SYNGRESS

CYBER WARFARE

Techniques, Tactics and Tools for Security Practitioners
Second Edition

Foreword by
Stephen Northcutt

Jason Andress
Steve Winterfeld

CYBER WARFARE

SECOND EDITION

This page intentionally left blank

CYBER WARFARE

Techniques, Tactics and Tools for Security Practitioners

SECOND EDITION

JASON ANDRESS

STEVE WINTERFELD

LILLIAN ABLON

Technical Editor

Acquiring Editor: *Chris Katsaropoulos*
Editorial Project Manager: *Benjamin Rearick*
Project Manager: *Punithavathy Govindaradjane*
Designer: *Mark Rogers*

Syngress is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA

Library of Congress Cataloging-in-Publication Data
Andress, Jason.
Cyber warfare : techniques, tactics and tools for security practitioners / Jason Andress, Steve Winterfeld. – Second edition.
pages cm
Includes bibliographical references and index.
ISBN 978-0-12-416672-1 (pbk.)
1. Information warfare–Handbooks, manuals, etc. 2. Computer networks–Security measures–Handbooks, manuals, etc. I. Winterfeld, Steve. II. Title. III. Title: Cyberwarfare, techniques, tactics and tools for security practitioners.
U163.A64 2014
355.3′43–dc23

2013034031

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-12-416672-1

Printed and bound in the United States of America
14 15 16 17 18 10 9 8 7 6 5 4 3 2 1

Contents

Acknowledgments

We thank our families and friends for their guidance, support, and fortitude throughout this project. We dedicate this book to those in the security industry who are making the world a better place through efforts like Hackers for Charity (You may have seen their T-shirts—"i hack charities." For more information, go to http://hackersforcharity.org/). To those who are not we say—get engaged!

This page intentionally left blank

Foreword

WHY A BOOK ON CYBER WARFARE IS IMPORTANT

"... it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation," Obama said, adding, "... we're not as prepared as we should be, as a government or as a country" [1].

According to the Director of National Intelligence James Clapper, "The cyber warfare threat facing the United States is increasing in scope and scale and its impact is difficult to overstate" [2]. A variety of educational institutions, both military and civilian, are grappling with the question, "What should we teach each and every one of our students about cybersecurity?" When these students take their places as leaders and officers in the defense of our country, they need to be aware of this persistent threat.

Today's threatscape is constantly changing, adapting to our countermeasures and continuing to successfully pursue various missions ranging from identity theft, to criminal and nation-based corporate espionage, and, in the case of a worm called Stuxnet, to sabotage. Only a decade ago we had kids attacking systems for the thrill of it; then it was criminals attacking identities. Now it appears to be more about social media, ideology, and insider threats. This book provides great graphics for the threatscape and challenges we are facing today.

In May, the Atlantic Wire reported China was winning the cyberwar, in part because they had accessed US physical war plans. Also last week Edward Snowden claimed the United States and Israel co-wrote the Stuxnet worm to damage the Iranian Nuclear program; today, we are still trying to figure out exactly how Stuxnet worked. And while WikiLeaks and Anonymous (the ideology-driven group intent on punishing organizations that did not support WikiLeaks) have been in the news of late, the theft of RSA two-factor authentication intellectual property is especially chilling. If access control fails, everything fails. Identity theft is so commonplace that it is no longer newsworthy. How many people in the United States have had their identity stolen? Many experts say all of them. There is just so much stolen data that the criminals have not yet figured out how to use them all. But they will. Criminal groups are hiring computer scientists to run their cyber-based scams and mine the results. The term *cyber warfare* is becoming part of discussions on national security. Cybersecurity is an issue that can impact us at the personal level as users of the Internet and at the national defense level as an advanced, persistent threat.

WHY SHOULD YOU READ THIS BOOK

Everyone needs to understand the risks to our information so that we can make an informed decision regarding the steps that we might take to secure it.

The Internet connection in your home that you use to talk to friends with Skype, play games, and send email may also be used to conduct crimes, undertake international espionage, and quite possibly fight a new kind of war.

