

Information Warfare Principles and Operations

Information Warfare Principles and Operations

Edward Waltz



Artech House
Boston • London

Library of Congress Cataloging-in-Publication Data

Waltz, Edward.

Information warfare : principles and operations / Edward Waltz.

p. cm.

Includes bibliographical references and index.

ISBN 0-89006-511-X (alk. paper)

1. Information warfare. I. Title.

U163.W38 1998

355.3'43—dc21

98-30140

CIP

British Library Cataloguing in Publication Data

Waltz, Edward

Information warfare principles and operations

1. Information warfare

I. Title

355.4'0285

ISBN 0-89006-511-X

Cover design by Lynda Fishbourne

© 1998 ARTECH HOUSE, INC.

685 Canton Street

Norwood, MA 02062

All rights reserved. Printed and bound in the United States of America. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Artech House cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

International Standard Book Number: 0-89006-511-X

Library of Congress Catalog Card Number: 98-30140

10 9 8 7 6 5 4 3 2 1

To my son Tim

Who has shown to me the truth of the Scripture: "The father of a righteous man has great joy; he who has a wise son delights in him." Proverbs 23:24

Contents

	Preface	<i>xiii</i>
1	Concepts of Information in Warfare	1
1.1	Information's Role in Warfare	2
1.2	An Information Model of Warfare	4
1.3	The Transformations of Warfare	10
1.4	The Forms of Information Warfare	15
1.5	Defining Information Warfare and Information Operations	19
1.5.1	A Functional Taxonomy of Information Warfare	22
1.5.2	A Taxonomy of Military Operations for Information Warfare	24
1.6	Expanse of the Information Warfare Battlespace	27
1.7	The U.S. Transition to Information Warfare	30
1.8	Information Warfare and the Military Disciplines	33
1.9	Information and Peace	35
1.10	The Current State of Information Warfare	37
1.10.1	State of the Military Art	38
1.10.2	State of Operational Implementation	38
1.10.3	State of Relevant Information Warfare Technology	38

1.11	Summary	41
	Endnotes	41
Part I	Information-Based Warfare	47
2	The Role of Information Science in Warfare	49
2.1	The Meaning of Information	50
2.2	Information Science	56
2.2.1	Philosophy (Epistemology)	56
2.2.2	Philosophy (Logic)	57
2.2.3	Information Theory	58
2.2.4	Decision Theory	64
2.2.5	Semiotic Theory	65
2.2.6	Knowledge Management	66
2.3	Comparison of Approaches	69
2.4	Measuring the Utility of Information in Warfare	70
2.5	Translating Science to Technology	78
	Endnotes	80
3	The Role of Technology in Information-Based Warfare	83
3.1	Knowledge-Creation Processes	84
3.2	Knowledge Detection and Discovery	89
3.3	Knowledge Creation in the OODA Loop	89
3.4	Deductive Data Fusion	92
3.5	Abductive-Inductive Data Mining	97
3.6	Integrating Information Technologies	103
3.7	Summary	105
	Endnotes	105
4	Achieving Information Superiority Through Dominant Battlespace Awareness and Knowledge	107

4.1	Principles of Information Superiority	108
4.1.1	Intelligence, Surveillance, and Reconnaissance (ISR)	113
4.2	Battlespace Information Architecture	124
4.3	Summary	133
	Endnotes	133
Part II	Information Operations for Information Warfare	137
5	Information Warfare Policy, Strategy, and Operations	139
5.1	Information Warfare Policy and Strategy	140
5.2	An Operational Model of Information Warfare	148
5.3	Defensive Operations	152
5.4	Offensive Operations	162
5.5	Implementing Information Warfare Policy and Strategy	168
	Endnotes	168
6	The Elements of Information Operations	171
6.1	The Targets of Information Operations	173
6.1.1	The Global Information Infrastructure (GII)	175
6.1.2	The National Information Infrastructure (NII)	177
6.1.3	Defense Information Infrastructure (DII)	186
6.2	Information Infrastructure War Forms	191
6.3	Information Operations for Network Warfare	194
6.3.1	A Representative Netwar Scenario	195
6.3.2	Taxonomy of Netwar Elements and Supporting Disciplines	200
6.4	Information Operations for Command and Control Warfare (C2W)	200
6.4.1	A Representative C2W Scenario	202

6.4.2	Taxonomy of C2W Functional Elements and Supporting Disciplines	206
6.5	The Component Disciplines of Information Operations	207
6.5.1	Psychological Operations (PSYOPS)	209
6.5.2	Operational Deception	211
6.5.3	Electronic Operations	213
6.5.4	Physical Destruction	217
6.5.5	Intelligence	219
6.5.6	Counterintelligence	220
6.5.7	Information Security (INFOSEC)	220
6.5.8	Operational Security (OPSEC)	222
6.6	Summary	222
	Endnotes	222
7	An Operational Concept (CONOPS) for Information Operations	229
	Endnotes	249
8	Offensive Information Operations	251
8.1	Fundamental Elements of Information Attack	254
8.2	The Weapons of Information Warfare	256
8.3	Network Attack Tactics	256
8.3.1	Network Attack Vulnerabilities and Categories	256
8.3.2	Network Attack Processes	259
8.3.3	Internet Service Attacks	265
8.4	Command and Control Warfare Attack Tactics	268
8.4.1	Command and Control Network Vulnerabilities	268
8.4.2	Attack Categories for Data Fusion Systems	269
8.4.3	Attack Matrix for C4I Data Fusion	273
8.5	IW Targeting and Weaponeeing Considerations	276
8.6	Information-Level (Network) Attack Techniques	276

8.6.1	Intelligence and Targeting	276
8.6.2	Weapon Delivery	281
8.6.3	Information Weapons	282
8.7	Physical-Level Attack Techniques	286
8.7.1	Kinetic Energy Weapons	286
8.7.2	Chemical and Biological Weapons (CBW)	287
8.7.3	Directed Energy Weapons (DEW)	288
8.7.4	Passive Conductive Measures	292
8.8	Offensive Operations Analysis, Simulation, and War Gaming	292
8.9	Summary	295
	Endnotes	296
9	Defensive Information Operations	301
9.1	Fundamental Elements of Information Assurance	307
9.2	Principles of Trusted Computing and Networking	310
9.3	Authentication and Access Control	316
9.3.1	Secure Authentication and Access Control Functions	316
9.3.2	Secure Access Systems: Firewalls	318
9.4	Cryptographic Encryption Measures	322
9.4.1	Encryption Alternatives	323
9.4.2	Digital Signatures	328
9.4.3	Key Management	328
9.5	Incident Detection and Response	329
9.6	Survivable Information Structures	334
9.7	Defense Tools and Services	336
9.8	Physical-Level System Security	339
9.9	Security Analysis and Simulation for Defensive Operations	345
9.10	Summary	350
	Endnotes	351

10	<u>The Technologies of Information Warfare</u>	357
10.1	A Technology Assessment	358
10.2	Information Dominance Technologies	365
10.2.1	Collection Technologies	366
10.2.2	Processing Technologies	370
10.2.3	Dissemination and Presentation Technologies	372
10.3	Offensive Technologies	373
10.4	Defensive Technologies	376
10.5	Summary	379
	Endnotes	379
	<u>About the Author</u>	383
	<u>Index</u>	385

Preface

The forms of cooperation, competition, conflict, and warfare in this world are changing as information technology is changing the way that we observe, understand, decide, and communicate. These changes are impacting every aspect of personal, corporate, and national security. This book provides a systems-level introduction of the means by which information technology is changing conflict and warfare.

At the conceptual level, volumes of articles and several books have explored the implications of the increasing and now dominant role of information in warfare. Futurists Alvin and Heidi Toffler have popularized the notion of warfare's new form, defense strategist Martin Libicki has developed an intellectual base for strategy, military author Alan Campen has illustrated how information has been applied in the Gulf War, and the U.S. Defense Science Board has laid the groundwork to prepare the U.S. infrastructure for future information wars. This book is intended to contribute to that body of knowledge by presenting a systems-level organization of the principles of information operations. It also moves deeper into those operations to clearly introduce the technical basis for this emerging area, articulating the core techniques and enabling technologies.

I am not a war fighter, but I have spent the majority of my career working with war fighters to improve the acquisition of data and processing of information to meet their unceasing demands for improved knowledge (intelligence) to perform military missions. This ubiquitous and preeminent demand for information has shaped the current recognition that war fighters must be information warriors—capable of understanding the value of information in all of its roles: as knowledge, as target, as weapon.

Today, war fighters must know how to quantify, value, and apply this intangible resource. This is a book for those war fighters, as well as the policy makers, commanders, and systems engineers who will implement the transition for strategy and concept to system design and implementation.

This book is based on materials I have presented at information warfare seminars and conferences in the United States and Europe since 1995 and the insight I have received from the enthusiastic response of defense ministry, military, and industry attendees. The U.S. Defense Science Board, the Department of Defense (DoD), and the National Defense University have been generous and open with the national studies of information warfare (IW), and I am indebted to the vast amount of material they have placed in the public domain.

Following an introduction to this emerging area, the book is divided into two major parts, describing the major components of information warfare.

Part I describes the basis for information-based warfare (IBW), beginning with the information sciences that define information (Chapter 2), and technologies to create knowledge from data (Chapter 3). Chapter 4 describes the means to apply these technologies to achieve dominant battlespace awareness and knowledge, the goal of IBW.

Part II details information operations (IO) that attack opponents' information systems and defend a nation's own systems. We describe first information warfare (IW) policy, strategy, and tactics (Chapter 5), then IO operations (Chapters 6 and 7) before detailing methods for offense (Chapter 8) and defense (Chapter 9). An overview of core, enabling, and emerging technologies in this area is provided in the conclusion (Chapter 10).

I am grateful to God for my patient and loving wife; without her encouragement and understanding, this book would not be possible. I am also indebted to my son and daughter who have also encouraged me and endured the period of writing that too often kept me from spending the time with them that I cherish.

Finally, my purpose in writing this book is not to promote warfare. Rather, it is to explain a warfare form that is already waged today—one that must be understood by those who cherish peace and wish to defend freedom and to deter warfare in all of its forms.

1

Concepts of Information in Warfare

Warfare, the alternative to resolution of issues by diplomatic means, is the highest level of human conflict. In warfare, the warring parties perceive each other's objectives as mutually exclusive and apply force and other means to achieve their own victory. Information warfare emphasizes the operations that apply the *other* means.

Warfare is the failure of diplomacy, often the result of escalation from legitimate competition and limited conflict. Warring parties include nation states in large-scale conflict, transnational organizations established for crime or terror, and corporate entities seeking market domination. Throughout history, technology has provided ever-changing means of waging war, for both the attacker and the defender. As humankind moves into an information age of global competition, information itself will take on a central role in competition, conflict, and even warfare. In this book, we explore the fundamental principles of applying information in conflict—principles of information in offense, defense, and dominance.

In later chapters, we will explore the technical meaning of *information* and find that the general term encompasses three levels of abstraction, distinguished by information as both content and process [1].

- *Data*—Individual observations, measurements, and primitive messages form the lowest level. Human communication, text messages, electronic queries, or scientific instruments that sense phenomena are the major sources of data.
- *Information*—Organized sets of data are referred to as information. The organizational process may include sorting, classifying, or

indexing and linking data to place data elements in relational context for subsequent searching and analysis.

- *Knowledge*—Information, once analyzed and understood, is knowledge. Understanding of information provides a degree of comprehension of both the static and dynamic relationships of the objects of data and the ability to model structure and past (and future) behavior of those objects. Knowledge includes both static content and dynamic processes. In the military context, this level of understanding is referred to as *intelligence*.

In the last quarter of the twentieth century, the role of electronically collected and managed information at all levels has increased to become a major component of both commerce and warfare. The electronic transmission and processing of information content has expanded both the scope and speed of business and military processes. In the last decade of this century, electronic communications and processing technologies have accelerated the role of the abstract information they convey to a place of preeminence. In the twenty-first century, information may become the very essence and manifestation of competition, conflict, and warfare.

1.1 Information's Role in Warfare

The importance of information and the central role it plays in warfare is not new. Writing in the tenth century B.C., the military commander and king, Solomon, emphasized the importance of knowledge (military intelligence), guidance (strategic and operational planning), and advisors (objective analysts) to be victorious in warfare: “A wise man has great power, and a man of knowledge increases strength; for waging war you need guidance, and for victory many advisers” [2].

In the sixth century B.C., Chinese military strategist Sun Tzu detailed in *The Art of War* [3] the importance of information. Consider four oft-quoted assertions that Sun Tzu made regarding information.

1. Information is critical for the processes of surveillance, situation assessment, strategy development, and assessment of alternatives and risks for decision making. Sun Tzu wrote,

“In respect of military method, we have, firstly, measurement; secondly, estimation of quantity; thirdly, calculation; fourthly, balancing of chances; fifthly, victory.”

2. Information in the form of intelligence and the ability to forecast possible future outcomes distinguishes the best warriors.

“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.”

3. The control of some information communicated to opponents, by deception (seduction and surprise) and denial (stealth), is a contribution that may provide transitory misperception to an adversary.

“All warfare is based on deception [of the enemy],” and, “O divine art of subtlety and secrecy! Through you we learn to be invisible, through you inaudible.”

4. The supreme form of warfare uses information to influence the adversary’s perception to subdue the will rather than using physical force.

“In the practical art of war, the best thing is to take the enemy’s country whole and intact....Hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy’s resistance without fighting.”

Each of these cardinal principles, applied even before the sixth century B.C., relied on the acquisition, processing, and dissemination of information. The principles have not changed, but the *means* of acquisition, processing, and dissemination have. Electronic means of acquiring and managing information have replaced earlier technologies, human couriers, and written communications. The increasing dependency on the electronic means of managing large volumes of information and the increasing value of that information have made the information *itself* a lucrative target and a valuable weapon of warfare. These changes are revolutionizing the role of information and the conduct of warfare.

1.2 An Information Model of Warfare

Before introducing broad concepts of information applied in large-scale warfare, it is important to understand the role of information in conflict at the basic functional level. Consider an elementary one-directional model of conflict to illustrate the role of information in warfare. (Later in this chapter, we will expand to a bi-directional and closed-loop conflict model of two combatants using this basic element.) The model can apply to two individuals in conflict, or two nation states at war.

An attacker, A, engages a defender, B, who must determine how to act, or react. The objective of A is to influence and coerce B to act in a manner favorable to A's objective. This is the ultimate objective of any warring party—to cause the opponent to act in a desired manner: to surrender, to err or fail, to withdraw forces, to cease from hostilities, and so forth. The attacker may use force or other available influences to achieve this objective. The defender may make a decision known to be in favor of A (e.g., to acknowledge defeat and surrender) or may fall victim to seduction or deception and unwittingly make decisions in favor of A.

Three major factors influence B's decisions and resulting actions (or reactions) to A's attack.

- *The capacity of B to act*—The ability of B to respond is a physical factor, measured in terms of capability to command and strength of force. Attrition warfare is based on the premise that the degradation of B's war-fighting capacity will ultimately cause B to make decisions that succumb to the attacker's objectives. Capacity is not measured in a single magnitude; rather, it is defined in many components, including "centers of gravity"—strategic characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight.
- *The will of B to act*—The will is a human factor, a measure of the resolve or determination of the human decision maker(s) of B and their inclination toward alternative actions. This element is the most difficult for the attacker to measure, model, or directly influence. The strength of will to take actions to achieve a stated objective or purpose may transcend "objective" decision criteria. Confronted with certain military or economic defeat, the will of a decision maker may press on, no matter how great the risk, reacting in ways that are irrational (in military or economic terms).

- *The perception of B*—The understanding of the situation from the perspective of B is an abstract information factor, measured in terms such as accuracy, completeness, confidence or uncertainty, and timeliness. The decisions that B makes are determined by the perception of the situation (A's attacks on B) and the perception of B's own capacity to act. Based on these perceptions, the perceived alternative actions available and their likely outcomes, and the human willpower of decision makers, B responds.

How then can A coerce B to act in a manner favorable to A's objectives? The attacker has several alternatives to influence the actions of B, based on these factors. The attacker can directly attack the capacity of B to act. This reduces the options available to B, indirectly influencing the will of B. The attacker can also influence the perception of B about the situation (attacks on capacity certainly do this directly, while attacks on sensors and communications can achieve this more indirectly); the constraints to action; or the possible outcomes of actions. While the attacker cannot directly attack or control the will of B, capacity and perception attacks both provide a means of access to the will, even if limited.

Now we can further detail the conflict model to illustrate the means by which A can influence the capacity of B and the flow of information that allows B to perceive the conflict situation. The detailed model (Figure 1.1) provides the flow of information from the attacker, A, across four domains to the decisions and actions of B. The model will allow us to explore the alternatives by which A may influence B's perception of the situation.

First, the physical domain is where B's capacity to act resides. People, production processes, stockpiles of resources, energy generation, weapons platforms, lines of communication, and command and control capabilities reside in the physical domain. The second domain is the information domain, the electronic realm where B observes the world, monitors the attacks of A, measures the status of his or her own forces, and communicates reports regarding the environment. In the next domain, a perceptual one, B combines and analyzes all of the observations to perceive or become oriented with the situation. This "orienting" process assesses the goals, the will, and the capacity of A. It also compares the feasible outcomes of reactions it may choose, based upon B's own capacity, which is provided through the observation process as forces report their status. In this domain, though supported by electronic processing and visualization processes, the human mind is the central element. The comprehension of the situation and the degree of belief in that view are primary influences on the next domain.

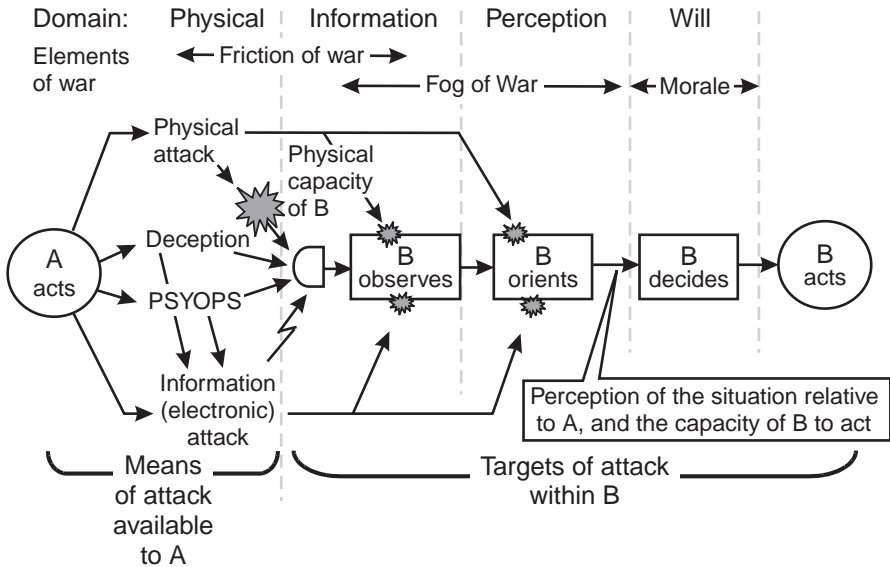


Figure 1.1 A basic model of the information processes in a conflict between attacker A and defender B.

Finally, in the domain of the human choice and will, B makes decisions regarding actions or reactions. These decisions are based on the perceived situation, options for action available, and possible outcomes of those alternative actions. The decision maker applies both experience and predisposition of the will to this process of judgment. As the human mind is the central element of the perceptual domain, even so the “heart” of the decision maker (resolve, determination, and human will) is a central element in this domain.

The model illustrates four basic options available for A to attack B in an effort to coerce B’s decisions.

- Physical attack*—Notice in the figure that physical attacks strike first in the physical domain, attacking the physical capacity of B to respond (military weapons, forces, bases, industrial capacity, bridges, and other resources). Physical force is the basic instrument of coercion and the traditional means of attrition warfare, applied as heat, blast, or fragmentation. The attack is designed to destroy or to functionally disable B’s capacity to observe, to orient, to command, or to react with force. Physical attacks on observation (sensors, communications) or orientation processes (command nodes) deny valuable information or otherwise corrupt the perception of decision makers.

- *Deception*—The attacker may enhance the effectiveness of all other attacks by reducing B's effectiveness in both defense and offense. Deceptive actions to achieve a degree of surprise in attacks and seducing B to take ineffective and vulnerable actions are essential elements of deception.
- *Psychological attack*—Attacks at human perception seek to manage (or at least influence) the perception of B about the circumstances of the conflict. While deception desires to induce specific behaviors, psychological operations (PSYOPS) are aimed at overall ability to perceive—to cause a desired *disorientation* rather than a correct orientation by B.
- *Information attack*—Electronic attacks also target the electronic processes and content of the information infrastructure (sensors, communication links, and processing networks) that provides observation and orientation to B's decision makers. These attacks have the potential to directly affect the ability and effectiveness of B to perceive the conflict situation. Unlike psychological and deception operations, which must pass through the sensors, information attacks may directly attack the electronic observation and orientation processes. They have the potential of inserting deception or psychological messages, disrupting or even destroying these processes. (Information attacks can certainly have effects that cascade back into the physical domain, too. Attacks on computers or links controlling physical processes, such as power plants, pipelines, and machinery, can cause destruction in the physical domain. Here, we are focusing only on the means to influence the behavior of B, without examining all of the causal relationships between domains in the model.)

Notice also that the model is sequential, and that time is a factor in the performance of the decision maker. Perception is a function of the timeliness of the information used for orientation. All of the attacks may influence the timeliness of the flow as well as the content of the information flowing through the model.

In the Gulf War, Coalition forces applied all of these attack avenues to subdue the will of Iraqi leaders, causing them to act in accordance with the Coalition objective—to withdraw forces that had annexed Kuwait. The well-known strategy included each of the attack avenues cited in our simple model. The strategic air campaign achieved attrition of Iraqi military capacity, including air defenses, military production, command and control nodes, and ground forces and their weapon systems. This attrition gained increasing superiority

of forces in the air, in the information domain, and, finally, on the ground. The subsequent ground war continued the attrition of Iraqi military capacity. Throughout the war, perceptual attacks included physical and electronic strikes on sensors and data links to destroy and disrupt the ability of Iraqi command to maintain awareness of Coalition actions or of their own force dispositions and status. Messages to Iraqi forces, both broadcast and physically delivered in leaflets, reinforced the (accurate) psychological perception that Coalition forces maintained overwhelming military intelligence and force. They also sustained the perception that specific warnings of attack to precisely identified Iraqi ground units were invariably followed by lethal action. Deceptive operations that exposed preparations for amphibious assaults while concealing massive ground movements also influenced the (incorrect) Iraqi perception of the Coalition ground strategy. Other political actions also influenced Iraqi perceptions of possible outcomes of their own actions. U.S. statements, for example, that indicated the United States would respond in kind to the use of weapons of mass destruction influenced Iraqi decisions to withhold use of available chemical-biological weapons [4]. The aggressor's will was ultimately subdued by the combination of physical and nonphysical actions against the Iraqi centers of gravity.

At the center of ongoing discussions of information warfare has been the issue of addressing what is *new* about the concept of information warfare.

The increasing reliance on electronic information technology to perform the “observe” and “orient” processes is one new element that gives credibility to the effectiveness of information attacks in the information and perception domains. These domains are increasingly dependent on electronic systems to measure complex situations, deliver organized information to aid the human perception, and control the battle. Information warfare operations concepts are new because of the increasing potential (or threat) to affect capacity and perception *in the information and perception domains as well as the physical domain*. These information operations are also new because *these domains are vulnerable to attacks that do not require physical force alone*. Information technology has not changed the human element of war. It has, however, become the preeminent means by which military and political decision makers perceive the world, develop beliefs about the conflict, and command their forces.

The second new aspect to information warfare is the expansion of the battlespace *beyond* the traditional military realm. Information targets and weapons can include the entire civil and commercial infrastructure of a nation. The military has traditionally attacked military targets with military weapons, but IW introduces the notion that all national information sources and processes are potential weapons and targets. In subsequent chapters, we will discuss how

military operations will deal with the operational aspects of this expansion of the battlespace.

The subject of the role and potential effectiveness of these information operations in warfare is not without controversy. Some foresee the long-term potential for information attacks to so influence the perception of human minds (both individually and en masse) as to provide the capability to subdue the human will with a minimum use of physical force. This view seeks to apply information operations to achieve the “supreme excellence” sought by Sun Tzu to “break the enemy’s resistance without fighting” [5]. Col. Richard Szafranski has articulated such a view, in which the epistemology (knowledge and belief systems) of an adversary is the central strategic target and physical force is secondary to perceptual force [6].

Others, however, see attacks at the information and perceptual levels as complementary and supplemental operations to conventional warfare—partners with physical forces, not substitutes, to subdue the human will. Arguing for this position, Maj. YuLin Whitehead has stated,

It is clear that while information may be used as a weapon, strategists must use it with caution and common sense. It is not a silver-bullet weapon. Rather, the strategist should plan the use of the information weapon in conjunction with more traditional weapons and employ it as a precursor weapon to blind the enemy prior to conventional attacks and operations [7].

Who is correct? We will see that there exists a spectrum of war forms, and that each may require appropriate mixes of lethal physical force and nonlethal information force to achieve the objectives established. Economic and psychological wars waged over global networks may indeed be successfully conducted by information operations alone. Large-scale conventional wars, on the other hand, will certainly require a greater mix of physical force. The role and effectiveness of information operations is determined by the context of the conflict.

War is an event, but the operations of warfare describe the *means* of conflict employed in the event. In this book, we will distinguish the *event* from the *operations*. In the next two sections, we will introduce the historical transformation of the process of warfare and the various forms of information warfare. In subsequent chapters, we explain the technical operations by which these war forms are conducted. Information superiority is the *end* (objective) of information operations (in the same sense that air superiority is an objective), while the operations are the *means* of conduct (in the sense that tactical air power is but one tool of conflict).

In later chapters, we will refine this simple warfare model to distinguish the processes and action of IW at each of the three domains or “layers” introduced: physical, information infrastructure, and perceptual. This will be the organizing model for our discussions of operations, both offensive and defensive, throughout the book.

1.3 The Transformations of Warfare

Since the Second World War, the steady increase in the electronic means of collecting, processing, and communicating information has accelerated the importance of information in warfare in at least three ways. First, intelligence surveillance and reconnaissance (ISR) technologies have extended the breadth of scope and range at which adversaries can be observed and targeted, extending the range at which forces engage. Second, computation and communication technologies supporting the command and control function have increased the rate at which information reaches commanders and the tempo at which engagements can be conducted. The third area of accelerated change is the integration of information technology into weapons, increasing the precision of their delivery and their effective lethality. Electronic combat matured as an integral element of warfare during the Vietnam War. This technology provided tactical intelligence while deceiving and disrupting the adversary’s intelligence and targeting capabilities. Since the Gulf War, military analysts and futurists alike have recognized a significant shift in military conflict from massive physical destruction toward precision and even nonphysical destruction—information warfare. This shift has moved the central resources—both targets and weapons—of conflict from physical weapons to the abstract information processes and contents that control and enable warfare at the physical level.

The shift is significant because the transition moves the object of warfare from the tangible realm to the abstract realm, from material objects to nonmaterial information objects. The shift also moves the realm of warfare from overt physical acts against military targets in “wartime” to covert information operations conducted throughout “peacetime” against even nonmilitary targets. This transition toward the dominant use of information (*information-based warfare*) and even the targeting of information itself (*information warfare*, proper) [8] has been chronicled by numerous writers.

Futurists Alvin and Heidi Toffler have articulated and popularized the explanation and implications of the world’s transition from an industrial age to an information age. They have most clearly articulated the explanation for this third great shift in the world’s means of wealth production and power projection in warfare. In 1980, Alvin Toffler introduced the hypothesis of the

great shift in *The Third Wave* [9], while a decade later, in *Powershift* [10], he detailed broader social and economic aspects of the shift, with evidence. *War and Anti-War* [11], the Tofflers' third work on the topic, described the impact of the shift on warfare, using examples from the Gulf War as evidence to further support their thesis of a decade earlier. According to the Tofflers, the information age shift is bringing about analogous changes in the conduct of business and warfare in ten areas.

1. *Production*—The key core competency in both business and warfare is information production. In business, the process knowledge and automation of control, manufacturing, and distribution is critical to remain competitive in a global market; in warfare, the production of intelligence and dissemination of information is critical to maneuvering, supplying, and precision targeting.
2. *Intangible values*—The central resource for business and warfare has shifted from material values (property resources) to intangible information. The ability to apply this information discriminates between success and failure.
3. *Demassification*—As information is efficiently applied to both business and warfare, production processes are shifting from mass production (and mass destruction) to precision and custom manufacturing (and intelligence collection, processing, and targeting).
4. *Worker specialization*—The workforce of workers and warriors that performs the tangible activities of business and war is becoming increasingly specialized, requiring increased training and commitment to specialized skills.
5. *Continuous change*—Continuous learning and innovation characterize the business and workforces of information-based organizations because the information pool on which the enterprise is based provides broad opportunity for understanding and improvement. Peter Senge has described the imperative for these *learning organizations* in the new information-intensive world [12].
6. *Scale of operations*—As organizations move from mass to custom production, the teams of workers who accomplish tangible activities within organizations will become smaller, more complex teams with integrated capabilities. Business units will apply integrated process teams, and military forces will move toward integrated force units.
7. *Organization*—Organizations with information networks will transition from hierarchical structure (information flows up and down)

toward networks where information flows throughout the organization. Military units will gain flexibility and field autonomy.

8. *Management*—Integrated, interdisciplinary units and management teams will replace “stovepiped” leadership structures of hierarchical management organizations.
9. *Infrastructure*—Physical infrastructures (geographic locations of units, physical placement of materials, physical allocation of resources) will give way to infrastructures that are based upon the utility of information rather than physical location, capability, or vulnerability.
10. *Acceleration of processes*—The process loops will become tighter and tighter as information is applied to deliver products and weapons with increasing speed. Operational concurrence, “just-in-time” delivery, and near-real-time control will characterize business and military processes.

The Tofflers’ *War and Anti-War* heightened the awareness and study of the implications of information warfare at a popular level. At the technical and operational levels, a number of publications, conferences, and formal studies by the U.S. DoD Defense Science Board have increased awareness. They have also increased the legitimacy of calls to prepare for information threats to national security in the United States and other nations with high information technology dependencies.

Military analysts have long studied the history of warfare, enumerating the application of new technologies to increase firepower and lethality, maneuverability, command and control, interoperability of forces, and precision application of force to achieve military objectives. Physical attrition and maneuver warfare concepts have dominated military thinking since Karl von Clausewitz’s classic military treatise, *On War* [13]. More recently, Martin van Creveld’s *The Transformation of War* exhaustively analyzed the twentieth century influences of technology and the limits of technology in future physical and ideological low intensity conflicts [14]. Numerous military thinkers recognized the potential transformations in the ways warfare will be conducted as a result of information technologies, but the most popular and widely cited general view of the transformation is that of the Tofflers [15].

The Tofflers’ thesis on the great waves of civilization that affect warfare can be summarized in four essential points. First, history can be described in terms of three distinct periods (phases or *waves*) during which humankind’s activity—both production and destruction—have changed in quantum transitions. In the conduct of both commerce and warfare, the necessary resources and core competencies radically shifted at the transition between waves.

Second, each distinct wave is characterized by its means of wealth production and a central resource at the core of the production mechanism. Third, technology is the cause of the rapid transitions because as new technologies are introduced, the entire basis for wealth (production) and power (the potential for destruction) change, with the potential to rapidly change the world order. Finally, each new wave has partitioned the nation states of the world into categories, each characterized by their maturity (e.g., an information age society is characterized as “third wave”). The world is now trisected into nations in each of the three wave categories.

