured Destruction (MAD). Both sides had the ultimate weapon, as well as a second-strike capability. Although cyber attacks do not possess the power of a nuclear explosion, they do pose a serious and increasing threat to international security, and anti-proliferation efforts appear futile. Welcome to the era of Mutually Assured Disruption.[402]

401 Specifically, it was the Soviet Union's ability to mass produce nuclear weapons, and to compete in the nuclear arms race, that changed the strategic equation in 1968.

402 Pendall, 2004; Derene, 2009.

8. ARMS CONTROL: CAN WE LIMIT CYBER WEAPONS?

As world leaders look beyond temporary fixes to the challenge of securing the Internet, one possible solution may be an international arms control treaty for cyberspace. The 1997 Chemical Weapons Convention (CWC) provides national security planners with a useful model. CWC has been ratified by 98% of the world's governments and encompasses 95% of the world's population. It compels signatories not to produce or to use chemical weapons (CW), and they must destroy existing CW stockpiles. As a means and method of war, CW have now almost completely lost their legitimacy. This chapter examines the aspects of CWC that could help to contain conflict in cyberspace. It also explores the characteristics of cyber warfare that seem to defy traditional threat mitigation.

Cyber Attack Mitigation by Political Means

The world has grown so dependent on the Internet that governments may seek far-reaching strategic solutions to help ensure its security. Every day, more aspects of modern society, business, government, and critical infrastructure are computerized and connected to the Internet. As a consequence and for the sake of everything from the production of electricity to the integrity of national elections, network security is no longer a luxury, but a necessity.[403]

A fundamental challenge to better network security is that computers are highly complex objects that are inherently difficult to secure. The Common Vulnerabilities and Exposures (CVE) List grows by nearly one hundred every month.[404] There are likely more pathways into your computer network than your system administrators can protect. And to a large degree, this explains the high return on investment enjoyed by cyber criminals and cyber spies.

In the future, if war breaks out between two or more major world powers, one of the first victims could be the Internet itself. The reason is that classified cyber attack tools and techniques available to military and intelligence agencies are likely far more powerful than those available to the general public.[405] However, as with chemical weapons (CW) and even with nuclear weapons, it is possible that non-state

403 Mostyn, 2000: At least a decade ago, the widespread use of anonymous email services to support criminal activity had convinced some that an international convention would be needed to regulate its use.

404 "Common Vulnerabilities and Exposures List," The MITRE Corporation, http://cve.mitre.org/.

405 McConnell, 2010: Mike McConnell, former director of the U.S. National Security Agency and Director of National Intelligence, recently wrote in the *Washington Post* that "the lion's share of cybersecurity expertise lies in the federal government."

actors, including terrorists, will acquire strategically significant cyber attack tools and techniques in the future.[406]

What is to be done? Severing one's connection to cyberspace is not an attractive option. The benefits of connecting to the Internet usually outweigh the drawbacks; this quickly undermines a fortress mentality. And even theoretically "closed" networks – those with no direct connection to the Internet – are still subject to a wide range of computer network attacks (CNA).[407]

In light of our dependence on such vulnerable technology, and due to the fact that CNA is difficult to stop, world leaders may try to negotiate international agreements designed to contain conflict on the Internet.[408] Cyber arms control is one possible strategy, and the 1997 Chemical Weapons Convention (CWC) may provide a strong candidate model.[409]

The Chemical Weapons Convention

Chemical weapons (CW) are almost as old as warfare itself. Archeologists have found poison-covered arrowheads dating to 10,000 BC.[410] In the First World War, CW may have caused one-third of the estimated 5 million casualties. Today, terrorists are attracted to CW not only for its killing power, but also due to its ease of acquisition.[411]

As a weapon, CW employs the toxic properties of certain chemicals in a way that can kill, injure or incapacitate humans and animals. Throughout history, each new generation of CW has been more dangerous than its predecessor.[412]

In 1997, 95 nations signed CWC, an international arms control agreement that has been a success by almost any measure. The treaty's purpose is reflected in its full name: *Convention on the Prohibition of the Development, Production, Stockpiling*

406 Lewis, 2010: James Lewis of *CSIS* recently stated: "It remains intriguing and suggestive that [terrorists] have not launched a cyber attack. This may reflect a lack of capability, a decision that cyber weapons do not produce the violent results terrorists crave, or a preoccupation with other activities. Eventually terrorists will use cyber attacks, as they become easier to launch...".

407 Military and intelligence agencies are capable of supply chain attacks, insider exploitation, the stand-off kinetic destruction of computer hardware, and the use of electromagnetic radiation to destroy unshielded electronics via current or voltage surges.

408 Markoff & Kramer, 2009a: According to *The New York Times*, Russian negotiators have long argued that an international treaty, similar to those that have been signed for WMD, could help to mitigate the threat posed by military activities to civilian networks, and that in 2009 the U.S. appeared more willing to discuss this strategy.

409 Others could be the Nuclear Non-Proliferation Treaty or the Biological Weapons Convention.

410 Mayor, 2008.

411 Newmark, 2001.

412 *Ibid.*

and Use of Chemical Weapons and on their Destruction. Its goal is to eliminate the entire category of weapons of mass destruction (WMD) that is associated with toxic chemicals and their precursors. The CWC Preamble declares that achievements in chemistry should be used exclusively for beneficial purposes, and that the prohibition on CW is intended "for the sake of all mankind."

Each signatory is responsible for enforcing CWC within its legal jurisdiction. This includes overseeing the destruction of existing CW and the destruction of all CW production facilities. Under the convention, all toxic chemicals are considered weapons unless they are used for purposes that are specifically authorized under CWC. Further, members are prohibited from transferring CW to or from other nations.

CWC is administered by the Organization for the Prohibition of Chemical Weapons (OPCW), based in The Hague, which is an independent entity working in concert with the United Nations. OPCW has a staff of 500 and a budget of EUR 75 million.[413]

Currently, 188 nations, encompassing 98% of the global population, are party to CWC. A mere 13 years old, CWC has enjoyed the fastest rate of accession of any arms control treaty in history.[414] Since 1997, over 56% of the world's declared stockpile of 71,194 metric tons of chemical agent has been destroyed, along with almost 50% of the world's 8.67 million chemical munitions and containers.[415]

CWC: Lessons for Cyber Conflict

Governments addressed the threat from CW by creating CWC. In order to counter the threat posed by cyber attacks and cyber warfare, world leaders may decide to create a similar regime, a *Cyber Weapons Convention*. In that event, international negotiators will likely examine CWC to see whether its principles are transferrable to the cyber domain. This author has identified five principles characteristic of CWC that may be useful in this context: political will, universality, assistance, prohibition, and inspection.[416]

Political will. On March 21, 1997, Presidents Bill Clinton and Boris Yeltsin issued a joint statement from Helsinki, stating that they were committed to the ratification of

413 OPCW website: www.opcw.org.

414 Challenges remain: Angola, Egypt, Israel, Myanmar, North Korea, Somalia, and Syria are still outside CWC; the U.S. and Russia are highly unlikely to meet the legally binding CW destruction deadline of April 2012; advances in science and technology pose constant challenges to the integrity of the inspections regime.

415 OPCW website: www.opcw.org.

416 I derived these five principles in part from the article Mikhail Gorbachev and Rogelio Pfirter wrote for *Bulletin of the Atomic Scientists* and from Oliver Meier's interview with Pfirter in *Arms Control Today*.

CWC in order to "banish poison gas from the Earth."[417] At the end of the Cold War, the U.S. and Russia possessed the lion's share of CW, and CWC could not have been a success without their leadership. However, all signatories had to be convinced that they had more to gain from joining CWC than they had to lose by remaining outside it. In the case of CW, there is a genuine abhorrence that the science of chemistry has been used for such lethal purposes, as well as a fear that terrorist groups – who lack the accountability of sovereign governments – will obtain CW.

Universality. In 1997, more than two dozen countries possessed CW.[418] Furthermore, since CW technology was not difficult to acquire, that number would have continued to grow. CWC authors therefore designed the convention as a universal treaty with a universal and permanent goal. All nations are encouraged to become members, and the treaty's endgame is the elimination of an entire class of WMD. Therefore, CWC represents the broadest possible multilateral security framework. At first glance, this strategy could be an obstacle to treaty advancement. However, universality also provides a strong recruitment incentive: peer pressure. A higher ratio of members to non-members increases one's sense of security gained by accession and heightens the isolation felt by those who remain on the outside.

Assistance. OPCW offers enormous practical aid to CWC members. Above all, signatories are helped to fulfill treaty requirements, beginning with the destruction of CW and CW production facilities. Further, OPCW actively promotes the advancement of peaceful uses of chemistry for economic development. This includes the provision of training for local experts. Finally, OPCW offers advocacy to treaty members in the event they are threatened by the CW of another state.

Prohibition. CWC has proven that verifiable destruction of CW and their production facilities is feasible. By 2010, over 50% of the world's declared chemical agent stockpiles had been verifiably destroyed, as well as nearly 50% of declared chemical munitions. Some states had completely eliminated their CW programs. At the current rate, over 90% of the world's known CW will be destroyed by 2012. Although seven nations remain outside CWC, no new states have acquired CW since 1997. The success of CWC stands in contrast to the 1968 Nuclear Non-Proliferation Treaty (NPT). Despite the efforts of NPT, the size of the world's nuclear club has grown from five[419] to nine.[420]

417 "The President's News Conference..." 1997.

418 Cole, 1996.

419 These are also the permanent members of the United Nations Security Council: China, France, Russia, UK, and the U.S.

420 Huntley, 2009: De facto members now include India, Israel, Pakistan, and North Korea.

Inspection. Since 1997, almost 4,000 CWC inspections have been conducted on the territory of 81 member states in order to verify treaty compliance. These have taken place at almost 200 known CW-related sites and at over 1,000 other industrial sites. Nearly 5,000 facilities around the world are liable to CWC inspection at any time. One of the primary benefits of CWC membership is the right to request a "challenge inspection" on the territory of a fellow member state, based on the principle of "anytime, anywhere," with no right of refusal.

Toward a Cyber Weapons Convention

Cyber warfare is not chemical warfare. Although they share some similarities – including ease of acquisition, asymmetric damage, and polymorphism – the tactics, strategies, and effects are fundamentally different. Chemical warfare kills humans; cyber warfare kills machines.[421]

As a means of waging war, however, both chemical and cyber attacks represent a potential threat to national security. As such, diplomats may be asked to negotiate international agreements designed to mitigate the risk of cyber warfare, just as they have done for CW.

The five principles described in the previous section have helped to make CWC a success. In this section, the author argues that the first three principles are clearly transferable to the cyber domain, while the final two are not.

Political will. International treaties require widespread agreement on the nature of a common problem. The threat posed by cyber attacks – based on national capabilities as well as the fear that terrorists will begin to master the art of hacking – could be strong enough to form such a political consensus. The 2010 cyber attack on Google was serious enough to begin discussion in the U.S. on whether to create an ambassador-level post, modeled on the State Department's counterterrorism coordinator, to oversee international cyber security efforts.[422] As with CWC, a convention intended to help secure the Internet would need the major world powers behind it to succeed. At a minimum, in today's world that means the U.S., Russia, China, and the EU.[423]

421 To be more specific, cyber attacks usually target the data resident on or functionality of a machine. It is also important to note that inoperable machines can kill humans: examples include medical equipment and national air defense systems. By the same token, chemical warfare can also kill flora, fauna, and human input to machines.

422 Gorman, 2010.

423 With CWC, the Middle East conflict continues to pose the most serious challenge to worldwide agreement, and it could do the same for a Cyber Weapons Convention.

