INFORMATION WARFARE AND SECURITY

by Dorothy E. Denning

Addison-Wesley, December 1998, ISBN: 0201433036, - 544 pages

In recent years, information warfare has captured the attention of government officials, information security specialists, and curious onlookers. The term is used to cover a broad spectrum of activity but especially a scenario wherein information terrorists, using not much more than a keyboard and mouse, hack into a computer and cause planes to crash, unprecedented power blackouts to occur, or food supplies to be poisoned. The terrorists might tamper with computers that support banking and finance, perhaps causing stock markets to crash or economies to collapse. None of these disasters has occurred, but the concern is that they, and others like them, could happen, given the ease with which teenagers have been able to romp through computers with impunity--even those operated by the U.S. Department of Defense.

This book may serve as introduction to information warfare. It is about operations that target or exploit information media in order to win some objective over an adversary. It covers a wide range of activity, including computer break-ins and sabotage, espionage and intelligence operations, telecommunications eavesdropping and fraud, perception management, and electronic warfare. The book is about teenagers who use the Internet as a giant playground for hacking, competitors who steal trade secrets, law enforcement agencies who use information warfare to fight crime and terrorism, and military officers who bring information warfare to the battleground. It is about information-based threats to nations, to business, and to individuals--and countermeasures to these threats. It spans several areas, including crime, terrorism, national security, individual rights, and information security.

The objectives of the book are fourfold. The first is to present a comprehensive and coherent treatment of offensive and defensive information warfare in terms of actors, targets, methods, technologies, outcomes, policies, and laws. Information warfare can target or exploit any type of information medium--physical environments, print and storage media, broadcast media, telecommunications, and computers and computer networks. All of these are treated within the book, albeit with a somewhat greater emphasis on computer media. The second objective is to present a theory of information warfare that explains and integrates operations involving this diverse collection of actors and media within a single framework. The theory is centered on the value of information resources and on "win-lose" operations that affect that value. The third is to separate fact from fiction. The book attempts to present an accurate picture of the threat, emphasizing actual incidents and statistics over speculation about what could happen. Speculation is not ignored, however, as it is essential for anticipating the future and preparing for possible attacks. A fourth objective is to describe information warfare technologies and their limitations, particularly the limits of defensive technologies. There is no silver bullet against information warfare attacks.

The book provides a reasonably comprehensive treatment of the methods and technologies of information warfare. It may be useful for making informed judgments about potential threats and defenses. The book is intended for a broad audience, from the student and layperson interested in learning more about the domain and what can be done to protect information assets, to the policy maker who wishes to understand the nature of the threat and the technologies and issues, to the information security specialist who desires extensive knowledge about all types of attacks and countermeasures in order to protect organizational assets. It was also written for an international audience. Although the focus is on activity within the United States, activity outside the United States is included.

The book is divided into three parts. Part I introduces the concepts and principles of information warfare. There are three chapters. Chapter 1, Gulf War--Infowar, begins with examples of information warfare taken from the time of the Persian Gulf War and the continuing conflict with Iraq. It summarizes the principles of information warfare and discusses trends in technology and information warfare. Chapter 2, A Theory of Information Warfare, presents a model of information warfare in terms of four main elements: information resources, players, offensive operations, and defensive operations. It relates information warfare to information security and information assurance. Chapter 3, Playgrounds to Battlegrounds, situates information warfare within four domains of human activity: play, crime, individual rights, and national security. It summarizes some of the activity in each of the areas.

Part II covers offensive information warfare operations. It is organized around media and methodologies and gives numerous examples of incidents in each category. There are eight chapters. Chapter 4, Open Sources, is about media that are generally available to everyone, including Internet Web sites. It covers open source and competitive intelligence, invasions of privacy, and acts of piracy that infringe on copyrights and trademarks. Chapter 5, Psyops and Perception Management, is about operations that exploit information media, particularly broadcast media and the Internet, in order to influence perceptions and actions. Chapter 6, Inside the Fence, is about operations against an organization's resources by insiders and others who get inside access. It covers traitors and moles, business relationships, visits and requests, insider fraud, embezzlement and sabotage, and physical break-ins. Chapter 7, Seizing the Signals, is about operations that intercept communications and use sensors to collect information from the physical environment. Telecommunications fraud and physical and electronic attacks that disrupt or disable communications are also covered. Chapter 8, Computer Break-Ins and Hacking, is about computer intrusions and remote attacks over networks. It describes how intruders get access and what they do when they get it. Chapter 9, Masquerade, is about imposters who hide behind a facade. It covers identity theft, forgeries, and Trojan horses. Finally, Chapter 10, Cyberplagues, is about computer viruses and worms.

Part III covers defensive information warfare, including strengths and limitations of particular methods. It has five chapters. Chapter 11, Secret Codes and Hideaways, is about methods that conceal secrets, including cryptography (encryption), steganography, anonymity, and locks and keys. Chapter 12, How to Tell a Fake, is about methods of determining whether information is trustworthy and genuine. It covers biometrics, passwords, integrity checksums, digital signatures, watermarking, and badges and cards. Chapter 13, Monitors and Gatekeepers, is about monitors that control access to information resources, filter information, and detect intrusions into information systems or misuse of resources. Chapter 14, In a Risky World, is about what organizations can do to deal with risk. It includes vulnerability monitoring and assessment, building and operating secure systems, risk management, and incident handling. Finally, Chapter 15, Defending the Nation, is about the role of the government in defensive information warfare. Three areas are covered: generally accepted system security principles, protecting critical infrastructure.

About the author:

Dorothy E. Denning is Professor of Computer Science at Georgetown University. She is the author of a classic book in the field, *Cryptography and Data Security*, a coeditor (with Peter J. Denning) of a more recent work, *Internet Besieged: Countering Cyberspace Scofflaws*, and the author of 100 papers on computer security. Her book provides a comprehensive and coherent treatment of offensive and defensive information warfare, identifying the key actors, targets, methods, technologies, outcomes, policies, and laws. Whatever your interest or role in the emerging field of information warfare, this book will give you the background you need to make informed judgments about potential threats and our defenses against them.