Table 1.1 summarizes the three waves identified by the Tofflers, with the current rapid transition moving from an industrial age to an information-based age in which:

- Information is the central resource for wealth production and power.
- Wealth production will be based on ownership of information—the creation of knowledge and delivery of custom products based on that knowledge.
- Conflicts will be based on geoinformation competitions over ideologies and economies.
- The world is trisected into nations still with premodern agricultural capabilities (first wave), others with modern industrial age capabilities (second wave), and a few with postmodern information age capabilities (third wave).

Table 1.1 shows the predicted transition toward information warfare, from attrition and mass destruction of machines to attrition and precision control of information.

The implications of information technology advances transcend the technical and functional impacts that are immediately apparent. Futurists have conceived significant ways that these technologies are transforming the world. The ultimate consequences, for not only wealth and warfare, will be the result of technology’s impact on infrastructure, which influences the social and political structure of nations, and finally, that impact on the global collection of nations and individuals.

Table 1.2 illustrates one cause-and-effect cascade that is envisioned. The table provides the representative sequence of influences, according to some futurists, that has the potential even to modify our current structure of nation states, which are defined by physical boundaries to protect real property. In that view, as the third wave brings a transition of value from real property to

Table 1.1

Three Waves of Civilization and Warfare According to the Toffler Thesis Presented in *The Third Wave* and *War and Anti-War*

Time Period:	5000 B.C.	A.D. 1700	A.D. 2000
Wave:	1 (Premodern, Agricultural)	2 (Modern, Industrial)	3 (Postmodern, Information)
Means of Wealth Production	Peasant-based crop production	Massified factory production	Demassified, custom information production
Central Resource	Land	Material resources	Information
Historical Milestones	Crop control Irrigation Planning and food storage	English industrial revolution (1800) American industrial revolution (1850), work mechanization, interchangeable parts Taylor scientific management (1900)—analysis Statistical process control (1945) Numerical control (1967) Computer integrated manufacturing (1987)	Introduction of the computer Economic introduction of processing and memory Interconnection of processing and databases Extraction of knowledge from data Increase process understanding and precision control
Conflict Triggers	Local land ownership Clash between rulers	Regional, geoeconomic competition Clash between peoples (states) by conscripted armies	Geoinformation competition Clash between ideologies and economies
Core Principle of Warfare	Attrition of infantry	Attrition of machines Mass destruction Armor and machines Hierarchy	Attrition of will and capability Precision control of perception Complex, adaptive, dispersed
Clash of Civilizations	Homogeneous conflict of powers	Bisected world (first- and second-wave states in conflict)	Trisected world (first-, second-, and third-wave states in conflict)
Military Authors	Sun Tzu	de Saxe Napoleon von Clausewitz	Sullivan Campen Libicki

Table 1.2

One View of Projected Social and Political Consequences of Information Technology in the Twenty-First Century

Technology Factors	Impact on Technical Infrastructures	Impact on Public (State) and Private Sectors (Individuals)	Potential Global Consequences
1. Information technology performance advances: <ul style="list-style-type: none"> • Strong cryptography • Communication • Processing • Storage • Display • Bandwidth 2. Integration of information services (telecom, data, voice, TV) 3. Widespread global application of information technology: <ul style="list-style-type: none"> • Immediate, global access to information • Global location of all objects, individuals 	Preeminence of information as resource of power (wealth and warfare) Increased dependence upon information technology with incumbent vulnerability Transition from hierarchical to networked infrastructures (knowledge delivery, finance, environment control) with widespread access	Reduced state control of information State and private access to private information changed: –Reduced (if encrypted) –Expanded (if not protected) Gap between influence of states and individuals reduced Ability to distinguish between states and individuals reduced Information becomes the form of capital Expanded, cross-culture global discourse at individual level	<i>Nation states</i> (defined by physical boundaries to protect physical resources) transition toward... <i>Interest states</i> (defined by ideological boundaries to protect knowledge interests)

knowledge and information property, the nation states’ roles of physical protection will give way to new means of information protection. These new means will reduce or greatly modify the traditional role of nation states.

As these changes occur, even so will the forms of conflict and warfare that will be waged at the information level.

1.4 The Forms of Information Warfare

Warfare at the information level may take on several possible forms (“war forms” that describe operations, not war events that may include all forms applied at different phases or concurrently during a war event). Numerous

authors have envisioned possible models of future information warfare at all levels of society.

The widely published think piece, “Cyberwar is Coming!” by RAND authors John Arquilla and David Ronfeldt distinguished four basic categories of information warfare based on the expanded global development of information infrastructures (Table 1.3) [16].

The war forms are organized in the table in descending levels of abstract, ideological conflict.

- *Net warfare (or netwar)*—This form is information-related conflict waged against nation states or societies at the highest level, with the objective of disrupting, damaging, or modifying what the target population knows about itself or the world around it. While the target of netwar may be a nation state, the attacker need not be. The

Table 1.3

Comparison of Major Information War Forms According to Arquilla and Ronfeldt

War Form	Objective	Means	Targets
Net warfare	Manage the perception of the target population to bring about a desired influence on national behavior	Perception management by means of networked communications, and control of information to influence the full range of potential social targets	Society at large (political, economic, military)
Political warfare	Influence national government leadership decisions and policy	Measures that influence national political systems and institutions of government	Political systems
Economic warfare	Influence national government leadership decisions and policy	Measures that influence national economy via the production and distribution of goods (e.g., sanctions, blockades, and technology theft)	Economic systems
C2W (cyber warfare)	Achieve military objectives by conducting operations against military targets	Military operations conducted on information-based principles that integrate knowledge exploitation, PSYOPS, deception, and electronic warfare	Military systems

network empowers attackers that may have no physical force, enabling them to mount an effective attack in the network domain, although their force is “asymmetric” relative to the target. The weapons of netwar include diplomacy, propaganda and psychological campaigns, political and cultural subversion, deception or interference with the local media, infiltration of computer databases, and efforts to promote dissident or opposition movements across computer networks [17]. The conflict is conducted over global information infrastructures (networks). (Some have categorized net warfare actions as weapons of mass destruction [WMD] used by terrorists, predicting that terrorism will adopt higher technology means to augment physical destruction. See, for example, [18].)

- *Political warfare*—Political power, exerted by institution of national policy, diplomacy, and threats to move to more intense war forms, is the basis of political warfare between national governments.
- *Economic warfare*—Conflict that targets economic performance through actions to influence economic factors (trade, technology, trust) of a nation intensifies political warfare from the political level to a more tangible level [19].
- *Command and control warfare (C2W)*—The most intense level is conflict by military operations that target opponent’s military command and control. Ronfeldt and Arquilla used the terminology *cyberwar* for this military conflict, where we adopt the widely accepted military term for these operations conducted by military organizations. The U.S. DoD defined C2W as “the military strategy that implements Information Warfare on the battlefield and integrates physical destruction. Its objective is to decapitate the enemy’s command structure from its body of command forces” [20].

The relationships between these forms of conflict may be viewed as sequential and overlapping when mapped on the conventional conflict time line that escalates from peace to war before de-escalation to return to peace (see Figure 1.5 later in Section 1.6). Many describe netwar as an ongoing process of offensive, exploitation, and defensive information operations, with degrees of intensity moving from daily unstructured attacks to focused net warfare of increasing intensity until militaries engage in C2W. This book focuses on the information operations of netwar and C2W, although these technical operations certainly contribute to political and economic warfare forms.

A prolific author on information warfare theory, Martin Libicki, has proposed seven categories of information warfare that identify specific type of operations [21].

1. *Command and control warfare*—Attacks on command and control systems to separate command from forces;
2. *Intelligence-based warfare*—The collection, exploitation, and protection of information by systems to support attacks in other warfare forms;
3. *Electronic warfare*—Communications combat in the realms of the physical transfer of information (radioelectronic) and the abstract formats of information (cryptographic);
4. *Psychological warfare*—Combat against the human mind;
5. *Hacker warfare*—Combat at all levels over the global information infrastructure;
6. *Economic information warfare*—Control of economics via control of information by blockade or imperialistic controls;
7. *Cyber warfare*—Futuristic abstract forms of terrorism, fully simulated combat, and reality control are combined in this warfare category and are considered by Libicki to be relevant to national security only in the far term.

Author Robert Steele has used two dimensions to distinguish four types of warfare and the “information warriors” that wage them [22]. Steele’s taxonomy is organized by dividing the means of conducting warfare into two dimensions.

- The means of applying technology to conduct the conflict is the first dimension. High-technology means includes the use of electronic information-based networks, computers, and data communications, while low-technology means includes telephone voice, newsprint, and paper-based information.
- The type of conflict is the second dimension, either abstract conflict (influencing knowledge and perception) or physical combat.

From these two dimensions, Steele defines four national-level domains of IW and four warrior classes (Table 1.4). In all four categories, the ultimate objective of conflict is to change human perception and decision making

Table 1.4
War Forms and Info Warriors According to Steele

War Form	Characteristics	Info Warriors	Conflict Type	Conflict Means	Power Base
C2W	Conducted in information domain with "cyber stealth" and targeting of information in databases	High-tech seers	Info conflict	High technology	Knowledge
Medium- and high-intensity conflicts (MIC/HIC)	Conducted in the physical domain with physical stealth and precision targeting	High-tech brutes	Physical conflict	High technology	Money
Low-intensity conflicts (LIC)	Conducted in physical domain with natural stealth and random targeting	Low-tech brutes	Physical conflict	Low technology	Ruthlessness
JIHAD (ideological conflict)	Conducted in the ideological domain with ideological stealth and mass targeting of the population	Low-tech seers	Ideological conflict	Low technology	Ideology

by affecting information, but the means is different. Of course, in war, an adversary may choose to conduct all four categories of warfare, orchestrated to achieve a common information objective.

Author Winn Schwartau has extended the terminology of information warfare to apply to three domains of society: personal, corporate (or institutional), and national (or global) [23]. Although not discussed in this book, the principles of information operations apply to criminal activities at the corporate and personal levels (Table 1.5). Notice that these are simply domains of reference, not mutually exclusive domains of conflict; an individual (domain 3), for example, may attack a nation (domain 1) or a corporation (domain 2).

1.5 Defining Information Warfare and Information Operations

A formal U.S. DoD definition of information warfare covers the three central aspects to this form of conflict at the national level: information dominance, information protection, and information attack.

Table 1.5
A Taxonomy of Domains of Information Aggression

Domains of Conflict	Representative Examples
1. National (global, public sector)	<ul style="list-style-type: none"> Network warfare Economic warfare Political warfare Command and control warfare
2. Corporate (institutional, private sector)	<ul style="list-style-type: none"> Network-based information espionage, sabotage, and source intelligence Inside agent espionage or sabotage Precision physical attack on information systems (EMP, etc.) Destruction of magnetic media Notebook computer theft Exploitation of former employees and competitor product, analysis Competitor trash capture and analysis Arson, other nonprecision attacks on information systems
3. Personal (personal sector)	<ul style="list-style-type: none"> e-commerce fraud Net impersonation, spoofing, e-mail harassment, spamming Wiretapping and cell phone intercept Bank card impersonation, bank card and credit card theft Telephone harassment, "shoulder surfing" and PIN capture Credit card and database theft Computer destruction

Information warfare includes actions taken to preserve the integrity of one's own information system from exploitation, corruption, or disruption, while at the same time exploiting, corrupting, or destroying an adversary's information system and the process achieving an information advantage in the application of force [24].

Within the definition, two operational components of warfare are often distinguished. The term *information-based warfare* (IBW) is applied to the component whose focus is to acquire, process, and disseminate information (or exploit information) to achieve a dominant awareness of the battlespace. This component contributes to the information advantage by gaining knowledge.

The next component protects that knowledge while attacking an opponent's knowledge to gain a differential knowledge advantage. That component includes *information attack* and *information defend* (IW-A and IW-D) elements. Both components contribute to the goal of achieving information superiority, but by different means. In Chapter 4, we develop the meaning of information superiority more completely.

The top-level operational components of information warfare are illustrated in Figure 1.2 to describe the relationship between the major functions that comprise information operations for IW-exploit, IW-defend, and IW-attack.

In addition to the term *information warfare*, several alternative terms have been adopted to refer to specific aspects of information warfare. *Infrastructure warfare* is used by some as the most general level of warfare, with guerrilla warfare, terrorism, and information warfare as types of infrastructure warfare [25]. The terms *knowledge*, *wisdom*, and *neocortical warfare* have also been used to emphasize that the objectives of warfare are focused on creating knowledge (dynamic human understanding) to influence the human perception with great effectiveness [26–28]. Numerous taxonomies of information warfare and its components may be formed, although no single taxonomy has been widely adopted. The next subsections provide the major alternative taxonomy approaches to decompose the discipline.

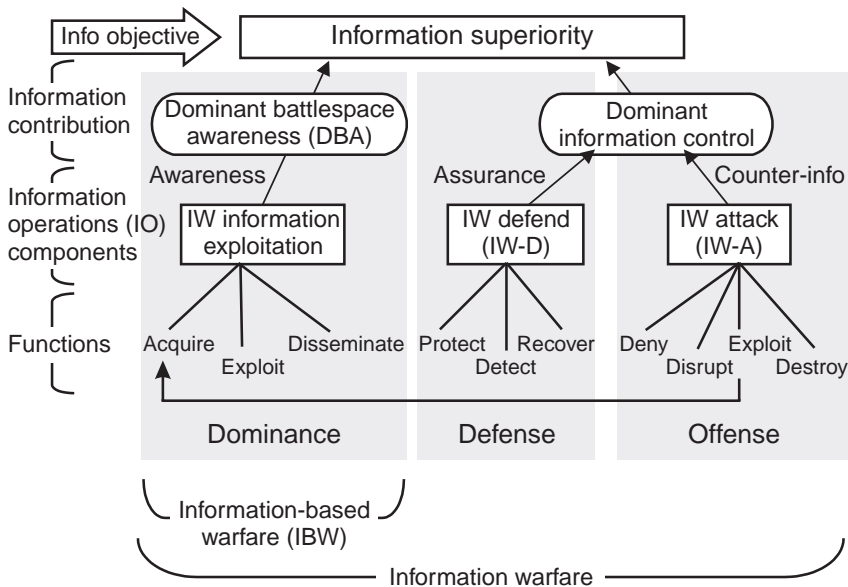


Figure 1.2 The components and goal of information warfare operations.

The emphasis of this book is on the *operations* of IW that apply at the national level where large-scale or high-technology intelligence collection, information management, command decision making, and dissemination of information are central to the warfare process. We now consider two taxonomies that categorize the functions and operations of IW.

1.5.1 A Functional Taxonomy of Information Warfare

A taxonomy may be constructed on the basis of information warfare objectives, functions (countermeasure tactics), and effects on targeted information infrastructures [29]. The structure of such a taxonomy (Figure 1.3) has three main branches formed by the three essential security properties of an information infrastructure and the objectives of the countermeasures for each.

- *Availability* of information services (processes) or information (content) may be attacked to achieve disruption or denial objectives.
- *Integrity* of information services or content may be attacked to achieve corruption objectives (e.g., deception, manipulation of data, enhancement of selective data over others).
- *Confidentiality* (or privacy) of services or information may be attacked to achieve exploitation objectives.

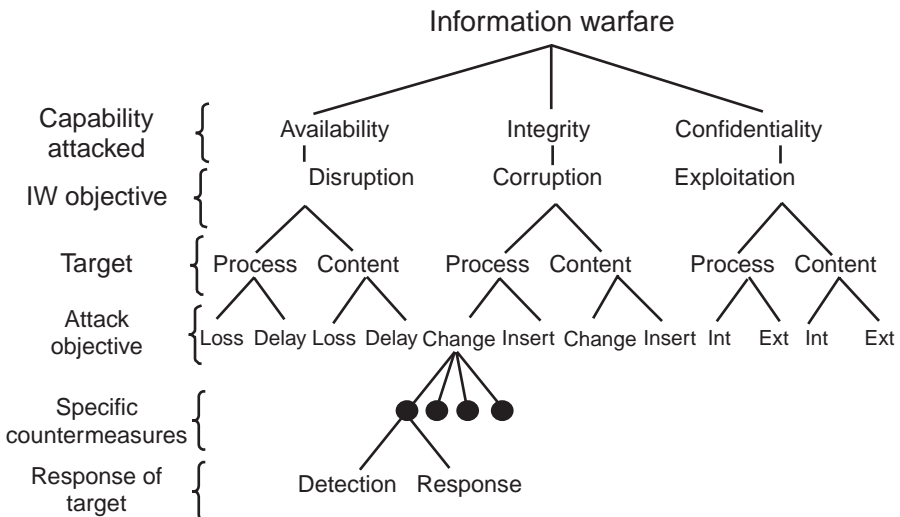


Figure 1.3 A functional taxonomy of information warfare.

Any given information warfare operation may include single or multiple complex combinations of specific tactic elements to achieve these basic objectives. The tactics may target an information service (e.g., observing the passing of messages to infer the state of an information process: idle, testing, operational, or overloaded) or the information content itself (e.g., intercepting and exploiting the information content of a message). At the branches of the taxonomy, the *functional* IW actions that are applied to achieve each objective are enumerated:

- *Disruption or denial* of services or information may be achieved by causing a loss or a temporal delay in either information content or processes (services). Jamming, overloading, or electromagnetic or physical destruction of links or processors are examples of the specific countermeasures in this category.
- *Corruption* may include replacing, inserting, or removing information or services to achieve many effects (including deception, disruption, or denial). Examples of specific countermeasures in this category include computer viruses with corruption engines, database worms, and sensor spoofers.
- *Exploitation* may be accomplished at external levels (outward observation) or at internal levels (gaining access to internal information or services by breaching security services) to gain information intended to remain confidential.

The figure illustrates how, for any given application, these branches may be extended to identify specific attack objectives for each functional type. At the bottom of the taxonomy, the degree of effect of each countermeasure may be categorized by the response of the targeted information system: detection, response, and recovery.

- *Detection*—The countermeasure may be (1) undetected by the target, (2) detected on occurrence, or (3) detected at some time after the after occurrence.
- *Response*—The targeted system, upon detection, may respond to the countermeasure in several degrees: (1) no response (unprepared), (2) initiate audit activities, (3) mitigate further damage, (4) initiate protective actions, or (5) recover and reconstitute.

This taxonomy does not extend beyond this first level of effects. The impact on any system and its users goes beyond this level and is unique to each operational attack. One type of attack, even undetected, may have minor consequences, for example, while another attack may bring immediate and cascading consequences, even if it is detected with response. For any given attack or defense plan, this taxonomy may be used to develop and categorize the countermeasures, their respective counter-countermeasures, and the effects to target systems. In later chapters, we will distinguish effects in terms of information system performance (technical degradation or destruction achieved) and their effectiveness (utility or impact on downstream users of the information system under attack.)

1.5.2 A Taxonomy of Military Operations for Information Warfare

The U.S. Air Force has established a taxonomy based on the categories of military operations that can be employed to conduct information warfare [30]. With this taxonomy, the air force defines information warfare as any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions. The first branch of the taxonomy (Table 1.6) distinguishes attack and defense operations from information operations that seek to exploit the content of information to enhance the employment of forces.

The information exploitation operations provide information by indirect collection of intelligence to infer the behavior of the adversary and the situation on the battlefield. Exploitation also includes the use of intercepted information

Table 1.6

A Military Taxonomy of Information Warfare. (From: U.S. Air Force "Cornerstones of Information Warfare," 1995.)

Operational Objective	Information Operation Category	Direct or Indirect Action	Example
Exploit information	Information exploitation operations—the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces	Direct	Interception of adversary communications to locate or extract other information
		Indirect	Surveillance and reconnaissance sensors with associated intelligence analysis

Table 1.6 (continued)

Operational Objective	Information Operation Category	Direct or Indirect Action	Example
Attack and defend information	Psychological operations—the use of information to affect the enemy’s reasoning	Direct	Insertion of video or audio messages into adversary’s media
		Indirect	Distribution of video or audio messages to public media
	Military deception—misleading the enemy about our capabilities or intentions	Indirect	Conduct misleading military operations that infer incorrect future plans or intentions
	Security measures—keeping the adversary from learning about our military capabilities and intentions		Direct defensive countermeasures
		Indirect defensive countermeasures	Physical defense, physical security, hardening, OPSEC, COMSEC, and counter-intelligence
	Electronic warfare—the denial of accurate information to the enemy using the electromagnetic spectrum	Direct	Use electromagnetic energy to directly couple deceptive information into an information system
			Indirect
	Physical destruction—affecting information system elements through the conversion of stored energy to destructive power	Direct	Attack information systems with directed energy (e.g., electromagnetic) weapons
		Indirect	Attack information centers with bombs and missiles to destroy physical infrastructure
	Information attack—corrupting information without visibly changing the physical entity within which it resides	Direct	Attack information system with malicious logic by penetrating security of an associated network to gain unauthorized access

acquired by direct access to adversary communications, networks, or information systems by penetration of security measures.

Notice that the air force document applies the term *information operations* to only these limited exploitation functions. Throughout this book, we apply this term more broadly to all information functions—exploit, defend, and attack. This adopts the broader U.S. Army definition of information operations:

Continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations: information operations include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities [31].

The attack and defend operations in this taxonomy include the following:

- *Psychological operations*—PSYOPS are activities that use information to influence the adversary's reasoning. Deception, physical destruction, information attacks, and electronic warfare may be used to achieve the psychological perception objectives that are developed by the PSYOPS activity.
- *Military deception*—Physical, electronic, and information attacks may be applied to mislead the adversary about intentions or capabilities of friendly forces.
- *Security measures*—Operation and technical security (computer and communications security) protect friendly information sources and processes to keep the adversary from learning about intents and capabilities.
- *Physical destruction*—Physical capabilities (computing, electrical power, communications, weapons, and other infrastructure) are destroyed by the conversion of stored energy to massive or surgical destructive power.
- *Electronic warfare*—Attacks through the electromagnetic spectrum are used to deny accurate information to the adversary's electronic sensors. More accurately called "electronic combat operations," this denial of accuracy includes deception, disruption, and destruction (selective or complete) of information.

Each of the above operations may be conducted by indirect means (operations that create phenomena that the adversary must then observe and analyze

to have the desired effect) or by direct means (direct attack on the information processes and content without involving the perception or analysis functions). The attack operation below applies only a direct approach.

- *Information attack*—These attacks directly corrupt the adversary’s information bases and processes by nonphysical means. In these attacks, there is no visible effect on the physical entity within which the information resides.

1.6 Expanse of the Information Warfare Battlespace

As indicated in the definitions, the IW battlespace extends beyond the information realm, dealing with information content and processes in all three realms introduced earlier in our basic functional model of warfare.

- *The physical realm*—Physical items may be attacked (e.g., destruction or theft of computers; destruction of facilities, communication nodes or lines, or databases) as a means to influence information. These are often referred to as “hard” attacks.
- *The information infrastructure realm*—Information content or processes may be attacked electronically (through electromagnetic transmission or over accessible networks, by breaching information security protections) to directly influence the information process or content without a physical impact on the target. These approaches have been distinguished as indirect or “soft” attacks.
- *The perceptual realm*—Finally, attacks may be directly targeted on the human mind through electronic, printed, or oral transmission paths. Propaganda, brainwashing, and misinformation techniques are examples of attacks in this realm.

Figure 1.4 depicts the information warfare battlespace from a functional perspective for traditional military C2W and a full information war. The figure applies the basic observe, orient, decide, act (OODA) loop developed by Col. John Boyd as a fundamental command and control model [32]. The conflict model introduced in Section 1.2 illustrated the concept without feedback, while this figure shows opposing OODA loops in conflict. In C2W, two opposing forces attempt to influence each other’s observations and military orient and decide processes.

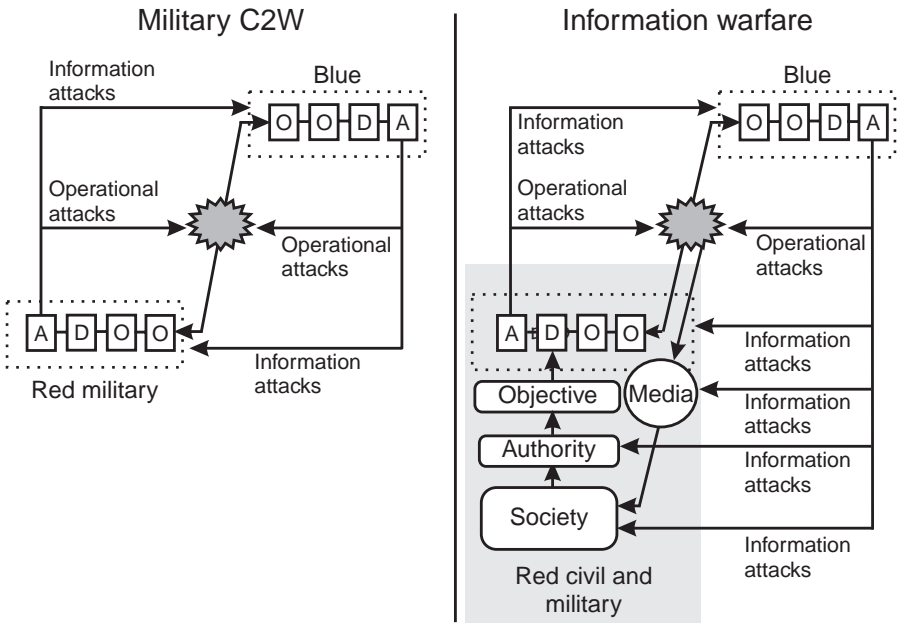


Figure 1.4 The battlespace expanse of information warfare extends beyond military C2W.

In contrast, the broader IW battlespace includes C2W attacking a defense information infrastructure (DII) and netwar that attacks a broader national information infrastructure (NII). The figure illustrates a blue IW attack on red in which society (population, private sector interests, economies); command authorities (political infrastructure and public sector); and media all come under attack in addition to the direct attack on red's DII. Both the DII and the NII are concurrent targets of a structured IW attack, which influences the OODA loop as well as the national objective of the “decide” element of the loop.

Viewed from an *operational* perspective, information warfare may be applied across all phases of operations (competition, conflict, to warfare) as illustrated in Figure 1.5. (Some lament the nomenclature “information warfare” because its operations are performed throughout all of the phases of traditional “peace.” Indeed, net warfare is not at all peaceful, but it does not have the traditional outward characteristics of war.) As in intelligence gathering (the classic information operation), network warfare activities are conducted prior to commitment to “hard attack” C2W operations in the conflict and warfare phases. In early strategic phases of competitive operations, intelligence preparation of the battlespace is performed: network topologies are surveyed,

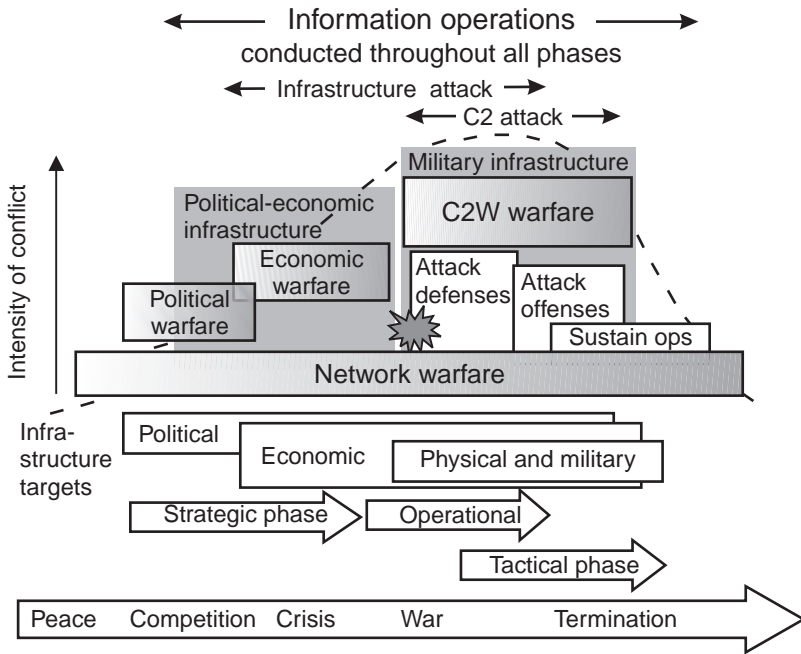


Figure 1.5 Information warfare activities extend from competition, through conflict, to war. (After: [33].)

information orders of battle are identified, and information infrastructures are modeled (political, economic, physical, and military). Political, economic, and psychological forces are applied through the global information infrastructure. As the escalation time line proceeds (competition escalates to conflict), tactical C2W activities begin attacks on the military infrastructure, beginning with defenses, with follow-on attacks on offensive capabilities, and sustained operations until resolution.

The political, economic, and physical infrastructures of many nations are in the private sector, and the defense of these nonpublic (and nonmilitary) assets becomes a joint public and private sector responsibility. While the military has always protected private sector assets in times of war, it has not had this responsibility throughout times of peace. Because information attacks are occurring in times of peace, the public and private sectors must develop a new relationship to perform the functions of indication and warning (I&W), security, and response. The U.S. Office of Management and Budget (OMB) has prepared an initial position on the role of the federal government in protecting this private sector NII. According to this report, the roles for the government

include (1) coordination of security functions, policy, and standards; (2) oversight and enforcement for public safety; and (3) technical security needs [34].

Because the IW battlespace is not defined in the physical realm (i.e., no spatial theater), it cannot be easily defined by the normal categories of conflict (crime versus war, public versus private espionage, tactical versus strategic attack distinctions or escalation criteria). “Blurred boundaries” between levels of aggression and types of attacks caused by the anonymity of net attacks complicate I&W functions and the ability to even discriminate domestic or foreign attacks [35–37]. Information warfare is also viewed as a potential adjunct to transnational threats, providing support to physical attacks with high explosives and chemical, biological, or nuclear weapons. In these cases, information operations are expected to be employed to amplify the psychological impact of physical attacks, increase panic, and impede the response of emergency services [38].

1.7 The U.S. Transition to Information Warfare

U.S. development of information warfare concepts and operations have their roots in the 1970s, when Dr. Tom Rona is credited with first coining the term [39]. Those developments were not made public until the 1990s when the DoD revealed command and control warfare concepts as a component of broader information warfare studies. Since *War and Anti-War*, a flurry of writers have published technical accounts of the information-based strategy of the Gulf War era. Col. Alan Campen’s *The First Information War* described the C4I component systems employed in the Gulf War and the benefits of the “information differential” provided by these systems to achieve deception, maneuver, and speed [40]. Neil Munro’s *The Quick and the Dead: Electronic Combat and Modern Warfare* provided specific details focusing on the essentials of electronic warfare and its impact on command and control [41]. In the same time frame, security consultant and author Winn Schwartau explained the broader threat to global information networks in a popular nonfiction book, *Information Warfare: Chaos on the Information Superhighway* [42].

Information warfare conferences, organized by the leaders of the defense and information security industry since 1993, created an open environment for the discussion of information warfare [43]. During the same period, the U.S. DoD Defense Science Board issued two separate studies and recommended significant investments in organization of IW responsibilities, protection of the DII, and IW research and development (R&D) [44,45].

Both the criticality (due to increasing dependence) and the potential vulnerability of national information systems are at the heart of this rising U.S.

concern over the threat of information conflict. In 1996, the United States acknowledged this emphasis by establishing a plan for critical information infrastructure protection via Executive Order 13010 [46].

The U.S. Joint Chiefs of Staff “Joint Vision 2010,” published in 1996, established “information superiority” as the critical enabling element that integrates and amplifies four essential operational components of twenty-first century warfare.