Universality. One of the primary challenges to improved computer security is the fact that the Internet is a worldwide enterprise. The jurisdiction of law enforcement and counterintelligence personnel ends every time a network cable crosses an international border. Even though thousands of miles may separate an attacker and defender in the real world, everyone is a neighbor in cyberspace, and attackers often have direct access to their victims. Smart hackers hide within the maze-like architecture of the Internet and route attacks through countries with which the victim's government has poor diplomatic relations or no law enforcement cooperation. In 2010, there are plenty of cyber safe havens where criminals, spies and terrorists can operate without fear of reprisal.[424] Although the global nature of cyberspace makes the practical task of securing the Internet inherently more difficult, the universal goals of CWC are highly appropriate in the cyber domain. Politicians, international negotiators, and the public will have no trouble understanding this characterization, and universality would be a cornerstone of a Cyber Weapons Convention.

Assistance. Vulnerabilities in computer networks and the advantages they create for an attacker will persist for the foreseeable future. Consequently, organizations have no choice but to invest more time and effort into computer security. However, a proper implementation of best practices such as risk management, awareness training, defense-in-depth, and incident handling[425] usually requires more expertise and resources than most organizations and even many countries have available. Within CWC, OPCW offers practical aid to its members. In the same fashion, a Cyber Weapons Convention could create an internationally-staffed institution dedicated to helping signatories improve their cyber defense posture and respond effectively to cyber attacks when they occur. Experts could provide technical, legal, and policy advice via consultation and training. A crisis response team could be available to deploy worldwide at a moment's notice, ready to publish its findings to the world. And as with CWC, the institution could actively promote the benefits of peaceful uses of computer technology for economic development and cooperation.

One significant but difficult step for governments to take would be the joint instrumentation and observation of the Internet and its network traffic flows. Many cyber threats, such as the one posed by botnet technology, simply move too quickly for the kind of traditional inspections that OPCW provides. Cyber attack mitigation requires immediate source identification and the ability to cross technical, legal, and national borders quickly. The best chance that future Cyber Weapons Convention

424 Gray & Head, 2009.

425 For example, the U.S. Computer Emergency Readiness Team (US-CERT) offers many free publications in the following categories: "General Internet security," "Securing your computer," "Recovering from an attack," and "Monthly and quarterly reports" (www.us-cert.gov/reading_room/); however, most system administrators simply do not have the time to study, absorb, and implement all such recommendations.

monitors would have is with access to real-time network data from across the whole of the Internet and the ability to collaborate immediately with treaty-empowered colleagues throughout the world.[426] National sovereignty and data privacy concerns would have to be carefully guarded. Furthermore, the technical and forensic side of the regime should be separated as much as possible from its legal and political ramifications. Data analysts could not have access to any personally identifiable information, but when cyber attacks are observed, the appropriate law enforcement organizations must be notified.

Prohibition. The proof that CWC has been a success lies in the large volume of CW that has been verifiably destroyed. The principle of prohibition, however, would be the most challenging aspect of CWC to apply in cyberspace. Malicious computer code is notoriously difficult to define. In the single month of May 2009, Kaspersky Anti-Virus Lab found 42,520 "unique malicious, advertising, and potentially unwanted" programs on its clients' computers.[427] Even in a well-designed and malware-free network, a legitimate path for remote system administration can be used by a masquerading hacker, who has correctly guessed or stolen its password, to thoroughly undermine its confidentiality, integrity, and/or availability. Any computer programmer can learn to write malware, and non-programmers can simply download professional-quality attack tools from well-known websites. Further, cyber warfare is unlike chemical warfare in that cyber attacks often demand stealth and anonymity. At a minimum, any prohibition on malware will require substantial progress on solving the cyber attack "attribution" problem.[428] This will take time, and involve technical, legal, and international cooperation on a level far higher than it exists today.

Inspection. Similar to prohibition, the CWC inspection regime has been a success, but it is difficult to imagine how the principle of inspection could easily be applied in cyberspace. Around the world, 5,000 industrial facilities are subject to CWC inspection at any time; this is a large but manageable number. Compare it to the amount of digital information that can be placed on one removable thumb drive. In 2010, a 256 GB USB Flash drive cost under $1000;[429] it held over 2 trillion bits of data. Even widely-published operating system and application code can be almost impossible to understand thoroughly – even for experts – because there is simply

426 Such an effort would be daunting from a technical perspective, but in theory, if this is possible to accomplish in one large country, it should be possible across the globe. On a human level, thousands of international CERT personnel already do it on a less formal basis every day.

427 "Monthly Malware Statistics..." 2009.

428 This refers to anonymous cyber attacks, described in the Universality section above.

429 The Kingston DataTraveler® 310 is currently advertised as the highest capacity USB Flash drive on the market.

too much information to analyze.[430][431] Malware can be written on any computer, and transmitted to the Net from any network access point. In the U.S. alone, there are 383 million computers connected directly to the Internet.[432] In theory, a Cyber Weapons Convention could require closer inspection and monitoring at the Internet Service Provider (ISP) level. However, such regimes are already commonplace, such as China's Golden Shield Project, the European Convention on Cybercrime, Russia's SORM,[433] and the USA PATRIOT Act. Each is unique in terms of guidelines and enforcement, but all face the same problem of overwhelming traffic volume.

The Challenges of Prohibition and Inspection

The challenge of securing the Internet appears to be worsening with time.[434] World leaders may eventually decide that the best way to mitigate the threat posed by cyber attacks is by signing an international cyber arms control treaty.[435]

The Chemical Weapons Convention (CWC) constitutes a useful model. It boasts the vast majority of world governments as signatories and has tangibly reduced the threat of chemical warfare, both by delegitimizing the use of chemical weapons (CW) and by dramatically reducing the quantity of CW in existence.

This chapter highlights five principles that have helped to make CWC a success, and examines each principle to see whether it could support the development of a *Cyber Weapons Convention*.

430 Cole, 2002.

431 Even if it were possible, software is dynamic. Programs constantly change their functionality via security patches and other updates.

432 This figure is from *The World Factbook*, published by the U.S. Central Intelligence Agency, and describes the number of "Internet hosts" in a country. These are defined as "a computer connected directly to the Internet ... Internet users may use either a hard-wired terminal ... or may connect remotely by way of a modem via telephone line, cable, or satellite to the Internet Service Provider's host computer."

433 *Система Оперативно-Розыскных Мероприятий* or "System for Operative Investigative Activities."

434 Geers, 2010.

435 "Espionage Report..." 2007; Cody, 2007: Many vignettes could be recited here. In 2007, German Chancellor Angela Merkel visited China for a state meeting which was overshadowed by a media claim that Chinese hackers had been caught attempting to steal data from Merkel's chancellery and other Berlin ministries. The Chinese government denied the allegations, but Prime Minister Wen Jiabao nonetheless told Merkel that measures would be taken to "rule out hacking attacks." The following month, Chinese Vice Information Industry Minister Lou Qinjian wrote in a Communist Party magazine that foreign intelligence services had also caused "massive and shocking" damage to China via computer hacking.

The first three principles – political will, universality, and assistance – are easy to apply in the cyber domain. None of them is a perfect fit, but as with CWC, all of them are appropriate to the nature and challenges of managing Internet security.

The final two principles – prohibition and inspection – are not helpful at this time. It is difficult to prohibit or inspect something that is hard to define and which grows by orders of magnitude on a regular basis. In fact, these two catches could prove significant enough that a future treaty may not be called Cyber Weapons Convention, but something more generic, such as *Internet Security Convention*.

On balance, the three applicable principles provide world leaders with a good starting point to explore the prospects for a Cyber Weapons Convention. If national and Internet security thinkers decide that an international cyber arms control treaty is the right way forward, political leaders may give scientists the funding they need to attack the technical challenges of prohibition and inspection.

IV. DATA ANALYSIS AND RESEARCH RESULTS

9. DEMATEL AND STRATEGIC ANALYSIS

In this research study, the author will employ the Decision Making Trial and Evaluation Laboratory (DEMATEL) to analyze the most important concepts and definitions. The goal of using DEMATEL is twofold: to increase the rigor of the author's analysis via scientific method, and to help provide decision makers with greater confidence as they attempt to choose the most efficient ways to mitigate the threat of cyber attacks and improve cyber security at the strategic level.

DEMATEL is a comprehensive scientific research method, developed in the 1970s by the Science and Human Affairs Program at the Battelle Memorial Institute in Geneva. It is used to solve scientific, political and economic problems that contain a complex array of important factors,[436] which may involve many stakeholders.[437] It has often been used, especially by researchers in Middle East and Far East, to investigate problems of strategic scope and significance.[438]

First, a DEMATEL researcher must identify and classify the key concepts or the most influential factors in a given system or in a particular area of research.

Second, all factors are placed into a pair-wise, "direct-influence" comparison matrix and prioritized by their level of influence on the other factors in the system: zero, or "no influence," to four, or "very high influence." The matrix isolates all of the factors within the system, as well as their one-to-one relationships.[439] It displays the level of influence that each factor exerts on every other factor in the system, and provides a clear ranking of alternatives by influence level.[440]

Third, the influencing factors are depicted in a causal loop diagram that graphically displays how each factor exerts pressure on, and receives pressure from, all other factors in the system, including the strength of each influence relationship.

436 Gabus & Fontela, 1972; Gabus & Fontela, 1973.

437 Jafari et al, 2008.

438 Several are cited in this paper, below.

439 Hu et al, 2010.

440 Dytczak & Ginda, 2010.

Fourth, DEMATEL calculates the combined effect of both the direct and indirect influence relationships, yielding a new overall influence score for all factors in the system. It is then possible to place all factors into a hierarchical structure.

In this way, DEMATEL helps to provide decision makers with the most efficient paths to a desired outcome. These contribute to workable solutions at the tactical level[441] and superior policy choices at the strategic level.[442]

DEMATEL Influencing Factors

Parts II and III of this book described cyber security as an emerging strategic concept and examined four mitigation strategies that governments will likely adopt to counter the cyber attack threat. Fig. 1, below, summarizes these concepts as DEMATEL "influencing factors." Each is defined in more detail in this chapter.

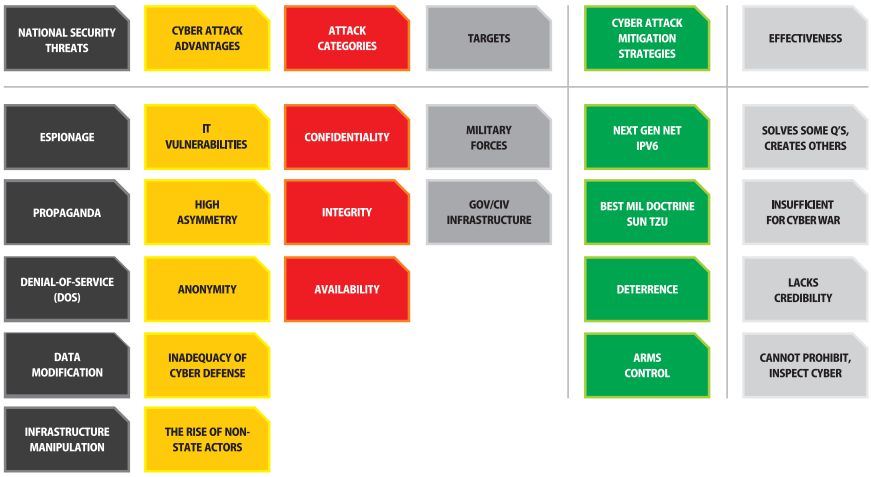

Figure 1. DEMATEL "Influencing Factors."

National Security Threats

A cyber attack is best understood not as an end in itself, but as an extraordinary means to a wide variety of ends. At the tactical level, there are many objectives that an attacker seeks. Here are five of the most important.

