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.