1. *Dominant maneuver* to apply speed, precision, and mobility to engage targets from widely dispersed units;
2. *Precision engagement* of targets by high-fidelity acquisition, prioritization of targets, and joint force command and control;
3. *Focused logistics* to achieve efficient support of forces by integrating information about needs, available transportation, and resources;
4. *Full-dimension protection* of systems processes and forces through awareness and assessment of threats in all dimensions (physical, information, perception).

Chapter 4 describes how this superiority in the information domain is enabled by command and control, fused all-source intelligence, dominant battlespace awareness, and both offensive and defensive information warfare [47].

As the specter of large-scale global information warfare has only been hypothesized, insight into possible U.S. responses to this transformation of war may be provided by the historical response to the threat of global nuclear warfare. Nuclear and information war are both technology-based concepts of warfare, but they are quite different. Consider first several similarities. Both war forms are conceptually feasible and amenable to simulation with limited scope testing, yet both are complex to implement, and it is difficult to accurately predict outcomes. They both need effective indications and warnings, targeting, attack tasking, and battle damage assessment. Nevertheless, the contrasts in the war forms are significant. Information warfare faces at least four new challenges beyond those faced by nuclear warfare.

The first contrast in nuclear and information war is the obvious difference in the physical effects and outward results of attacks. A nuclear attack on a city and an information warfare attack on the city’s economy and infrastructure may have a similar *functional* effect on its ability to resist an occupying force, but the *physical* effects are vastly different.

Second, the attacker may be difficult to identify, making the threat of retaliatory targeting challenging. Retaliation *in kind* and *in proportion* may be

difficult to implement because the attacker's information dependence may be entirely different than the defender's.

The third challenge is that the targets of information retaliation may include private sector information infrastructures that may incur complex (difficult to predict) collateral damages.

Finally, the differences between conventional and nuclear attacks are distinct. This is not so with information operations that may begin as competition, escalate to conflict, and finally erupt in to large-scale attacks that may have the same functional effects as some nuclear attacks. There are no quantum leaps in destruction as in the step-up to nuclear destruction. In the future, the IW continuum may be able to smoothly and precisely escalate in the dimensions of targeting breadth, functional coverage, and impact intensity. (This does not imply that accurate effects models exist today and that the cascading effects of information warfare are as well understood as nuclear effects, which have been thoroughly tested for over three decades.)

The development of the U.S. global strategy since the Second World War (Table 1.7) illustrates the transitions, paced by technology, that were employed to implement a strategy of deterrence to nuclear war. (Alternatives or supplements to deterrence strategies include arms control and pure defense; both are also applicable to IW.)

In each phase of an increasing nuclear threat from the Soviet Union, the United States responded with increasing maturity in two areas of capability, which lends credibility to deterrence.

- *Assured indications and warning*—National technical means were developed to quantify the threat and provide indications of preparations for attack to provide sufficient warning to react.
- *Absorption and retaliation*—Capabilities were developed to absorb a first strike and provide a credible retaliation with attacks on remaining forces and their command authorities (counterforce). This credible capability supported the doctrines of mutual assured destruction and, later, the more flexible “countervailing” strategy that emphasized balanced response to assure rapid retargeting, endurance, and survivability of forces.

Richard Harknett has succinctly summarized his valuable insight on the issue of information warfare deterrence: “As we move closer to the 21st century, ironically, it is the approach to war that dominated the early part of the 20th century (offense-defense) rather than its latter half (deterrence) that may be

Table 1.7
U.S. Global Warfare Strategy 1950–2000

1950s	1960s	1970s	1980s	1990s
Massive Retaliation	Mutual Assured Destruction (MAD)	Countervailing Strategy (CVS)	IW Defense Deterrence	
Cuban Crisis —●	Soviet Parity —●	●— PD-59	●— Gulf War	
Limited Soviet Threat	Growing Soviet Nuclear Threat	Mature Soviet Nuclear Threat	Limited but Growing IW Threat	
Small, plausible air nuclear threat	Growing ballistic missile nuclear threat—in terms of magnitude, flexibility of weapon utilization	Mature first strike capability Mobile launchers	Small unstructured threats, developing structure and technologies	
Limited covert airborne surveillance of threats	Development and deployment of national technical capabilities to monitor threat	Integrated indications and warnings Focused intelligence and surveillance from all sources	Transition to information infrastructure surveillance, intelligence	
No nuclear flexibility Limited warning Limited air defense Limited strategic power	Ability to absorb first strike and retaliate with assured destruction Second-strike counterforce capability with flexible targeting	MAD retained Flexible response: Counterforce targeting Endurance Survivability Flexible command and control	Initial IW strategy development Limited warning Limited defense Initial development of integrated information operations	

most useful for understanding information warfare” [48]. (See also [49,50] for discussions of the implications of IW and deterrence strategies.)

1.8 Information Warfare and the Military Disciplines

Organized information conflict encompasses many traditional military disciplines, requiring a new structure to orchestrate offensive and defensive operations at the physical, information, and perceptual levels of conflict.

Table 1.8 compares the roles of traditional military disciplines that must be organized in a structure that synchronizes these roles to focus offense and defense on information objectives. The functions of the OODA loop are organized across the top of the matrix, and the current military disciplines requiring synchronization are ordered on the left of the matrix. The matrix illustrates that while IW does not require the introduction of all new disciplines, it does require the careful coordination of many that already exist.

In 1996, the U.S. Defense Science Board identified the importance of revising defense organizational structure to orchestrate military disciplines. The top two recommendations to prepare for information warfare included organization activities:

Table 1.8

IW Requires Coordination of Many Existing Disciplines To Orchestrate All Information Assets To Meet IW Objectives

Discipline:	Observe		Orient		Decide	Act	
	Prepare Database	Collect	Process	Disseminate	Command	Attack Info	Defend Info
Intelligence	IPB MASINT	HUMINT, MASINT SIGINT (COMINT, ELINT) IMINT, RADINT, FISINT, OSINT		Intel linking broadcast			
Security			OPSEC				INFOSEC TCSEC COMSEC
Electronic Combat		ES (ESM)				EA (ECM, EMP, EO/IRCM)	EP (ECCM)
Command and Control	C2 doctrine		C2				
Special Operations						Special ops PSYOPS	
Network Operations	Network IPB					Network attack ops	

Designate an accountable IW focal point—This is the most important recommendation the Task Force offers. The Task Force believes the Secretary of Defense needs a single focal point charged to provide staff supervision of the complex activities and interrelationships that are involved in this new warfare area. This includes oversight of both offensive and defensive information warfare planning, technology development and resources [51].

And the second recommendation:

Organize for IW-D—This key recommendation identifies the need for specific IW-D [IW-Defense] related capabilities and organizations to provide or support the capabilities. While not specifically addressed by the Task Force, virtual organizations that draw on existing assets and capabilities can be established [51].

Some have even suggested that the traditional structure of second-wave geophysical-based armed forces (air, land, sea) must be revised to conduct third-wave information warfare. Martin Libicki, in *The Mesh and the Net*, introduces the concept of a separate information corps as a natural outcome of increasing emphasis on information doctrine. Such a corps would be responsible for establishing information warfare doctrine, developing battle plans, and carrying them out. Libicki argues that the creation of such a corps would, “promote jointedness where it is critically needed (information interoperability), elevate information as an element of war, develop an information warrior ethos and curriculum, and heighten [U.S.] DoD attention to the global civilian net” [52]. This is a long-term view, indeed, that would essentially place all services under direction of such a command to conduct IW. While the United States has assigned the strategic nuclear mission to the strategic command (STRATCOM), the nuclear mission is not as pervasive as that of IW. The U.S. DoD has chosen, instead, to emphasize joint service command and control, information security, and intelligence coordination rather than designating a strategic service with the mission of information warfare.

1.9 Information and Peace

Information technology not only provides new avenues for conflict and warfare, but it also provides new opportunities for defense, deterrence, de-escalation, and peace. While this book focuses on the defensive and offensive

aspects of information warfare, it is necessary that information-based deterrence be briefly considered here because deterrence, the decisions to commit to war, and approaches to peace have counterparts in information technology.

In *War and Anti-War*, the Tofflers argue that while the third-wave war form is information warfare, the third-wave peace form is also driven by the widespread availability of information to minimize misunderstanding of intentions, actions, and goals of competing parties. Even as information is exploited for intelligence purposes, the increasing availability of this information has the potential to reduce uncertainty in nation states' understanding of each other. Notice, however, that information technology is a two-edged sword, offering the potential for cooperation and peace, or its use as an instrument of conflict and war. As with nuclear technology, humankind must choose the application of the technology.

Consider a few of the practical means by which information availability may be supportive of the goals of cooperation rather than competition and conflict.

- *Open networks*—Open networks enable a free exchange of ideas, promoting democratic practices while countering oppressive forms of government that control information flow. The open flow of information between countries also reduces misunderstanding of capabilities, intentions, and doctrine.
- *Open space and skies*—The availability of commercial spaceborne imagery and aircraft overflights by treaty [53] reduces errors in estimation of neighbor's military capabilities, operations, and posture.
- *Open treaties*—Open inspection treaties on weapons of mass destruction and the flow of information on capabilities and remedies further reduces errors in estimates of threats [54].
- *Open communication*—The increased capability for communication at global distance provides the means for rapid and continuous exchange of information to deescalate misunderstandings and to respond to provocation with effective, informed diplomatic actions.

In addition to the negative concept of information as a deterrent force, some view information capabilities as a positive force. Nye and Owens have enumerated four ways in which the United States should apply its information edge (advantage) as a diplomatic “soft power” force multiplier to attract (rather than coerce) nations toward American democracy and free markets [55]. They

suggest that information resources provide powerful tools to engage nations in security dialogue and to foster emerging democracies by the power to communicate directly to those living under hostile, undemocratic regimes. The authors recommended four peace-form activities that may be tasked to information peacemakers.

1. *Engage undemocratic states and aid democratic traditions*—Information tools, telecommunications, and broadcast and computer networks provide a means to supply accurate news and unbiased editorials to the public in foreign countries, even where information is suppressed by the leadership.
2. *Protect new democracies*—Ideological training in areas such as democratic civil/military relationships can support the transfer from military rule to democratic societies.
3. *Prevent and resolve regional conflicts*—Telecommunication and network information campaigns provide a means of suppressing ethnonationalist propaganda while offering an avenue to provide accurate, unbiased reports that will abate rather than incite violence and escalation.
4. *Deter crime, terrorism, and proliferation, and protect the environment*—Information resources that supply intelligence, indications and warnings, and cooperation between nations can be used to counter transnational threats in each of these areas.

1.10 The Current State of Information Warfare

At the writing of this book, it has been well over a decade since the concept of information warfare was introduced as a critical component of the current revolution in military affairs (RMA). In this short period, investments in technology, operational analyses, and military restructuring have been committed to define the implementation of an information warfare capability in several third-wave nations, led by the United States. These developments are in flux. The student of this discipline must keep abreast of the state of the military art, the state of the operational implementations, and the state of relevant information warfare technology. The following paragraphs briefly summarize the state of these areas in the U.S. at the current time.

1.10.1 State of the Military Art

The U.S. National Defense University has established a School of Information Warfare and Strategy curriculum for senior officers to study IW strategy and policy and to conduct directed research at the strategic level. The Joint Chiefs of Staff have issued a Memorandum of Policy on Information Warfare (MOP 30) and the DoD has issued Directive 3600.1 defining the mission and roles for IW. Each of the services and the Joint Chiefs of Staff are preparing lower level directives and documents guiding the phased implementation of IW organizations and doctrine. Each of the military services have established IW “centers of excellence” to conduct IW war-gaming and vulnerability analyses, to provide technical R&D and technical liaison to users, to develop computer emergency response teams (CERTs), and to conduct training. Concurrent with the development of policy and doctrine, the implications of information warfare on international law and treaties are being examined to assess the legal and moral stature of this new war form [56]. The United States is investigating transitional and future legal bases for the conduct of information warfare because the character of some information attacks (anonymity, lack of geospatial focus, ability to execute without a “regulated force” of conventional “combatants,” and use of unconventional information weapons) are not consistent with current accepted second-wave definitions in the laws of armed conflict.

1.10.2 State of Operational Implementation

The doctrine of information dominance (providing dominant battlespace awareness and battlespace visualization) has been established as the basis for structuring all command and control architectures and operations. The services are committed to a doctrine of joint operations, using interoperable communication links and exchange of intelligence, surveillance, and reconnaissance (ISR) in a global command and control system (GCCS) with a common software operating environment (COE). In addition, the services have also established dedicated initial operational IW units with offensive missions. Joint service war-gaming and training are beginning to integrate IW strategy, operations, and tactics into conventional operations. The emphasis on information dominance has also accelerated the development of IW-D doctrine.

1.10.3 State of Relevant Information Warfare Technology

The technology of information warfare, unlike previous war forms, is driven by commercial development rather than classified military research and

development. The breadth of IW technology is wide, including the use of commercial information technologies (only a few are export-controlled) and the development of selected military-unique technologies. Unlike nuclear warfare or early information technologies (e.g., cryptography, information security [INFOSEC], TEMPEST electromagnetic hardening) developed over the past 25 years, military control of the technology is very limited. Key technology areas now in development include the following:

- Intelligence, surveillance, and reconnaissance (ISR) and command and control (C2) technologies provide rapid, accurate fusion of all-source data and mining of critical knowledge to present high-level intelligence to information warfare planners. These technologies are applied to understand geographic space (terrain, road networks, physical features) as well cyberspace (computer networks, nodes, and link features).
- Information security technologies include survivable networks, multi-level security, network and communication security, and digital signature and advanced authentication technologies.
- Information technologies, being developed in the commercial sector and applicable to information-based warfare, include all areas of network computing, intelligent mobile agents to autonomously operate across networks, multimedia data warehousing and mining, and push-pull information dissemination.
- Electromagnetic weapon technologies, capable of nonlethal attack of information systems for insertion of information or denial of service.
- Information creation technologies, capable of creating synthetic and deceptive virtual information (e.g., morphed video, synthetic imagery, duplicated virtual realities).

For a continuing update of these rapidly developing areas, the sources listed in Table 1.9 provide basic sources for monitoring the state of the art. In addition, numerous Web sites in governments, academia, and industry must be also monitored to maintain current in this area. The final chapter of this book details these technology areas and recommends that serious students of information warfare must maintain a watch on the progress in these critical technologies.

Table 1.9

Primary Sources for Information Warfare Policy, Strategy, Operations, and Technology Developments

Area	Principal Sources
National policy, operations, standards, and military science	<p>U.S. National Defense University—<i>Strategic Forum</i>, monographs, and conference papers by staff and researchers</p> <p><i>Journal of Infrastructure Warfare</i>—Prepares high-level analyses and publishes articles on infrastructure warfare and conflict activities worldwide</p> <p>U.S. Defense Science Board—Annual reports and results of studies</p> <p>RAND Corp—Review, research briefs, and research reports</p> <p>CERT—Reports and advisories of the computer emergency response team (CERT) Coordinating Center of the Software Engineering Institute of the Carnegie Mellon University</p> <p>U.S. National Security Agency—INFOSEC security standards</p> <p>National Institute of Standards and Technology (NIST)—Standards and technical publications on cryptography, digital signatures, and key management</p>
Technologies	<p><i>Aviation Week and Space Technology</i>—Weekly publication reports on information warfare technologies, threats, and reported operations</p> <p><i>Proceedings of InfoWarCon Conferences</i>—Administered by the International Computer Security Association (ICSA) and associated organizations (including Interpact and OSS)</p> <p><i>ICSA News</i>—Periodical of the International Computer Security Assoc.</p> <p><i>Proceedings of IEEE Conferences on Computer Security</i></p> <p><i>Journal of Electronic Defense</i>—Technical articles on INFOSEC and electronic warfare</p> <p><i>Communications of the ACM</i>—Computer technology and network security</p> <p>Defense Advances Research Projects Agency (DARPA)—Reports on information survivability technologies from the Information Technology Office (ITO) and information technology for C4ISR from the Information Systems Office (ISO)</p> <p><i>Proceedings of the National Sensor and Data Fusion Symp.</i>—Annual U.S. DoD symposium on research in sensor and data fusion technologies</p> <p><i>Signal</i>—Magazine of the Armed Forces Communications Electronics Assoc. (AFCEA) describes IW technology and operations</p> <p><i>Proceedings of Open Source Solutions (OSS) Technology Conferences</i>—Sponsored by Open Source Solutions to study open source intelligence, multimedia information analysis</p> <p><i>Proceedings of International Conferences on Command and Control</i>—Sponsored annually by the National Defense University on advanced command and control research and technology</p> <p><i>Janes' Intelligence Review</i>—International intelligence periodical includes articles on military operational and technological capabilities</p>

1.11 Summary

Information warfare is real. Information operations are being conducted by both military and non-state-sponsored organizations today. While the world has not yet witnessed nor fully comprehended the implications of a global information war, it is now enduring an ongoing information competition with sporadic conflicts in the information domain.

The following chapters focus not on the event of information war, but on the operations of information warfare. The book is divided into two parts, following the taxonomy we have adopted to partition information warfare.

Part I (Chapters 2–4) describes the elements of information-based warfare that focus on information dominance. Chapter 2 introduces the information sciences that define and quantify what we mean by information. Chapter 3 introduces the information technologies that permit the creation of knowledge from raw data. Approaches to achieve dominant battlespace awareness and knowledge, the goal of information-based warfare, are then described in Chapter 4.

Part II (Chapters 5–10) focuses on the offensive and defensive operations of information warfare. The basis of IW strategy, policy, and operations are described in Chapter 5. In Chapter 6, the operations for C2W and net warfare are explained, and an operational concept (CONOPS) for IW is developed in Chapter 7. Offensive and defensive operational tactics and technical techniques are detailed in Chapters 8 and 9, respectively. Chapter 10 enumerates the core, enabling, and emerging technologies that will pace the implementation of information operations in the future.

Endnotes

- [1] These engineering distinctions are refinements of the common terminology to distinguish three levels of information *content*. General dictionary definitions of information often include data and knowledge as synonyms.
- [2] Proverbs 24:5–6, New American Standard Version of the Bible (NASB).
- [3] The quotations are based upon *Sun Tzu on the Art of War*, translated by Lionel Giles, 1910. (Electronic text in the public domain May 1994.)
- [4] Statements by U.S. secretary of state indicating in-kind response to weapons of mass destruction are presumed to be an influencing factor in Iraqi command withholding available chemical-biological weapons. Due to weapons conventions, the United States does not maintain chemical-biological weaponry, but considers nuclear forces as mass destruction weapons, implying the threat of a nuclear response to chemical-biological attacks. See

- Baker, J. A. III, with T. M. DeFrank, *The Politics of Diplomacy: Revolution, War and Peace, 1989–1992*, New York: G. P. Putnam's Sons, 1995, p. 359.
- [5] Military strategist Karl von Clausewitz perhaps would not consider some forms of information warfare as “warfare” at all, because they are “bloodless” events.
- [6] Szafranski, R., (Col. USAF), “A Theory of Information Warfare: Preparing for 2020,” *Airpower Journal*, Vol. 9, No. 1, Spring 1995.
- [7] Whitehead, Y. L., (Maj. USAF), “Information as a Weapon: Reality Versus Promise,” *Airpower Journal*, Vol. 11, No. 3, Fall 1997.
- [8] Information-based warfare (IBW) emphasizes the use and exploitation of information for advantage—often in support of physical weapons and targets—while information warfare (IW) emphasizes the use of information *itself* as a weapon and target.
- [9] Toffler, A., *The Third Wave*, New York: Bantam, 1980.
- [10] Toffler, A., *Powershift*, New York: Bantam, 1990.
- [11] Toffler, A., and H. Toffler, *War and Anti-War*, Boston: Little, Brown and Company, 1993.
- [12] Senge, P. M., *The Fifth Discipline: The Art and Practice of the Learning Organization*, New York: Doubleday, 1990.
- [13] von Clausewitz, C., *On War*, New York: Viking Press, 1983.
- [14] van Creveld, M., *The Transformation of War*, New York: Free Press, 1991.
- [15] See, for example, Lind, W. S., et al., “The Changing Face of War: Into the Fourth Generation,” *Marine Corps Gazette*, Oct. 1989, p. 23. In this article, four generations of warfare types are enumerated: (1) massed manpower warfare, (2) massed firepower warfare, (3) maneuver warfare, and (4) terrorism-like warfare. This concept was refined by Hammes to modify the fourth category to be net warfare. See Hammes, T. X., “The Evolution of War: The Fourth Generation,” *Marine Corps Gazette*, Sept. 1994, p. 35.
- [16] Arquilla, J., and D. F. Ronfeldt, “Cyberwar is Coming!,” *J. Comparative Strategy*, Vol. 12, No. 2, Apr.–June, 1993, pp. 141–165.
- [17] Adapted from, Arquilla, J., and D. F. Ronfeldt, “Cyberwar is Coming!,” In this seminal work on information warfare, the authors use the term “cyberwar” to refer to the category C2W and “netwar” to refer more broadly to high-technology, abstract warfare of the future.
- [18] Campbell, J. K., *Weapons of Mass Destruction Terrorism*, Interpact Press, 1997.
- [19] Fialka, J. J., *War by Other Means*, New York: W.W. Norton, 1997.
- [20] U.S. Memorandum of Policy, MOP 30, see also Joint Services Publication 3-13, and DODD 3222.4, “Electronic Warfare (EW) and Command and Control Warfare (C2W) Countermeasures,” July 31, 1992. USD(A) provides the following detailed definition: “The integrated use of operations security (OPSEC), joint military deception, psychological operations (PSYOPS), electronic warfare (EW), and physical destruction, mutually

supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions.”

- [21] Libicki, M., “What Is Information Warfare?,” Center for Advanced Concepts and Technology, National Defense University, 1995, p. 7.
- [22] Steele, R. D., (USMCR), “The Transformation of War and the Role of the Future of the Corps,” USMC document approved for public release, April 28, 1992. For a refined presentation of the concept, see “Creating a Smart Nation: Information Strategy, Virtual Intelligence, and Information Warfare” in *Cyberwar: Security, Strategy and Conflict in the Information Age*, Fairfax, VA: AFCEA Press, pp. 78–79.
- [23] Schwartz, W., *Information Warfare: Chaos on the Information Superhighway*, New York: Thunder’s Mouth Press, 1994.
- [24] Joint Chiefs of Staff, JCS Pub 1-02, Mar. 1995. It is important to note that numerous definitions have been proposed and this is cited as a *representative* definition.
- [25] *The Journal of Infrastructure Warfare*, electronic online journal only, URL: www.iwar.com.
- [26] Murphy, E. F., (Lt. Col.), et al., “Information Operations: Wisdom Warfare for 2025,” Maxwell AFB, Apr. 1996.
- [27] Baumard, P., “From InfoWar to Knowledge Warfare: Preparing for the Paradigm Shift,” in *Cyberwar: Security, Strategy and Conflict in the Information Age*, Fairfax, VA: AFCEA Press, 1996, pp. 147–160.
- [28] Szafranski, p. 44.
- [29] For the basis of this taxonomy, see Appendix C, *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)*, Office of Undersecretary of Defense for Acquisition and Technology, Pentagon, Washington, D.C., Nov. 1996.
- [30] “Cornerstones of Information Warfare,” Department of the Air Force, 1995.
- [31] “Information Operations,” FM-100-6, HQ Department of the Army, Washington, D.C., Aug. 27, 1996, Glossary.
- [32] The OODA loop was developed by Col. John Boyd (USAF) in a classic briefing presented at Maxwell AFB entitled “A Discourse on Winning and Losing,” in Aug. 1987. The concept is described in Orr, G. E., *Combat Operations C3I: Fundamentals and Introductions*, Maxwell AFB, AL: Air University Press, p. 198.
- [33] Caldarella, R. J. (Capt., USN), “Information Warfare: The Vision,” in *Proc. of TMSA Information Warfare Conference*, Washington, D.C., June 12–13, 1995, p. 32.
- [34] “NII Security: The Federal Role,” U.S. Office of Management and Budget, June 14, 1995.
- [35] Molander, R. C., A. S. Riddle, and P. A. Wilson, “Strategic Information Warfare: A New Face of War,” MR-661-OSD, RAND Corp., 1996.

- [36] Anderson, R. H., and A. C. Hearn, "An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: The Day After... in Cyberspace II, MR-797-DARPA," Santa Monica, CA, RAND, 1996.
- [37] Hundley, R. O., and R. H. Anderson, "Emerging Challenge: Security and Safety in Cyberspace," RAND/DRR-1382-CMS, RAND Corp., 1996.
- [38] "DSB Warns IW Will Be Amplifying Tool of Transnational Threats," Defense Information and Electronics Report, Jan. 9, 1998, p. 3.
- [39] Dr. Thomas P. Rona is often credited with first applying the term "information warfare" and has performed research for the U.S. DoD throughout the mid 1990s on the historical, theoretical, and operational concepts of IW. See his article, "From Scorched Earth to Information Warfare" in *Cyberwar: Security, Strategy and Conflict in the Information Age*, Fairfax, VA: AFCEA Press, pp. 9–11.
- [40] Campen, A., *The First Information War*, Fairfax, VA: AFCEA International Press, 1992.
- [41] Munro, N., *The Quick and the Dead: Electronic Combat and Modern Warfare*, New York: St. Martin's Press, 1991.
- [42] Schwartau, W., *Information Warfare: Chaos on the Information Superhighway*, New York: Thunder's Mouth Press, 1994.
- [43] Sponsors include the International Computer Security Industry Association (ICSA), Interpact, and Open Source Solutions.
- [44] "Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield," Defense Science Board, Office of Secretary of Defense, Oct. 1994.
- [45] "Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)," Defense Science Board, Office of Secretary of Defense, Nov. 1996.
- [46] Executive Order 13010, "Critical Infrastructure Protection," July 15, 1996, Federal Register: March 3, 1997, Vol. 62, No. 41, pp. 9349 ff.
- [47] "Joint Vision 2010," U.S. Joint Chiefs of Staff, 1996.
- [48] Harknett, R. J., "Information Warfare and Deterrence," *Parameters*, U.S. Army War College, Autumn 1996, pp. 93–107.
- [49] Berkowitz, B. D., "Warfare in the Information Age," *Issues in Science and Technology*, National Academy of Sciences, Fall 1995, pp. 59–66.
- [50] Thomas, T. L., "Deterring Information Warfare: A New Strategic Challenge," *Parameters*, U.S. Army War College, Winter 1996–97, pp. 81–91.
- [51] "Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)," Defense Science Board, Office of Secretary of Defense, Nov. 1996, p. 11.
- [52] Libicki, M., *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, National Defense University, Washington, D.C., 1994, p. 69.

-
- [53] Krepton, M., and A. Smithson, *Open Skies, Arms Control and Cooperative Security*, New York: St. Martin's Press, 1992.
 - [54] Tsipsis, K., D. Hafemeister, and P. Janeway, (eds.), *Arms Control Verification: The Technologies That Make It Possible*, Washington, D.C.: Pergamon-Brassey's, 1986.
 - [55] Nye, J. S. Jr., and W. A. Owens, "America's Information Edge," *Foreign Affairs*, Mar./Apr., 1996, pp. 20–36.
 - [56] Aldrich, R. W. (Maj. USAF), "The International Implications of Information Warfare," *Airpower Journal*, Fall 1996, pp. 99–110.

Part I

Information-Based Warfare

2

The Role of Information Science in Warfare

Because information is the central resource for competition, conflict, and warfare in both nation states and businesses, it is critical that this resource be accurately defined, measured, and valued. We would like to measure, quantify, and inventory the information resource (and its production rate), like the resources of civilization's prior waves, to assess the effectiveness of businesses or war-fighting capabilities. However, this is not an easy task and, indeed, it is a key challenge of the information age. Information, as a resource, is not like the land or material resources that were central to the first and second waves.

Consider several characteristics of the information resource that make it unique, and difficult to quantify.

- *Information is abstract*—It is an intangible asset; it can take the form of an entity (a noun—e.g., a location, description, or measurement) or a process (a verb—e.g., a lock combination, an encryption process, a patented chemical process, or a relationship).
- *Information has multiple, even simultaneous uses*—The same unit of information (e.g., the precise location and frequency of a radio transmitter) can be used to exploit the transmissions, to selectively disrupt communications, or to precisely target and destroy the transmitter. Information about the weather can be used simultaneously by opposing forces, to the benefit of both sides.
- *Information is inexhaustible, but its value may perish with time*—Information is limitless; it can be discovered, created, transformed, and

repeated, but its value is temporal: recent information has actionable value, old information may have only historical value.

- *Information's relationship to utility is complex and nonlinear*—The utility or value of information is not a function simply of its volume or magnitude. Like iron ore, the utility is a function of content, or purity; it is a function of the potential of data, the content of information, and the impact of knowledge in the real world. This functional relationship from data to the impact of knowledge is complex and unique to each application of information technology.

Because of these characteristics, it is essential to precisely define information, the critical resource of all forms of warfare, and especially information warfare. In this chapter, the disciplines of philosophy and science that study and define information and knowledge are introduced, and alternative measures of information will be described. We will then apply these principles to information warfare by describing methods to measure the utility of information to determine its contribution in warfare.

2.1 The Meaning of Information

In the first chapter, we introduced the notion of distinguishing three levels of abstraction for the resource we call information: data, information, and knowledge. Before moving on, we will further characterize this information model and use it as the basis for the remainder of this book.

Figure 2.1 illustrates the three-level cognitive hierarchy that moves from data (the least abstract, or most detailed and specific) to knowledge (the most general, or abstract, or conceptual form) [1]. The *observation* process acquires data about some physical process (e.g., combatants on the battlefield, a criminal organization, a chemical plant, an industry market) by the measurement and quantification of observed variables. The observations are generally formatted into *reports* that contain items such as time of observation, location, collector (or sensor or source) and measurements, and the statistics describing the level of confidence in those measurements. An *organization* process converts the data to *information* by indexing the data and organizing it in context (e.g., by spatial, temporal, source, content, or other organizing dimensions) in an information base for subsequent retrieval and analysis. The *understanding* process creates *knowledge* by detecting or discovering relationships in the information that allow the data to be explained, modeled, and even used to predict future behavior of the process being observed. At the highest (and uniquely human) level,

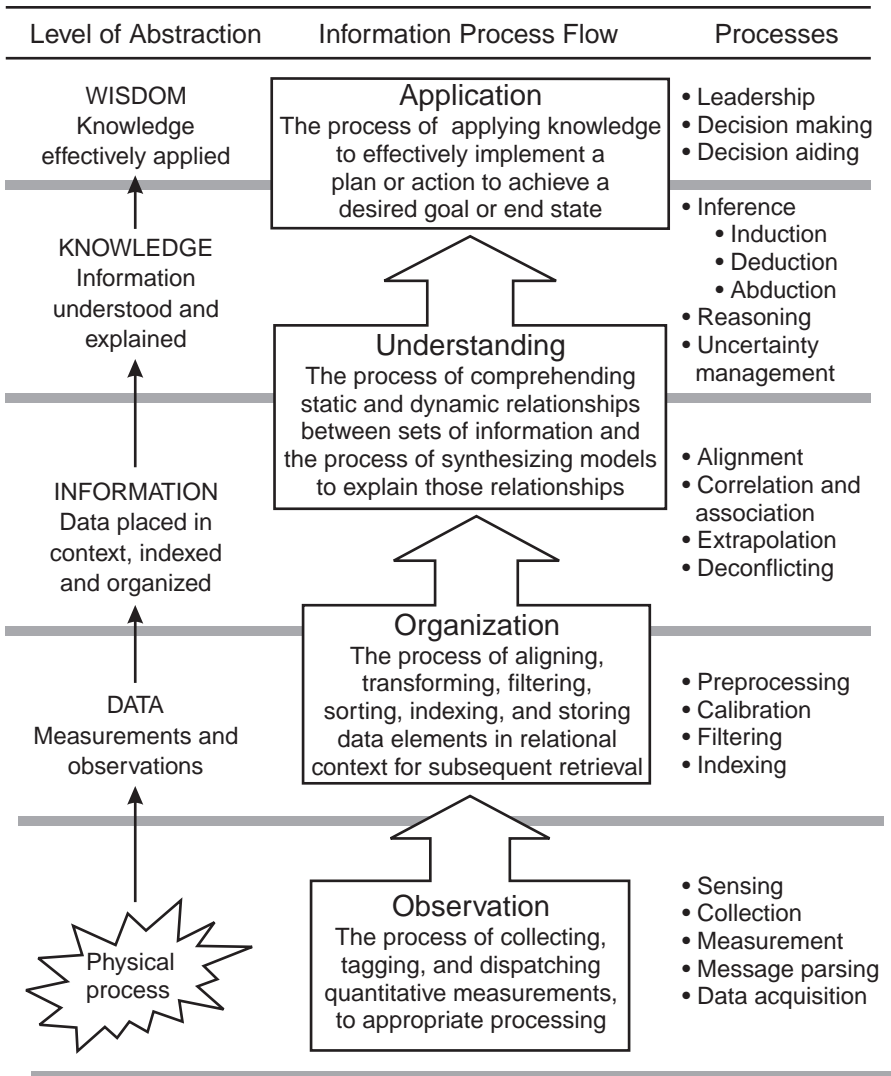


Figure 2.1 Information hierarchy defines three levels of information: data, information, and knowledge.

wisdom is the ability to effectively apply knowledge to implement a plan or action to achieve a desired goal or end state.