441 Hu et al, 2010.

442 Moghaddam et al, 2010.

Espionage. Every day, anonymous computer hackers steal vast quantities of computer data and network communications. In fact, it is possible to conduct devastating intelligence-gathering operations, even on highly sensitive political and military communications, remotely from anywhere in the world.

Propaganda. Cheap and effective, this is often the easiest and the most powerful form of cyber attack. Propaganda dissemination may not need to incorporate any computer hacking at all, but simply take advantage of the amplification power of the Internet. Digital information, in text or image format and regardless of whether it is true – can be instantly copied and sent anywhere in the world, even deep behind enemy lines. And provocative information that is censored from the Web can reappear elsewhere in seconds.

Denial-of-Service (DoS). The simple strategy behind a DoS attack is to deny the use of data or a computer resource to legitimate users. The most common tactic is to flood the target with so much superfluous data that it cannot respond to real requests for services or information. Today, black market botnets provide anyone with massive Distributed DoS (DDoS) resources and a high level of anonymity. Other DoS attacks include the physical destruction of computer hardware and the use of electromagnetic interference, designed to destroy unshielded electronics via current or voltage surges.

Data modification. A successful attack on the integrity of sensitive data is insidious because legitimate users (human or machine) may make subsequent critical decisions based on maliciously altered information. Such attacks range from website defacement, which is often referred to as "electronic graffiti," but which can still carry propaganda or disinformation, to the corruption of advanced weapons or command-and-control (C2) systems.

Infrastructure manipulation. National critical infrastructures are, like everything else, increasingly connected to the Internet. However, because instant response may be required, and associated hardware could have insufficient computing resources, security may not be robust. Furthermore, the infrastructure could require instant or automatic response, so it may be unrealistic to expect that a human would be available to concur with every command the infrastructure is given.[443]

Complicating matters is the fact that most critical infrastructures are in private hands. Internet Service Providers (ISP), for example, typically lease communication lines to government as well as to commercial entities, and it is not uncommon for

443 Geers, 2009.

satellite management corporations to offer bandwidth to multiple countries at the same time.[444]

The management of electricity is essential for national security planners to evaluate because electricity has no substitute, and all other infrastructures, including computer networks, depend on it.[445] Finally, it is important to note that many critical infrastructures are in private hands, outside of government protection and oversight.

Key Cyber Attack Advantages

As a medium through which a nation-state or a non-state actor can threaten the security or national security of a rival or adversary, cyberspace offers attackers numerous key advantages that facilitate and amplify the three traditional attack categories of confidentiality, integrity and availability. These are illustrated in Fig. 2, below.

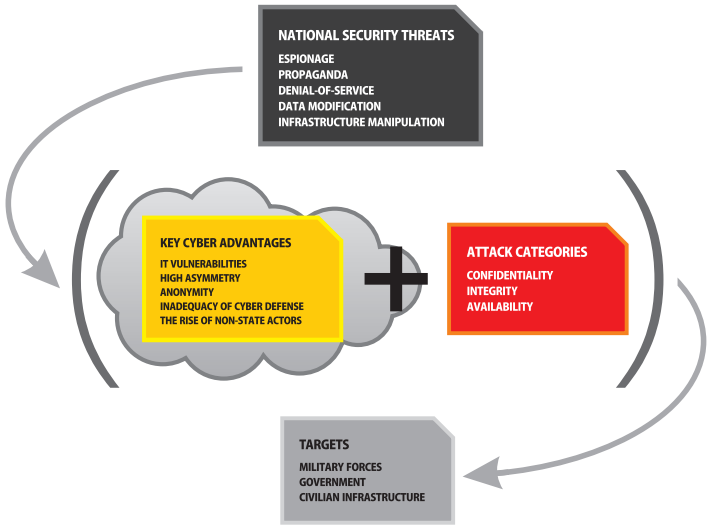

Figure 2. Key Cyber Attack Advantages.

Vulnerability. The Internet has an ingenious modular design that is remarkably resilient in the face of many classes of cyber attack. However, hackers regularly find sufficient flaws in its architecture to secretly read, delete, or modify information stored on or traveling between computers. Further, the rapid proliferation in

444 *Ibid.*

445 Divis, 2005.

communications technologies provides sensitive sites with a level of redundancy unimagined in the past. However, on the downside it is a challenge for defenders to keep up with the latest attack methods. In fact, there are about 100 additions to the Common Vulnerabilities and Exposures (CVE) database each month.[446] Constantly evolving malicious code often gives hackers more paths into a network than its system administrators can protect.

Asymmetry. Nations, organizations, and individual hackers find in computer hacking a very high return on investment. An attacker's common goals are self-explanatory: the theft of research and development data, eavesdropping on sensitive communications, and the delivery of propaganda behind enemy lines. The elegance of computer hacking lies in the fact that it may be attempted for a fraction of the cost – and risk – of many other information collection or manipulation strategies.

Anonymity. The maze-like architecture of the Internet offers cyber attackers a high degree of anonymity. Smart hackers route their attacks through countries with which the victim's government has poor diplomatic relations or no law enforcement cooperation. Even successful cyber investigations often lead only to another hacked computer. Governments today face the prospect of losing a cyber conflict without even knowing the identity of their adversary.

Inadequacy of cyber defense. Computer network security is still an immature discipline. Traditional security skills are of marginal help in cyber warfare and it is difficult to retain personnel with marketable technical expertise. Challenging computer investigations are further complicated by the international nature of the Internet. Moreover, in the case of state-sponsored cyber operations, law enforcement cooperation is naturally non-existent.

The rise of non-state actors. The Internet era offers to everyone vastly increased participation on the world stage. Historically, governments have endeavored to retain as much control as they can over international conflict. However, globalization and the Internet have considerably strengthened the ability of anyone to follow current events and have provided a powerful means to influence them. Domestic and transnational subcultures now spontaneously coalesce online, sway myriad political agendas, and may not report to any traditional chain-of-command. A future challenge for world leaders is whether their own citizens could spin delicate international diplomacy out of control.

446 "Common Vulnerabilities and Exposures List," The MITRE Corporation, http://cve.mitre.org/.

Cyber Attack Categories

There are three basic forms of cyber attack, from which all others derive.

Confidentiality. This encompasses any unauthorized acquisition of information, including surreptitious "traffic analysis," in which an attacker infers communication content merely by observing communication patterns. Because global network connectivity is currently well ahead of global network security, it can be easy for hackers to steal enormous amounts of information.

Cyber terrorism and cyber warfare may still lie in our future, but we are already living in a Golden Age of cyber espionage. The most famous case to date is "GhostNet," investigated by *Information Warfare Monitor*, in which a cyber espionage network of over 1,000 compromised computers in 103 countries targeted diplomatic, political, economic, and military information.[447]

Integrity. This is the unauthorized modification of information or information resources such as a database. Integrity attacks can involve the "sabotage" of data for criminal, political, or military purposes.

Cyber criminals have encrypted data on a victim's hard drive and then demanded a ransom payment in exchange for the decryption key. Governments that censor Google results return part, but not all of the search engine's suggestions to an end user.

Availability. The goal here is to prevent authorized users from gaining access to the systems or data they require to perform certain tasks. This is commonly referred to as a denial-of-service (DoS) and encompasses a wide range of malware, network traffic, or physical attacks on computers, databases and the networks that connect them.

In 2001, "MafiaBoy," a 15 year-old student from Montreal, conducted a successful DoS attack against some of the world's biggest online companies, likely causing over $1 billion in financial damage.[448] In 2007, Syrian air defense was reportedly disabled by a cyber attack moments before the Israeli air force demolished an alleged Syrian nuclear reactor.

447 "Tracking GhostNet..." 2009.

448 Verton, 2002.

Strategic Cyber Attack Targets

Cyber attacks of strategic significance do not occur every day. In fact, it is likely that the most powerful cyber weapons may be saved by militaries and intelligence agencies for times of international conflict and war.

Some war tactics will change in order to account for the unique nature of cyberspace and for the latent power of cyber warfare, but the ultimate goal of war – victory – will not change. As in past wars and as with other types of aggression, there are two broad categories of strategic targets that cyber attackers will strike.

Military forces. The first category of cyber attacks would be conducted as part of a broader effort to disable the adversary's weaponry and to disrupt military command-and-control (C2) systems.

In 1997, the U.S. Department of Defense (DoD) held a large-scale cyber attack red team exercise called Eligible Receiver. The simulation was a success. As James Adams wrote in *Foreign Affairs*, thirty-five National Security Agency (NSA) personnel, posing as North Korean hackers, used a variety of cyber-enabled information warfare tactics to "infect the human command-and-control system with a paralyzing level of mistrust ... as a result, nobody in the chain of command, from the president on down, could believe anything."[449]

In 2008, unknown hackers broke into a wide range of DoD computers, including a "highly protected classified network" of Central Command (CENTCOM), the organization which manages both wars in which the U.S. is now engaged. The Pentagon was so alarmed by the attack that Chairman of the Joint Chiefs Michael Mullen personally briefed President Bush on the incident.[450]

In the event of a future war between major world powers, it is wise to assume that the above-mentioned attacks would pale in comparison to the sophistication and scale of cyber tools and tactics that governments may hold in reserve for a time of national security crisis.

Government/civilian infrastructure. The second category of cyber attacks would target the adversary's ability and willingness to wage war for an extended period of time. The targets would likely include an adversary's financial sector, industry, and national morale.

One of the most effective ways to undermine a variety of these second-tier targets is to disrupt the generation and supply of power. President Obama's announcement

449 Adams, 2001.

450 Barnes, 2008.

that unknown hackers had "probed our electrical grid" and "plunged entire cities into darkness"[451] in Brazil[452] should serve as a wake-up call for many. Referring to theoretical cyber attacks on the financial sector, former U.S. Director of National Intelligence (DNI) Mike McConnell stated that his primary concern was not the theft of money, but a cyber attack that would target the integrity of the financial system itself, designed to destroy public confidence in the security and supply of money.[453]

In a future war between major world powers, militaries would likely exploit the ubiquity of cyberspace and global connectivity to conduct a wide range of cyber attacks against adversary national critical infrastructures, on their home soil, deep behind the front lines of battle.

Cyber Attack Mitigation Strategies

This research has shown that cyber attackers possess significant advantages over cyber defenders, and that governments must now take the threat of strategic-level cyber attacks seriously. The four mitigation strategies examined in Part III are summarized below.

Fig. 3 is a causal loop diagram that shows how cyber attack mitigation strategies are designed to reduce the impact of cyber attack advantages, with the ultimate goal of reducing threats to national security via cyberspace.

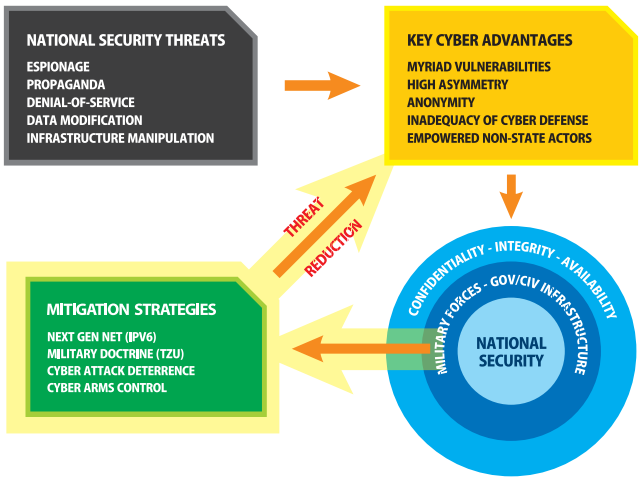

Figure 3. Cyber Attack Mitigation Strategies.