This new Wild West of the Internet matters to each of us at both the personal and national levels. *Cyber Warfare* is focused more on the national level and what the Department of Defense (DoD) has done and is doing.

A week doesn't go by without a story of a cyber attack, hacker group causing a data breach or malcode spreading across the Internet. Cyber Warfare puts the threatscape into context by showing how the threat operates as well as how all the different stories relate to one another.

If you work with the US government, or want to know what the US government is doing to organize and respond to the cyber threat, *Cyber Warfare* lays it out in comprehensive detail. The authors will show you how cyber attacks and defense intersect with each of the classic warfighting domains of land (Army), sea (Navy), air (Air Force), space (Joint, with Air Force in the lead), and cyber (ubiquitous, with US Cyber Command [USCYBERCOM] just getting organized).

Cyber Warfare covers the doctrine being developed today and lays out the tactics, techniques, and procedures of Computer Network Operations (CNO) including attack, defend, and exploit (the military term for reconnaissance or spying), plus the new aspect of social engineering. On a personal note, it is easy to read about social engineering and think "yeah, yeah, yeah," but I, among many others, friended Robin Sage, a fake personality created by a security researcher to see how much data could be collected, on Facebook.

Switching from the "what" to "how" in the later chapters, *Cyber Warfare* considers the "why," as the authors explore the ethics and legal issues of this new battlefield. Then the book defines and analyzes the challenges facing cyberspace. Finally, it looks at trends in this arena.

Cyber Warfare will provide readers with a strong foundational understanding of a threat they see every week in the news. Here is why that matters: In the beginning of this Foreword, I said my head was spinning. Why? Because there is so much new stuff that I can't keep track of? Actually, no. What amazes and scares me is that we are having the same conversations we had 13 years ago when I was chief for information warfare at the Ballistic Missile Defense Organization. Granted, today there are more acronyms, and more money is involved. But none of the fundamental issues have changed. Back then, the Russians were pursing international agreements to treat cyber attacks as strategic weapons. We did not listen, I think, because we thought our technology and techniques were superior. In addition, a lot of people were in denial—"Is this cyber attack stuff really an issue?" And far more people just did not have a clue. If it did not have to do with the Redskins or Cowboys, it could not possibly matter. But we forgot something. We had the most to lose. The United States has more information online than any other country, and that makes us the biggest target. We had an opportunity more than a decade ago to begin the dialog of government–private industry partnerships. We had an opportunity to begin to establish international agreements. We largely squandered those opportunities. Now they have returned. Compelling evidence suggests that there is a cyber threat. We need to educate ourselves, do our part, and encourage our legislators to engage. We need to hold the government accountable to spend our tax dollars wisely in the cyber

warfare realm, not to just throw dollars in the air and hope they will land where they will do some good. *Cyber Warfare* will allow you to educate yourself, to form an opinion on where the nation should be moving and the risks we face if we take no action. More than a decade ago we missed our opportunity to take comprehensive action, and we have paid a terrible price. What are we going to do this time around?

Stephen Northcutt

References

[1] President Barack Obama. Remarks by the president on securing our nation's cyber infrastructure [home page on the Internet]. Washington, DC: The White House, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/; 2010 [accessed 15.02.10].

[2] Allen V. Cyber warfare threats to U.S. are increasing: top spy [home page on the Internet]. New York: Thomson Reuters, http://www.reuters.com/article/2011/02/10/us-usa-intelligence-cyberspace-idUSTRE7194E320110210; 2010 [accessed 15.02.10].

This page intentionally left blank

Introduction

INFORMATION IN THIS CHAPTER

- Book Overview and Key Learning Points
- Book Audience
- How this Book is Organized

BOOK OVERVIEW AND KEY LEARNING POINTS

This book is designed to cover the strategic, operational, and tactical aspects of the conflicts in cyberspace today. The perspectives of the two authors balance the viewpoints of what many are calling cyber warfare today. One comes from a commercial background and the other brings the military viewpoint. The book is designed to help anyone understand the essentials of what is happening today, as well as provide a strong background on the issues we are facing.