Throughout this book, we will carefully distinguish between these levels, and use the general term *information* when referring to information in all of its forms.

If we apply the hierarchical definitions to the four information-intense disciplines of business, technology, philosophy, and military science, we can readily distinguish each level of information and define the ultimate objective for using information (Table 2.1). In business, for example, the objective is to create capital value, and the data necessary is a description of the marketplace (customers, purchase volumes, demographics, parametric trends). This data is organized and analyzed to provide the information base describing the market, its segments, and the potential positions for products and services. From this base, a business plan explains the market and the strategic approach (knowledge) to carry out the business, with predictions of outcomes for alternative moves. Similarly, the military objective is to achieve a desired end state in a conflict (e.g., conquest, de-escalation, termination, and resolution). Data collected includes the opponent's order of battle, the environment (battlespace), and other constraints to the conflict. From this data, an information base is prepared ("intelligence preparation of the battlespace"). From this base, the situation and potential courses of action are modeled and explained (knowledge, or in military parlance, *intelligence*), and human commanders choose the strategy and tactics. In this book, we will discuss the information technology (IT) and automation of these information-intensive processes for information warfare applications.

We also use the terminology *creation* or *discovery* to refer to the effect of transforming data into useful knowledge. Several examples of discovering previously unknown knowledge by the processes of analyzing raw data include the detection or location of a battlefield target, the identification of a purchasing pattern in the marketplace, distinguishing a subtle and threatening economic action, the cataloging of the relationships between terrorist cells, or the classification of a new virus on a computer network.

Notice that knowledge is not necessarily equivalent with human perception because perception is yet a deeper process than studied in immaterial terms by psychology. Meaning itself, the object of perception, is even more difficult to measure. The authors of the *Measurement of Meaning* have summed up the issue:

[Meaning] certainly refers to some implicit process or state which must be inferred from observables, and therefore it is a sort of variable that contemporary psychologists would avoid dealing with as long as possible. And there is also, undoubtedly, the matter of complexity—there is an implication in the philosophical tradition that meanings are uniquely and infinitely variable, and phenomena of this kind do not submit readily to measurement [2].

Table 2.1
Representations of Data, Information, and Knowledge in Four Information-Intense Disciplines

Area of study	Business	Technology	Philosophy	Military Science
Focus of study:	How do I create capital value?	How do I innovate?	How do I know?	How do I win the conflict?
Data Observations The data or basic elements that are the source of all further study	Market and economic measurements (e.g., market parameters, sales, bookings, profit/loss, capital expenses)	Physical measurements Abstract concepts	Empirical observations about the world Conceptual reasoning about ideas	Observations of the environment and actions of friendly and opponent's forces
Information Related, organized data	Analyses and models of market and economic behavior	Theories and models of physical properties and processes, and abstract information processes	Theories of reality and truth developed by reasoning (deduction, induction)	Analyses and models of force behavior Target tracks Organization structure
Knowledge Related, organized, contextualized information Understanding	Knowledge about business processes: Strategic concepts, plans Markets and customers Competition Economy	Knowledge about objects of science: Physical processes and properties Abstract information concepts and processes)	Knowledge about reality and knowledge itself: What is ultimate reality (metaphysics) What is knowledge (epistemology) What is right (ethics)	Knowledge about conflict processes: Environment and influence on conflict Tactical courses of action Opponent intent
Wisdom Applying knowledge to achieve an end	Applied to defining and achieving business success	Applied to research into new properties and processes and to the development of applications	Applied to the quest for human knowledge and understanding	Applied to peaceful resolution, de-escalation and conquest (social, economic, military)

In addition to the levels of abstraction of information, we may distinguish between different types of information. In the business classic on the use of information, *The Virtual Corporation*, Davidow and Malone [3] distinguish four categories of information (Table 2.2).

- *Content information*—This describes the state of physical or abstract items. Inventories and accounts maintain this kind of information; the military electronic order of battle (EOB) is content information.
- *Form information*—This describes the characteristics of the physical or abstract items; the description of a specific weapon system in the EOB is a form.
- *Behavior information*—In the form of process models this describes the behavior of objects or systems (of objects); the logistics process supporting a division on the battlefield, for example, may be modeled as behavior information describing supply rate, capacity, and volume.
- *Action information*—This is the most complex form, which describes reasoning processes that convert information to knowledge, upon which actions can be taken. The processes within command and control decision support tools are examples of Davidow’s action information category.

In a classic text on strategic management of information for business, *Managing Information Strategically*, the authors emphasized the importance of understanding its role in a *particular* business to develop business strategy first, then to develop information architectures. They note, “Leading organizations have elevated information to the same level as other critical resources, such as capital and labor. They pursue a strategy design process that considers information and information technology capabilities as a key design variable from the outset” [4]. The authors identify three competitive strategies to exploit IT in business, and each is applicable to IBW [5].

- *Information leverage*—In this strategy, IT enables process innovation, amplifying competitive dimensions. An IBW example of this strategy is the application of data links to deliver real-time targeting to weapons (sensor-to-shooter applications) to significantly enhance precision and effectiveness.
- *Information product*—This strategy captures data in existing processes to deliver information or knowledge (a by-product) that has a benefit

Table 2.2
Four Categories of Information With Examples in Business and Information Warfare

Category	Level of Understanding	Business Applications	Warfare Applications
Content information	Historical record describing the existence, location, and state of physical items (inventory) and abstract entities (accounts)	Inventory systems Customer files Billing systems	Force inventory Orders of battle Orders, personnel records
Form information	Static description of the physical shape and composition of objects	Product description Real estate property description CAD/CAM models Geographic information systems (GIS) for demographic information	Automatic target recognition (ATR) target descriptions (model-based) Force model descriptions Geographic information systems (GIS) for battlefield environment
Behavior information	Dynamic description of the behavior of an object or system of objects—a behavior model	Engineering simulations Market dynamic models	Weapon simulations (design) Weapon simulations for real-time threat models Battle management simulation tools
Action information	Reasoning processes that provide decision-making advice and perform independent control of business operations	Industrial robotics Machine vision for inspection Automated stock trading	Battle management decision aids Automated fire control Automated sensor management

(market value) in addition to the original process. Intelligence processes in IBW that collect vast amounts of data may apply this strategy to utilize the inherent information by-products more effectively. These by-products may support civil and environmental applications (markets) or support national economic competitive processes [6].

- *Information business*—The third strategy “sells” excess IT capacity, or information products and services. The ability to share networked computing across military services or applications will allow this

strategy to be applied to IBW applications, within common security boundaries.

2.2 Information Science

We find useful approaches to quantifying data, information, and knowledge in at least six areas: the epistemology and logic branches of philosophy, the engineering disciplines of information theory and decision theory, the semiotic theory, and knowledge management. Each discipline deals with concepts of information and knowledge from a different perspective, and each contributes to our understanding of these abstract resources. In the following sections, we summarize the approach to define and study information or knowledge in each area.

2.2.1 Philosophy (Epistemology)

The study of philosophy, concerned with the issues of meaning and significance of human experience, presumes the existence of knowledge and focuses on the interpretation and application of knowledge. Because of this, we briefly consider the contribution of epistemology, the branch of philosophy dealing with the scope and extent of human knowledge, to information science.

Representative of current approaches in epistemology, philosopher Immanuel Kant [7] distinguished knowledge about things in space and time (*phenomena*) and knowledge related to faith about things that transcend space and time (*noumena*). Kant defined the processes of sensation, judgment, and reasoning that are applied to derive knowledge about the phenomena. He defined three categories of knowledge derived by judgment: (1) *analytic a priori* knowledge is analytic, exact, and certain (such as purely theoretical, imaginary constructs like infinite straight lines), but often uninformative about the world in which we live; (2) *synthetic a priori* knowledge is purely intuitive knowledge derived by abstract synthesis (such as purely mathematical statements and systems like geometry, calculus, and logic), which is exact and certain; and (3) *synthetic a posteriori* knowledge about the world, which is subject to human sense and perception errors. The sensed data and derived information and knowledge discussed in this book are of the latter category—the world of science and engineering. From a philosophical viewpoint, this knowledge is the most unreliable and least useful in the study of metaphysical (beyond physics) subjects and ultimate reality, and therefore it is the least studied in philosophy; but it is also the most applied in science and engineering.

2.2.2 Philosophy (Logic)

Philosophy has also contributed the body of logic that has developed the formal methods to describe reasoning. Logic uses inductive and deductive processes that move from premises to conclusions through the application of logical arguments. Consider two simple examples of these forms of argumentation, as shown in Table 2.3.

The general characteristics of these forms of reasoning can be summarized.

1. Inductive arguments can be characterized by a “degree of strength” or “likelihood of validity,” while deductive arguments are either valid (the premises are true and the conclusion *must always* be true) or invalid (as with the non sequitur, in which the conclusion does not follow from the premises). There is no measure of degree or uncertainty in deductive arguments; they are valid or invalid—they provide information or nothing at all.
2. The conclusions of inductive arguments are probably, but not necessarily, true if all of the premises are true because all possible cases can never be observed. The conclusions of a deductive argument must be true if all of the premises are true (and the argument logic is correct).
3. Inductive conclusions contain information (knowledge) that was not implicitly contained in the premises. Deductive conclusions contain information that was implicitly contained in the premises. The deductive conclusion makes that information (knowledge) explicit.

To the logician, deduction cannot provide “new knowledge” in the sense that the conclusion is implicit in the premises. Only induction leads to new knowledge, previously unknown. In our context, however, we will show how

Table 2.3
Simple Inductive and Deductive Argument Forms

Inductive Argument	Deductive Argument
Every type 4 network that has been observed has a single mail file server (therefore) type 4 networks have a single mail file server	Every type 4 network has a single mail file server All of bank X’s offices use type 4 networks (therefore) every bank X office has a single mail file server

deduction can provide to the user knowledge that was not revealed before the deductive process. Hence, in this text we will attribute knowledge-creating capabilities to deduction. The pure logician would not.

Four common forms of valid deductive arguments are summarized in Table 2.4 to illustrate the formality applied in common logic [8].

While these deductive argument forms are appropriate for deduction, in both textual and Boolean expressions, fuzzy logic has been developed to deal with uncertain premises and conclusions [9]. Induction, due to the uncertainty in conclusions, has been treated by statistical methods of inference in which probabilities are used to represent the measure of uncertainty in conclusions that are inferred. The principles of logic are applied throughout information processes to implement both deductive and inductive reasoning to infer information from data, and then knowledge from that information.

2.2.3 Information Theory

The engineering science of information theory provides a statistical method for quantifying information for the purpose of analyzing the transmission, formatting, storage, and processing of information. Based on the work of Claude Shannon [10], information theory develops bounds on the maximum transmission rate (capacity) of communication channels, methods for measuring the redundant information in communicated messages, and the means for determining the most efficient compression rates for messages.

Information, when defined in terms of statements or messages about the state of a system (or an event), may be quantified by the uniqueness of the message relative to all possible messages that can occur. Consider, for example, a surveillance system monitoring a conflict on the battlefield. Sensors may report millions of possible tactical messages: location reports for vehicles, movements of forces, activation of radar and jammers, and so forth. Each of these reports has a likelihood of occurrence—the more likely reports that occur frequently (e.g., trucks moving on main roads in areas of conflict) provide much smaller information “value” than those that are very unlikely (e.g., the detonation of a tactical nuclear weapon). Shannon used this concept of *uniqueness* of a message (the likelihood of occurrence of that message) to define and quantify information content. The likelihood of each of message relative to all possible message occurrences is inversely related to the information content the individual message.

Let $M = (x_1, x_2, \dots, x_i, \dots)$ be the set of all possible messages from the system X , which may take on any one of n states, and define the information content of any message, m_i , about the state of X as a function of m_i . Shannon defined the primary information-related measure (of each message), H , as a function of

Table 2.4
Four Standard Forms of Valid Deductive Arguments

Argument	Form	Simple Example
Modus poens	Infer by direct deduction: P→Q premise P premise ∴ Q conclusion	If an aircraft has a type 55 radar, it is a fighter Aircraft A has a type 55 radar ∴ Aircraft A is a fighter
Modus tollens	Infer by denying the consequent: P→Q premise ¬Q premise ∴ ¬P conclusion	If an aircraft has a type 55 radar, it is a fighter Aircraft A is not a fighter ∴ Aircraft A does not have a type 55 radar
Hypothetical syllogism (chain argument)	String of IF-THEN statements: P→Q premise Q→R premise R→S premise ∴ PS conclusion	If an aircraft has a type 55 radar, it is a fighter If an aircraft is a fighter, it has weapons If an aircraft has weapons, it is a threat ∴ If an aircraft has a type 55 radar, it is a threat
Disjunctive syllogism	Denying terms of a disjunctive statement: P ∨ Q premise ¬Q premise ∴ P conclusion	Either aircraft A or B is a fighter Aircraft A is not a fighter ∴ Aircraft B is a fighter

Symbols used: P→Q means if P (antecedent) is true, then Q (consequent) is true
P ∨ Q means either P or Q
¬P means negation of the premise
∴ means therefore, and is followed by the conclusion

the probability of transmission (or occurrence) of each message, and used the logarithm to the base 2 for the typical case where binary messages are considered:

$$H = \sum_{i=1..n} p_i \log_2 p_i \quad (2.1)$$

Where:

H = Entropy (measured in bits when \log_2 is used)

p_i = Probability that the random variable is in state i

n = Number of possible states of the system X

Shannon called this value H “entropy” because the form of the equation and the intuitive meaning of the value are similar to entropy in statistical mechanics. Entropy is a measure of the “disorder” or “uncertainty” about the state of the system. (Entropy is not, per se, the measure of information, but we will see that the *decreases* in entropy due to received messages can be used to measure information gains. The goal of sensing, communication, and processing is to decrease uncertainty and increase information.)

Consider three cases to develop an intuitive feel for the basic entropy values.

- If there is only one possible message that is always reported from X , $n = 1$, and $H = 0$. Zero entropy indicates that there is no information value in the single message, which is certain to occur.
- If all messages are equally likely, the entropy (information content of messages) of the system is nonzero and takes on increasing value with n . The information associated with all messages are equal. For the simplest 2-state case (e.g., flipping a coin) where $n = 2$, entropy is unity, $H = 1$ (bit).
- Entropy increases as the number of possible outcomes increase: for $n = 16$ equally likely outcomes, $H = 4$ (bits), four times that of the binary case.

When all messages are equally likely, there is no prior statistical “knowledge” about which message may be received at any time, and therefore, the entropy is maximum and each message conveys the maximum potential of revealing the unknown. If the messages are *not* equally likely, it follows that there is prior knowledge about the state of the system, and the entropy of the system is less than the equally likely case.

Figure 2.2 illustrates the principal information theoretic measures based upon entropy in a typical sensing, communication, and processing system.

In addition to entropy, the following measures are defined as measures of information:

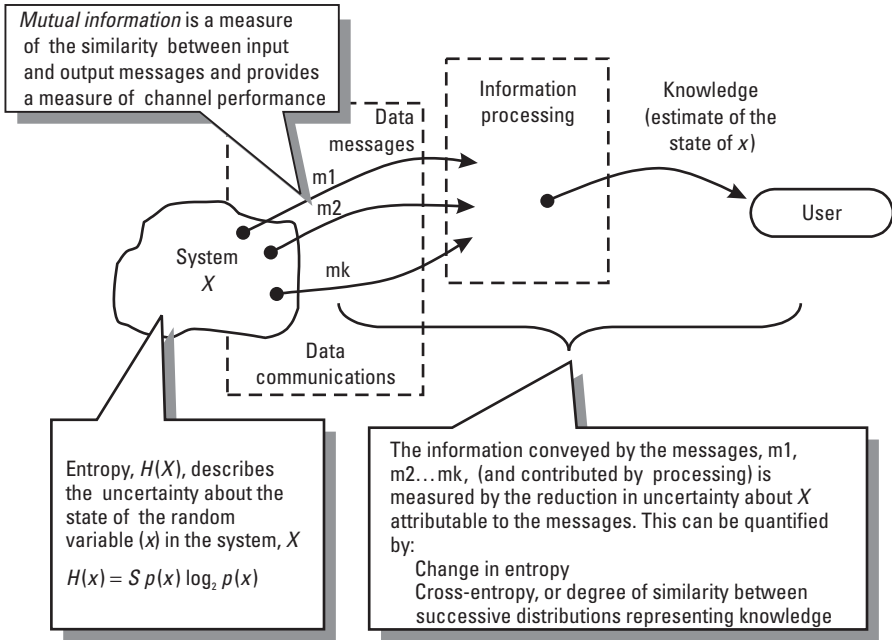


Figure 2.2 The principal measures of information in a communication and processing system.

- *Mutual information* quantifies and measures the information performance of a transmission channel as a function of the entropy attributable to the noise contributed by the channel:

$$H(X;Y) = \sum_i p_i \left[\sum_j p(j|i) \log_2 \left(\frac{p(j|i)}{p_j} \right) \right] \quad (2.2)$$

Where:

$H(X;Y)$ = Mutual information between output state (Y) and input state (X)

p_i = Probability that the random variable is in state i

p_j = Probability that the random variable is in state j

$p(j|i)$ = Conditional probability relating input state i to output state j

- *Entropy change*, or *information increase* is simply the measure of reduction in uncertainty about the state of X , determined by the change in entropy H due to a message (or a succession of messages):

$$I_i = H_{\text{Before message}} - H_{\text{After message}} \quad (2.3)$$

- *Cross-entropy*, or *discrimination* is a measure of the degree of similarity between two probability distributions (before message and after message) representing the probabilities of each possible state of X :

$$D(p, q) = \sum_{i=1, n} p_i \log_2 \left(\frac{p_i}{q_i} \right) \quad (2.4)$$

Where:

$D(p, q)$ = Cross-entropy between distribution $\{p\}$ and $\{q\}$

p_i = Probability of element i in distribution $\{p\}$

q_i = Probability of element i in distribution $\{q\}$

To illustrate how these measures may be used in an information system to determine the information gains due to incoming messages from sensors, consider a simple surveillance system example. The system attempts to locate a target along a roadway. The road is divided into 16 possible cells, and 16 probabilities describe the estimate of the state of the target. The probability distribution formed by these 16 values is illustrated in Figure 2.3 for 5 of 10 successive observations along the road.

Initially, there is no knowledge of the location and all cells are equally probable. As sensor reports come in, the distribution reveals that the target is located on one end of the road: interval 3 narrows its location to within 5 cells, interval 6 to within 3 cells, and by interval 10 the target is located within 1 cell with high probability. The figure shows the probability of the target occurring in cell 13 (the correct location), the successive reductions in entropy, and the increases in information and cross entropy. Figure 2.4 plots these parameters over the 10 observation intervals.

These measures provide both theoretical and practical means of quantifying information gains, using statistical knowledge of the system being measured and the allowable messages and their information content. In order to use these metrics to measure information gains in real systems, the states (which are often much more complex than our simple example) and allowable messages must be modeled and statistically described. While information theoretic measures have been widely used in communications problems, their adoption for knowledge creation applications has been very limited due to these complexities. Concepts

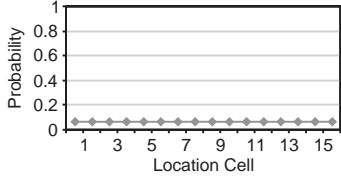
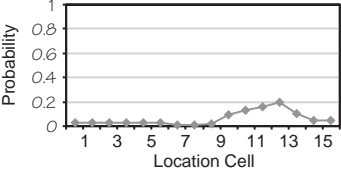
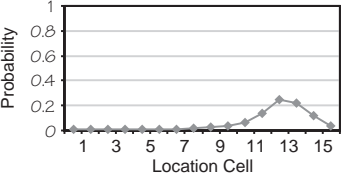
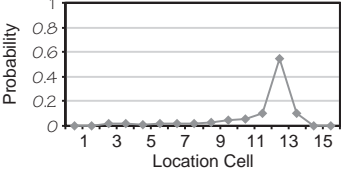
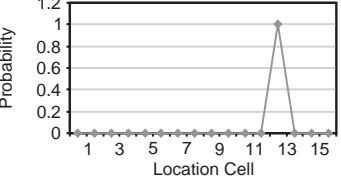
Interval T	Location Probability Distribution	Pr (C = 13)	Entropy (Bits)	Δ Entropy (Bits)	Cross-Entropy (Bits)
1		0.0625	2.33	0	0
2		0.2	2.48	0.06	0.50
3		0.25	2.26	0.07	0.86
6		0.55	1.43	0.89	1.57
10		0.998	.01	2.31	3.977

Figure 2.3 Entropy decrease and information increase is illustrated by a simulated series of sensor messages.

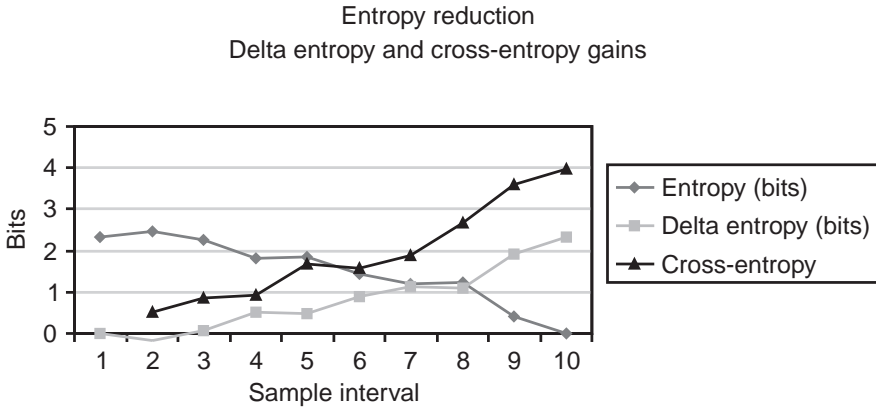


Figure 2.4 Reduction in entropy and increase in information measures in the simulated data of Figure 2.3.

and theory for the use of these measures have been proposed, but the metrics have not yet achieved wide application [11].

2.2.4 Decision Theory

Decision theory provides analytical means to make decisions in the presence of uncertainty and risk by choosing among alternatives. The basis of this choice is determined by quantifying the relative consequences of each alternative and choosing the best alternative to optimize some objective function. A rich set of techniques has been developed in decision theory to model alternatives, quantify the consequences, and rank the alternatives. In the presence of uncertainty in the data used for decision making (and risk due to undesirable consequences of erroneous decision making), the theory provides the concept of a *utility function* to quantify the desirability of courses of action (decisions).

Decision theory distinguishes two categories of utility functions that provide decision preferences on the basis of value or risk [12].

- *Value*—These utility functions determine a preferred decision on the basis of value metrics where no uncertainty is present.
- *Risk*—These functions provide a preferred decision in the presence of uncertainty (and therefore a risk that the decision may not deliver the highest utility).

Consider the most common form of the value function, a summation of weighted attributes, each of which characterizes an alternative (e.g., performance, efficiency, reliability, unit cost, life-cycle cost). The function provides a numerical utility value for each alternative:

$$U(x) = \sum_{i=1}^n v_i(x_i) \quad (2.5)$$

Where:

$U(x)$ = The utility of an alternative (x) considering n difference between attributes

v_i = The conditioning variable weighting the relative importance of attribute i

x = The value of attribute i

Generally, $\sum_{i=1}^n v_i = 1$, to normalize the value of $U(x)$

The value of $U(x)$ is computed for each alternative, and (in this form) the alternative with the highest utility is chosen.

While not offering a direct means of measuring information per se, utility functions provide a means of measuring the effect of information on the application in which it is used. The functions provide an intuitive means of measuring effectiveness of information systems, as we shall illustrate in Section 2.4.

2.2.5 Semiotic Theory

C. S. Peirce (1839–1914) introduced philosophical notions, including a “semiotic” logic system that attempts to provide a “critical thinking” method for conceptual understanding of observations (data) using methods of exploratory data analysis [13]. This system introduced the notion of *abduction* as a means of analyzing and providing a “best explanation” for a set of data. Expanding on the inductive and deductive processes of classical logic, Peirce viewed four stages of scientific inquiry [14].

- *Abduction* explores a specific set of data and creates plausible hypotheses to explain the data.
- *Deduction* is then applied to refine the hypothesis and develops a testable means of verifying the hypothesis using other premises and sets of data.

- *Induction* then develops the general explanation that is believed to apply to all sets of data viewed together in common. This means the explanation should apply to future sets of data.
- *Deduction* is finally applied, using the induced template to detect the presence of validated explanations to future data sets.

Abduction has been applied in artificial intelligence reasoning systems as the means of creating hypothetical explanations of data, and later in this chapter, we describe applications of the concept to knowledge discovery.

2.2.6 Knowledge Management

The management of information, in all of its forms, is a recognized imperative in third-wave business as well as warfare. The discipline of “knowledge management” developed in the business domain emphasizes both information exploitation (identified in Table 2.5) and information security as critical for businesses to compete in the third-wave marketplace. (For classic articles in this field, see [15–18].)

Central features of this developing discipline are the emerging means of defining information (information as both objects and processes) and placing value on intangible information assets (valuation, depreciation, and tax efficiency of information). The overall intellectual capital of an organization is made up of *human capital* (the knowledge contained in the humans comprising the organization: training, experience, contacts) and *structural capital* contained in the information infrastructure of the organization (sources, data warehouses, information networks, processes, and decision makers). Several alternative methods have been suggested to quantify the structural capital component.

One straightforward method of defining the value of an object of information, based on capital utility, is the difference between information net worth and the cost of acquisition [19]:

Information Value (I_v) = [Assets – Liabilities] – Total Cost of Ownership

$$I_v = ([A_t - A_n] - [L_t - L_n]) - \sum_{n=1}^7 I_n \quad (2.6)$$

Where, assets include

- A_t = The assets derived from the information at time of arrival;

Table 2.5
 Knowledge Management Principles Applied in the Business Domain

Relative to Organization Structure	Knowledge Management Area	Specific Knowledge Management Functions
External	Data collecting	Gain knowledge from customers Apply point-of-origin data collection, warehousing
	Knowledge dissemination	Provide additional knowledge to sales, distributors, customers
Internal	Information exploitation	Mine business data (data mining) Develop, apply knowledge-creating processes Create, refine, and apply business analyses, simulations
	Value knowledge	Measure, monitor, optimize, and audit corporate knowledge and intangible information assets Establish means to assure quality of information Insert information technologies to enhance knowledge creation, marketing, and management Identify, secure (e.g., patent), and protect intellectual and knowledge property
	Market knowledge	Market and sell knowledge products, services, or by-products Coordinate sales of tangible products with intangible knowledge products
Knowledge-based organizational structure and culture	Map and understand all business processes by the means by which information is handled Capture and distribute knowledge of individuals: knowledge sharing, creative culture Establish knowledge bases including best practices, lessons learned Create learning organizational culture Create additional revenue from existing knowledge bases	

- A_n = The assets if the information did not arrive;
- L_t = The liabilities derived from the information at time of arrival;
- L_n = The liabilities if the information did not arrive;
- I_n = Total cost associated with the information;
- I_1 = The cost to generate the information;
- I_2 = The cost to format the information;
- I_3 = The cost to reformat the information;
- I_4 = The cost to duplicate the information;
- I_5 = The cost to transmit or transport the information (distribute);
- I_6 = The cost to store the information;
- I_7 = The cost to use the information, including retrieval.

Information strategist Paul Strassmann has also defined high-level aggregate values of information in the organization to allow valuation and management of both the structural and human of the organization [20]. The efficiency of the organization in applying knowledge is measured in productivity:

$$\text{Information productivity} = \left[\frac{\text{Cost of information operations}}{\text{Cost of information management}} \right] \quad (2.7)$$

This productivity can be viewed as the annual return on accumulated knowledge, in terms of the impact on cost of operations. The wealth of an organization, then, can be then measured by the value added by useful knowledge relative to the interest rate paid for the equity capital to gain that knowledge. Strassmann defines this value as “knowledge capital”:

$$\text{Knowledge capital}^{\text{TM}} = \left[\frac{\text{Value added by information}}{\text{Interest rate for equity capital}} \right] \quad (2.8)$$

Notice that the value added by information may be determined by a utility function as earlier. These measures quantify, in the aggregate, the intangible values of such items as personnel experience, skills, training, relationships, learning capacity, communication ties and networks; suppliers, distributors, and customer communication and knowledge-sharing; and information technology (IT) infrastructure. They are based on the highest level *financial* parameters in the organization and require accounting, which separates

information technology expenditures and value metrics. (See [21] for a detailed description of these concepts.) The measure of value is closely related to the usefulness or utility of the information: its impact on the business activity for which it is required.

The objective of knowledge management is ultimately to understand the monetary value of information. These measures of the utility of information in the discipline of business knowledge management are based on capital values. The comparison between business competition and information-based warfare (IBW) is summarized in Table 2.6.

2.3 Comparison of Approaches

Each of the approaches to describing information and knowledge contributes to the development of the technologies applied to information warfare. These individual contributions can be applied in the following ways:

- *Epistemology* deals with truth and human perception, the ultimate target of information warfare. Epistemological principles may provide guidance in determining truth and objective perception in the presence of deception.

Table 2.6
Similarities Between Business Knowledge Management and Military IBW

Characteristics	Business Knowledge Management	Information-Based Warfare
Arena of operations	Competition	Escalation from competition to open conflict
Operational objectives	Market share Market value	Conquest Affect behavior
Measures of information utility	Capital value (economic gain)	Military value (economic attrition)
Typical metrics	Market share gained, captured Market value increased	Targets denied, destroyed Capability reduced (attrition of capacity)

- *Classic and semiotic logic* principles are applied in reasoning systems to create or discover knowledge. These are the methods of transforming data to knowledge, and they will be discussed further in this and the following chapter.
- *Information theory* provides a sound theoretical tool for measuring the performance or information gains in processing and communication chains, where the statistics of the sources, sensing, and channels can be modeled.
- *Decision theory* defines practical metrics to measure information performance, effectiveness, and military utility on the basis of its impact on the application.
- *Knowledge management* offers the means to measure the economic utility of information processes.

Table 2.7 summarizes the characteristics of these six approaches to define and measure information and the applicability to information warfare, particularly information exploitation processes.