451 "Remarks..." 2009.

452 "Cyber War..." 2009.

453 *Ibid.*

IPv6: The complex and evolving nature of IT tends to favor an attacker, who often finds a surfeit of network vulnerabilities to exploit. At the same time, the benefits of connectivity continue to ensure that returning to pen and paper is not an option. If there is a leading current technical solution to the cyber attack problem, a reasonable argument can be made for Internet Protocol version 6 (IPv6), which is replacing IPv4 as the "language" of the Internet. The first benefit of IPv6 is that it instantly solves the world's shortage of computer addresses.[454] However, its chief security enhancement – mandatory support for Internet Protocol Security (IPSec) – is in fact an optional feature that may not be widely used for reasons of convenience. Furthermore, during the long transition phase ahead, there will be an increased "attack surface" as hackers exploit vulnerabilities in both IP languages at once.[455]

Military doctrine: Cyberspace is a new warfare domain, in which computers are both a weapon and a target. Future military concepts and doctrine must find a way to encompass cyber attack and defense strategies and tactics. However, even the most influential military treatise in history, Sun Tzu's *Art of War*, which is renowned for its flexibility and adaptability to new means and methods of war, has great difficulty subsuming many aspects of cyber warfare. The author described ten distinctive characteristics of the cyber battlefield, none of which fits easily into Sun Tzu's paradigm.

Deterrence: There are only two deterrence strategies available to nation-states: denial of a threatening technology (e.g., nuclear weapons) and punishment. With cyber weapons, denial is a non-starter because hacker skills and tools are easy to acquire. Punishment via retaliation is the only option, but to be an effective deterrent, a threat has to be credible. Here again, the challenges of poor attacker attribution and high attack asymmetry in cyberspace undermine the credibility of deterrence. Further, they create problematic doctrinal questions for military rules of engagement.[456]

Arms Control: In the future, world leaders may negotiate an international treaty on the use of cyber weapons.[457] However, arms control relies on two principles that are not easy to apply in cyberspace: prohibition and inspection. First, it is difficult to prohibit something that is hard to define, such as malicious code. And even in a malware-free organization, hackers are adept at using legitimate paths to network access, such as by guessing or stealing a password. Second, it is hard to inspect something that is difficult to count: a USB Flash drive now holds up to 256 GB or

454 IPv4 contains around 4 billion IP addresses; IPv6 has 340 undecillion, or 50 octillion IPs for every human on planet Earth.

455 Geers & Eisen, 2007.

456 Geers, 2010b.

457 Markoff & Kramer, 2009a: Russian negotiators have long argued that an international treaty, similar to those that have been signed for WMD, could help to mitigate the cyber threat. In 2009, the U.S. was reportedly more willing to discuss this proposal than in the past.

over 2 trillion bits of data, and in the U.S. alone, there are over 400 million Internet-connected computers.[458]

A summary of the four mitigation strategies and their relative effectiveness is depicted in Fig. 4.

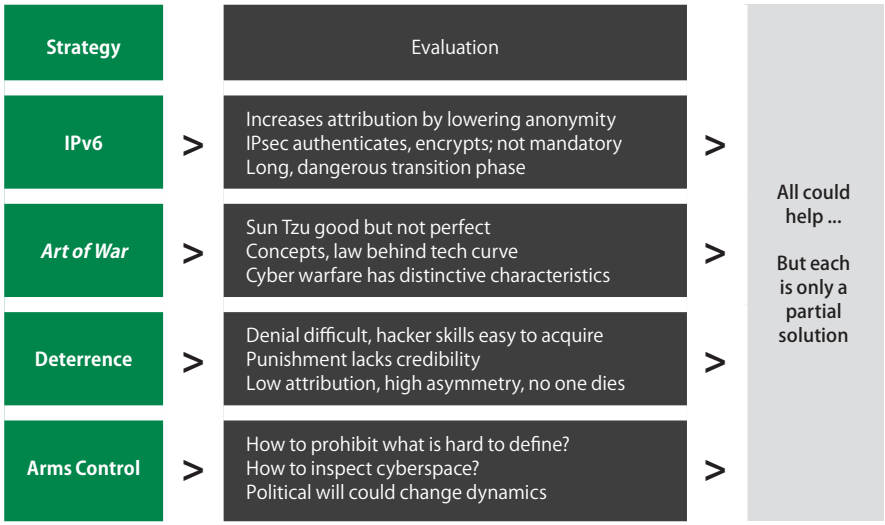

Figure 4. Mitigation Strategy Effectiveness.

This chapter summarized the key concepts, or influencing factors, in this research. The next chapter will examine the two most important concept categories – "key cyber attack advantages" and "cyber attack mitigation strategies" – with the aid of DEMATEL. The goal is to derive a more precise conclusion to this book via stronger scientific method.

458 Geers, 2010c.

10. KEY FINDINGS

The author will employ the DEMATEL method to analyze the two most important categories of influencing factors in this research – cyber attack advantages and cyber attack mitigation strategies – with four primary objectives in mind:

- to understand how the key concepts in this book, both individually and categorically, influence one another;
- to visualize the system they comprise with the aid of a causal loop diagram;
- to understand the extent to which the system may be controllable; and
- to prioritize the mitigation strategies for decision makers according to their impact on reducing the cyber attack advantages and on positively affecting the system of strategic cyber security as a whole.

The "Expert Knowledge" Matrix

Matrix *X*, depicted in Fig. 5, is a DEMATEL "Expert Knowledge" influence matrix that juxtaposes the cyber attack advantages and mitigation strategies according to their level of influence on one another. The advantages are lettered A-E, and the strategies are F-I.

Each individual influence value in the matrix is based on the research presented in this book and on the author's judgment as a subject matter expert with over ten years working as a cyber intelligence analyst. As detailed in the Bibliography, the author has published peer-reviewed research examining and evaluating the efficacy of all nine influence factors.

For future research purposes, it is clear that different influence estimates will pertain in different national contexts, and that the dynamic nature of cyberspace will ensure that most if not all the variables will change over time.

The reader is thus encouraged to tailor the matrix to his or her needs and to aggregate or disaggregate individual influence factors for more general or for more specific research goals.

The mathematics, however, are well-founded, and remain the same.

	DEMATEL "Expert Knowledge" Influence Matrix *X* None =0 Low=1 Medium=2 High=3 Very High=4	A IT Vulnerabilities	B Asymmetry	C Anonymity	D Inadequate Cyber Defense	E Emp. Non-State Actors	F Next Gen Internet: IPv6	G Best Mil Doctrine: Sun Tzu	H Cyber Attack Deterrence	I Cyber Arms Control	Direct Influence
A	IT Vulnerabilities	0	4	4	4	3	3	2	3	3	26
B	Asymmetry	2	0	1	4	4	2	4	4	3	24
C	Anonymity	2	4	0	4	4	4	4	4	4	30
D	Inadequate Cyber Defense	4	3	3	0	2	2	3	4	2	23
E	Empowered Non-State Actors	1	2	2	1	0	2	4	3	3	18
F	Next Gen Internet: IPv6	3	2	4	2	1	0	2	2	2	18
G	Best Mil Doctrine: Sun Tzu	3	3	2	4	2	1	0	4	2	21
H	Cyber Attack Deterrence	1	2	2	2	2	1	2	0	3	15
I	Cyber Arms Control	1	1	2	2	2	1	2	3	0	14
	Level Influenced	17	21	20	23	20	16	23	27	22	

Figure 5. DEMATEL "Expert Knowledge" Influence Matrix *X*.

A quick glance at Matrix *X* shows that it is dominated by the cyber attack advantages, which are much more influential in this system of influences than the mitigation strategies. The average "direct influence" strength of the advantages is 24.2, versus a mitigation strategy average of 17. The attack advantages also possess the overwhelming majority of scoring at the "very high" influence level: 17 to 3.

This result appears intuitive. It correlates to the common perception in the world today that cyber attackers have enormous advantages over their cyber defense counterparts.

Fig. 6, below, ranks all factors in Matrix *X* by the simple addition of their individual influence levels, by row. To keep them visually distinct, the advantages are in yellow, and the mitigation strategies are colored dark green.

	Factor	Direct Influence
C	Anonymity	30
A	IT Vulnerabilities	26
B	Asymmetry	24
D	Inadequate Cyber Defense	23
G	Best Mil Doctrine: Sun Tzu	21
E	Empowered Non-State Actors	18
F	Next Gen Internet: IPv6	18
H	Cyber Attack Deterrence	15
I	Cyber Arms Control	14

Figure 6. "Direct Influence" by Factor.

According to Matrix *X*, the most influential factor in strategic cyber security today is the ability of so many cyber attackers to remain anonymous to their victims. The second most important factor is the seemingly endless list of IT vulnerabilities from which cyber attackers are able to choose.

The most effective mitigation strategy in this list, and the only one to rank as more influential than any one of the attacker advantages, is the application of the world's most influential military treatise, Sun Tzu's *Art of War,* to cyber conflict. The least influential mitigation strategy is cyber arms control, which suffers enormously from the fact that it is difficult to define a cyber weapon and even more difficult to conduct a cyber weapons inspection.

Fig. 7 adds the columns of Matrix *X* in order to show each factor's level of susceptibility to influence from the other factors in the matrix.

	Factor	Susceptibility to Influence
H	Cyber Attack Deterrence	27
G	Best Mil Doctrine: Sun Tzu	23
D	Inadequate Cyber Defense	23
I	Cyber Arms Control	22
B	Asymmetry	21
E	Empowered Non-State Actors	20
C	Anonymity	20
A	IT Vulnerabilities	17
F	Next Gen Internet: IPv6	16

Figure 7. Susceptibility to Influence.

The results are intriguing: both the highest- and lowest-ranked factors are mitigation strategies. This appears illogical, but a closer look reveals why. The most influenced factor in Matrix *X* – deterrence – is a purely psychological condition, highly dependent on human perception and emotion; thus, it is not surprising that deterrence would be highly susceptible to outside influence. The least influenced factor is IPv6, which is pure technology and therefore tied to human failings to a far lesser degree.

Unfortunately for cyber defense, this list shows that cyber attack advantages not only have a higher "direct influence" score than the mitigation strategies, but that they are also more resistant to outside influence. In Fig. 7, the mitigation strategies have an average score of 22, compared to just 20.2 for the advantages. IPv6 scores well, but the other three strategies do not.

One way to interpret Fig. 7 is to view the "susceptibility to influence" score as a measure of a factor's reliability, as well as the confidence that a decision maker could place in it. Thus, cyber attackers are able to rely on their advantages to a much greater degree than cyber defenders can count on current attack mitigation strategies. At this point in time, three examined strategies – deterrence, doctrine, and arms control – are of dubious help to cyber defense.

Perhaps even more ominously, the two most influential cyber attack advantages – anonymity and IT vulnerabilities – are also the two most difficult cyber attack advantages to influence. Thus, they may prove extremely difficult challenges for cyber defenders to overcome in the future.

On a positive note, Fig. 7 shows that finding ways to improve cyber defense, such as by hiring the right personnel and by providing them quality training, could yield a high return on investment. "Inadequate cyber defense" has the fourth-highest "direct influence" score in Matrix *X*, and it is also the third-highest factor in terms of susceptibility to outside influence. This makes it a critical factor in the strategic cyber security environment.

Causal Loop Diagram

The next step in DEMATEL analysis involves constructing a causal loop diagram, as seen in Fig. 8. Such a visual representation of complex data can facilitate human understanding by making the information clearer and more compelling. All factors are placed into a systemic cause-and-effect illustration.