This book is unique in that it provides the information in a manner that can be used to establish a strategic cybersecurity vision for an organization, but it is also designed to contribute to the national debate on where cyber is going.

BOOK AUDIENCE

This book will provide a valuable resource to those involved in cyber warfare activities regardless of whether their focus is policy maker, CEO, CISO, doctrinal development, penetration testers, security professionals, network and systems administrators, or college instructors. The information provided on cyber tactics and attacks can also be used to assist in engineering better and more efficient procedures and technical defenses.

Those in management positions will find this information useful, as well, from the standpoint of developing better overall risk management strategies for their organizations. The concepts covered in this book will help determine how to allocate resources and can be used to drive security projects and policies, in order to mitigate some of the larger issues discussed.

HOW THIS BOOK IS ORGANIZED

This book is designed to take the reader through a logical progression for a foundational understanding of today's cyber battlespace, but the content and organization of the topics in this book are built as standalone modules of information. It is not necessary to read the book from front to back or even in any particular order. In the areas where we refer to information

located in other chapters in the book, we have endeavored to point out where the information can be found. The following descriptions will provide an overview of the contents of each chapter:

Chapter 1: What is Cyber Warfare?

In this chapter, we discuss how the concept of what a war means is changing and examine whether we are in a cyber war today. We discuss the differences between conventional and cyber wars and how conventional warfare is a poor standard against which to measure its cyber equivalent. We talk about how holding to the strict definition of warfare being one nation state declaring war on another sovereign nation may no longer be valid and how a cyber war, whether strictly cyber in nature or in combination with traditional war, could lead to an international disaster, changing economies, enabling an increased cyber crime wave, and facilitating unprecedented espionage, and why we need to act now to be prepared for these potential events.

Chapter 2: Cyber Threatscape

This chapter presents an overview of the cyber threatscape. It covers the methodology, tools, and techniques used by the different types of attackers, as well as a review of the key parts of the defensive infrastructure employed to protect our systems. In addition, it discusses the general categories of information that present prime targets for attackers.

Chapter 3: The Cyberspace Battlefield

In this chapter, we study the boundaries of cyber warfare and examine the many different perspectives that are used to define it. We cover the traditional war-fighting domains of land, sea, and air, and space both as they relate to cyber operations and what we can learn from them as cyber becomes more mature as the fifth war-fighting domain. We also review the different threats, the impacts they are having, and what their motivations might be. Finally we examine how acquisition is enabling and fettering cybersecurity.

Chapter 4: Cyber Doctrine

This chapter explores the state of current cyber warfare doctrine on both the nation state and military. We discuss how every country with a dependence on IT infrastructure is developing strategies and capabilities to protect and exercise national power and examine some of the traditional tactics and products that the military needs to adapt to the cyberspace environment. We also cover some of the directives used by federal agencies and governments to guide behavior in this virtual environment. Finally, we look at how organizations are training to both develop new doctrine and execute their current plans.

Chapter 5: Cyber Warriors

In this chapter, we examine who cyber warriors are. As cyber warfare is a rapidly developing field, we cover both the existing forces, and we talk about what might come in the future. We cover what those working in the cyber field presently look like from the standpoint

of education, training, certifications, and experiences and what the differences between those that are selected for traditional warfare and cyber warfare might be. We also discuss the present cyber warfare forces in countries around the globe and what we might need to train the next generation of cyber warriors.

Chapter 6: Logical Weapons

In this chapter, we discuss the various tools that we might use in conducting Computer Network Operations (CNO) and the methods that we might use to defend against an attacker using them. We discuss the tools for reconnaissance, access and privilege escalation, exfiltration, sustaining our connection to a compromised system, assault tools, and obfuscation tools, many of which are free, or have free versions, and are available to the general public.

Chapter 7: Physical Weapons

In this chapter, we discuss the use of physical weapons in cyber warfare. We talk about the intersection of the physical and logical realms and how making changes to either realm can affect the other, sometimes to a disastrous extent. We also talk about infrastructure concerns, primarily those that have to do with the Supervisory Control and Data Acquisition (SCADA) systems that control the various industrial, infrastructure, and facility processes that are in constant use all over the world. In addition, we cover supply chain concerns and the potential consequences of corruption or disruption in the supply chain.