2.4 Measuring the Utility of Information in Warfare

The relative value of information can be described in terms of the information *performance* within the information system, or in terms of the *effectiveness* (which relates the *utility*), or the ultimate impact of information on the user. In this section, we apply the methods of information and decision theory to develop quantitative metrics to measure information.

Table 2.7
Alternative Methods to Define and Measure Information

Discipline and Approach	Basis of Definition of Information	Information Metrics	Application to Information Exploitation
Philosophy—epistemology	Knowledge is an assertion of truth about the noumenal (things as they are in themselves) and phenomenal (things as they appear to be) aspects of the world	No metrics are used: knowledge (an assertion) is described by the ability to verify its validity	This discipline is mostly applied to issues of metaphysics, not engineering and science

Table 2.7 (continued)

Discipline and Approach	Basis of Definition of Information	Information Metrics	Application to Information Exploitation
Philosophy—classical logic	Information is defined as “true” or “false” assertions, whose validity is determined by logical calculations; relative value of information is not defined	<p>Deductive logic provides conclusions that are either true or false</p> <p>Inductive logic provides conclusions that only have a degree of validity</p>	<p>Predicate logic is applied to reasoning systems to make true/false assertions based on source inputs</p> <p>Bayesian or fuzzy logic approaches provide algebraic means to perform deduction with uncertain data</p> <p>Statistical inference techniques provide means of performing limited induction and learning</p>
Computer science semiotic logic		Abductive logic provides the “best explanation” for a given set of data	Abduction is applied to explaining particular sets of data as a limited form of induction
Information theory	Information value is defined by “entropy,” a measure of uniqueness of an assertion, which is a function of the probability that the assertion will occur out of all possible assertions	<p><i>Entropy</i>—A measure of the uncertainty about the state of a system</p> <p><i>Information gain</i>—The arithmetic change in entropy due to a message</p> <p><i>Cross-entropy</i>—The change in statistical distribution of state due to a message</p>	Information theoretic measures provide a means of measuring the performance of components (sensors, communication channels, and processing) and systems in terms of the reduction in uncertainty about the state of a system being observed
Decision theory	Information is measured by its application benefit to the user of information	<i>Utility</i> —The value of the application of the information, as measured by the user, in terms of achievement of an application objective	Utility measures provide a means of measuring the military effectiveness of information-processing systems
Business knowledge management	Information is measured by its economic return to the user, relative to capital investment	<i>Capital</i> —The economic value of information measured as utility added for interest paid to secure the information	Capital measures provide a means of measuring the economic effectiveness of information-processing systems

Utility is a function of both the accuracy and timeliness of information delivered to the user. The utility of estimates of the state of objects, complex situations, or processes is dependent upon accuracies of locations of objects, behavioral states, identities, relationships, and many other factors. Utility is also a function of the timeliness of information, which is often perishable and valueless after a given period. The relationships between utility and many accuracy and timeliness variables are often nonlinear and always highly dependent upon both the data collection means and user application.

To develop the concept of utility, consider the military utility of several types of messages containing data, information, or knowledge about a battlespace relative to the size or length of the message. Figure 2.5 illustrates that there is no correlation between message size and utility. The data describing an individual target location, such as a GPS precision location and identification message, can be contained in approximately 100 bits. The message containing location coordinates for a lieutenant and a general officer are the same, but their military utilities are quite different.

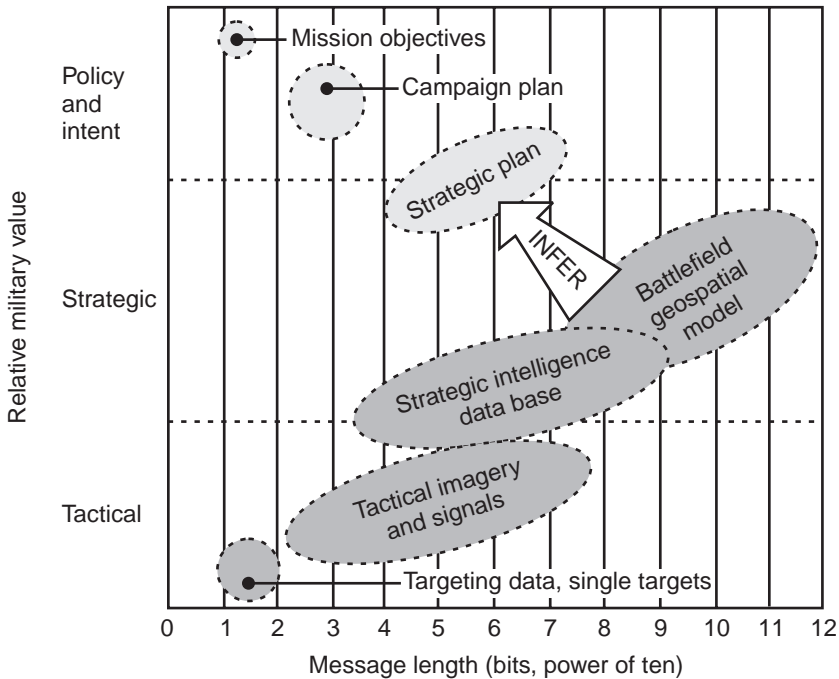


Figure 2.5 Military utility of information as a function of message (or information base) size.

Although there is no direct correlation, the figure illustrates the process of collecting many small (data) messages to assemble organized information bases describing group composition and behavior in order to infer knowledge about an opponent's strategy and intent, which are, again, small messages, but of high utility. We proceed from small data messages, through vast information bases, to infer knowledge, expressed in small messages.

Beginning in the lower left-hand quadrant we see that tactical data such as individual target reports are described in messages of less than 1,000 bits. Imagery and signal intelligence datasets collected over a region may comprise megabit databases. Strategic intelligence databases that describe orders of battle, activities, and the environment of a theater of operations may require gigabits of storage. Projected geospatial databases require terabits of storage. All of these datasets build from small individual reports to large information bases that have the intent of inferring knowledge about an opponent's strategic plan, individual campaign plans, or strategic intent (that can be expressed in much smaller message lengths).

The means by which the utility of information and derived knowledge is enhanced in practical systems usually includes one (or all) of four categories of actions. The objective of each of these actions is to refine the information processes to optimize the exploitation of available data and distribution of knowledge to appropriate users.

- *Acquire the right data*—The type, quality, accuracy, timeliness, and rate of data collected have a significant impact on knowledge delivered.
- *Optimize the extraction of knowledge*—The processes of transforming data to knowledge may be enhanced or refined to improve efficiency, throughput, end-to-end speed, or knowledge yield.
- *Distribute and apply the knowledge*—The products of information processes must be delivered to users on time, in understandable formats, and in sufficient quantity to provide useful comprehension to permit actions to be taken.
- *Ensure the protection of information*—In the competitive and conflict environments, information and the collection, processing, and distribution channels must be protected from all forms of attack. Information utility is a function of both reliability for and availability to the user.

Table 2.8 follows our earlier pattern of illustrating each of these categories of actions in the analogous applications of business and information warfare.

Table 2.8
Methods of Increasing the Utility of Information

Area	Enhancements	Business Enhancements	Info Warfare Enhancements
Acquire the right data	Improve the quantity, quality, accuracy, rate of update, and range of datatypes to achieve full understanding of processes to permit precision control	Statistical sampling TQM- Taguchi methods Point-of-sales analysis	Sensor system refinements in coverage, detection, (P_d/P_{fa}) precision, revisit rate, and dwell Multisensor coverage
Optimize the extraction of knowledge from data	Refine the process of converting data to actionable knowledge: speed, accuracy, uncertainty management, and decision support	Data warehousing Data fusion Data mining Statistical process control	Intelligence warehousing Data fusion Data mining C4I decision aids
Distribute and apply the knowledge effectively	Provide timely and widely distributed information to all process participants in appropriate formats with appropriate content	Electronic mail Collaborative electronic interaction tools Multiple- access business database	Intelligence distribution (intelligence links) Enhanced connectivity, interoperability Real-time C4I for the warrior
Ensure the protection of information	Protect the source data, information extraction, warehousing, and distribution from corruption, exploitation (eavesdropping), and deterioration	Industrial info security Database backup Commercial encryption Internet security (firewalls, encryption) e-mail security	Military INFOSEC Spread-spectrum and frequency-hopping modulation

In order to quantify the value of any bit of information, we must relate that information, or a marginal improvement attributable to the information, to military effectiveness or utility. Consider several practical military examples.

- Increased information on *target location* (increased three-dimensional accuracy) can be directly related to its influence on weapon performance (target kill probabilities) and therefore on military effectiveness.
- Improved information on the *relationships* between forces can improve the understanding of their most likely behavior, thereby allowing improved prediction and greater warning time—reducing vulnerability or increasing offensive lethality and military effectiveness.
- More timely information on *target behavior* (increased sensor revisit, more accurate tracking and identification) can be related to the speed with which targeting and attack can occur and to the resultant influence on military effectiveness.

In each case cited above, information must be quantified and mathematically related to the effect on the weapon or warning system's effectiveness to measure the effects of improved information on military actions.

As the value of information in warfare has grown, so has the need to measure and compare the processes that convert data to processed intelligence, enhancing the value of that information. In particular, program managers require utility/effectiveness measures for cost/benefit analyses to evaluate alternative technology solutions, and system engineers require performance measures to compare systems. Three categories of issues must be addressed: element performance, system effectiveness, and relative cost/benefit (Table 2.9).

Based on the utility function of decision theory, metrics for information-based systems have been defined for command and control [22] and data fusion [23] systems in classic texts. These methods have the following characteristics:

- Dimensional parameters describing data (e.g., pixels, pulses, bit error rate, time delay, signal to noise ratio) are related to measures of information performance (MOPs) that measure system information characteristics (e.g., accuracy, variance, detection/false alarm statistics, coverage). This relationship (transfer function) influences the processing stages that filter, align, associate, combine, and mine the data to produce knowledge.
- MOPs are then related to the functional effectiveness of the information system—measures of information effectiveness (MOEs) that can be directly related to the systems they support (defensive indications and warning systems or offensive weapon systems).

Table 2.9
Three Categories of Critical Questions Regarding Information Technology

Issue Area	Critical Questions
Processing element performance	How can information value be quantified for all data contributors? What is the relative information contribution of each source? What are the processing and delay factors influencing value? Which processing elements are most critical in terms of information contribution? What is the information gain (reduced uncertainty) provided by each stage of processing?
Intelligence chain effectiveness	What is the overall effectiveness of the all-source fusion process? What are the relative effectiveness contributions of each processing element? What is the effect of cumulative delay on effectiveness? What is the effect of correlation accuracy on effectiveness? What is the trade space for delivering uncertain data (or multiple hypotheses) sooner or higher confidence data later?
Cost/benefit	Where in the information chain can we achieve the greatest gain for a fixed investment? What are the relative potential cost benefits of alternative fusion, evaluation, or dissemination technologies?

- The overall military utility to the war fighter is determined as a function of many attributes of information and its influence on the military systems it supports.

Tables 2.10, 2.11, and 2.12 enumerate representative metrics in a typical military command and control system that may be used to measure information performance, effectiveness, and military utility, respectively. The hierarchical linking of these metrics (Figure 2.6) illustrates how functional relationships exist between successive metrics in a simple warning system example. The system correlates two sensors and a database of accumulated human reports to deduce if an attack is occurring.

Table 2.10

Representative Measures of Performance (MOPs) for a Military Command and Control System

Metric Category	Typical Data-Level Metrics	Description
Detection: ability to detect objects, events	Detection probability False alarm rate Miss probability	Probability of detection on single look False alarms per coverage Probability of fail to detect on single look
State estimation: ability to associate and estimate kinematic state	State accuracy Track accuracy Track persistence Correlation error probability	Accuracy of x , y , z and derivatives Accuracy of derivatives predictions Sustained estimation, dynamic target Probability of miscorrelation
Identification: ability to classify objects, events	Probability ID ID accuracy	Probability of correct ID Aggregate accuracy of ID decisions
Timeliness: time response of sensor/processing	Observation rate Sensing delay Processing delay Decision rate	Rate of revisits to observe object Delay from observation to report Delay from sensor report to decision Rate of update of output decision updates

- Sensor detection *performance* at the data level influences the correlation performance that links sensor data, and therefore the inference process that detects an opponent's hostile action (event).
- Event detection performance (timeliness and accuracy) influences the *effectiveness* of reasoning processes to assess the implications of the event.
- Effectiveness of the assessment of the impact on military objectives influences the decisions made by commanders and, in turn, the outcome of those responses. This is a measure of the utility of the entire information process. It is at this last step that knowledge is coupled to military decisions and ultimately to military utility.

Table 2.11

Representative Measures of Effectiveness (MOEs) for a Military Command and Control System

Metric Category	Typical Information-Level Metrics	Description
Capacity: ability to handle the information flow volume and rate	Throughput	Rate of translation of data to intelligence
	Surge process rate	Maximum short period rate
	Correlation rate	Rate of correlation of data elements
	Data leakage rate	Rate of loss of uncorrelated data items
	Storage (look-back capacity)	Capacity to store past data reports
Awareness quality: degree of vigilance and use of all available data	Correlation accuracy	Accuracy of associations between datasets
	Detection	$P_{\text{detection}}/P_{\text{false alarm}}$ operating characteristic
	Identification	$P_{\text{correct ID}}$ type ID accuracy
	Geopositioning accuracy	Spatial accuracy for targeting
	Prediction accuracy	Temporal/spatial behavior predict accuracy
Timeliness: speed with which information is processed and products are delivered to users	Time to accumulate	Accumulation delay to awareness decision
	Time to generate alternatives	Time to create alternative explanations
	Time to project	Extrapolation time for projections
	Time to plan and select	Time to synthesize response plans
	Time to decision	Composite decision-making time

The figure also serves to illustrate the counter performance, effectiveness, and utility measures an attacker may also desire to achieve by attacking a single sensor. The effect of the denial of a sensor propagates upward, degrading the functions (and their information) that deliver benefit to the user. The metrics that measure the impact of offensive and defensive information warfare are discussed in Section 8.8.

2.5 Translating Science to Technology

This chapter has provided an overview of the alternative means of defining and quantifying information. We must remember that information, as process

Table 2.12
Representative Utility Metrics for a Military Command and Control System

Metric Category	Typical Applied Knowledge-Level Metrics	Description
Collection: surveillance and reconnaissance resources required	Collectors required Collection tasking Bandwidth utilization Processing required	Number of collection assets required Loading on collection assets Percent of link bandwidth used Processing resources required
Targeting: weapon resources required to achieve objective	Weapons required Targeting efficiency Sortie generation rate Sorties required Vulnerability	Number and mix of weapons required Percent correct targeting decisions Rate at which sorties can be generated Number of sorties required to achieve objective Degree of vulnerability of assets
C2: command and control utility	OODA cycle time Decision accuracy	Aggregate decision cycle Aggregate command decision accuracy (% correct)

and content, is neither static nor inorganic. To view information as the static organized numbers in a “database” is a limited view of this resource. Information can be dynamic process models, capable of describing complex future behavior based on current measurements. Information also resides in humans as experience, “intuitive” knowledge, and other perceptive traits that will always make the human the valuable organic element of information architectures. We have introduced the alternatives for measuring information at the current state of the science. Much work must be completed before we will measure this resource like the tangible resources of the industrial age.

While this chapter has explored the sciences for defining and quantifying the abstract resource of information, the next will discuss the application of those sciences in information technologies for creating knowledge. While the term *information technology* covers a broad field (e.g., telecommunications, computing, networking), we will focus on the issue of how collected data is translated to knowledge and the technologies that automate those processes.

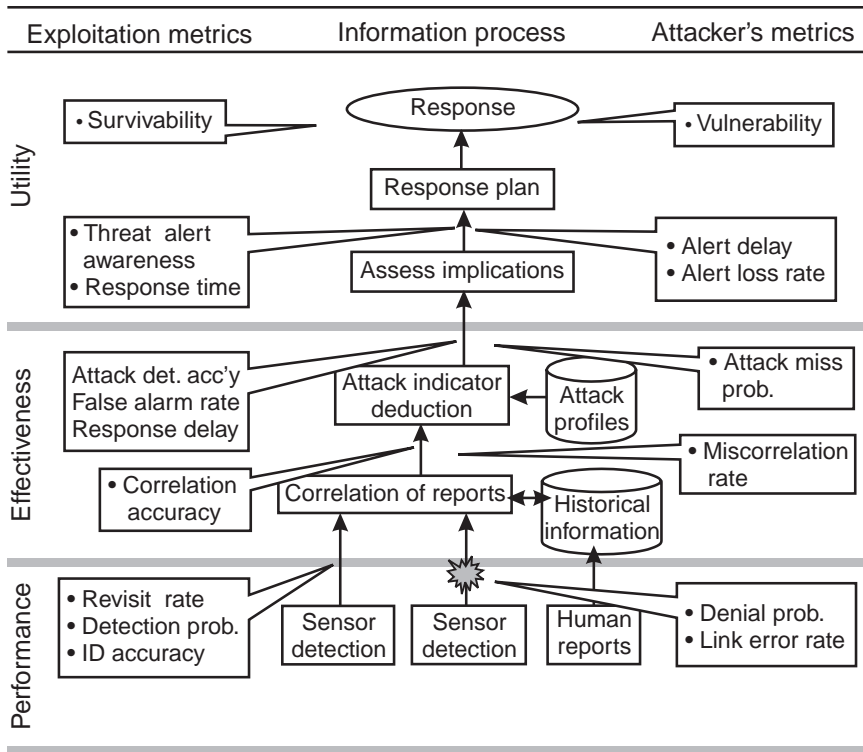


Figure 2.6 Information gains (and attack points) in the information exploitation path.

Endnotes

- [1] Some authors provide a four-level hierarchy, placing understanding as a level of information between knowledge and wisdom. In those models, understanding is a distinct level above knowledge.
- [2] Osgood, C. E., G. C. Suci, and P. H. Tannenbaum, *The Measurement of Meaning*, Urbana, IL: University of Illinois Press, 1957, p. 1.
- [3] Davidow, W. H., and M. S. Malone, *The Virtual Corporation*, New York: Harper-Collins, 1992, see Chapter 3.
- [4] McGee, J. V., L. Prusak, and P. J. Pyburn, *Managing Information Strategically: Increase Your Company's Competitiveness and Efficiency by Using Information as a Strategic Tool*, New York: John Wiley & Sons, 1993, p. 34.
- [5] *Ibid.*, pp. 68–69.
- [6] The use of national intelligence for commercial economic competitive intelligence purposes is a controversial policy issue in the United States, although numerous nations have well-integrated national-commercial intelligence processes.

-
- [7] Kant's concepts were first captured in his classic, *Critique of Pure Reason*, first published in 1781.
- [8] Stewart, D., and H. G. Blocker, *Fundamentals of Philosophy*, New York: MacMillan, 1987, pp. 65–71.
- [9] Zadeh, L., and J. Kacprzyk, *Fuzzy Logic for the Management of Uncertainty*, New York: John Wiley & Sons, 1991.
- [10] The classic Shannon paper may be found in: Shannon, C. E., and W. Weaver, *A Mathematical Theory of Communications*, Urbana, IL: University of Illinois Press, 1949. A more recent tutorial may be found in Cover, T., and J. Thomas, *Elements of Information Theory*, New York: John Wiley & Sons, 1991.
- [11] Mahler, R., "Information Theory and Data Fusion," *Proc. of 8th National Sensor Fusion Conf.*, IRIS, 1995, pp. 279–292.
- [12] Watson, S. R., and D. M. Buede, *Decision Synthesis*, Cambridge, NY: Cambridge University Press, 1987.
- [13] Brent, J., C. S. Peirce, *A Life*, Indianapolis, IN: Indiana University Press, 1993.
- [14] Yu, C. H., "Is There a Logic of Exploratory Data Analysis?," *Proc. of American Educational Research Assoc.*, New Orleans, LA, Apr. 1994.
- [15] Drucker, P. F., "The Coming of the New Organization," *Harvard Business Review*, Jan./Feb. 1988, pp. 45–53.
- [16] Davenport, T. H., S. L. Jarvenpaa, and M. C. Beers, "Improving Knowledge Work Process," *Sloan Management Review*, Summer 1996, pp. 53–65.
- [17] Davis, S., and J. Botkin, "The Coming of Knowledge-Based Business," *Harvard Business Review*, Sept./Oct. 1994, pp. 165–170.
- [18] Nonaka, I., "The Knowledge-Creating Company," *Harvard Business Review*, Nov./Dec. 1991, pp. 96–104. Also, "A Dynamic Theory of Organizational Knowledge Creation," *Organization Science*, Vol. 5, No. 1, Feb. 1994, pp. 14–37.
- [19] Taylor, C., "Business Information—What's It Really Worth?," *Information Strategy*, Vol. 2, No. 4. This method is attributed to George Harmon.
- [20] Strassman, P., "The Economics and Politics of Information Management," *KPMG Impact Programme Seminar*, London, June 27, 1996.
- [21] Strassmann, P., *The Squandered Computer*, New Canaan, CT: Information Economics Press, 1997.
- [22] Wohl, J. G., D. Gootkind, and H. D'Angelo, "Measures of Merit for Command and Control," MTR-8217, MITRE Bedford, Jan. 15, 1981.
- [23] Waltz, E., and J. Llinas, *Multisensor Fusion*, Norwood, MA: Artech House, 1990, see Chapter 11.

3

The Role of Technology in Information-Based Warfare

Can knowledge be created? Indeed, it can. The discovery of a unique signature that characterizes an information terrorist attacking a computer, and the use of that signature later to detect his or her subtle intrusion, are examples of created knowledge. In this chapter, we focus on these techniques of knowledge creation—both *discovery* and *detection*.

In the first chapter, information-based warfare was distinguished as the component that acquires, processes, and distributes information to achieve dominant awareness of the battlespace. We now apply the information science principles developed in the last chapter to describe the core information-processing methods of information-based warfare: acquisition of data and creation of “actionable” knowledge. (We will describe the dissemination process in later chapters.) The knowledge-creating process is often called *exploitation*—the extraction of military intelligence (knowledge) from collected data. These are the processes at the heart of intelligence, surveillance, and reconnaissance (ISR) systems and are components of most command and control (C2) systems. These processes must be understood because they are, in effect, the weapon factories of information-based warfare and the most lucrative targets of information warfare [1].

3.1 Knowledge-Creation Processes

Knowledge, as described in the last chapter, is the result of transforming raw data to organized information, and then to *explanations* that model the process from which the data was observed. The basic reasoning processes that were introduced to transform data into understandable knowledge apply the fundamental functions of logical inference.

- *Deduction*—The method of reasoning by which a specific case can be inferred to be true if it satisfies the conditions of a more general mathematical statement. The conclusion follows necessarily from the premises.

General statement: CP is present if $a = 5$, $b > 6$, $c < 2$

Specific case: $a = 5$, $b = 9$, $c = 1$

Deduced knowledge: CP is present

- *Induction*—The method of reasoning by which the general validity of a mathematical statement may be inferred from the demonstration of its validity over an acceptable range of specific cases. The conclusion expresses an empirical conjecture that goes beyond what the premises actually state.

Specific cases: $(x, y) = (1, 1), (2, 4), (4, 16), \dots (8, 64)$

Hypothesis of general relationship: $y = f(x)$

General statement: $y = x^2$

In addition to these two classic elements of symbolic logic, another element of inference is often included as a stage of the inference process that leads to knowledge.

- *Abduction*—The first stage of inference in which candidate hypotheses are synthesized (conjectured) to explain the observed data (but not a general explanation beyond the observed data, as in induction). C. S. Peirce defined abduction as a separate stage of critical thinking, although not an element of formal symbolic logic. This stage might precede a large number of tests on empirical data or larger searches to refine the hypothesis, and this stage can therefore be viewed as a precursor or component of induction.

Specific cases: $(x, y) = (1,1), (2,4), (4,16), \dots (8,64)$

Hypothesis of general relationship: $y = f(x)$

Refined hypothesis proposition: $y = x^N$

Recommendation: Test x, y over greater range of values of x

These three logical elements of inference are summarized in Table 3.1.

In each reasoning case, collected data is used to make more general or more specific inferences about patterns in the data to detect the presence of entities, events, or relationships that can be used to direct the actions of the user to achieve some objective.

In the military or information warfare domain, these methods are used in two ways. First, both abduction (dealing with specific cases) and induction (extending to general application) are used to learn templates that describe discernible patterns of behavior or structure (of an opponent). Because both are often used, we will call this stage abduction-induction [2].

Second, deductive processes are used in the exploitation or intelligence analysis to detect and understand situations and threats based on the previously learned patterns. This second phase often occurs in a hierarchy of knowledge elements.

Table 3.1
Logical Actions and Roles of Inference Processes

Function	Logical Action	Role in Knowledge Creation
Abduction	<i>Create hypotheses</i> —Creating hypotheses to “explain” the causes for or relationship between specific cases of data, moving from specific cases to candidate explanations for the specific case	Conceiving the best explanation
Induction	<i>Test hypotheses and assert validity</i> —Analyzing, deciding, and adopting explanations for specific cases of data, then moving from the specific cases to the general assertions	Discovering and learning
Deduction	<i>Match learned assertions against observations</i> —Use general explanations to synthesize specific cases to test against new observations and to explain new data, moving from the general case to specific cases	Applying and matching

1. Detect the presence, identify and locate or dynamically track individual entities (e.g., weapons, personnel, facilities, garrison areas) and events (e.g., decisions, assembly actions, command transmissions).
2. Determine relationships between entities and events to detect organizations of entities (e.g., military units comprised of many entities) and identify their structure and capabilities (e.g., logistical, physical order of battle, information order of battle).
3. Determine the hierarchical relationships between units to develop a model of the command structure.
4. From the model, project the potential courses of action and intent of individual units or the force hierarchy.
5. Analyze the opposing courses of action and assess the alternatives in terms of outcome, risk, and potential to achieve military objectives.
6. Finally, make the command decision to issue orders.

Both inductive-abductive and deductive processes are applied to perform this task by integrating many primitive inference functions into a process capable of describing complex structures and behavior in large datasets.

Figure 3.1 illustrates the general “critical reasoning” process using all three forms of reasoning, based on the semiotic approach described in the last chapter.

First, observations are collected and abduction provides the “best explanation” of the limited set of observed data. In the simple graphical example in the figure, abduction infers the best (in terms of some criteria, such as least square error) function $y = F(x)$. Over the course of time (as more observations are received), the abducted hypothesis may be validated or invalidated and, by induction, a general principal that extends beyond the observed data may be justified (again, against some defined criteria, such as probability). The initial process of these stages is referred to as the *knowledge discovery*, or the *learning phase*. The induced general patterns (templates) are then used in a subsequent knowledge-detection phase where, by deduction, the learned templates may be used to explain and predict y , given any observation of x with some degree of belief.

The paths of deductive reasoning may also take on either of two directions, as illustrated in Figure 3.2 for a simple case of detecting a command and control node from sensor data. Assume prior inductive processes have determined two general rules.

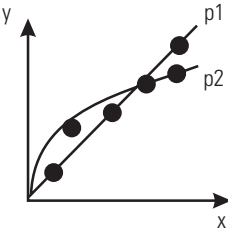
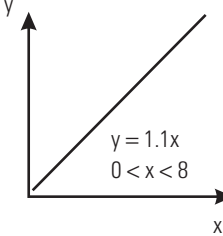
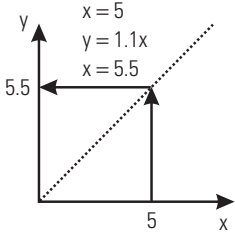
Logic Stage and Process	1 Abduction	2 Induction	3 Deduction
Function	Search for a pattern in specific data cases (observations) of a phenomenon and <i>suggest</i> hypotheses to explain data	Test hypotheses with empirical data and <i>justify</i> the validity of the general assertion of new knowledge, and <i>assert</i> a general principle	Apply the general principle to other observations to explain those observations
Objective	Hypothesize existence of an explanation and create a proposition (p) to explain a <i>specific</i> set of observations	Assert generality and validity of explanation that may explain <i>future</i> sets of observations	Determine possibility of all consequences of the proposition to explain <i>all</i> observations
Example			
Outcome	Propositions that explain specific observations	Assertions of new (empirical-based) knowledge that explains all future observations	Explanations of future observations

Figure 3.1 The process of analyzing data, abducting specific explanations, inducing general explanations, and applying the principle to deduce the explanations of future sets of data.

- *Rule 1*—IF the entity emits signal “E123N” and uses communication link “NOVA,” THEN the entity is a weapon designated type M23a.
- *Rule 2*—IF a type M23a weapon exchanges data via the data link “Complex,” THEN the type M23a is acting in the role as a type 3 command and control node.

(These rules have the standard form IF [Boolean expression of *conditions*] THEN *consequent*. The process of satisfying the conditions is referred to as *instantiation*.)

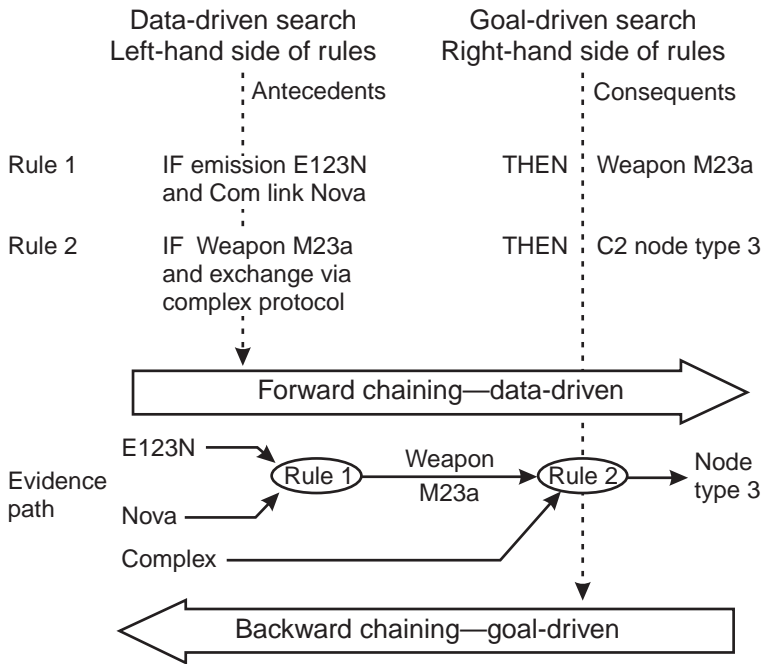


Figure 3.2 Forward and backward reasoning paths implement deductive reasoning.

Two possible paths of deduction can be implemented. The data-driven, or *forward-chaining* path accepts each new piece of data (e.g., the detection and correlation of E123N, NOVA, and complex emissions from a single entity) to assemble hypotheses that match the rules to derive the highest level knowledge that explains the data. Rule-based systems that implement forward-chaining reasoning are triggered by each new element of data received and initiate search processes to derive all possible new deductions from the new data plus all prior data. Each new data element (e.g., detection of E123N) is used to locate all rules that have that data as a condition on the left-hand side, and then a search is conducted to locate the other conditions necessary to instantiate the candidate rules (in rule 1, a detection of NOVA is also required to confirm M23a).

In contrast, goal-driven, or *backward-chaining* processes are triggered by goals (or questions such as, “Do there exist any type 3 nodes?” or, “Do there exist any complex signals that may be matched with E123N but have not yet detected NOVA?”). In this case, the search process begins by examining the right side of all rules to find consequents containing type 3 nodes. If rules are found, the database (of all current conditions) is searched to determine if any

of the candidate rules can be instantiated by data present to achieve the goal of answering the question posed.