In general, the fewer number of parameters that a system contains, the easier it is to control, and the easier it is to display in a graph. Matrix *X* is large enough – 9x9, or 81 values – that it is already a complex system.

In order to make the diagram most useful for this analysis, the author has chosen to display only the "very high" levels of influence between the factors in Matrix *X*.

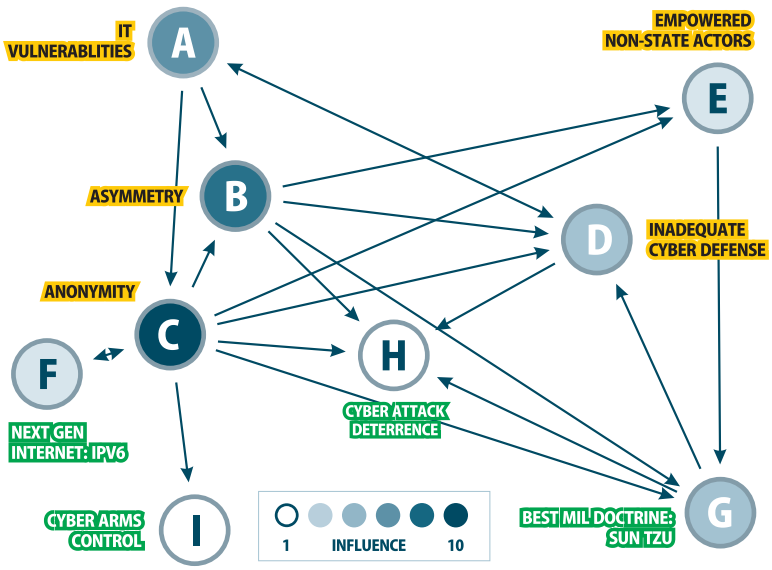

Figure 8. Strategic Cyber Security: Causal Loop Diagram.

The color of each factor is shaded according to the number of "very high" levels of influence it projects to the other factors in the system. Thus, as "anonymity" is the most influential factor in Matrix *X*, it has the darkest color of all factors in Fig. 8. Anonymity impacts almost every other factor in the system at the highest possible level.

Two factors, deterrence and arms control, remain white because they do not affect any other factor at the highest level. These are the least influential factors in Matrix *X*, in Fig. 6, and in this diagram. Cyber attack deterrence, in particular, is dominated by four other, high-impact factors, making it the most susceptible of all factors to outside influence, and the least reliable mitigation strategy for strategic cyber defense.

A causal loop diagram reveals another key aspect of the interrelationship between factors in a system: some have multiple important connections to other factors, regardless of whether the influence is given or received, while others have few. After anonymity – asymmetry, military doctrine, and inadequate cyber defense each have at least five "very high" influence relationships with other factors. This allows them to play a critical role in the system. If decision makers are able to change the nature of any one of these factors in a significant way, the resultant impact on the system as a whole could be considerable.

Calculating Indirect Influence

A close analysis of the causal loop diagram above reveals that each factor not only has a direct influence on every other factor in the system, but that it also has indirect or transitive influences on the other factors. Eventually, every factor in the system will even influence itself.

Fig. 9 below depicts the dynamic of indirect influence at work.

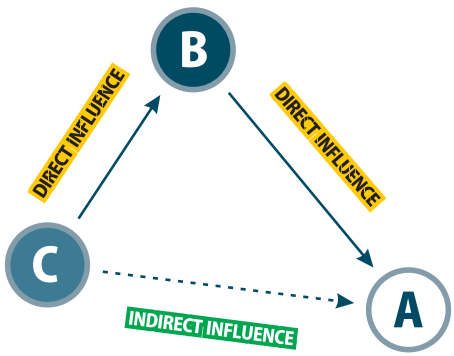

Figure 9. Indirect Influence.

The DEMATEL method is one of the easiest and most useful ways to calculate the sum of direct and indirect influences for a group of interrelated factors.[459] First, Matrix *X* is transformed into normalized Matrix *D*. The new numbers are derived by dividing the values in Matrix *X* by the single highest sum found in the rows/columns, which is Anonymity (whose "direct influence" score is 30).

Thus, the new influence levels are: 0=0, 1=.0333, 2=.0667, 3=.1000, and 4=.1333. Matrix *D* is depicted in Fig. 10.

	DEMATEL Normalized Matrix *D*	A IT Vulnerabilities	B Asymmetry	C Anonymity	D Inadequate Cyber Defense	E Empowered Non-State Actors	F Next Gen Internet: IPv6	G Best Mil Doctrine: Sun Tzu	H Cyber Attack Deterrence	I Cyber Arms Control
A	IT Vulnerabilities	0	.1333	.1333	.1333	.1000	.1000	.0667	.1000	.1000
B	Asymmetry	.0667	0	.0333	.1333	.1333	.0667	.1333	.1333	.1000
C	Anonymity	.0667	.1333	0	.1333	.1333	.1333	.1333	.1333	.1333
D	Inadequate Cyber Defense	.1333	.1000	.1000	0	.0667	.0667	.1000	.1333	.0667
E	Empowered Non-State Actors	.0333	.0667	.0667	.0333	0	.0667	.1333	.1000	.1000
F	Next Gen Internet: IPv6	.1000	.0667	.1333	.0667	.0333	0	.0667	.0667	.0667
G	Best Mil Doctrine: Sun Tzu	.1000	.1000	.0667	.1333	.0667	.0333	0	.1333	.0667
H	Cyber Attack Deterrence	.0333	.0667	.0667	.0667	.0667	.0333	.0667	0	.1000
I	Cyber Arms Control	.0333	.0333	.0667	.0667	.0667	.0333	.0667	.1000	0

Figure 10. DEMATEL-Normalized Matrix *D*.

459 Moghaddam et al, 2010.

Second, Matrix *D* is transformed into "Total Influence" Matrix *T*, in which DEMATEL calculates both the direct and indirect influence levels for each factor.[460] Matrix *T* is illustrated in Fig. 11.

	DEMATEL "Total Influence" Matrix *T*	A IT Vulnerabilities	B Asymmetry	C Anonymity	D Inadequate Cyber Defense	E Empowered Non-State Actors	F Next Gen Internet: IPv6	G Best Mil Doctrine: Sun Tzu	H Cyber Attack Deterrence	I Cyber Arms Control	Direct Influence
A	IT Vulnerabilities	.1850	.3441	.3298	.3645	.3095	.2643	.3114	.3799	.3285	2.8170
B	Asymmetry	.2257	.1954	.2186	.3324	.3075	.2077	.3365	.3747	.2979	2.4964
C	Anonymity	.2664	.3632	.2310	.3867	.3556	.3047	.3911	.4366	.3785	3.1138
D	Inadequate Cyber Defense	.2842	.2944	.2801	.2223	.2579	.2162	.3101	.3771	.2753	2.5176
E	Empowered Non-State Actors	.1562	.2117	.2022	.1997	.1448	.1738	.2856	.2867	.2508	1.9115
F	Next Gen Internet: IPv6	.2274	.2305	.2765	.2462	.1947	.1295	.2427	.2740	.2374	2.0589
G	Best Mil Doctrine: Sun Tzu	.2420	.2749	.2329	.3201	.2397	.1712	.1999	.3555	.2550	2.2912
H	Cyber Attack Deterrence	.1386	.1906	.1821	.2038	.1884	.1304	.2063	.1687	.2289	1.6378
I	Cyber Arms Control	.1317	.1543	.1755	.1937	.1791	.1242	.1961	.2482	.1290	1.5318
	Indirect Influence	1.8572	2.2591	2.1287	2.4694	2.1772	1.7220	2.4797	2.9014	2.3813	

Figure 11. "Total Influence" Matrix *T*.

The indirect influences not only transform the matrix, but also transform our understanding of the nature of the system. Indirect influences are "feedback" influences, which allow each factor to influence every other factor in the system, and over time, to influence even itself.

460 The DEMATEL formula here is T=D * (E-D)^-1, where E is the identity matrix.

Analyzing Total Influence

Based on DEMATEL-calculated indirect influences, Fig. 12 reveals a more complete picture of cause and effect, based on the "total influence" of each factor within the system.

Factor	Direct Influence Index	Indirect Influence Index	Total Influence ***
Anonymity	3.1138	2.1287	5.2425
Inadequate Cyber Defense	2.5176	2.4694	4.9870
Best Mil Doctrine: Sun Tzu	2.2912	2.4797	4.7709
Asymmetry	2.4964	2.2591	4.7555
IT Vulnerabilities	2.8170	1.8572	4.6742
Cyber Attack Deterrence	1.6378	2.9014	4.5392
Empowered Non-State Actors	1.9115	2.1772	4.0887
Cyber Arms Control	1.5318	2.3813	3.9131
Next Gen Internet: IPv6	2.0589	1.7220	3.7809

Figure 12. Initial Total Influence Index.

The combined direct and indirect "total influence" calculation yields an alternative ranking of the factors. Here, the top four are the same factors identified in the causal loop diagram as having the highest number of very influential relationships with other factors, regardless of whether the influence was given or received.

Anonymity is still the most important factor in the system. However, the addition of indirect influence scores reorders other factors in the list. Inadequate cyber defense and military doctrine surpassed IT vulnerabilities and asymmetry in importance (compared to Fig. 6), while deterrence and arms control gained influence at the expense of non-state actors and IPv6.

The final step of this DEMATEL analysis subtracts the indirect influences from the direct influences in Fig. 12 to create a final normalized total influence index, which is shown in Fig. 13.

	DEMATEL Normalized "Total Influence" Index	Score
1	Anonymity	.9851
2	IT Vulnerabilities	.9598
3	Next Gen Internet: IPv6	.3369
4	Asymmetry	.2373
5	Inadequate Cyber Defense	.0481
6	Best Mil Doctrine: Sun Tzu	-.1886
7	Empowered Non-State Actors	-.2654
8	Cyber Arms Control	-.8496
9	Cyber Attack Deterrence	-1.2636

Figure 13. Final Total Influence Index.

After this final calculation, the overall ranking by factor returns closer to the original direct influence ranking in Fig. 6. In fact, the order of the cyber attack advantages is unchanged, as seen in Fig. 14.

BEFORE		AFTER
1. Anonymity	→	1. Anonymity
2. IT Vulnerabilities	→	2. IT Vulnerabilities
3. Asymmetry	→	3. Asymmetry
4. Inadequate Cyber Defense	→	4. Inadequate Cyber Defense
5. Empowered Non-State Actors	→	5. Empowered Non-State Actors

Figure 14. Cyber Attack Advantage Summary.

However, there is now a much larger statistical gap between the two most important factors, anonymity and IT vulnerabilities, and the third and fourth place cyber attack advantages, asymmetry and inadequate cyber defense. Non-state actors received a negative overall score in the final index, which indicates that this concept is a net receiver, and not provider, of influence in the system of strategic cyber security today.

The movement of the mitigation strategies in the final index is much more striking. Fig. 15 reveals that all four strategies moved in the list, especially IPv6, which was

the only factor in the system to move more than one place in the overall ranking order.

BEFORE		AFTER	
1.	Doctrine: Sun Tzu	1.	Next Gen Net: IPv6
2.	Next Gen Net: IPv6	2.	Doctrine: Sun Tzu
3.	Deterrence	3.	Arms Control
4.	Arms Control	4.	Deterrence

Figure 15. Mitigation Strategy Summary.

Following the final DEMATEL "total influence" calculation, IPv6 rose to the third-highest factor in strategic cyber security, behind only anonymity and IT vulnerabilities. Fig. 16 summarizes the factor rankings, before and after the inclusion of indirect influence scoring.