Chapter 8: Psychological Weapons

In this chapter, we cover social engineering and discuss how it can be a dangerous threat vector to all organizations and individuals. We look at this from a military mindset and pull lessons from how they conduct interrogations and conduct counterintelligence. We talk about how the security policies, culture, and training must be reinforced often to insure the work force stays vigilant and how a great technical security infrastructure can be subverted by just going after the people.

Chapter 9: Computer Network Exploitation

In this chapter, we discuss the basics of Computer Network Exploitation (CNE). We explain that exploitation in this context means reconnaissance or espionage, and then discuss how it is conducted. We cover identifying our targets, in the sense of both gleaning information from targets of attacks and identifying targets to be surveilled. We talk about reconnaissance and how it might be used to conduct planning operations for future attacks, including Computer Network Attack (CNA) and Computer Network Defense (CND). We cover the three major divisions of reconnaissance, Open Source Intelligence (OSINT), passive, and Advanced Persistent Threat (APT), and the differences between them. In addition, we go over surveillance tactics and techniques, and how they differ from reconnaissance.

Chapter 10: Computer Network Attack

In this chapter, we discuss Computer Network Attack (CNA). We talk about the different factors involved in cyber warfare, including the physical, logical, and electronic elements of warfare. We also discuss the different phases of the attack process: reconnaissance, scanning, accessing systems, escalating privileges, exfiltrating data, assaulting the system, sustaining our access, and obfuscating any traces that might be left behind. We compare how this parallels and differs from typical hacker attacks.

Chapter 11: Computer Network Defense

In this chapter, we discuss Computer Network Defense (CND). We talk about what exactly it is that we attempt to secure, in the sense of data and information, as well as security awareness and training efforts, in order to mitigate what sometimes is the weakest link in our defenses, this being authorized normal users. We also present some of the different strategies that we recommend be used to defend ourselves against attack.

Chapter 12: Non-State Actors in Computer Network Operations

In this chapter, we discuss the various non-state actors that might take part in cyber warfare, including the place of corporations in cyber warfare, how cyber terrorism comes into play in cyber warfare activities, and how cyber criminal groups are a major consideration in cyber warfare. We also cover the participation of autonomous actors in cyber activities.

Chapter 13: Legal System Impacts

In this chapter, we review the different legal systems across the world and some of the current laws that can impact how cyber warfare is conducted. The importance of these can be found in the overlap with Chapter 1 on the definition of cyber warfare, Chapter 2 on the warfighting domains, Chapter 3 on doctrine, and Chapter 13 on ethics. We look at the laws that impact cyber warfare due to the unique fact that it is the only warfighting domain that must use commercial infrastructure. We discuss the need to balance methods to fight the interconnected cyber crime, espionage, and warfare with the right to privacy. Finally, we dive into the need for digital forensics to support cyber warfare.

Chapter 14: Ethics

In this chapter, we discuss the ethical issues surrounding cyber warfare, such as the Law of Armed Conflict and Just War Theory. Such issues differ significantly from those in conventional warfare due to the potential for cyber attacks to be misattributed. We discuss attacking ethically in cyber war, including issues such as secrecy in attacks, noncombatant immunity, and what constitutes use of force in cyber warfare. We also cover issues that may arise as to the determination or improper determination regarding the specifics of an attack.

Chapter 15: Cyberspace Challenges

We define the thirty key issues that are impacting cybersecurity and map how they should be categorized. We then break them out into levels of difficulty and resources required to solve. We also discuss how they are interrelated. Finally, we look at both who and how they should be addressed, to include rough timelines on when they might be resolved.

Chapter 16: The Future of Cyber War

As we look to what lies ahead we examine the logical evolution based on current cybersecurity trends. We then talk about the most likely and most dangerous course of action for conflicts in the cyber domain. Next, we examine potential impacts from some of the new technologies and problems on the horizon. Finally, we discuss what needs to be done through international interactions.