3.2 Knowledge Detection and Discovery

Two primary categories of knowledge-creation processes can be distinguished, based on their approach to inference. Each is essential to information-based warfare exploitation processes that seek to create knowledge from volumes of data described.

The abductive-inductive process, *data mining*, discovers previously unrecognized patterns in data (new knowledge about *characteristics* of an unknown pattern class) by searching for patterns (relationships in data) that are in some sense “interesting.” The discovered candidates are usually presented to human users for analysis and validation before being adopted as general cases.

The deductive exploitation process, *data fusion*, detects the presence of previously known patterns in many sources of data (new knowledge about the *existence* of a known pattern in the data) by searching for specific templates in sensor data streams to understand a local environment.

The characteristics of these two processes are contrasted in Table 3.2. The datasets used by these processes for knowledge creation are incomplete and dynamic and contain data contaminated by noise. These factors make the following process characteristics apply:

- *Pattern descriptions*—Data mining seeks to induce general pattern descriptions (reference patterns, templates, or matched filters) to characterize data understood, while data fusion applies those descriptions to detect the presence of patterns in new data.
- *Uncertainty in inferred knowledge*—The data and reference patterns are uncertain, leading to uncertain beliefs or knowledge.
- *Dynamic state of inferred knowledge*—The process is sequential and inferred knowledge is dynamic, being refined as new data arrives.
- *Use of domain knowledge*—Knowledge about the domain (e.g., constraints or context) may be used in addition to observed data.

3.3 Knowledge Creation in the OODA Loop

The observe-orient-decide-act (OODA) model of command and control introduced earlier in Chapter 1 may now be expanded to show the role of the

Table 3.2

Comparison of Knowledge Detection and Discovery Methods.

(Source: [3] ©IEEE 1998, used by permission.)

	Technology	
	Data fusion	Data mining
Knowledge Created	Detection of the <i>presence</i> of known entity or event types in time or space	Discovery of the <i>existence</i> of previously unknown entities or events in time or space
Reasoning Process	Deduction: Detection of previously known patterns in data to infer the <i>presence</i> and <i>identity</i> of the entity or event represented by that pattern	<i>Abduction-induction</i> : Discovery of sufficient, correlated relationships in data to infer a general <i>description</i> (or rule set) that may be always or generally (to some quantified degree) true
Knowledge Patterns Used To Detect/Discover Knowledge	<i>Known</i> : (Specific) models are used as templates to detect similar patterns in data	<i>Unknown</i> : (General) model of interesting data properties is used as template to detect qualifying candidates for "new" knowledge in data
Detection/Discovery Process	Correlation of data with multiple <i>specific</i> models	Correlation of data with a simple <i>general</i> model (of interesting properties), followed by validation analysis
Object of Detection/Discovery Process and Knowledge Gained	<i>Detection</i> of individual and related sets of entities and events <i>Detection</i> of the presence, type, and location of known types of entities or events in large volumes of data	<i>Discovery</i> of interesting general relationships and patterns of behavior, which may be validated as general models of relationships or behavior <i>Discovery</i> of new types of entities or events by previously unidentified and unknown patterns in large volumes of data
Applications	<i>Testing</i> known models of entities or events (templates) to detect those items: <ul style="list-style-type: none"> • Target recognition • Event detection • Military network identification • System status recognition 	<i>Learning</i> new models of relationships or behavior to describe entities or events: <ul style="list-style-type: none"> • Subtle behavior detection • Machine learning (to provide specific models for data fusion) • New statistical patterns in datasets

knowledge-creation processes in the OOD stages of the loop. Figure 3.3 details these information functions in the context of the loop.

Observe functions include technical and human collection of data. Sensing of signals, pixels, and words (signals, imagery, and human intelligence) forms the core of information-based warfare observation.

Orient functions include data mining to discover or learn previously unknown characteristics in the data that can be used as templates for detection and future prediction in data fusion processes.

Decide functions include both automated and human processes. Simple, rapid responses can be automated upon the detection of preset conditions, while the judgment of human commanders is required for more complex, critical decisions that allow time for human intervention.

OODA Loop:	Observe	Orient	Decide	Act
Functions	Sensing Reporting Sensing control	Inference of current situation by <i>deduction</i> from known templates Inference of new templates (learning) by <i>abduction-induction</i>	Explaining alternative views of the situation Predicting alternative feasible futures Planning alternative courses of action and predicted outcomes Human perception Human judgment Automated responses	Human and automated actions
Model				
Technologies To Implement the Functions	Remote sensing Network communications	Data fusion Data mining	Decision support Collaborative analysis	

Figure 3.3 Knowledge creation within the OODA loop model.

We now describe the data fusion and mining processes that are central to the orient phase of the loop.

3.4 Deductive Data Fusion

Data fusion is an adaptive knowledge-creation process in which diverse elements of similar or dissimilar observations (data) are aligned, correlated, and combined into organized and indexed sets (information), which are further assessed to model, understand, and explain (knowledge) the makeup and behavior of a domain under observation [4].

The process is performed cognitively by humans in daily life (e.g., combining sight, sound, and smells to detect a threat) and has long been applied for manual investigations in the military, intelligence, and law enforcement. In recent decades, the automation of this process has been the subject of intense research and development within the military, particularly to support intelligence and command and control [5]. As sensors and database sources of data become increasingly available, automated data fusion technologies are required to support humans to cope with the increasing data load.

The process is deductive in nature because it compares sensed data with previously learned (induced) templates or patterns to detect, identify, and model objects and groups of objects within the observed domain. Deduction is performed at the data, information, and knowledge levels.

The U.S. DoD Joint Directors of Laboratories (JDL) have established a reference process model of data fusion that decomposes the process into four basic levels of information-refining processes (based upon the concept of levels of information abstraction).

- *Level 1: object refinement*—Correlation of all data to refine individual objects within the domain of observation. (The JDL model uses the term *object* to refer to real-world entities; however, the subject of interest may be a transient event in time as well.)
- *Level 2: situation refinement*—Correlation of all objects (information) within the domain to assess the current situation.
- *Level 3: meaning refinement*—Correlation of the current situation with environmental and other constraints to project the meaning of the situation (knowledge). (The meaning of the situation refers to its implications to the user, such as threat, opportunity, or change. The JDL adopted the terminology *threat refinement* for this level; however,

we adopt *meaning refinement* as a more general term encompassing broader applications than military threats.)

- *Level 4: process refinement*—Continual adaptation of the fusion process to optimize the delivery of knowledge against a defined knowledge objective.

A sequential flow of the data fusion process, following our three-level information model, illustrates the four JDL levels (Figure 3.4). The process is

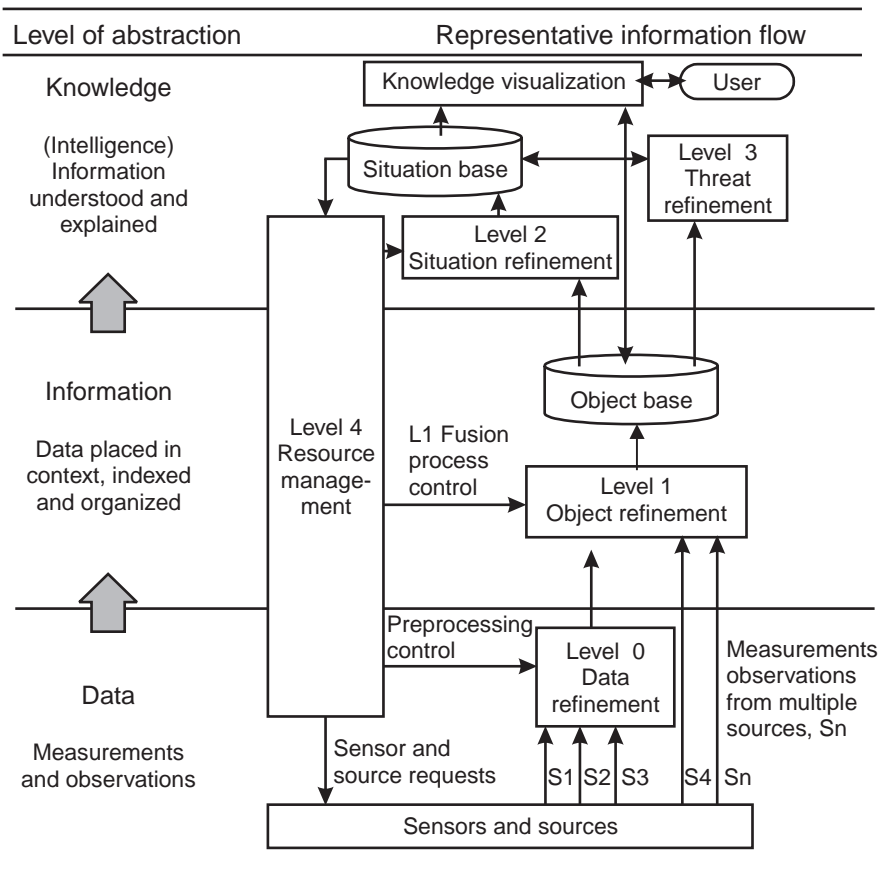


Figure 3.4 Data fusion is a process of deductive reasoning to correlate and combine multiple sources of data to understand a complex physical process.

characterized by the expected upward fusion flow from sources to data, then information, then knowledge, and also a downward feedback flow that controls the process and the sensors or sources acquiring data. To fit our model, we also introduce a fifth level that may occur before the JDL level 1 to allow for sensor-level processing and correlation before decision reports are issued [6]. The following paragraphs describe each functional level.

Level 0: Data Refinement

Raw data from sensors may be calibrated, corrected for bias and gain errors, limited (thresholded), and filtered to remove systematic noise sources. Object detection may occur at this point—in individual sensors or across multiple sensors (so-called predetection fusion). The object detection process forms observation reports that contain data elements such as observation identifier, time of measurement, measurement or decision data, decision, and uncertainty data.

Level 1: Object Refinement

Sensor and source reports are first aligned to a common spatial reference (e.g., a geographic coordinate system) and temporal reference (e.g., samples are propagated forward or backward to a common time.) These *alignment* transformations place the observations in common time-space coordinate system to allow an *association* process to determine which observations from different sensors have their source in a common object. The association process uses a quantitative correlation metric to measure the relative similarity between observations. The typical correlation metric, C , takes on the form:

$$C = \sum_{i=1}^n w_i x_i \quad (3.1)$$

Where:

w_i = Weighting coefficient for attribute x_i

x_i = i th correlation attribute metric

Values of x_i may include spatial distances (how close were the physical locations of the observations?), statistical distances (how similar were the measurements?), or spectral compatibility (how feasible were the measurement to occur from a common source?). The weighting coefficients w_i may be used to weight each contribution by relative importance or by absolute strength of contribution (e.g., inverse weighting by covariance statistics). The correlation metric may be used to make a hard decision (an *association*), choosing the most

likely pairings of observations, or a deferred decision, assigning more than one hypothetical pairing and deferring a hard decision until more observations arrive. Once observations have been associated, two functions are performed on each associated set of measurements for common object.

- *Tracking*—For dynamic targets (e.g., vehicles or aircraft), the current state of the object is correlated with previously known targets to determine if the observation can update an existing model (“track”). If the newly associated observations are determined to be updates to an existing track, the state estimation model for the track (e.g., a Kalman filter) is updated; otherwise, a new track is initiated.
- *Identification*—All associated observations are used to determine if the object identity can be classified to any one of several levels (e.g., friend/foe, vehicle class, vehicle type or model, or vehicle status or intent).

Level 2: Situation Refinement

All objects placed in space-time context in an information base are analyzed to detect relationships based on spatial or temporal characteristics. Aggregate sets of objects are detected by their coordinated behavior, dependencies, proximity, common point of origin, or other characteristics using correlation metrics with high-level attributes (e.g., spatial geometries or coordinated behavior). The synoptic understanding of all objects, in their space-time context, provides situation knowledge or awareness.

Level 3: Meaning (or Threat) Refinement

Situation knowledge is used to model and analyze feasible future behaviors of objects, groups, and environmental constraints to determine future possible outcomes. These outcomes, when compared with user objectives, provide an assessment of the implications of the current situation. Consider, for example, a battlefield situation that is analyzed in the sequence in Table 3.3.

Level 4: Process Refinement

The entire process is controlled to achieve information objectives by this activity. At the top level, current knowledge (about the situation) is compared to the knowledge required to achieve operational objectives to determine knowledge shortfalls. These shortfalls are parsed downward into information, then data needs, which direct the future acquisition of data (sensor management) and the control of internal processes. Processes may be refined, for example, to focus on

Table 3.3
Typical Situation Analysis, Prediction, and Planning Sequence




Current Situation	Constraints
Order of battle	Weather
Time, locations	Terrain
	Logistics
↓	↓
Model opponent's feasible courses of action (COA)	
COA 1—Hold at garrison	
COA 2—Attack path 1	
COA 3—Attack path 2	
↓	
Assess implications to own objectives	
COA 1—No impact	
COA 2—Immediate threat to Div 4	
COA 3—Delayed threat to Div 8	
↓	
Plan alternative responses and score	
Response A—95	
Response B—84	
Response C—55	

certain areas of interest, object types, or groups. This forms the feedback loop of the data fusion process.

General distinctions in the four correlation and combining levels (0, 1, 2, and 3) of the process are characterized in Table 3.4 to distinguish the difference in the resources, functions, and temporal focus at each level.

The technology development in data fusion has integrated disciplines such as the computer sciences, signal processing, pattern recognition, statistical analysis, and artificial intelligence to develop R&D and operational systems. The systems architectures and mathematical alternatives to implement data fusion are summarized in Table 3.5. Several texts detail the engineering methods and mathematical techniques underlying the functions described here [7–9].

Table 3.4
Distinctions Between the Data Fusion Information-Processing Levels

	0 Data Refinement 	1 Object Refinement 	2 Situation Refinement 	3 Meaning Refinement
Level of Information Abstractions	Data (measurements and observations)	Objects	Situation (resulting from groups of objects)	Meaning (the implications of the situation)
Functions Performed	Signal estimation: Composite sensor detection	Object estimation: Detection Association Combination Tracking Classification	Group estimation: Group detection (aggregation) Group association Group combination Group tracking Group classification	Impact prediction: Model associations and behavior Predict future behavior (courses of action) Assess impact and implications to objective(s)
Temporal Focus	A sensor observation period	A small sequence of observations	A large period of observations	Implications to a future time
General Output Products	Object reports	Object reports and behavior models	Group associations and group models	Predictions, alternatives, and implications

3.5 Abductive-Inductive Data Mining

Data mining is a knowledge-creation process in which large sets of data (in data warehouses) are cleansed and transformed into organized and indexed sets (information), which are then analyzed to discover hidden and implicit but previously undefined patterns that reveal new understanding of general structure and relationships (knowledge) in the data of a domain under observation.

The object of discovery is a “pattern,” which is defined as a statement in some language, L , that describes relationships in subset F_i of a set of data F such that:

Table 3.5

Design Issues and Implementation Alternatives for Data Fusion [10]

Data Fusion Process Level	System and Processing Design Issue	Alternative Engineering Implementation Approaches
Represent, manage, and combine uncertain sensor data	Data fusion levels 0 and 1: Select the most effective means to measure, represent, and combine values of sensor uncertainty across all sources of data	Certain data (Boolean logic) Uncertainty or confidence intervals Probabilities (Bayesian inferencing) Multivalued probabilities (Dempster-Shafer evidential reasoning) Fuzzy sets (fuzzy logic) Random sets (combinatorial algebras) Multiple hypothesis maintenance
Represent and link information	Data fusion level 2: Represent and store information in a manner that permits efficient access, linkage, and retrieval	Rules or frames Semantic networks Neural networks Graphical relationships (space, time, spectrum) Vector/raster spatial data
Inference, reasoning, and evaluation	Data fusion levels 2 and 3: Partition (associate) and combine raw data to optimize the estimates of parameters about the source of data, and infer higher level information about the source and its context	Abduction-induction Deduction Exhaustive or incomplete search Default inference Case-based reasoning Boolean Bayesian Evidential reasoning Fuzzy logic
Processing control	Data fusion level 4: Control the sensing and processing functions in accordance with a defined objective function	Control theory Monotonic reasoning Nonmonotonic reasoning Opportunistic reasoning
Architecture	Interconnect sensors and sources in accordance with network bandwidth, security, distribution, and processing constraints	<i>Centralized</i> fusion processing at a common node in a network <i>Distributed</i> fusion processing throughout a heterogeneous network

1. The statement holds with some certainty, c ;
2. The statement is simpler (in some sense) than the enumeration of all facts in F_s [11].

Mined knowledge, then, is formally defined as a pattern that is (1) interesting, according to some user-defined criterion, and (2) certain to a user-defined measure of degree. As an example, consider the following case.

Terrorist organization patterns:

1. Interesting criteria are “frequent” telecommunication between, physical proximity of, or correlated statements by different terrorist cells.
2. Measures of degree for these criteria are more than three messages within a week, travel to the same city at the same time, or statements opposed to common interests posted within one week [12].

In application, the mining process is extended from explanations of limited datasets (abduction) to more general applications (induction). In the example above, a relationship pattern between three terrorist cells may be discovered (abducted) that includes intercommunication, periodic travel to common cities, and correlated statements posted on the Internet. This pattern may be more fully analyzed over many known terrorist cells and extended (by induction) to be a general pattern of behavior for detecting cells.

Data mining (also called knowledge discovery) is distinguished from data fusion by two key characteristics.

- *Inference method*—Data fusion employs known patterns and deductive reasoning, while data mining searches for hidden patterns using abductive-inductive reasoning.
- *Temporal perspective*—The focus of data fusion is *retrospective* (determining current state based on past data), while data mining is both *retrospective* and *prospective*, focused on locating hidden patterns that may reveal predictive knowledge.

The data mining literature has predominantly addressed business applications that seek to locate economic or buying-pattern warehouses of data, including point-of-sales data [13]. The increased availability of warehoused data and the potential economic benefits of improved knowledge of purchasing patterns have spurred significant R&D in the mining process. The term is used to refer to a range of processes, from manual analysis of data using visualization

tools alone, to automated techniques that navigate and explore data searching for “interesting” patterns.

While there is no standard reference model for fusion, the general stages of the process as shown in Figure 3.5 illustrate a similarity to the data fusion process [14–16]. Beginning with sensors and sources, the data warehouse is populated with data, and successive functions move the data toward learned knowledge at the top. The sources, queries, and mining processes may be refined, similar to data fusion. The functional stages in the figure are described in the sections that follow.

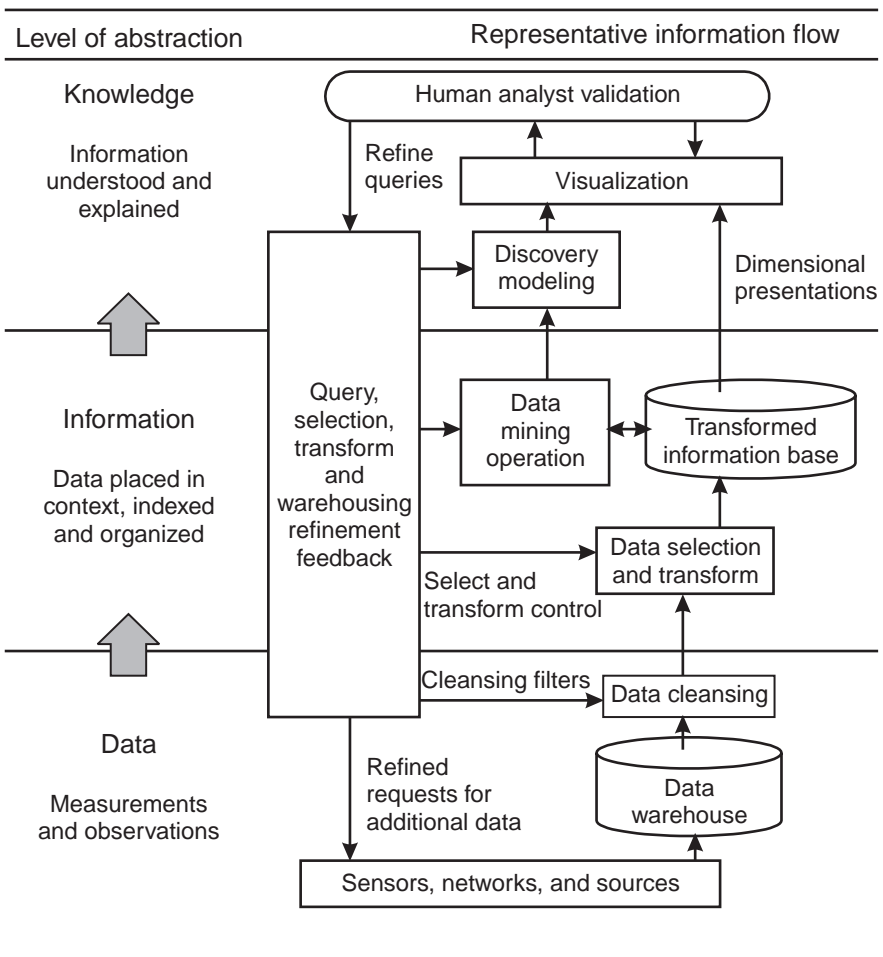


Figure 3.5 Data mining is an abductive-inductive process of evaluating data to locate patterns in the data that explain previously unknown general relationships in the underlying physical processes.

Data Warehouse

Data from many sources are collected and indexed in the warehouse, initially in the native format of the source. One of the chief issues facing many mining operations is the reconciliation of diverse databases that have different formats (e.g., field and record sizes or parameter scales), incompatible data definitions, and other differences. The warehouse collection process (*flow-in*) may mediate between these input sources to transform the data before storing in common form [17].

Data Cleansing

The warehoused data must be inspected and cleansed to identify and correct or remove conflicts, incomplete sets, and incompatibilities common to combined databases. Cleansing may include several categories of checks.

- *Uniformity checks* verify the ranges of data, determine if sets exceed limits, and verify that formats versions are compatible.
- *Completeness checks* evaluate the internal consistency of datasets to make sure, for example, that aggregate values are consistent with individual data components (e.g., “verify that total sales is equal to sum of all regional sales, and that data for all sales regions is present”).
- *Conformity checks* exhaustively verify that each index and reference exists.
- *Genealogy checks* generate and check audit trails to primitive data to permit analysts to “drill down” from high-level information.

Data Selection and Transformation

The types of data that will be used for mining are selected on the basis of relevance. For large operations, initial mining may be performed on a small set, then extended to larger sets to check for the validity of abducted patterns. The selected data may then be transformed to organize all data into common dimensions and to add derived dimensions as necessary for analysis.

Data Mining Operations

Mining operations may be performed in a supervised manner in which the analyst presents the operator with a selected set of “training” data in which the analyst has manually determined the existence of pattern classes. Alternatively, the operation may proceed without supervision, performing an automated search for patterns. As shown in Table 3.6, a number of techniques are

Table 3.6
Common Data Mining Operator Techniques

Mining Operator Methods	Description
Clustering	Segment the data into clusters (subsets of data) that share common properties; analyze the clusters for patterns that meet the interesting properties sought
Association or sequence discovery	Analyze the causal (sequence) or structural (association) relationships between sets of data to locate cause-effect relationships that meet interesting pattern properties
Statistical analysis	Determine the statistical (occurrence probabilities) characteristics of subsets of data, and quantify the statistically significant (e.g., high occurrence) sets
Rule abduction	Analyze data to abduct IF-THEN-ELSE rules that describe the structure; test rules for validity in general, and statistically characterize each
Link or tree abduction	Analyze the structural relationships between sets of data to locate links between data and tree structures that meet interesting connecting pattern properties
Deviation analysis	Locate deviations from statistically normal behavior and analyze for interest
Neural abduction	Train artificial neural networks to match data, then extract network coefficients (node weights) and network structure as abducted rules

available, depending upon the type of data and search objectives (interesting pattern types).

Discovery Modeling

Prediction or classification models are synthesized to fit the data patterns detected. This is the proscriptive aspect of mining: modeling the historical data in the database (the past) to provide a model to predict the future. The model attempts to abduct a generalized description that explains discovered patterns of interest and, using statistical inference from larger volumes of data, seeks to induct generally applicable models. Simple extrapolation, time-series trends, complex linked relationships, and causal mathematical models are examples of models created.

Visualization

The human analyst uses visualization tools that allow discovery of interesting patterns in the data. The automated mining operations “cue” the operator to

discovered patterns of interest (candidates), and the analyst then visualizes the pattern and verifies if, indeed, it contains new and useful knowledge.

On-line analytic processing (OLAP) refers to the manual visualization process in which a data manipulation engine allows the analyst to create data views from the human perspective, and to perform the following categories of functions:

1. *Multidimensional analysis* of the data across dimensions, through relationships (e.g., hierarchies), and in perspectives natural to the analyst (rather than inherent in the data);
2. *Transformation* of the viewing dimensions or *slicing* of the multidimensional array to view a subset of interest;
3. *Drill down* into the data from high levels of aggregation, downward into successively deeper levels of information;
4. *Reach through* from information levels to the underlying raw data, including reaching beyond the information base back to raw data by the audit trail generated in genealogy checking;
5. *Modeling* of hypothetical explanations of the data, in terms of trend analysis and extrapolations.

Refinement Feedback

The analyst may refine the process by adjusting the parameters that control the lower level processes, as well as requesting more or different data on which to focus the mining operations.

3.6 Integrating Information Technologies

It is natural that a full reasoning process would integrate the discovery processes of data mining with the detection processes of data fusion to coordinate learning and application activities. Waltz has illustrated a general application of these integrated tools to support automatic target recognition (ATR) processes searching for “nonliteral” target signatures [3]. (Nonliteral target signatures refer to those signatures that extend across many diverse observation domains and are not intuitive or apparent to analysts, but may be discovered only by deeper analysis of multidimensional data.) The integrated architecture, as shown in Figure 3.6, illustrates the complementary nature of the two processes. The mining component searches the accumulated database of sensor data with discovery processes focused on relationships that may have relevance to the

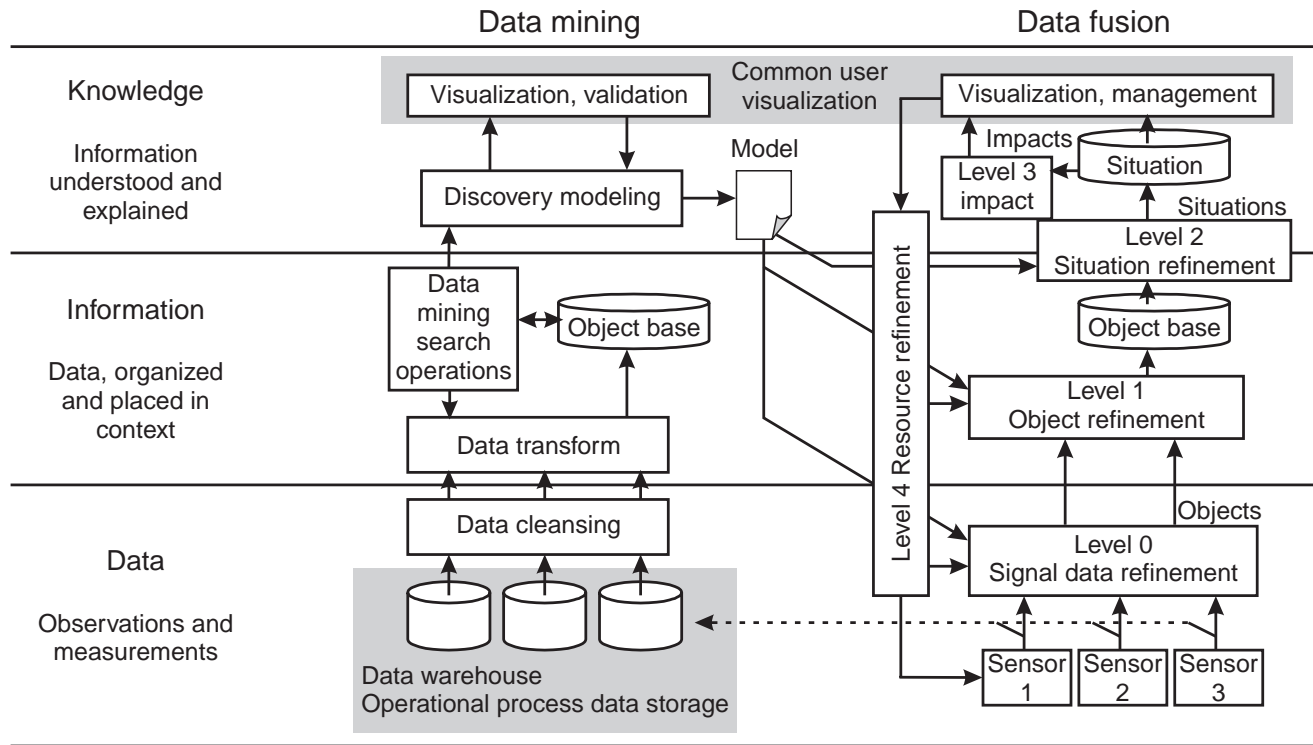


Figure 3.6 An integrated data mining and fusion architecture. (Source: [3] ©IEEE 1998, used by permission.)

nonliteral target sets. Discovered models (templates) of target objects or processes are then tested, refined, and verified using the data fusion process. Finally, the data fusion process applies the models deductively for knowledge detection in incoming sensor data streams.

3.7 Summary

The automation of the reasoning processes of abduction, induction, and deduction provides the ability to create actionable knowledge (military intelligence) from large volumes of data collected in IBW. As the value of information increases in all forms of information warfare, even more so is the importance of developing these reasoning technologies. While the scope of the global information infrastructure (and global sensing) increases, these technologies are required to extract meaning (and commercial value) from the boundless volumes of data available.

Data fusion and mining processes are yet on the initial slope of the technology development curve, and development is fueled by significant commercial R&D investments. Integrated reasoning tools will ultimately provide robust discovery and detection of knowledge for both business competition and information warfare.

Endnotes

- [1] If information is the target and weapon of information warfare, the knowledge creation processes are the weapon producers, created knowledge provides targeting for information weapons (the “byte bombs”), and an opponent’s perception of reality is the ultimate target.
- [2] Logicians are not in broad agreement on the use of or partitions between abduction and induction, nor in the distinctions in application. We use the term *abduction-induction* to recognize that the techniques from both functions may be applied at this stage.
- [3] Waltz, E. L., “Information Understanding: Integrating Data Fusion and Data Mining Processes,” *Proc. of IEEE International Symposium on Circuits and Systems*, Monterey, CA, May 31–June 4, 1997.
- [4] Definition from the article “Data Fusion” by D. Buede and E. Waltz in *McGraw-Hill Encyclopedia of Science and Technology*, New York: McGraw-Hill, 1998. An expanded definition provided by the U.S. DoD Joint Directors of Laboratories is: “A process dealing with the association, correlation, and combination of data and information from single

and multiple sources to achieve refined position and identity estimates, and complete and timely assessments of situations and threats, and their significance. The process is characterized by continuous refinements of its estimates, and by evaluation of the need for additional sources, or modification of the process itself to achieve improved results.”