Anonymity	30	Anonymity	.9851
IT Vulnerabilities	26	IT Vulnerabilities	.9598
Asymmetry	24	Next Gen Net: IPv6	.3369
Inadequate Cyber Defense	23	Asymmetry	.2373
Doctrine: Sun Tzu	21	Inadequate Cyber Defense	.0481
Empowered Non-State Actors	18	Doctrine: Sun Tzu	-.1886
Next Gen Net: IPv6	18	Empowered Non-State Actors	-.2654
Deterrence	15	Arms Control	-.8496
Arms Control	14	Deterrence	-1.2636

Figure 16. DEMATEL Indirect Influence Summary.

This research suggests that IPv6 has the potential to be a more influential factor in strategic cyber security than three current cyber attack advantages, including asymmetry and inadequate cyber defense. This result is the most significant revelation in this study.

DEMATEL analysis highlights two powerful IPv6 attributes. First, IPv6 is extremely resistant to outside influence, so it is more "reliable" than other factors in the system. Second, IPv6 influences the single most powerful cyber attack advantage, anonym-

ity, at a "very high" level. These factors combine, via indirect influence calculations, to radiate the impact of IPv6 throughout the system and to magnify its importance.

Thus, for decision makers, this research suggests that IPv6 is currently the single most efficient way to change the dynamics of strategic cyber security in favor of cyber defense.

Fig. 17 is a modified causal loop diagram which specifically highlights the significant influence relationship between IPv6 and the rest of the system.

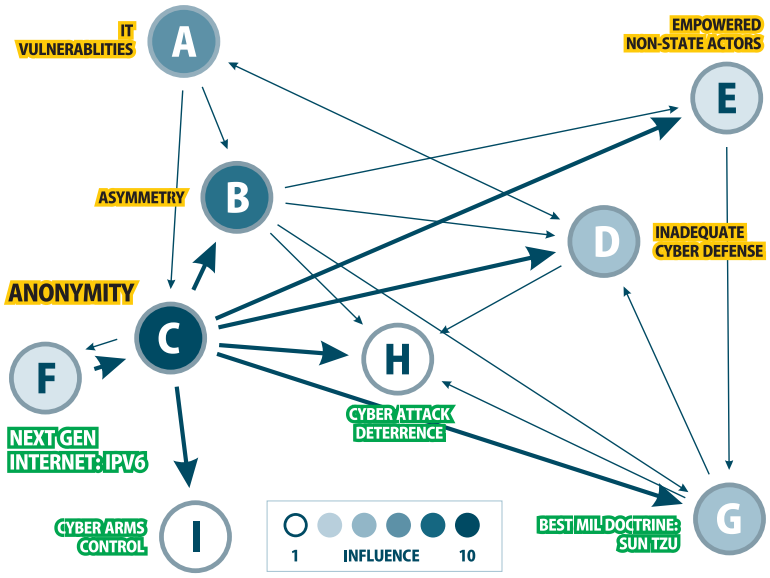

Figure 17. Causal Loop Diagram: IPv6 System Impact.

All three other mitigation strategies received negative scores in the final index (Fig. 13), which means they are net receivers, and not providers, of influence in the system. The second place mitigation strategy is the application of the world's best military doctrine, *Art of War*, to cyber conflict. It is the only other mitigation strategy to finish ahead of even one cyber attack advantage. Cyber arms control and deterrence remain at the bottom of the list, for reasons cited earlier in this book.

In summary, this analysis suggests that, even beyond the four cyber attack mitigation strategies evaluated by the author, decision makers could prioritize their investment in other mitigation strategies by category, according to the following formula.

1. Technical
2. Military
3. Political

A technology-centric approach has a greater DEMATEL-calculated influence on the system of strategic cyber security due in part to the fact that it is more reliable than counting on a human-dependent approach – especially when politics come into play. Thus, IPv6 finished first in this list of strategies, and arms control (a hybrid political/technical approach) moved ahead of deterrence (which relies only on political/military factors) in the final calculation.

V. CONCLUSION

11. RESEARCH CONTRIBUTIONS

In the post-World War II era, cyber security has evolved from a technical discipline to a strategic concept. The power of the Internet, our growing dependence upon it, and the disruptive capability of cyber attackers now threaten national and international security.

The nature of a security threat has not changed, but the Internet provides a new delivery mechanism that can increase the speed, scale, and power of an attack. National critical infrastructures are now at risk – not only during war, but also in times of peace. As a consequence, all future political and military conflicts will have a cyber dimension, whose size and impact are difficult to predict.

World leaders must address the threat of strategic cyber attacks with strategic responses in favor of cyber defense. In this book, the author examines four strategies that nation-states will likely adopt to mitigate the cyber attack threat: deterrence, arms control, doctrine, and technology.

Cyber attack deterrence lacks credibility because hacker skills are easy to acquire, and because attackers are often able to conduct high-asymmetry attacks even while remaining anonymous to their victims.

Cyber arms control appears unlikely, because cyberspace is too big to inspect, and malicious code is even hard to define. However, political will, perhaps in the wake of a future cyber attack, could change the status quo.

The world's best military doctrine, *Art of War*, is more helpful than the first two strategies, but there are at least ten distinctive aspects of the cyber battlefield, none of which fits easily into Sun Tzu's paradigm.

IPv6 answers some of our current security problems, but unfortunately it also creates new problems, including a necessarily long and dangerous transition phase.

However, in spite of the shortcomings of IPv6, the DEMATEL method clearly shows that among the four examined mitigation strategies, IPv6 is the most likely to have a tangible impact on reducing the key advantages of a cyber attacker, and thus it is the most likely strategy to improve a nation's strategic cyber defense posture. The simple reason is that it can reduce the most influential advantage of a cyber attacker, anonymity, and it does so with a higher degree of reliability than the other factors

in this research. Thus, the influence of IPv6 grows over time and impacts all other factors in strategic cyber security.

DEMATEL provided a way to analyze the four proposed mitigation strategies with scientific rigor. It calculated specific levels of influence for each key concept identified, and it created a causal loop diagram of the system they comprise. Finally, it calculated the most efficient way – among the four strategies in question – to reduce the threat of strategic cyber attack.

The contributions of this book are summarized as follows:

- an argument that computer security has evolved from a technical discipline to a strategic concept;
- the evaluation of four distinct strategic approaches to mitigate the cyber attack threat and to improve a nation's cyber defense posture;
- the use of the Decision Making Trial and Evaluation Laboratory (DEMATEL) to analyze this book's key concepts; and
- the recommendation to policy makers of IPv6 as the most efficient of the four cyber defense strategies.

Suggestions for Future Research

The DEMATEL method has helped to clarify the landscape of strategic cyber security. The author believes that DEMATEL could also be used to examine other outstanding problems related to cyber security. Here are three possibilities:

Can a cyber attack be an act of war?[461] The dynamic nature of cyberspace makes it difficult to predict the next cyber attack, or how serious it could be. An effects-based approach seems inevitable: if the level of human suffering or economic damage is high enough, national leaders will retaliate. This applies both to government and private sector critical infrastructures. A key challenge for national security planners is that the hacker tools and techniques required for cyber espionage are often the same as for cyber attack.[462] The difference lies in motivation: does the hacker desire merely to steal information, or is the attack a prelude to war?

Can we solve the attribution problem? Smart hackers exploit the international, maze-like architecture of the Internet to conduct anonymous or deniable cyber at-

461 More precisely, the question may be whether a cyber attack could be considered an "armed attack" as specified by the UN Charter.

462 These may be differentiated by the terms computer network exploitation (CNE) and computer network attack (CNA).

tacks. The trail of evidence often runs through countries with which the victim's government has poor diplomatic relations or no law enforcement cooperation, and cyber investigations typically end at a hacked, abandoned computer, where the trail goes cold. This dynamic encourages "false flagging" operations – where the attacker tries to pin the blame on a third party – and creates an environment in which even terrorists can find a home on the Internet.[463] Solving the attribution problem will require harmonizing cyber crime laws, improving cyber defense methods, and generating the political will to share evidence and intelligence.

Can we shift the advantage to cyber defense? Hackers today have enormous advantages over cyber defenders, including anonymity and asymmetry. In fact, if there is a future war between major world powers, a significant degree of the fighting may take place in cyberspace, and the first victim of the conflict could even be the Internet itself. To shift the balance, cyber defenders require a higher level of trust in hardware and software,[464] improved performance metrics for defense strategies, and the ability to realistically model the hacker threat in a laboratory. Because it is impossible to eliminate all malicious code from a network, cyber defenders need better ways to neutralize what they cannot find. Governments could also require Internet Service Providers (ISP) to play a more helpful role in preventing the spread of malware.

463 Gray & Head, 2009.

464 Supply chain subversion, i.e. inserting malicious code in the design or production phase of product development, can be almost impossible to detect by the end user.

VI. BIBLIOGRAPHY

"53/70: Developments in the field of information and telecommunications in the context of international security," (4 Jan 1999) United Nations General Assembly Resolution: Fifty-Third Session, Agenda Item 63.

Acoca, B. (Jul 2008) "Online identity theft," *The OECD Observer*, Organisation for Economic Cooperation and Development, 268, 12.

"Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation," (2010) NATO website: **www.nato.int**.

Adams, J. (2001) "Virtual Defense," *Foreign Affairs* 80(3) 98-112.

"Advisory 01-009, Increased Internet Attacks against U.S. Web Sites and Mail Servers Possible in Early May," (26 Apr 2001) Federal Bureau of Investigation (FBI) National Infrastructure Protection Center (NIPC).

"Air Force Association; Utah's Team Doolittle Wins CyberPatriot II in Orlando," (10 Mar 2010) *Defense & Aerospace Business*, 42.

Aitoro, J.R. (2 Oct 2009) "Terrorists nearing ability to launch big cyberattacks against U.S." *NextGov*: **www.nextgov.com**.

Allen, P.D. & Demchek, C.C. (Mar-Apr 2003) "The Cycle of Cyber Conflict," *Military Review*.

Anonymous. (28 Mar 2009) "Thai cybercrime law denounced as 'threat to freedom'." *Bangkok Post* website, Bangkok, Thailand in English, reported by *BBC* Monitoring Asia Pacific (29 Mar 2009).

Arquilla, J. & Ronfeldt, D. (Apr 1993) "Cyberwar is Coming!" *Comparative Strategy* 12(2) 141-165.

Barnes, J.E. (28 Nov 2008) "Pentagon computer networks attacked," *Los Angeles Times*.

Barrera, D., Wurster, G., & van Oorschot, P.C. (14 Sep 2010) "Back to the Future: Revisiting IPv6 Privacy Extensions," Carleton University School of Computer Science, Ottawa, ON, Canada.

"Belarus," *Press Reference*: **www.pressreference.com/A-Be/Belarus**.

Bliss, J. (23 Feb 2010) "U.S. Unprepared for 'Cyber War', Former Top Spy Official Says," *Bloomberg Businessweek*.

Brodie, B. (1946) *THE ABSOLUTE WEAPON: Atomic Power and World Order*. New York: Harcourt, Brace and Co.

Bullough, O. (15 Nov 2002) "Russians Wage Cyber War on Chechen Websites," *Reuters*.

Caterinicchia, D. (12 May 2003) "Air Force wins cyber exercise," *Federal Computer Week* 17(14) 37.

Chan, W.H. (25 Sep 2006) "Cyber exercise shows lack of interagency coordination," *Federal Computer Week* 20(33) 61.

Chen, T. & Robert, J-M. (2004) "The Evolution of Viruses and Worms," *Statistical Methods in Computer Security*, William W.S. Chen (Ed), (NY: CRC Press) Ch.16, 265-286.

Churchman, D. (2005) *Why we fight: theories of human aggression and conflict* (MD: UP of America) Ch.2, 16.