Appendix: Cyber Timeline

We have also included an appendix with a timeline of the major events that have impacted or driven the conflicts in cyberspace.

CONCLUSION

Writing this book was a true journey. A considerable amount of debate among all those involved in the book took place over what would build the best foundation to address the subject, but in the end a solid balance was struck between the broad perspective and specific practical techniques. The hope is that this book will contribute to the national discussion on both where cyberspace is headed and what role each one of us can play.

This page intentionally left blank

CHAPTER

1

What is Cyber Warfare?

INFORMATION IN THIS CHAPTER

- What is Cyber Warfare?
- Have We Seen a Cyber War?
- Why Cyber Warfare is Important

We are constantly bombarded with news about cyber events today. There are constant headlines: *cybercrime is up, watch out for the latest phishing attack trying to steal our identity, update our antivirus to avoid infection, patch the operating system to avoid a hacker taking control, new zero day attack against smartphones, Facebook privacy compromised, someone took down Twitter*, and now we cannot go for more than a week without hearing about cyber war.

When establishing the boundaries of the battlefield in the physical world it is usually straightforward. When two countries go to war there is a battlefront established between the two armies where active combat occurs. Wars have traditionally been fought over land, and typically on the very land the countries are fighting for but in the current war on terrorism, the reasons and boundaries are less defined, with no set battlefront where the forces clash, and distributed forces conducting guerrilla or asymmetric warfare with no formal rank structure or doctrine.

Still, even in unconventional warfare the two sides operate within the same geographical area; in cyberspace the traditional physical boundaries disappear.

WHAT IS CYBER WARFARE?

Background

We have been reading about cyber acts of aggression for years now. Cliff Stoll first published *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* in 1989 about Soviet Bloc countries breaking into Department of Defense (DoD) sponsored networks. Seven years later we see a very similar storyline from both sides of the hack in

Cyber Warfare, Second Edition
http://dx.doi.org/10.1016/B978-0-12-416672-1.00001-5

Take-Down: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw-By the Man Who Did It by Tsutomu Shimomura and John Markoff with its opposing view in the book *The Fugitive Game: Online with Kevin Mitnick* by Jonathan Littman. Today we see a host of books on crime, hacking, defensive practices, and certification prep guides not to mention cyber plots in fiction books like *The Blue Nowhere* by Jeffrey Deaver, *Debt of Honor* by Tom Clancy, or *The Scorpion's Gate* by Richard A. Clarke.

NOTE

Here are some recent notable mentions around the topic of Cyber showing the national leadership of the U.S. is concerned about this domain:

- President Obama—Talked about cybersecurity in State of Union address and signed PPD-21: Critical Infrastructure Security and Resilience [1].
- Director of National Intelligence James Clapper told Congress that cyberattacks and cyberspying can damage critical infrastructure like power grids. But in prepared testimony, he says advanced cyber-actors like Russia and China are unlikely to launch such attacks unless they are threatened by conflict [2].
- Defense Secretary Leon Panetta has also been a strong advocate for increased governmental grip on the web and in October warned that the U.S. is facing a possible "cyber-Pearl Harbor" by foreign hackers [3].
- Homeland Security Secretary Janet Napolitano issued the warnings Jan 2013, claiming that inaction could result in a "cyber 9/11" attack that could knock out water, electricity and gas, causing destruction similar to that left behind by Hurricane Sandy [3].
- Representative Mike Rogers, a Michigan Republican who leads the House Intelligence Committee, has said foreign intruders "are stealing literally billions" of dollars from companies [2].
- Army General Keith Alexander, head of U.S. Cyber Command and the National Security Agency, called cybercrime "the greatest transfer of wealth in history" [2].
- Chief of Staff of the U.S. Air Force Gen. Mark Welsh III said he worried the investments made in cyber could be disappearing into a "black hole." Welsh will wait until he understands the cyber topic better, he said [4].
- Commander Army Cyber Command Lieutenant General Rhett Hernandez: Army Cyber Command/Second Army said he is tasked to operate and defend all Army networks and prepare for full-spectrum cyber-operations to support our forces worldwide [5].