- [5] Waltz, E. L., and D. M. Buede, “Data Fusion and Decision Support for Command and Control,” *IEEE Trans. on Systems, Man and Cybernetics*, Vol. SMC-16, No. 6, Nov./Dec. 1986, pages 865–879.
- [6] As of the preparation of this manuscript, the JDL is considering addition of a level similar to that described as “Level 0.”
- [7] Waltz, E. L., and J. Llinas, *Multisensor Data Fusion*, Norwood, MA: Artech House, 1990.
- [8] Hall, D., *Mathematical Techniques in Data Fusion*, Norwood, MA: Artech House, 1992.
- [9] Antony, R., *Principles of Data Fusion Automation*, Norwood, MA: Artech House, 1995.
- [10] Adapted from table contributed by Ed Waltz for “New World Vistas: Air and Space Power for the 21st Century,” USAF Scientific Advisory Board, Sensors Vol., Table 3-2, page 23, 1995.
- [11] Piatetsky-Shapiro, G., and W. J. Frawley, (eds.), *Knowledge Discovery in Databases*, Menlo Park, CA: AAAI Press/MIT Press, 1991, p. 3.
- [12] This example is very specific for purposes of illustration; however, mining criteria can be much more general in nature (yielding more possible relationships).
- [13] *An Overview of Data Mining at Dun & Bradstreet*, DIG white paper 95/01, Cambridge, MA: Pilot Software, Sept. 1995.
- [14] Mattison, R., and R. M. Mattison, *Data Warehousing and Data Mining for Telecommunications*, Norwood, MA: Artech House, 1997.
- [15] Gardner, C., “IBM Data Mining Technology,” IBM Corporation, Apr. 11, 1996.
- [16] Fayyad, U. M., G. Piatetsky-Shapiro, and P. Smyth, (eds.), *Advances in Knowledge Discovery and Data Mining*, Cambridge, MA: MIT Press, 1996.
- [17] Wiederhold, G., “Mediators in the Architecture of Future Information Systems,” *IEEE Computer*, Mar. 1992, pp. 38–49.

4

Achieving Information Superiority Through Dominant Battlespace Awareness and Knowledge

The objective of information-based warfare is ultimately to achieve military goals with the most efficient application of information resources. *Full-spectrum dominance* is the term used to describe this effective application of military power by information-based planning and execution of military operations. The central objective is the achievement of information superiority or dominance [1]. *Information superiority* is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same [2]. It is that degree of dominance in the information domain that permits the conduct of operations without effective opposition [3].

In this chapter, the principles of information superiority are developed, and the contributing methods of creating and delivering an “uninterrupted flow of information” are described, including the information architecture, intelligence, and command and control (C2) processes. The objective of this flow is to provide the following:

- *Dominant battlespace awareness (DBA)*—The understanding of the current situation based, primarily, on sensor observations and human sources;

- *Dominant battlespace knowledge (DBK)*—The understanding of the meaning of the current situation, gained from analysis (e.g., data fusion or simulation).

DBK is dependent upon DBA, and DBA is dependent on the sources of data that observe the battlespace. Both are necessary for information superiority.

The focus of this chapter is on the principles of information superiority and the processes to achieve this objective. In later chapters, we will explore the complementary component of superiority that is focused on attacking the adversary's information systems while defending one's own.

4.1 Principles of Information Superiority

Information superiority is a component of an overall strategy for application of military power and must be understood in that context. The U.S. Joint Vision (JV) 2010 articulates one strategy that may be used to understand the role of information superiority [4]. The hierarchy of the JV 2010 strategy, as depicted in Figure 4.1, is focused on achieving massed effects of force application to meet the U.S. Defense strategy of transforming military forces to (1) conduct highly efficient joint forces operations and multinational operations; (2) effectively deter, and when deterrence fails conduct C2W to defeat adversaries who may employ weapons of mass destruction (WMD) with long-range precision delivery systems; and (3) conduct both offensive and defensive information operations required to support both C2W and net warfare [5]. Massed effects are achieved by four operating concepts that provide a high degree of synergy from widely dispersed forces that perform precision targeting of high-lethality weapons at longer ranges.

1. *Dominant maneuver*—Information superiority will allow agile organizations with high-mobility weapon systems to attack rapidly at an aggressor's centers of gravity across the full depth of the battlefield. Synchronized and sustained attacks will be achieved by dispersed forces, integrated by an information grid.
2. *Precision engagement*—Near-real-time information on targets will permit responsive command and control, and the ability to engage and reengage targets with spatial and temporal precision (“at the right place, just at the right time”).

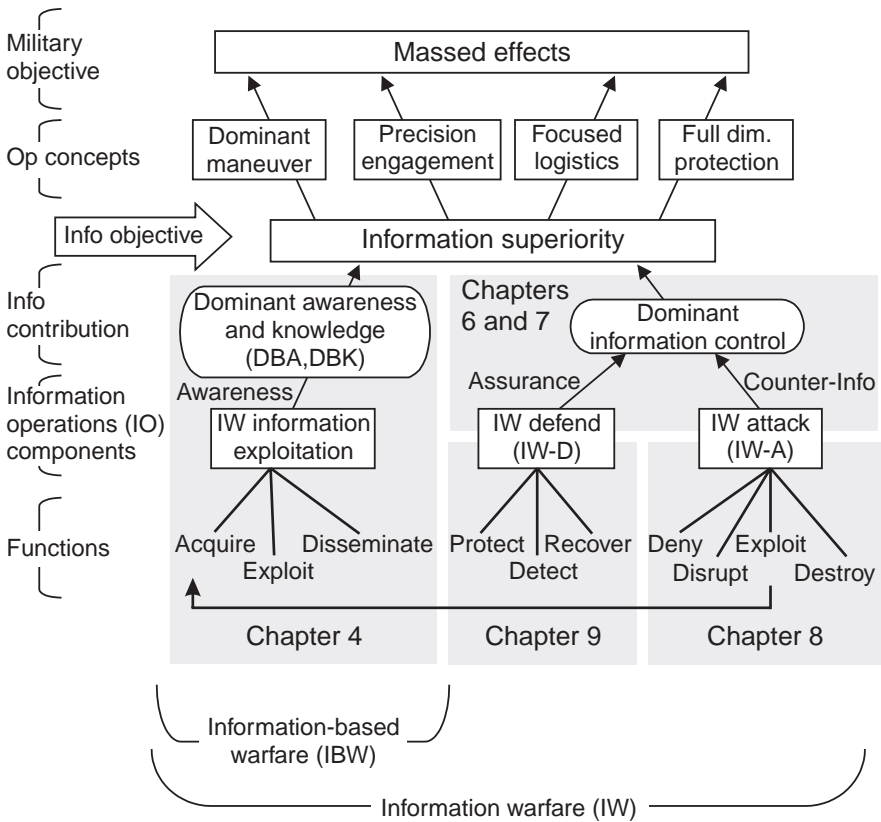


Figure 4.1 Information superiority is the enabling capability for four military operating concepts for advanced command and control warfare.

3. *Focused logistics*—Information superiority will also enable efficient delivery of sustainment packages throughout the battlefield, optimizing the logistic process.
4. *Full-dimension protection*—Protection of forces during deployment, maneuver, and engagement will provide freedom of offensive actions and can be achieved only if superior information provides continuous threat vigilance.

Information superiority must create an operational advantage to benefit the applied military power and can be viewed as a precondition for these military operations in the same sense that air superiority is viewed as a precondition to certain strategic targeting operations.

The figure illustrates that the *effect* of information superiority is to integrate the four operating concepts to amplify their effectiveness. The two contributing *components* of superiority are as follows:

- *Dominant battlespace awareness (DBA) and knowledge (DBK)*—The comprehensive awareness of all the decision-relevant elements within a defined battlespace, and the ability to predict with very high confidence near-term enemy actions and combat outcomes [6];
- *Information operations*—Actions taken to affect adversary information and information systems while defending one’s own information and information systems [7].

This chapter focuses on the acquisition, exploitation, and dissemination functions of DBA/DBK, while information operations against adversarial information systems are covered in later chapters.

DBA provides a synoptic view, in time and space, of the conflict and supplies the commander with a clear perception of the situation and the consequences of potential actions. It dispels the “fog of war” described by Clausewitz. Cooper has enumerated the following capabilities that DBA provides to commanders. DBA allows commanders to:

- Forge a common purpose for dispersed combat forces;
- Assess the battlespace accurately by understanding its evolving dynamics and correlated patterns;
- Develop their own adaptive vision of combat operations;
- Project the consequences of their decisions across the space and time of combat;
- Recognize periods and places of potential vulnerability as they evolve;
- Create, not just find or identify, windows of opportunity that can be exploited [8].

DBA/DBK is a complement to precision forces, whose precision must be matched to the level of information performance to achieve targeting effectiveness and economic efficiency. Force effectiveness, measured as the aggregate value of targets destroyed, is a function of the performance of individual weapons (measured in kill probability, P_k) and the degree of awareness and resulting precision of targeting. Perfect information and perfect command and

control establish the upper limit on the effectiveness of a force, while DBA/DBK (Figure 4.2) optimizes effectiveness by enhancing the information component.

To be effective, DBA/DBK also must provide a consistent view of the battlespace, distributed to all forces—although each force may choose its own perspective of the view. At the tactical level, a continuous dynamic struggle occurs between sides, and the information state of a side may continuously change from dominance, to parity, to disadvantage.

The information advantage delivered by DBA/DBK has the potential to deliver four categories of operational benefits, as detailed in Table 4.1, when properly matched with precision forces.

- *Battlespace preparation*—Intelligence preparation of the battlespace (IPB) includes all activities to acquire an understanding of the physical, political, electronic, cyber, and other dimensions of the battlespace. Dimensions such as terrain, government, infrastructure, electronic warfare, and telecommunication/computer networks are mapped to define the structure and constraints of the battlespace [10]. IPB includes both passive analysis and active probing of specific targets

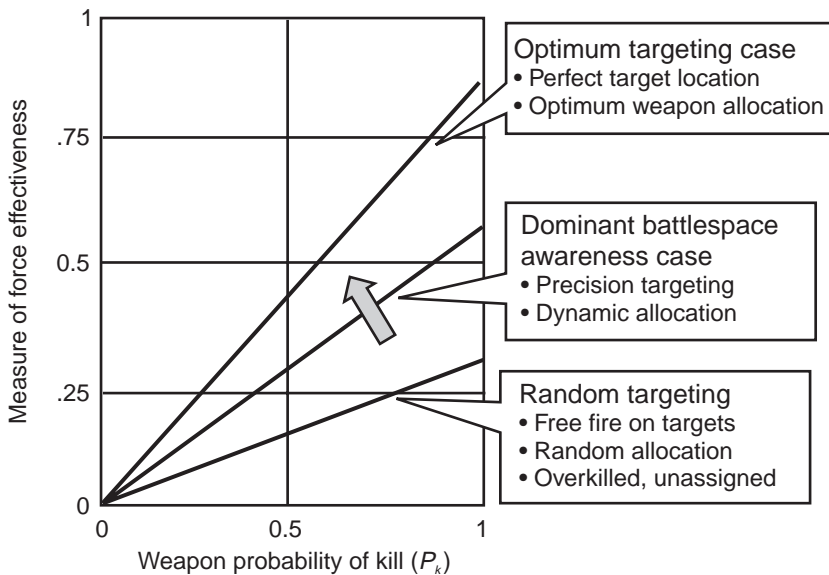


Figure 4.2 The potential value of DBA/DBK is to maximize overall force effectiveness. (After: Alberts [9].)

Table 4.1
Operational Values of DBA/DBK Component of Information Superiority

Operational Area	Operational Benefits	Potential Value Added—Contributions by Dominant Battlespace Awareness
Battlespace preparation	Predictive planning Operational rehearsal	Accurate intelligence preparation of the battlespace Information operations mission rehearsal
Battlespace surveillance and analysis	Predictive planning and preemption Effective employment of forces	Consistent battlespace understanding Modeling of battlespace constraints, alternatives to understand possibilities Prediction of adversary reactions to C2W attacks
Battlespace visualization	Full-dimension situation awareness Rapid, precision response to dynamic activities, within adversary's decision cycle	Detailed and distributed battlespace understanding Detailed understanding of constraints, opportunities, threats Execution of time-critical targeting Precision targeting
Battlespace awareness dissemination	Common, ubiquitous situation awareness Synchronized force application	Timely distribution of appropriate awareness intelligence tailored to each user Precise, immediate awareness

to detail their characteristics. Orders of battle and decision-making processes are modeled, vulnerabilities and constraints on adversaries' operations are identified, and potential offensive responses are predicted. The product of this function is comprehension of the battlespace environment.

- *Battlespace surveillance and analysis*—Continuous observation of the battlespace and analysis of the collective observations provide a detailed understanding of the dynamic states of individual components, events, and behaviors from which courses of action and intents can be inferred. The product is comprehensive state information.
- *Battlespace visualization*—This is the process by which the commander (1) develops a clear understanding of the current state with relation to the enemy and environment, (2) envisions a desired end state that

represents mission accomplishment, and then (3) subsequently visualizes the sequence of activities that moves the commander's force from its current state to the end state [11]. The product of this visualization is human comprehension and a comprehensive plan.

- *Battlespace awareness dissemination*—Finally, the components of awareness and knowledge are distributed to *appropriate* participants at *appropriate* times and in formats compatible with their own mission. The product here is available and “actionable” knowledge.

Table 4.2 summarizes the technologies that enable each of these four operational areas of benefit. Notice that these areas address the basic means of achieving the information gains presented in general terms earlier in Chapter 2.

At the core of DBA/DBK is the ability to collect pertinent data and to produce timely and accurate knowledge—the traditional role of the intelligence, surveillance, and reconnaissance (ISR) community. Before describing an implementation of these operations and technologies, the next section describes the functions and products of intelligence operations.

4.1.1 Intelligence, Surveillance, and Reconnaissance (ISR)

Intelligence, the information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding [13], is the product that provides battlespace awareness [14].

Three major categories of intelligence products can be distinguished: strategic, military-operational, and military-tactical intelligence. Table 4.3 contrasts the categories, which are complementary and often share the same sources to deliver their intelligence products. The primary difference in the categories is the perspective (long- to near-term projection) and the reporting cycle (annual to near-real-time updates).

The process that delivers strategic and operational intelligence products is generally depicted in cyclic form (Figure 4.3), with six distinct phases [15].

- *Collection planning*—Government and military decision makers define, at a high level of information abstraction, the knowledge that is required to make policy, strategy, or operational decisions. The requests are parsed into information required to deduce the required answers. This list of information is further parsed into the individual elements of data that must be collected to form that

Table 4.2

Technology Contributors to DBA/DBK. (Adapted from: "Joint Warfighter Science and Technology Plan" [12] and ABIS Task Force Report.)

Operational Area	Required Enabling Technology Contributions
Battlespace preparation	Rapid mapping of terrestrial features, terrain Rapid mapping of information infrastructures, electronic orders of battle, and decision processes Automatic extraction of physical and cyber features for mapping Virtual realism mission rehearsal tools
Battlespace surveillance and analysis	Full-dimensional, continuous surveillance Space sensors Air vehicle sensors (standoff, endurance, tactical) Ground sensors (attended, unattended) Integrated management of surveillance collection Dynamic all source data fusion and data mining Mediated integration of distributed, heterogeneous databases
Battlespace visualization	Rapid spatial analysis and visualization of terrain Spatial reasoning in geographic information systems (GIS) Hypermedia visualizations Intelligent agents for search and cueing, recognition, and routing Natural language command interaction
Battlespace awareness dissemination	Automated language, syntax, and protocol translation Adaptive, multimedia distribution networks Heterogeneous, collaborative multimedia conferencing Self-adapting tactical/mobile networking

required information base. The required data is used to establish a plan of collection, which details the elements of data needed and the targets (people, places, and things) from which the data may be obtained.

- *Collection*—Following the plan, human and technical sources of data are tasked to perform the collection. Table 4.4 summarizes the major collection sources, which include both open and closed access sources and human and technical means of acquisition.

Table 4.3
Major Categories of Intelligence

Intelligence Category	Focus (Intelligence Users)	Objects of Analysis	Reporting Cycle
Strategic or national intelligence	Understanding of current and future status and behavior of foreign nations (<i>national policymakers</i>)	Foreign policy Political posture National stability Socioeconomics Cultural ideologies Science and technology Foreign relationships Military strength, intent	Infrequent (annual, monthly) long-duration estimates and projections (months, years) Frequent status reports (weekly, daily)
Military-operational intelligence	Understanding of military powers, orders of battle, technology maturity, and future potential (<i>military commanders</i>)	Orders of battle Military doctrine Science and technology Command structure Force strength Force status, intent	Continually updated status databases (weekly) Indications and warnings (hours, days)
Military-tactical intelligence	Real-time understanding of military units, force structure, and active behavior (current and future) on the battlefield (<i>war fighters</i>)	Military platforms Military units Force operations Courses of action (past, current, potential future)	Weapon support (real-time, seconds) Situation awareness applications (minutes, hours)

- *Processing*—The collected data is indexed and organized in an information base, and progress on meeting the requirements of the collection plan is monitored. As a result of collection, this organized data may adjust the plan on the basis of received data.
- *Analysis*—The organized information base is processed using deductive inference techniques (described earlier in Chapter 3) that fuse all source data in an attempt to answer the requester's questions.
- *Production*—Intelligence may be produced in the format of dynamic visualizations on a war fighter's weapon system or in formal reports to

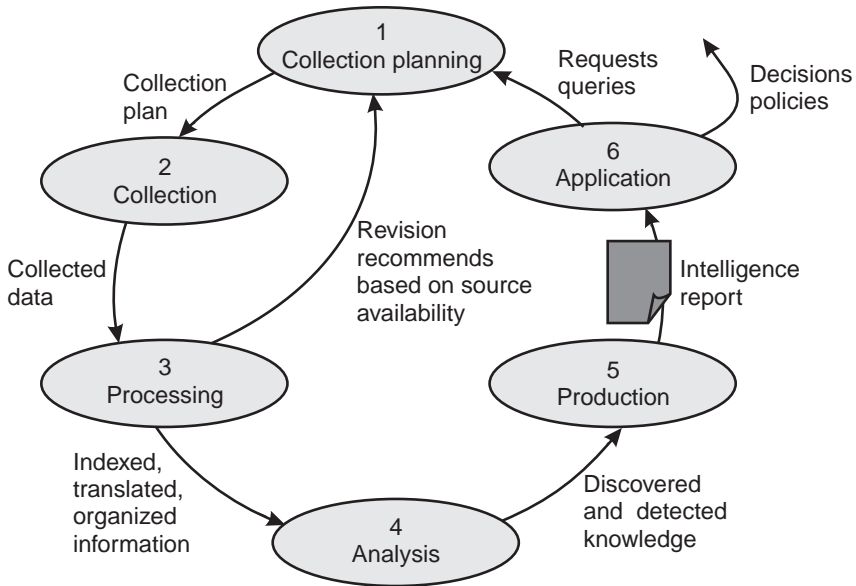


Figure 4.3 The intelligence cycle delivers reports in response to specific requests and queries for knowledge to make decisions and set policies.

policymakers. Three categories of formal strategic and tactical intelligence reports are distinguished by their past, present, and future focus: (1) *current intelligence reports* are news-like reports that describe recent events or indications and warnings; (2) *basic intelligence reports* provide complete descriptions of a specific situation (order of battle or political situation, for example); and (3) *intelligence estimates* attempt to predict feasible future outcomes as a result of current situations, constraints, and possible influences [16].

- *Application*—The intelligence product is disseminated to the user, providing answers to queries and estimates of accuracy of the product delivered. Products range from strategic intelligence estimates in the form of large hardcopy or softcopy documents for policy makers, to real-time displays that visualize battlespace conditions for a war fighter.

4.1.1.1 Sources of Intelligence Data

A taxonomy of intelligence data sources (Table 4.4) includes sources that are openly accessible or closed (such as denied areas, secured communications, or clandestine activities). Due to the increasing access to electronic media

Table 4.4

Major Intelligence Categories Are Partitioned by Access (Open or Closed) and Collection Means (Human or Technical)

Source Type	Intelligence Category	Representative Sources
Open sources: Human and technical means	OSINT: Open source intelligence	Foreign radio and television news sources Foreign printed materials: books, magazines, periodicals, journals Diplomatic and attaché reporting Shortwave radio, telecomm, Internet conversations Foreign network computer sources Gray literature (printed and electronic)
Closed sources: Human means	HUMINT: Human intelligence	Reports from agents in foreign nations Discussions with personnel in foreign nations Reports from defectors from foreign nations Messages from friendly third-party sources
Closed source: Technical means	IMINT: Imagery intelligence	Surveillance imagery (static air and space imagery of the Earth) Surveillance imagery (terrestrial static and video imagery)
	SIGINT: Signals intelligence	ELINT electromagnetic signals monitoring (<i>externals</i> : events, activities, relationships, frequency of occurrence, modes, sequences, patterns, signatures; or <i>internals</i> : contents of messages) Moving target indications (MTI) tracking data COMINT communications traffic monitoring for externals and internals FISINT—foreign instrumentation signals intelligence (telemetry: TELINT, beacons, video links)
	NETINT: Network Intelligence	Network analysis and monitoring Network message interception, traffic analysis Computer intrusion, penetration, and exploitation
	MASINT: Measurements and signals intelligence	Technically derived intelligence from all sources (parametric data) to support real-time operations (e.g., electronic support measures, combat identification, tactical intelligence analysis) MASINT exploits physical properties (nuclear, biological, chemical), emitted/ reflected energy (RF, IR, shock waves, acoustics), mechanical sound, magnetic properties, motion, and materials composition

(telecommunications, video, and computer networks) and the global expansion of democratic societies, open source intelligence (OSINT) is becoming an increasingly important source of global data. While OSINT must be screened and cross-validated to filter errors, duplications, and deliberate misinformation (as do all sources), it provides an economical source of public information and is a contributor to other sources for cueing, indications, and confirmation [17].

In contrast with open sources, clandestine human intelligence (HUMINT) and technical means of collection provide data on objects that are protected by denial of access or secrecy [18].

Imagery intelligence (IMINT) provides assessments of resolvable objects from imagery of the Earth, revealing the location, composition, and characterization of resources, infrastructure, facilities, and lines of communication to perform order of battle estimates, indications and warning, situation assessment, targeting, and battle damage assessment functions. Signals intelligence (SIGINT) monitors electromagnetic signals for electronic data (e.g., radar) and communications (e.g., voice and data telecommunications) to detect traffic and geolocate individual emitters. The emerging requirement to collect intelligence from networked traffic (rather than radiated emissions) is developing the introduction of a new discipline, described as NETINT in the chart. This involves the understanding of network infrastructures, access to computer nodes, exploitation of networked computers, network traffic externals, and data communication internals. (Some have called this source HACKINT, and some categorize this as a subset of traditional SIGINT.) Measurements and signatures intelligence (MASINT) is technically derived knowledge from a wide variety of sensors, individual or fused to (1) perform special measurements of objects or events of interest, or (2) obtain signatures for use by the other intelligence sources. MASINT is used to characterize the observable phenomena (“observables”) of the environment and objects of surveillance.

U.S. intelligence studies have pointed out specific changes in the use of these sources as the world increases globalization of commerce and access to social, political, economic, and technical information [19–21].

- The increase in unstructured and transnational threats requires the robust use of clandestine HUMINT sources to complement extensive technical verification means developed during the Cold War.
- Technical means of collection are required for both broad area coverage and detailed assessment of the remaining denied areas of the world.

Competitive intelligence operations are also conducted in the commercial business world, with growing use of open sources available on the Internet and

electronic collection sources. The same principles of strategic intelligence planning, development of the intelligence cycle processes, source development, and analysis apply. Leonard Fuld's *The New Competitor Analysis* details the intelligence processes applied to commercial businesses and the sources available in this domain [22]. In the United States, the roles of national intelligence and business intelligence are distinct and separated, although limited use of national intelligence to support global business has been reported.

4.1.1.2 Technical Intelligence Collection

Technical collection is performed by a variety of electronic sensors placed on platforms in space, the atmosphere, on the ground, and at sea to measure physical phenomena (observables) related to the objects of surveillance interest. A wide variety of sensor-platform combinations (Table 4.5) collect data that may be used for tactical, operational, or strategic intelligence. The operational utility of these collectors for each intelligence application depends upon several critical factors.

- *Timeliness*—The time from collection of event data to delivery of a tactical targeting cue, operational warnings and alerts, or a formal strategic report;
- *Revisit*—The frequency with which a target of interest can be revisited to understand or model (track) dynamic behavior;
- *Accuracy*—The spatial, identity, or kinematic accuracy of estimates and predictions;
- *Stealth*—The degree of secrecy with which the information is gathered and the measure of intrusion required.

The technical collection process requires the development of a detailed collection plan, which begins with the decomposition of the subject target into activities, observables, and then collection requirements. From this plan, technical collectors are tasked and data is collected and fused (a reconstruction that is the dual of the decomposition process) to derive the desired intelligence about the target.

This methodology is illustrated in Figure 4.4, which uses an illicit drug manufacturing and distribution operation example for analysis. The example follows the common intelligence collection plan that may be established by a local police force (on a small scale) or by a nation state intelligence agency to understand a global drug cartel [23]. Beginning with the hypothesized model of the targeted drug operation process at the top, the elements of activity that

Table 4.5

Surveillance and Reconnaissance Sources Include a Wide Variety of Sensors on Space, Air, Ground, and Sea Platforms

Source Types:	Radar and IFF	IMINT	SIGINT	MASINT
Space Platforms: Geostationary spacecraft Polar orbital spacecraft Low-earth orbit spacecraft Cooperative spacecraft constellations	Spaceborne radar (MTI or target tracking modes) surveillance	Weather satellites Imaging broad area search and precision imaging	SIGINT ferrets	IR missile warning/tracking Nuclear detection
Air Platforms: Tactical aircraft Standoff manned reconnaissance aircraft Penetrating high, medium altitude endurance unmanned air vehicles (UAVs)	Airborne warning and control aircraft Fighter aircraft	SAR, EO, IR, and multispectral imaging sensors on manned and unmanned reconnaissance	Airborne SIGINT standoff and penetrating UAVs	IR/EO, Laser surveillance aircraft Atmospheric sampling Nonacoustic ASW sensors
Ground Platforms: Attended fixed sites Mobile manned vehicles Manned portable sensors Unattended ground sensors in denied areas	Air defense, air surveillance sensors Counter-battery radar Ground surveillance (intrusion) radar	Combat tactical digital cameras Long-range IR/EO video IR night vision IR search and track	Ground-based ESM sites and vehicles Unattended ESM sensors	Seismic arrays Acoustic arrays IR radiometers
Sea (Undersea) Platforms: Shipboard sensors Submarine sensors Ship/sub towed sensors Heliborne dipping, air-dropped sensors Fixed, autonomous buoys Underwater arrays	Shipboard and sub air, surface, surveillance radar	Ship and sub long-range IR/EO video IR search and track	Ship, sub, and heliborne ESM sensors UAV ESM sensors	Ship-, sub-towed sonar array Ship, sub hull sonar array Nonacoustic ASW sensors Sonobuoys Dipping sonar

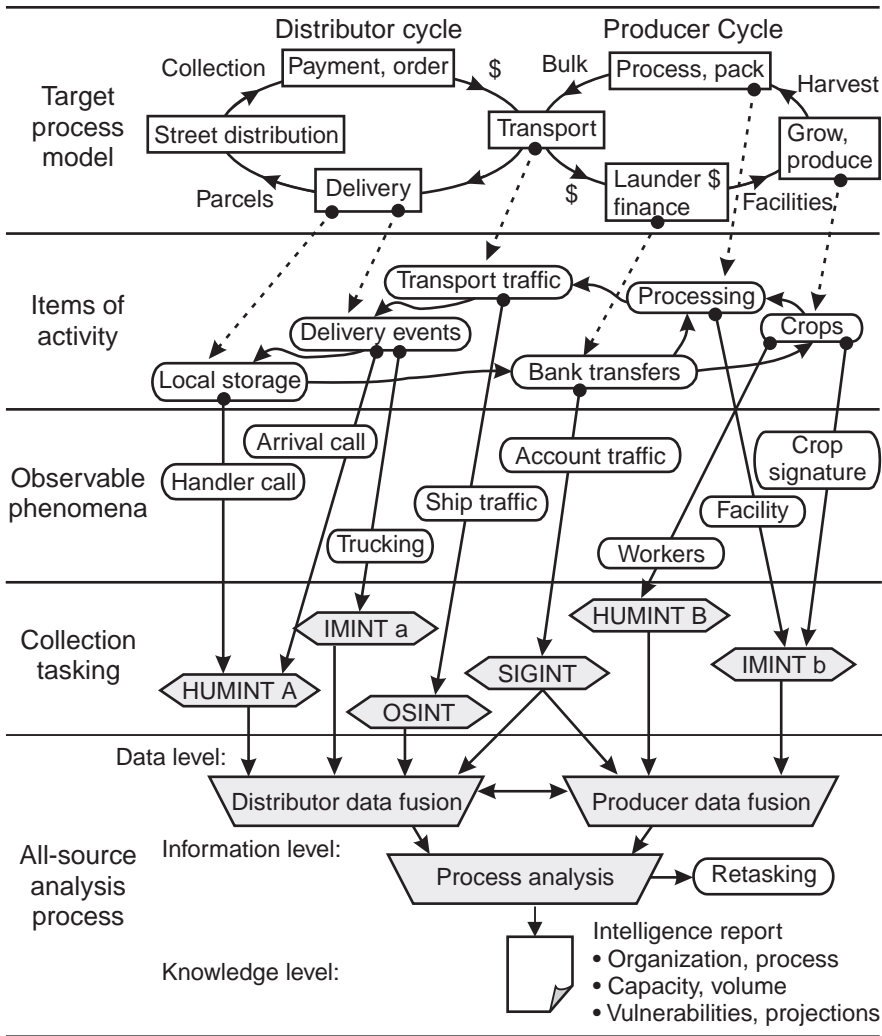


Figure 4.4 Process analysis, decomposition, and collection plan for a hypothetical surveillance and analysis of a drug operation.

characterize each step in the production and distribution processes are identified. In this oversimplified example, these activities are the most observable six events that are time-sequenced in the process model: (1) planting of the crops, (2) harvesting and processing, (3) transportation of bulk products, (4) delivery to local distributors, (5) local covert storage, and (6) bank transfers closely related to delivery. The observable phenomena from each of these events are

identified and assigned to technical (and, in this case HUMINT) collectors. The collectors include OSINT (shipping traffic logs), airborne IMINT (IMINT B in the figure, observing crop activities and potential processing facilities), ground-based video surveillance of shipping depots (IMINT A in the figure), and SIGINT analysis of electronic transfers of funds via court-authorized intercepts.

The example illustrates the complementary nature of HUMINT and technical sources, in which two HUMINT sources are required to guide the technical intelligence sources. HUMINT source A provides insight into trucking routes to be used, allowing video surveillance to be focused on most likely traffic points. HUMINT source B, closely related to crop workers, monitors the movements of harvesting crews, providing valuable cueing for airborne sensors to locate crops and processing facilities. The technical sources also complement the HUMINT sources by providing verification of uncertain cues and hypotheses for the HUMINT sources to focus attention. The collected data is analyzed for the existence of evidence and the synchronization of events to verify process cycles. The analysis process delivers a report that describes the organization, process flow, capacity, volume, and projected output, as well as the vulnerabilities that may be exploited by law enforcement.

4.1.1.3 Automated Intelligence Processing

The intelligence process must deal with large volumes of source data, converting a wide range of text, imagery, video, and other media types into processed products. Information technology is providing increased automation of the information indexing, discovery, and retrieval (IIDR) functions for intelligence, especially the exponentially increasing volumes of global OSINT [24]. The information flow in an automated or semiautomated facility (depicted in Figure 4.5) requires digital archiving and analysis to ingest continuous streams of data and manage large volumes of analyzed data. The flow can be broken into three phases: capture and compile, preanalysis, and exploitation (analysis).

The capture and compile phase includes the acquisition of volumes of multimedia data and conversion to digital form for storage and analysis. Electronic data (network sources) are directly formatted, while audio, video, and paper documents must be converted to digital form. Foreign sources may be translated by natural language analysis to convert to a common language base.