Cody, E. (13 Sep 2007) "Chinese Official Accuses Nations of Hacking," *Washington Post*.

Cole, E. (2002) *Hackers Beware* (London: New Riders) 727.

Cole, L.A. (1996) "Countering Chem-Bio Terrorism: Limited Possibilities," *Politics and the Life Sciences* 15(2) 196.

"Common Vulnerabilities and Exposures List," The MITRE Corporation: **http://cve.mitre.org/**.

"Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land," (18 Oct 1907) The Hague, International Committee of the Red Cross.

Crampton, T. (19 Mar 2006) "Innovation may lower Net users' privacy," *The New York Times*.

"Cyber Command's strategy becomes more clear," (22 Mar 2011) *Federal Computer Week*, written by the Defense Systems Staff.

"Cyber War: Sabotaging the System," (8 Nov 2009) CBS: *60 Minutes*.

Dawson, R. (2003) *Living Networks: Leading Your Company, Customers, and Partners in the Hyper-Connected Economy*, Ch.7: "The Flow Economy: Opportunities and Risks in the New Convergence," (New Jersey: Prentice Hall) 141-168.

Denning, D.E. (2002) "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," *Networks and Netwars: the Future of Terror, Crime, and Militancy*, Arquilla, J. & Ronfeldt, D. (Eds.) (RAND Corporation) Ch.8, 239-288.

Derene, G. (2009) "Weapon of Mass Disruption," *Popular Mechanics* 186(4) 76.

Divis, D.A. (9 Mar 2005) "Protection not in place for electric WMD," *UPI*.

Dobbs, M. (24 Oct 2001) "Online Agitators Breaching Barriers in Mideast: London-Based Saudi Dissidents and Fugitives Find Ways Around Government Censorship," *Washington Post*.

"Doctoring photos of Egypt's Hosni Mubarak," (21 Sep 2010) *Economist*.

Dytczak, M. & Ginda, G. (2010) "Common Input Data Structure for Multiple MADA Methods Application for Objects Evaluation in Civil Engineering." *The 10th International Conference "Modern Building Materials, Structures and Techniques"* (Vilnius Gediminas Technical University Publishing House "Technika") 399–402.

Cody, E. (13 Sep 2007) "Chinese Official Accuses Nations of Hacking," *Washington Post*.

Eichin M.W. & Rochlis, J.A. (1989) "With Microscope and Tweezers: an Analysis of the Internet Virus of November 1988," *IEEE Computer Society Symposium on Security and Privacy* 326-343.

"Espionage Report: Merkel's China Visit Marred by Hacking Allegations," (27 Aug 2007) *Spiegel*.

Essex, D. (31 Jan 2008) "IPv6 in Japan," *Federal Computer Week*.

"Evidence Mounts of Pro-Serbian Internet Attack on NATO Countries," (17 Apr 1999) *mi2g*: **www.mi2g.com**.

Falkenrath, R.A. (26 Jan 2011) "From Bullets to Megabytes," *The New York Times*.

Freiling, F.C., Holz, T. & Wicherski, G. "Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks," (2005) De Capitani di Vimercati, S. et al (Eds.) ESORICS 2005, Springer: LNCS 3679, 319-335.

Fulghum, D.A. (2006) "Redefining Victory," *Aviation Week & Space Technology* 165(10) 58.

Fulghum, D.A., Wall, R. & Butler, A. (26 Nov 2007) "Cyber-Combat's First Shot," *Aviation Week & Space Technology* 167(21) 28.

Gabus, A., & Fontela, E. (1973) "Perceptions of the World Problematique: Communication Procedure, Communicating with those Bearing Collective Responsibility," DEMATEL Report No. 1 (Geneva: Battelle Geneva Research Centre).

Gabus, A., & Fontela, E. (1972) "World Problems an Invitation to Further Thought within the Framework of DEMATEL," (Geneva: Battelle Geneva Research Centre).

Gardner, F. (10 May 2000) "Saudis 'defeating' internet porn," *BBC News Online*.

Gavi, S. (24 Nov 1999) "Crossing Censorship Boundaries," The Middle East Online, Online Journalism Review (Modified: 4 Apr 2002).

Geers K. (2010) "A Brief Introduction to Cyber Warfare," *Common Defense Quarterly* (Spring) 16-17.

Geers K. (2010b) "The challenge of cyber attack deterrence," *Computer Law and Security Review* 26(3) 298-303.

Geers, K. & Feaver, P. (2004) "Cyber Jihad and the Globalization of Warfare," *DEF CON, Black Hat*.

Geers K. (2009) "The Cyber Threat to National Critical Infrastructures: Beyond Theory," *The Information Security Journal: A Global Perspective* 18(1) 1-7. Re-printed (2010) in *Journal of Digital Forensic Practice* 3(2) 124-130.

Geers K. (2010c) "Cyber Weapons Convention," *Computer Law and Security Review* 26(5) 547-551.

Geers K. (2008) "Cyberspace and the Changing Nature of Warfare," *Hakin9* E-Book, 19(3) No. 6, *SC Magazine* (27 AUG 08), *Black Hat* 1-12.

Geers K. (2011) "Demystifying Cyber Warfare," forthcoming in *per Concordiam* 1-6.

Geers K. (2011) "From Cambridge to Lisbon: the quest for strategic cyber defense," in peer-review at *Journal of Homeland Security and Emergency Management* 1-16.

Geers K. (2007a) "Greetz from Room 101," *DEF CON*, *Black Hat* 1-24.

Geers, K. (2005) "Hacking in a Foreign Language: a Network Security Guide to Russia," *DEF CON*, *Black Hat*.

Geers, K. & Eisen, A. (2007) "IPv6: World Update," *ICIW 2007: Proceedings of the 2nd International Conference on Information Warfare and Security* 85-94.

Geers K. (2010) "Live Fire Exercise: Preparing for Cyber War," *Journal of Homeland Security and Emergency Management* 7(1) 1-16.

Geers K. (9 Feb 2011) "Sun Tzu and Cyber War," *Cooperative Cyber Defence Centre of Excellence* 1-23.

Geers K. & Temmingh, R. (2009) "Virtual Plots, Real Revolution," *The Virtual Battlefield: Perspectives on Cyber Warfare*, Czosseck, C. & Geers, K. (Eds) (Amsterdam: IOS Press) 294-301.

Gerth, J. & Risen, J. (2 May 1999) "1998 Report Told of Lab Breaches and China Threat," *The New York Times*.

Gibbs, W.W. (2000) "Red Team versus the Agents," *Scientific American* 283(6) 20, 24.

Giles, L. See Sun Tzu, below.

Glendinning, L. (10 May 2006) "Briton faces extradition for 'biggest ever military hack'," *Times Online*.

Goble, P. (9 Oct 1999) "Russia: analysis from Washington: a real battle on the virtual front," *Radio Free Europe/Radio Liberty*.

Godara, V. (2010) *Strategic Pervasive Computing Applications: Emerging Trends* (IGI Global) 39-40.

Golding, D. (28 Feb 2006) "Do we really need to have IPv6 when Nat conserves address space and aids security?" *Computer Weekly*.

Goldstein, E. (1 Jul 1999) "The Internet in the Mideast and North Africa: Free Expression and Censorship," Human Rights Watch.

Gomes, L. (31 Mar 2003) "How high-tech games can fail to simulate what happens in war," *Wall Street Journal*.

Gorbachev, M. & Pfirter, R. (16 Jun 2009) "Disarmament lessons from the Chemical Weapons Convention," *Bulletin of the Atomic Scientists*.

Gorman, S. (17 Aug 2009b) "Cyber Attacks on Georgia Used Facebook, Twitter, Stolen IDs," *The Wall Street Journal*.

Gorman, S. (7 May 2009a) "FAA's Air-Traffic Networks Breached by Hackers," *The Wall Street Journal*.

Gorman, S. (23 Mar 2010) "U.S. Aims to Bolster Overseas Fight Against Cybercrime," *The Wall Street Journal*.

Gorman, S., Cole, A. & Dreazen, Y. (21 Apr 2009) "Computer Spies Breach Fighter-Jet Project," *The Wall Street Journal*.

"Government-Imposed Filtering Schemes Violate the Right to Free Expression," (2000) Human Rights Watch.

Graham, B. (8 Nov 1999) "Military Grappling with Guidelines for Cyber Warfare: Questions Prevented Use on Yugoslavia," *The Washington Post*.

Gray, D.H. & Head, A. (2009) "The importance of the internet to the post-modern terrorist and its role as a form of safe haven," *European Journal of Scientific Research* 25(3) 396-404.

Grossetete, P., Popoviciu, C. & Wettling, F. (2008) *Global IPv6 Strategies: From Business Analysis to Operational Planning* (Indianapolis: Cisco Press) 195.

Hagen, S. (2002) *IPv6 Essentials* (CA: O'Reilly Media, Inc.) 97.

Handbook for Bloggers and Cyber-Dissidents (March 2008) Reporters Without Borders: **http://en.rsf.org/**.

Hess, P. (29 Oct 2002) "China prevented repeat cyber attack on US," *UPI*.

"How Users can Protect their Rights to Privacy and Anonymity," (1999) Human Rights Watch.

Hu, A.H., Hsu, C-W & Chen, S-H. (2010) "Incorporating carbon management into supplier selection in the green supply chain: Evidence from an electronics manufacturer in Taiwan."

"Human rights investigators needed to investigate crackdown on journalists," (15 March 2011) Reporters Without Borders.

Huntley, W.L. (2009) "Abandoning Disarmament? The New Nuclear Nonproliferation Paradigms," *The Challenge of Abolishing Nuclear Weapons*, Krieger D. (Ed.) (New Jersey: Transaction Publishers).

"International cyber exercise takes place in Tajikistan," (6 Aug 2009) *Avesta* website, Dushanbe, Tajikistan (reported by *BBC* Monitoring Central Asia).

"The Internet and Elections: The 2006 Presidential Election in Belarus (and its implications)," (April 2006) OpenNet Initiative: Internet Watch.

"Israel lobby group hacked," (3 Nov 2000) *BBC News*.

Jafari, M., Amiri, R.H. & Bourouni, A. (2008) "An Interpretive Approach to Drawing Causal Loop Diagrams," Department of Industrial Engineering, Iran University of Science and Technology (IUST).

Joch, A. (28 Aug 2006) "Terrorists brandish tech sword, too," *Federal Computer Week*.

Jolly, D. (31 Jul 2009) "In French Inquiry, a Glimpse at Corporate Spying," *The New York Times*.

Keizer, G. (11 Aug 2008) "Cyber Attacks Knock out Georgia's Internet Presence," *Computerworld*.

Keizer, G. (28 Jan 2009) "Russian 'cyber militia' knocks Kyrgyzstan offline," *Computerworld*.

Kelly, J. (27 Jan 2011) "The piece of paper that fooled Hitler," *BBC News Magazine*.

Kennicott, P. (23 Sep 2005) "With Simple Tools, Activists in Belarus Build a Movement," *Washington Post*.

Kirk, J. (30 Oct 2009) "Europe moving slow on IPv6 deployment," IDG News Service.

Krekel, B. (9 Oct 2009) "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" (Northrop Grumman Corporation: prepared for *The US-China Economic and Security Review Commission*).

Lam, F., Beekey, M., & Cayo, K. (2003) "Can you hack it?" *Security Management* 47(2) 83.

Lawlor, M. (2004) "Information Systems See Red," *Signal* 58(6) 47.

Lee, J.S. (19 Nov 2001) "Companies Compete to Provide Saudi Internet Veil," *The New York Times*.

Lee, M. (10 May 2006) "Who is Gary McKinnon?" *ABC News*.