We also see touches of cyber warfare in the movies starting with *War Games* in 1983 where a kid breaks into a military network and accidently almost starts World War III to *Sneakers* in 1992 where all data encryption is compromised to *Swordfish* 2001 where intelligence agencies use hacking to support their activities to the epic *Die Hard 4: Live Free* or *Die Hard* in 2007 when criminals pose as terrorists and take down the Internet and all the critical infrastructure it supports. There are a lot of great books and movies not mentioned but this sample list points to the evolution of Cyber Warfare into mainstream thinking and how it can be used as a tool to conduct espionage, crime, terror, and warfare.

America's information dominance tools, which helped win the Cold War, have become its Achilles heel of the cyber conflict we are in today. U.S. technology was far ahead of any competitor nation and we outspent them to keep the edge. Today we are more dependent on this technology than ever before, most of which is now available to our partners, competitors, and adversaries. At the same time the cost of entry into this arms race is incredibly low. Furthermore, the benefits of attacking someone far outweigh the dangers. This has led to what many are calling a Cyber War.

Definition for Cyber Warfare

A definition of Cyber Warfare is not easy. In fact definitions for Cyber or Warfare are both under debate. We will start with a simple definition of Cyber or Cyberspace. For the purpose of this chapter, we will frame the definition in the context of military environment.

DoD defines *cyberspace* as the "notional environment in which digitized information is communicated over computer networks" (Figure 1.1) [7]. There is no official definition for just "cyber." When you hear it by itself it could mean cybersecurity, computer network operations, electronic warfare or anything to do with the network. It is important to agree on what it means, for this book it will generally refer to cyberspace and be discussed in terms of computer network operations (attack, defend, and exploit).

The National Military Strategy for Cyberspace Operations defines *cyberspace* as the "domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures" [6].

DoD (Joint Publication 3.0 Joint Operations 17 September 2006 Incorporating Change 2, 22 March 2010) defines *cyberspace* as a "global domain within the information environment. It consists of the interdependent network of information technology infrastructures, including

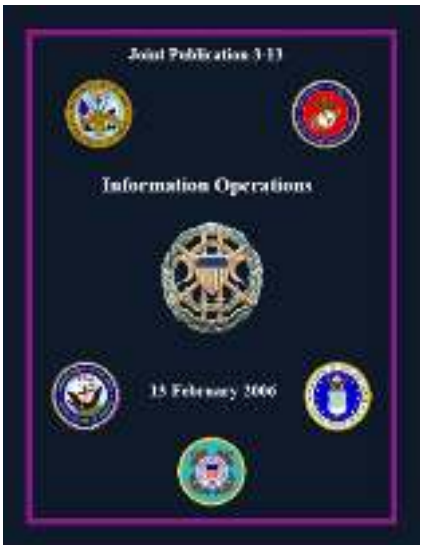

FIGURE 1.1 Cyber or computer network operations falls under this doctrinal manual JP 3-13 information operations [6]. Department of Defense (DoD) joint publication 3-13 information operations 13 February 2006.

the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

Within cyberspace, electronics and the electromagnetic spectrum are used to store, modify, and exchange data via networked systems. Cyberspace operations employ cyberspace capabilities primarily to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid (GIG) [8].

United Nations (UN) defines cyber as "the global system of systems of Internetted computers, communications infrastructures, online conferencing entities, databases and information utilities generally known as the Net." This mostly means the Internet; but the term may also be used to refer to the specific, bounded electronic information environment of a corporation or of a military, government, or other organization [9].

For a definition of warfare we cannot turn to an authoritative source. The UN does not have a definition, so we will default to the two historical standards for military doctrine: *On War*, the exhaustive work documenting tactics during the Napoleonic War period in 1873 and *The Art of War* a more condensed version of how to conduct warfare composed in sixth century BC.