Lewis, J.A. (Dec 2002) "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," Center for Strategic and International Studies (CSIS).

Lewis, J.A. (8 Dec 2008) "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies (CSIS).

Lewis, J.A. (11 Mar 2010) "The Cyber War Has Not Begun," Center for Strategic and International Studies (CSIS).

Libicki, M.C. (2009) "Sub Rosa Cyber War," *The Virtual Battlefield: Perspectives on Cyber Warfare*, Czosseck, C. & Geers, K. (Eds) (Amsterdam: IOS Press) 53-65.

Lynn, W.J. (2010) "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89(5) 97-108.

The Manual of the Law of Armed Conflict (2004) Section 2.2 (Military Necessity), United Kingdom: Ministry of Defence (Oxford: OUP).

Montalbano, E. (29 Sep 2010) "White House Sets IPv6 Transition Deadlines," *InformationWeek*.

Markoff, J. & Kramer, A.E. (13 Dec 2009a) "In Shift, U.S. Talks to Russia on Internet Security," *The New York Times*.

Markoff, J. & Kramer, A.E. (27 Jun 2009b) "U.S. and Russia Differ on a Treaty for Cyberspace," *The New York Times*.

Matthews, J. (19 Dec 2000) "SafeWeb Doubles Usage, Blocked by Saudis," Internetnews: **www.internetnews.com**.

Mayor, A. (2008) *Greek Fire, Poison Arrows, and Scorpion Bombs: Biological & Chemical Warfare in the Ancient World* (Overlook TP).

McConnell, M. (28 Feb 2010) "Mike McConnell on how to win the cyber-war we're losing," *Washington Post*.

Meier, O. (2007) "The Chemical Weapons Convention at 10: An Interview with OPCW Director-General Rogelio Pfirter," *Arms Control Today* 37(3) 14.

Meller, P. (27 May 2008) "European Commission Urges Rapid Adoption of IPv6," IDG News Service.

Meserve, J. (26 Sep 2007) "Sources: Staged cyber attack reveals vulnerability in power grid," Cable News Network.

Milhollin, G. & Lincy, V. (29 Sep 2009) "Lifting Iran's Nuclear Veil," *The New York Times*.

Miller, E. K. (1989) "The computer revolution," *IEEE Potentials* 8(2) 27-31.

Mishra, S. (2003) "Network Centric Warfare in the Context of Operation Iraqi Freedom," *Strategic Analysis* 27(4) 546-562.

Moghaddam, N.B., Sahafzadeh, M., Alavijeh, A.S., Yousefdehi, H. & Hosseini, S.H. (2010) "Strategic Environment Analysis Using DEMATEL Method Through Systematic Approach: Case Study of an Energy Research Institute in Iran," *Management Science and Engineering* 4(4) 95-105.

"Monthly Malware Statistics: May 2009," (2009) Kaspersky Lab: **www.kaspersky.com**.

Montagne, R. "Reuters Retracts Altered Beirut Photo," (8 Aug 2006) National Public Radio: **www.npr.org**.

"Moore's Law," Intel Corporation, **www.intel.com/technology/mooreslaw/**.

Morgenthau, H.J. (1948) *Politics among nations: the struggle for power and peace* (A. A. Knopf) 440.

Mostyn, M.M. (2000) "The need for regulating anonymous remailers," *International Review of Law, Computers & Technology* 14(1) 79.

Nakashima, E. & Mufson, S. (19 Jan 2008) "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," *Washington Post*.

"NATO 2020: Assured Security, Dynamic Engagement: Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO," (17 May 2010) NATO Public Diplomacy Division: **www.nato.int**.

Neumann, P.G. (1998) "Protecting the Infrastructures," *Communications of the ACM* 41(1) 128.

Newmark, J. (2001) "Chemical warfare agents: A primer," *Military Medicine* 166(12) 9.

Nizza, M. & Lyons, P.J. (10 July 2008) "In an Iranian Image, a Missile Too Many," *New York Times*.

"The North Atlantic Treaty," (4 April 1949) Washington D.C., NATO website: **www.nato.int/**.

Oberdorfer Nyberg, A. (2004) "Is All Speech Local? Balancing Conflicting Free Speech Principles on the Internet," *Georgetown Law Journal* 92(3) 663-689.

Oppy, G. & Dowe, D. (2008) "The Turing Test," *The Stanford Encyclopedia of Philosophy* (*SEP*): **http://plato.stanford.edu/**.

Orr, R. (2 Aug 2007) "Computer voting machines on trial," *Knight Ridder Tribune Business News*.

Orton, M. (14 Jan 2009) "Air Force remains committed to unmanned aircraft systems," United States Air Force website: **www.af.mil**.

Orwell, G. (2003) *Nineteen Eighty-Four* (London: Plume).

"Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," (Aug 2009) U.S. Cyber Consequences Unit.

Pavlyuchenko, F. (2009) "Belarus in the Context of European Cyber Security," *The Virtual Battlefield: Perspectives on Cyber Warfare*, Czosseck, C. & Geers, K. (Eds) (Amsterdam: IOS Press) 156-162. Research paper written in Russian, translated to English by Kenneth Geers.

Page, B. (11 Nov 2000) "Pro-Palestinian Hackers Threaten AT&T," *TechWeb News*.

Parks, R.C. & Duggan, D.P. (5-6 June, 2001) "Principles of Cyber-warfare," *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, United States Military Academy, West Point, NY.

Pendall, D.W. (2004) "Effects-Based Operations and the Exercise of National Power," *Military Review* 84(1) 20-31.

Piscitello, D. (11 May 2010) "Conficker Summary and Review," ICANN.

Popoviciu, C., Levy-Abegnoli, E. & Grossetete, P. (2006) *Deploying IPv6 Networks* (Cisco Press) 248.

Preimesberger, C. (2006) "Plugging Holes," *eWeek* 23(35) 22.

"The President's News Conference with President Boris Yeltsin of Russia in Helsinki," (21 Mar 1997) The American Presidency Project, UC Santa Barbara: **www.presidency.ucsb.edu**.

Ramaswamy, V.M. (Oct 2006) "Identity-Theft Toolkit," *The CPA Journal* 76(10) 66.

Rarick, C.A. (Winter 1996) "Ancient Chinese advice for modern business strategists," *S.A.M. Advanced Management Journal* 61(1) 42.

"Regime steps up censorship and online disruption to block protests," (15 February 2011) Reporters Without Borders.

"Remarks by the President on Securing our Nation's Cyber Infrastructure," (29 May 2009) The White House: Office of the Press Secretary: **www.whitehouse.gov**.

"Renumbering the net," (10 Mar 2011) *The Economist*.

Rona, T.P. (1976) *Weapon Systems and Information War* (WA: The Boeing Corporation).

Rose, A. (25 Oct 1999) "China studies the art of cyber-war," *National Post*.

Rowland, J.B. (2002) "The role of automated detection in reducing cyber fraud," *The Journal of Equipment Lease Financing* 20(1) 2.

Sartori, L. (1983) "The weapons tutorial-Part five: When the bomb falls," *Bulletin of the Atomic Scientists* 39(6) 40-47.

Saltzer, J.H. & Schroeder, M.D. (1975) "The protection of information in computer systems," *Proceedings of the IEEE* 63(9) 1278-1308.

"Saudi Arabia to double number of banned sites," (01 May 2001) *The China Post*.

"Saudi Arabian Response and Reasoning," Virginia Tech Department of Computer Science Digital Library, Computer Science 3604: Professionalism in Computing.

Sawyer, R.D. (1994) *Sun Tzu: Art of War* (Oxford: Westview Press).

Saydjari, O.S. (2004) "Cyber Defense: Art to Science," *Communications of the ACM* 47(3) 53-57.

Shimeall, T., Williams, P. & Dunlevy, C. (Winter 2001/2002) "Countering cyber war," *NATO Review* 16-18.

Shultz, G.P., Perry, W.J., Kissinger, H.A., & Nunn, S. (4 Jan 2007) "A World Free of Nuclear Weapons," *The Wall Street Journal*.

Skoudis, E. (2006) *Counter Hack Reloaded: a Step-By-Step Guide to Computer Attacks and Effective Defenses* (NJ: Prentice Hall) 1.

"Smurf IP Denial-of-Service Attacks," (1998) CERT Advisory CA-1998-01.

SNORT Users Manual 2.9.0, (6 Jan 2011) The Snort Project.

"Spain, a week on: An election bombshell," (18 Mar 2004) *The Economist*.

Stoil, R.A. & Goldstein, J. (28 Jun 2006) "One if by Land, Two if by Modem," *The Jerusalem Post*.

Stöcker, C., Neumann, C. & Dörting, T. (18 Jun 2009) "Iran's Twitter Revolution: Ahmadinejad's Fear of the Internet," *Spiegel*.

"Stuxnet may be the work of state-backed hackers," (Sep 2010) *Network Security*, Mansfield-Devine, S. (Ed.) 1-2.

Sun Tzu. (1994) *Sun Tzu on the Art of War: The Oldest Military Treatise in the World*, Project Gutenberg eBook (translated in 1910 by Giles, L.) **www.gutenberg.org/etext/132**.

Thomas, T.L. (2002) "Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?" Fort Leavenworth: Foreign Military Studies Office and (2003) in Chapter 11 of *Russian Military Reform 1992-2002*, Frank Cass Publishers.

"Tracking GhostNet: Investigating a Cyber Espionage Network," (29 Mar 2009) Information Warfare Monitor.

Tran, M. (28 Sep 2007) "Internet access cut off in Burma," *The Guardian*.

United States Strategic Bombing Survey: Summary Report (European War), (30 Sep 1945) United States Government Printing Office, Washington, D.C.

"'USA Today' Website Hacked; Pranksters Mock Bush, Christianity," (11 Jul 2002) *Drudge Report*.

Usher, S. (17 March 2006) "Belarus stifles critical media," *BBC News*.

Van Creveld, M. (1987) *Command in War* (MA: Harvard UP).

Van Riper, P.K. (2006) *Planning for and Applying Military Force: an Examination of Terms* (U.S. Army War College: Strategic Studies Institute).

Verton, D. (2002) *The Hacker Diaries: Confessions of Teenage Hackers* (NY: McGraw-Hill/Osborne).

Verton, D. (2003) "Black ice," *Computerworld* 37(32) 35.

Verton, D. (4 Apr 1999) "Serbs Launch Cyberattack on NATO," *Federal Computer Week*.

Voeux, C. (2 Nov 2006) "Going online in Cuba – Internet under surveillance." Cuba: News from and about Cuba: **http://cuba.blogspot.com**.

Wagner, D. (9 May 2010) "White House sees no cyber attack on Wall Street," *Associated Press*.

Wagstaff, J. (30 Apr 2001) "The Internet could be the site of the next China-U.S. standoff," *The Wall Street Journal*.

Waterman, S. (10 Mar 2008) "DHS stages cyberwar exercise," *UPI*.

Weaver, N., Paxson, V., Staniford, S. & Cunningham, R. (27 Oct 2003) "A taxonomy of computer worms," *Proceedings of the 2003 ACM Workshop on Rapid Malcode (WORM'03)*, Washington, DC, 11-18.

Weisman, R. (13 June 2001) "California Power Grid Hack Underscores Threat to U.S." *Newsfactor*.

Whitaker, B. (26 Feb 2001) "Losing the Saudi cyberwar," *Guardian*.

Whitaker, B. (11 May 2000) "Saudis claim victory in war for control of web," *Guardian*.

"Yugoslavia: Serb Hackers Reportedly Disrupt U.S. Military Computer," (28 Mar 1999) Bosnian Serb News Agency SRNA (reported by *BBC* Monitoring Service, 30 Mar 1999).