> ON WAR—We shall not enter into any of the abstruse definitions of war used by publicists. We shall keep to the element of the thing itself, to a duel. War is nothing but a duel on an extensive scale. If we would conceive as a unit the countless number of duels which make up a war, we shall do so best by supposing to ourselves two wrestlers. Each strives by physical force to compel the other to submit to his will: his first object is to throw his adversary, and thus to render him incapable of further resistance. War therefore is an act of violence to compel our opponent to fulfill our will [10].
>
> ART OF WAR—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. The art of war, then, is governed by five constant factors, to be taken into account in one's deliberations, when seeking to determine the conditions obtaining in the field. These are: (1) The Moral Law; (2) Heaven; (3) Earth; (4) The Commander; (5) Method and discipline [11].

Are these definitions applicable to what is happening on the Internet today? Can these historical concepts be applied to the virtual world? Is the military perspective the right one to look at this problem through? The answer to all questions is a declarative: YES. That is where this book becomes applicable: to help solidify what cyber warfare means. First there is no governing body to determine what definition we should use, so the definition is normally based on the perspective of the person speaking. Governments, finance companies, Internet providers, international corporations, organizations with a specific cause, and lawyers all give us a different answer. As for historical concepts, there are many that are based on geography which no longer apply, but most principles and practices can be modified to be useful when it comes to the new World Wide Web's Wild West. Finally, we think if we are going to use the term warfare we should use the military perspective but throughout this book we will take the time to explore the other options because our systems are connected to the same battlefield on which the nation states are fighting!

Tactical and Operational Reasons for Cyber War

The motivations for war are as old as time. Whether individuals or nations, going to war generally is based on power/patriotism/greed versus protection of self/ideology/country.

Traditionally warfare was focused on controlling limited resources but today the power of a network is not determined by resources but the number of nodes on it which equates to the power of information/influence. Additionally in some cases resources may not be as important as ability to react quickly or cycle time. Be it access to proprietary information, classified networks, interconnections on a social network, applications, or data about customers or systems that run the critical infrastructure, the more connected, the more value.

NOTE

The tactical level of war is where individual battles are executed to achieve military objectives assigned to tactical units or task forces. In the Army this would normally be at the Brigade/Regimental level.

The operational level of war is where multiple battles are combined into campaigns within a theater, or larger operational area. Activities at this level link strategy and tactics by establishing operational objectives needed to achieve the strategic objectives through a series of tactical battles. This would normally be at the Joint Task Force or Division level.

The strategic level of war is where a nation, or coalition of nations, determines national political objectives that will be enforced by military forces and other instruments of national power. This is normally controlled at the Combatant Commander level and higher.

Today's critical infrastructure networks are key targets for cyber attack because they have grown to the point where they run the command and control systems, manage the logistics, enable the staff planning and operations, and are the backbone of the intelligence capabilities. More importantly today, most command and control systems, as well as the weapon systems themselves, are connected to the GIG or have embedded computer chips. Airplanes have become flying routers receiving and sending targeting information constantly. Air Defense and Artillery are guided by computer systems and they shoot smart munitions that adjust their flight based on Global Positioning System (GPS) updates to guide themselves to the target. The Intelligence Surveillance and Reconnaissance systems gather so much information the challenge is sifting through it to find the critical data. Today's infantry squad has communication gear, GPS, tracking devices, cameras, and night vision devices. The computer chip is ubiquitous and has become one of the U.S.' centers of gravity. It is both a nations' strength and could be turned into our weakness if taken away. The loss of GPS satellites would take away many of our advantages on the battlefield.

When we consider the military maxim "amateurs study tactics; professionals study logistics," [12][a] it quickly becomes clear how important the logistical systems are. When we deploy forces into a theater of operations our capability to fight is shaped by the forces, weapons, equipment, and supplies that can be moved to the right place at the right time. Today, that is calculated and controlled by computers. An enemy can understand our intentions and abilities by tracking what is happening in the logistics system. If they can modify actions and data, they can interdict, or at least impact, our capabilities.

[a]There is much dispute as to who uttered this military maxim. It has been attributed to General Omar Bradley and U.S. Marine Corps Commandant General Robert H. Barrow. In various other forms, it has also been attributed to Napoleon, Helmuth von Moltke, and Carl von Clausewitz. For the purposes of this book, its origin is far less important than its message.