The preanalysis phase *indexes* each data item (e.g., article, message, news segment, image, or book chapter) by (1) assigning a reference for storage; (2) generating an abstract that summarizes the content of the item and metadata describing the source, time, reliability-confidence, and relation to other items (“*abstracting*”); and (3) extracting critical descriptors that characterize the contents (e.g., keywords) or meaning (“*deep indexing*”) of the item

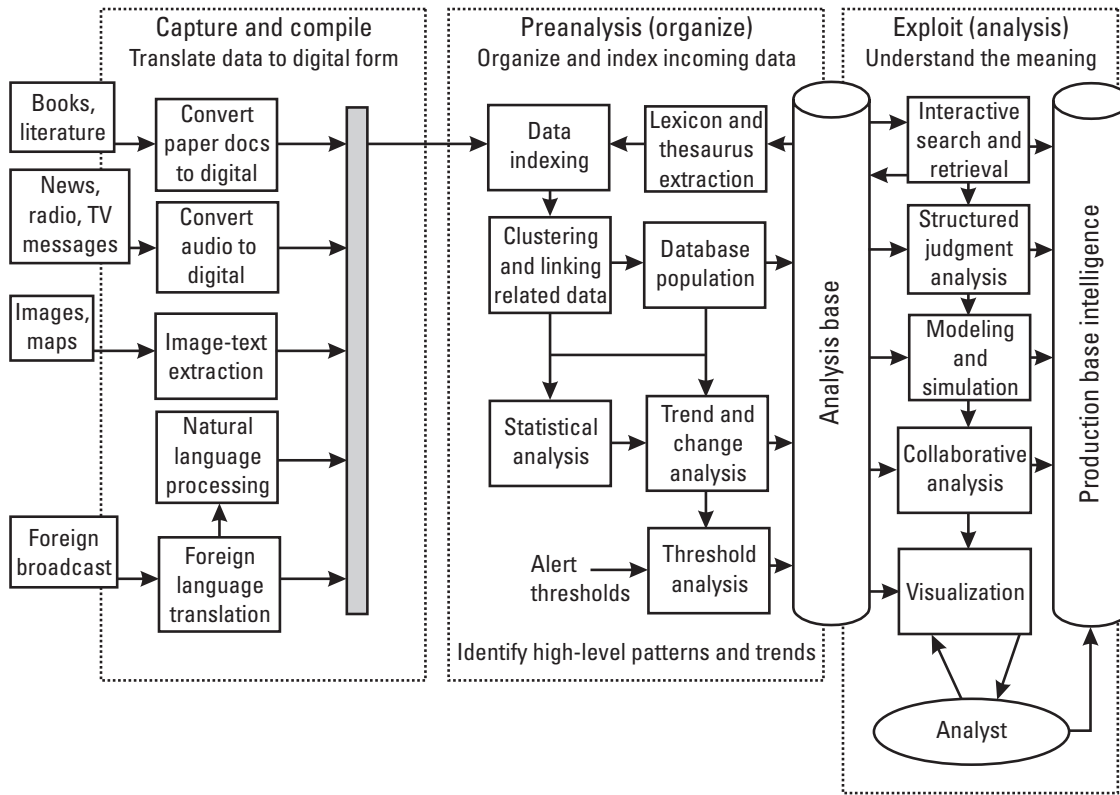


Figure 4.5 Intelligence processing and analysis flow includes three distinct phases to develop the production intelligence base.

for subsequent analysis. Spatial data (e.g., maps, static imagery, video imagery) must be indexed by spatial context (spatial location) and content (imagery content). The indexing process applies standard subjects and relationships, maintained in a lexicon and thesaurus that is extracted from the analysis information base. Following indexing, data items are clustered and linked before entry into the analysis base. As new items are entered, statistical analyses are performed to monitor trends or events against predefined templates that may alert analysts or cue their focus of attention in the next phase of processing. For example, if analysts are interested in relationships between nations A and B, all reports may be scored for a “tension factor” between those nations, and alerts may be generated on the basis of frequency, score intensity, and sources of incoming data items.

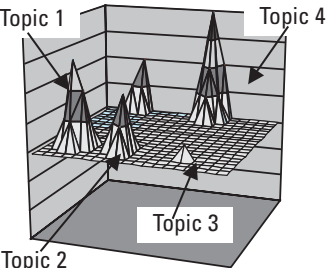
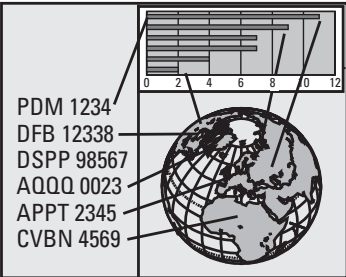
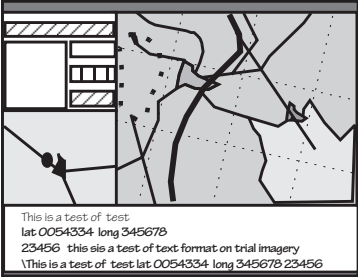
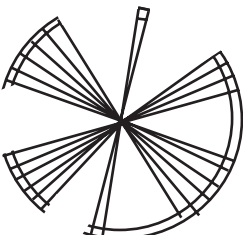
The third, exploitation, phase of processing presents data to the human intelligence analyst for examination using visualization tools to bring to focus the most meaningful and relevant data items and their interrelationships. The categories of automated tools that are applied to the analysis information base include the following [25]:

- *Interactive search and retrieval* tools permit analysts to search by topic, content, or related topics using the lexicon and thesaurus subjects.
- *Structured judgment analysis* tools provide visual methods to link data, synthesize deductive logic structures, and visualize complex relationships between datasets. These tools enable the analyst to hypothesize, explore, and discover subtle patterns and relationships in large data volumes—knowledge that can be discerned only when all sources are viewed in a common context.
- *Modeling and simulation* tools model hypothetical activities, allowing modeled (expected) behavior to be compared to evidence for validation or projection of operations under scrutiny.
- *Collaborative analysis* tools permit multiple analysts in related subject areas, for example, to collaborate on the analysis of a common subject.
- *Data visualization* tools present synthetic views of data and information to the analyst to permit patterns to be examined and discovered. Table 4.6 illustrates several examples of visualization methods applied to the analysis of large-volume multimedia data.

4.2 Battlespace Information Architecture

We have shown that dominant battlespace awareness is achieved by the effective integration of the sensing, processing, and response functions to provide a

Table 4.6
 Representative Visualization Methods for Analysis of Large Volumes of Multiple Media
 Intelligence Data

Visualization Method	Application	Example View
Themescape	Provides an aggregate view of a collection of documents or images, clustered in ND ($N > 3$) and presented in 3-D by topics or themes. Magnitude of peaks indicate number of correlated items, distance between peaks, the dissimilarity between topics. (Source: Pacific Northwest Laboratories.)	
Linked multimedia	Multiple views of different formats (e.g., text, video, maps, graphical) are presented in windows with links between related items displayed as overlays. Views can be "dragged" onto a common display from independent media views. (Source: Carnegie Mellon University.)	
Spatial view	Tactical map integrates conventional topographic map view with other data windows providing supporting nonspatial views (e.g. network views, effectiveness graphs).	
Wheel relationship	Complex relationships between large numbers of entities (e.g. communication nodes, contacts, transactions) can be visualized in aggregate, then drilled down to view for detail. Entities are segments of the annulus of a ring; spokes indicate relationships.	

comprehensive understanding of the battlespace, and possible futures and consequences. The integration of these functions in a representative architecture will provide insight into developing approaches to achieve DBA/DBK. The advanced battlespace information system (ABIS) is one such conceptual information infrastructure developed by the U.S. Joint Service Task Force to achieve the DBA/DBK objectives of JV2010 for C2 warfare [26].

ABIS provides a reference architecture toward which the United States will transition the current command, control, communications, computation, and intelligence (C4I) to achieve JV2010 objectives. The integration of U.S. C4I elements in the Gulf War has been described by Campen as the basis for information superiority, as detailed in *The First Information War* [27]. Emphasizing the importance of DBA/DBK in information-based warfare, Campen claimed,

By leveraging information, U.S. and allied forces brought to warfare a degree of flexibility, synchronization, speed and precision heretofore unknown. More to the point, Desert Storm shows that by leveraging information, a much smaller and less expensive military force can continue to underpin U.S. foreign policy in an unpredictable and disorderly new world [28].

Table 4.7 enumerates representative elements of the U.S. C4I infrastructure, which will be refined, upgraded, and integrated to achieve the goals of the ABIS architecture, including the following [29]:

- On-line collaborative spatial map and environmental views of tens of thousands of square kilometers of battlespace;
- Continuously updated all-source RED pictures of the battlespace: 98% awareness of “movers,” releasable coalition pictures within one minute, enemy forces identified with tactical unit associations and uncertainty;
- Continuously updated BLUE picture that represents status, planned events, capabilities, and uncertainty;
- Situation projection for own and enemy forces’ courses of action (COAs): continuous 1–5 minute projections for designated targets, 20-minute to 1-hour projections for movers, and 6–24 hour projections for major forces;
- Continuous DBA/DBK in the presence of hostile activities and deception.

Table 4.7

Representative U.S. Military System Elements That Comprise the Defense Command, Control, Communications, Computation, and Intelligence (C4I) Infrastructure

Information Process	Functions	Representative U.S. Military Systems	Applications
Sensing and collecting (Observe)	Wide area search	Navy AN/SPY-1, E2-C	Airborne early warning
	Detection	Air Force AWACS	Airborne warning and control
	Tracking		
	Identification	Air Force U2-R	Imaging surveillance
	Monitor	Air Force JSTARS	Radar surveillance
	Indications and warning	Air Force Rivet Joint RC-135	Signals surveillance
		Army Guardrail	Signals surveillance
		Unmanned air vehicles (UAVs)	Battlefield SIGINT
			Unmanned surveillance
Mark XII IFF		Cooperative IFF link	
	Fighter radars (AN/APG-XX)	Air surveillance	
	National technical means	Surveillance	
Information organization and understanding (Orient and Decide)	Dynamic tracking (behavior modeling)	Air Force AWACS	Air tracker/correlator
		Navy AN/SYS	Air tracker/correlator
	Track maintenance	Patriot/ TSQ-XX	Air defense radar node
	Data fusion node	Army All-Source Analysis System	Battlefield correlation
		Navy Joint Maritime Command Information System	Maritime correlation
	C2 Subsystem	Navy NTDS/ACDS/Aegis	Ship/fleet C2
	C2 Display System	Airborne C2 System	Air/land coordination
	C2 Decision Support	Joint IntelOps Center	Air coordination
C2 Command Functions	Army Battle Command System	Battlefield C2	
Dissemination (Act)	Tactical data exchange	TADIL-J (Link 16) Mode-S	Tactical cooperative link
	Tactical broadcast	TIBS/TRAP	Civil ATC link
	Global broadcast	Battlefield Transmission System	Intel broadcast services
		SINCGARS	BITS architecture
	Position report net	Enhanced Pos/Loc Report	Secure voice nets
	Voice net	System (EPLRS)	Position reporting

The ABIS functional architecture is based on a framework of three tiers (Figure 4.6) that are organized in a hierarchy with lower tiers providing services that enable the tiers above.

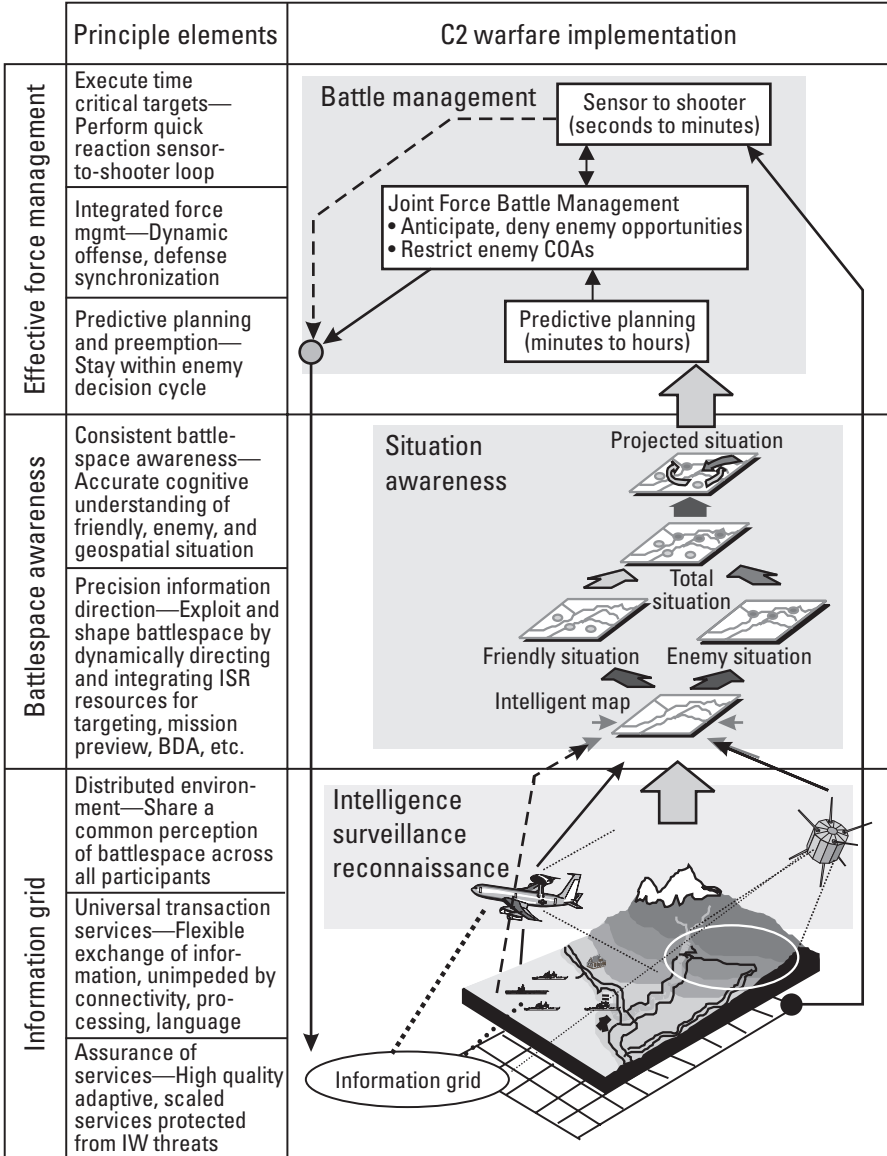


Figure 4.6 ABIS components depend upon the information grid. (Adapted from: [10].)

At the lowest tier is the *information grid*, an infrastructure that allows the flow of information from precision sensors, through processing, to precision forces. This tier is the forward path observe function of the OODA loop, and the feedback path distribution channel to control the act function of the loop and collaborative exchange paths. The grid provides for secure, robust transfer of four categories of information (Table 4.8) across the battlespace: (1) information access, (2) messaging, (3) interpersonal communications, and (4) publishing or broadcasting. The grid provides secure and universal transactions between all pairs of sensors, commands (at multiple echelons), and shooters. At this level, the ISR sensors and sources are networked to processing nodes, for distribution of time critical data to weapons (for rapid targeting of time critical targets) and data to intelligence analysis for longer-term surveillance and battle management. Current generation data links, such as the U.S. digital military links (Table 4.9), must be fully integrated with new links to achieve complete grid interaction across nets.

Table 4.8
Major Classes of Connectivity Provided by the Information Grid



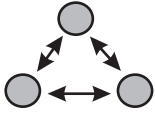
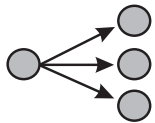
Connectivity Class	Topology	Representative Services
Information access		Sensor data reports Status report Data, information exchanges
Messaging		Conversation Sequential message traffic Command/confirm messages
Interpersonal communication		Collaborative discussion Collaborative analysis
Publishing or broadcasting		Direct broadcast of intelligence Broad area warning Weather, environment Situation, news reports

Table 4.9
Representative U.S. Military Digital Data Links

Type	Link	Description
Tactical data links	ATDL-1	Army TDL
	PADIL	Patriot TDL
	Link -11, 11B (UHF)	TADIL A, B messages
	Link 4	TADIL C messages
	Link 16 (L-Band)	TADIL-J (JTIDS) TDMA messages
UAV Links	Common	LOS link
	Satcom	Uplink to Satcom
Intel	TIBS	UHF tactical information broadcast service
Broadcasts	TRAP	UHF tactical recover and related broadcast
	TADIXS	Tactical data info exchange service
Dedicated sensor links	ASARS	SAR imagery
	JSTARS	MTI, SAR data
Wideband	Common data link	274 Mbps general wideband data link

The information grid must also carry a wide variety of data and information among command and control nodes, sensors, and shooters (weapons). The transaction services that manage these diverse information types (Table 4.10) must dynamically balance the use of grid bandwidth and channels among users on the basis of mission priorities, timeliness, security, and connectivity.

The middle tier of the architecture, *battlespace awareness capability*, controls the information grid and provides the orient function of the OODA model. *Precision information direction* tailors the flow of information on the grid, responding dynamically to the environment to allocate resources (e.g., bandwidth and content) to meet mission objectives. The tier includes the data fusion and mining processes that perform the intelligence-processing functions described in previous sections. These processes operate over the information grid, performing collaborative assessment of the situation and negotiation of resource allocations across distributed physical locations. The geospatial battlespace is modeled in an “intelligent map” upon which friendly and enemy situations are modeled and alternative future courses of actions (COAs) are predicted to project possible future behaviors.

Table 4.10
Command and Control Information Categories

Direction	Category	Representative Types of Information
To C2 nodes	Sensor/source data	Sensor reports (processed or raw data) Information requests, data needs
	Force data	Force location reports Status reports (events, entities, states) Plan data
From C2 nodes to forces	System control	Sensor management (cueing, control) Link management (e.g., demand assignments, channel control) Processing control (adaptive control)
	Broad intelligence	Status and individual reports (free, formatted text reports) Weather reports Friendly plan coordination data Warning and alerts
	Order of battle	Friendly force data (locations, types, plans, status) Hostile force data (locations, types, plans, status)
	Targeting	Target assignments Targeting data (type, location, threats, approach, coordination) Target imagery—annotated
	Bulk data	Raster data: secondary image dissemination (annotated imagery) Vector graphics (maps, terrain, weather charts, planning charts)

The highest tier is *effective force management*, which interacts with human judgment to provide the following:

- *Predictive planning and preemption*—Commanders are provided predictions and assessments of likely enemy and planned friendly COAs

with expected outcomes and uncertainties. Projections are based upon the information regarding state of forces and environmental constraints (e.g., terrain and weather). This function also provides continuous monitoring of the effectiveness of actions and degree of mission accomplishment. The objective of this capability is to provide immediate response and preemption rather than delayed reaction.

- *Integrated force management*—Because of the information grid and comprehensive understanding of the battlespace, force operations can be dynamically synchronized across echelons, missions, components, and coalitions. Both defense and offense can be coordinated, as well as the supporting functions of deployment, refueling, airlift, and logistics.
- *Execution of time-critical missions*—Time-critical targets can be prosecuted by automatic mission-to-target and weapon-to-target pairings, due to the availability (via the information grid) of immediate sensor-derived targeting information. Detection and cueing of these targets permit rapid targeting and attack by passing targeting data (e.g., coordinates, target data, imagery) to appropriate shooters.

The ABIS concept provides for a network of information distribution (the information grid) as well as force management by a network. Figure 4.6 illustrated the hierarchical nature of functions within ABIS, but did not imply a single hierarchical *organization* (like those that characterized second-wave warfare and conventional command and control). Force management is performed throughout the network, with long-term, high-volume joint force management occurring on one scale, and time-critical, low-volume, precision sensor-to-shooter management on another. Figure 4.7 illustrates the distinction between the OODA loop processes of the time-critical sensor-to-shooter mission and the longer term theater battle management mission.

The traditional long-term loop (measured in minutes to hours for a full-cycle planning to strike, with hundreds of missions) must accommodate and synchronize dozens of highly responsive and autonomous missions against time-critical targets, without conflict. The outer loop represents the typical sequence of the single air tasking order (ATO) process that plans hundreds of air sorties on a daily basis, while the nested sensor-to-shooter loop represents many independent tactical opportunities to respond and strike fleeting and mobile targets whose dynamic behavior exceeds the cycle time of the ATO loop.

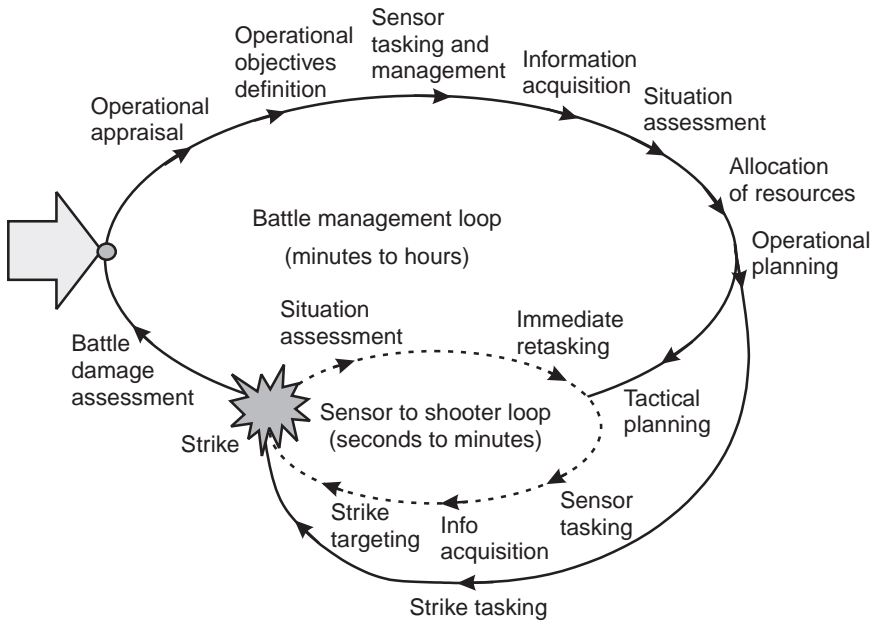


Figure 4.7 ABIS operational concept for nested OODA loops.

4.3 Summary

Dominant battlespace awareness and knowledge is dependent upon the ability to both acquire and analyze the appropriate data to comprehend the *meaning* of the current situation, the ability to project possible future *courses of action*, and the wisdom to know when sufficient awareness is achieved to act. The degree of DBA/DBK that is achieved by a military force in the conduct of C2W is dependent upon both technology and human operations. The introduction of technologies to provide increased volumes of information, common views of the battlespace, immediate and precise targeting, and accurate force projections must be complemented by new strategies, operational doctrine, and training. In the next chapter, we examine the process of establishing the new policies and strategies that will enable the implementation of new operations to conduct both C2W and net warfare.

Endnotes

- [1] These terms have been considered to be equivalent; *superiority* has been adopted by U.S. DoD (DODD S-3600.1 and Draft JCS Pub 3-13), while some prefer the term *dominance*,

- distinguishing *superiority* as a quantitative term and *dominance* as a qualitative term. U.S. Army FM-100 (information operations) defines dominance as the sufficient degree of superiority achieved: “Information Dominance is the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations short of war, while denying those capabilities to the adversary.”
- [2] Standard terminology adopted by “DoD Directive for Information Operations,” DODD S-3600.1 and DoD Joint Pub 3-13, “Joint Doctrine for Information Operations.”
 - [3] DoD Joint Publication 1-02, “DoD Dictionary of Military and Associated Terms.”
 - [4] “Joint Vision 2010,” US DoD Joint Chiefs of Staff, U.S. Government Printing Office, 1977.
 - [5] Cohen, W. S., “Report of the Quadrennial Defense Review,” Office of Secretary of Defense, U.S. Government Printing Office, May 1997.
 - [6] “National Cryptologic Strategy for the 21st Century,” National Security Agency, Goal 2: Military Operations, 1997.
 - [7] DoD Joint Pub 3-13.
 - [8] Cooper, J., “DBK and Future Warfare,” pp. 91–92, in Johnson, S. E., and M. C. Libicki, (eds.), *Dominant Battlespace Knowledge*, Washington, D.C.: National Defense University, 2d ed., 1966.
 - [9] Alberts, D., “The Future of Command and Control with DBK,” p. 72, in Johnson, S. E., and M. C. Libicki, (eds.), *Dominant Battlespace Knowledge*, Washington, D.C.: National Defense University, 2d ed., 1966.
 - [10] The classical terminology *intelligence preparation of the battlefield* refers to analysis of the physical space (e.g., terrain, lines of communications, vegetation, waterways, cultural features) and is described in FM-34-130 “Intelligence Preparation of the Battlefield,” July 8, 1994. I have adopted the battlespace terminology to emphasize expansion beyond the physical space. U.S. Army Field Manual FM 100-6, “Information Operations,” retains the classical terminology to encompass information infrastructure.
 - [11] “Battlefield Visualization Concept,” TRADOC PAM 525-70, Department of the Army, Headquarters, United States Army Training and Doctrine Command, Fort Monroe, VA, 23651-5000, Oct. 1, 1995.
 - [12] “Joint Warfighter Science and Technology Plan,” Office of Secretary of Defense, 2d ed., Nov. 1997, DTIC site www.dtic.mil/dstp/DSTP/97_jwstp/jwstp.htm.
 - [13] From definition (2) in Joint Pub 1-02.
 - [14] Four instruments of the intelligence discipline are often enumerated: (1) collection, (2) analysis and reporting, (3) counterintelligence, and (4) covert action. This section deals only with the first two, as elements of awareness. Counterintelligence is a function of defensive IW, and covert action is a function of offensive IW.
 - [15] DoD Joint Pub 1-02 defines five steps in the cycle by including processing and analysis in a single step.

-
- [16] Shulsky, A. N., *Silent Warfare—Understanding the World of Intelligence*, Washington, D.C.: Brasey's (U.S.), 2d ed., pp. 63–69.
- [17] Interview: Dr. Joseph Markowitz, in *Open Source Quarterly*, Vol. 1, No. 2, pp. 8–15.
- [18] Herman, M., *Intelligence Power in Peace and War*, Cambridge, NY: Cambridge University Press, 1996, see Chapter 4.
- [19] “Preparing for the 21st Century: An Appraisal of Intelligence,” U.S. Congressional Commission, U.S. Government Printing Office, Mar. 1, 1996.
- [20] “Making Intelligence Smarter: The Future of U.S. Intelligence,” Independent Task Force of Council on Foreign Relations, New York, 1996.
- [21] *Strategic Assessment: 1996*, Washington, D.C.: National Defense University, 1996, see Chapter 6.
- [22] Fuld, L. M., *The New Competitor Intelligence: The Complete Resource for Finding, Analyzing, and Using Information About Your Competitors*, New York: John Wiley & Sons, 1994.
- [23] Holden-Rhodes, J. F., *Sharing the Secrets: Open Source Intelligence and the War on Drugs*, Westport, CT: Praeger, 1997.
- [24] “Preparing U.S. Intelligence for the Information Age,” Director Central Intelligence, STIC 95-003, June 1995.
- [25] “Preparing U.S. Intelligence for the Information Age,” Director Central Intelligence, Part II: Analytic Tools To Cope with the Open Source Explosion, STIC 93-007, Dec. 1993, and Part III: Analytic Tools Recommendations for Open Source Information, STIC 95-002, Apr. 1995.
- [26] “Advanced Battlespace Information System (ABIS) Task Force Report,” U.S. DoD DDR&E and Joint Staff J-6, May 1996.
- [27] Campen, A. D., *The First Information War*, Washington, D.C.: AFCEA Press, 1992.
- [28] *Ibid.*, p. xi.
- [29] “Advanced Battlespace Information System (ABIS) Task Force Report,” U.S. DoD DDR&E and Joint Staff J-6, May 1996, Volume III, pp. 2–31.

Part II
Information Operations for Information
Warfare

5

Information Warfare Policy, Strategy, and Operations

Preparation for information warfare and the conducting of all phases of information operations at a national level requires an overarching policy, an implementing strategy developed by responsible organizations, and the operational doctrine and personnel to carry out the policy. The conceptual development of IW has led numerous study panels, national boards, and commissions in the United States and other emerging third-wave, information-intense nations to begin the establishment of policies and strategies to prepare for future information operations.

Information warfare is conducted by technical means, but the set of those means does not define the military science of C2W or netwar. Like any form of competition, conflict, or warfare, there is a policy that forms the basis for strategy, and an implementing strategy that governs the tactical application of the technical methods. While this is a technical book describing the methods, the system implementations of information warfare must be understood in the context of their guiding implementation. This chapter briefly introduces that context and sets the stage for the following chapters that describe information operation techniques. We begin by describing the policy and strategic foundations that are necessary to implement defensive and offensive operations.

Offensive information operations as described in future netwar and orchestrated netwar/C2W scenarios are considered by some to be operations of *mass disruption* or *mass protection*, with potential economic and social consequences on the order of those caused by chemical, biological, and even nuclear weapons of *mass destruction* [1,2]. Because of the uncertainty of consequences

and the potential impact of information operations on civilian populations, policy and strategy must be carefully developed to govern the use of information operations technologies—technologies that may even provide capabilities *before* consequences are understood and policies for their use are fully developed.

5.1 Information Warfare Policy and Strategy

The technical methods of information warfare are the *means* at the bottom of a classical hierarchy that leads from the *ends* (objectives) of national security policy. The hierarchy proceeds from the policy to an implementing strategy, then to operational doctrine (procedures) and a structure (organization) that applies at the final tactical level the technical operations of IW. The hierarchy “flows down” the security policy, with each successive layer in the hierarchy implementing the security objectives of the policy.

Table 5.1 illustrates this hierarchy with examples of representative U.S. documents that occur at each layer. Although the figure lists only *military* strategic, operational, and tactical documents, a comprehensive policy implementation must incorporate levels in all areas of the national infrastructure [3]. The principles described here are developed in the national context (for class 1 global IW), but they are equally applicable to corporate and even personal IW domains, as described in Chapter 1.

Security Policy

Policy is the authoritative articulation of the position of a nation, defining its interests (the objects being secured), the security objectives for those interests, and its intent and willingness to apply resources to protect those interests. The interests to be secured and the means of security are defined by policy. The policy may be publicly declared or held private, and the written format must be concise and clear to permit the implementing strategy to be traceable to the policy.

Any security policy addressing the potential of information warfare must consider the following premises:

1. *National interest*—The national information infrastructure (NII), the object of the information security policy, is a complex structure comprised of public (military and nonmilitary) and private elements. This infrastructure includes the information, processes, and structure, all of which may be attacked. The structure, contents, owners, and security

responsibilities must be defined to clearly identify the object being protected. The NII includes abstract and physical property; it does

Table 5.1

Hierarchy of U.S. Policy, Strategy, and Operations That Address Information Warfare (From a Military Perspective)

Level (Authority)	Role Description	Representative U.S. Documents
<p>Policy (government policymakers, Department of Defense)</p>	<p>Define the objects of security (interests), the security objectives for those interests, and their intent and willingness to apply resources to protect those interests.</p>	<p>National Cryptologic Policy National Security Act (1947 and revisions) National Infrastructure Protection Policy Memorandum of Policy MOP-30 Joint Chiefs of Staff, Command and Control Warfare, 8 March 1993 CJCSI 3210.01, Joint Information Warfare Policy, 2 January 1996 CJCSI 3210.03, Joint Command and Control Warfare Policy, 31 March 1996 AR 525-21, Battlefield Deception Policy, 30 October 1989 AR 525-20, Information Warfare/Command and Control Warfare (IW/C2W) Policy (draft) DoD Directive 3600.1. Information Warfare, 09 December 1996</p>
<p>Strategy (military joint staff, services)</p>	<p>Develop a plan to apply political, economic, psychological, and military force as necessary during peace and war to afford the maximum support to policies.</p>	<p>National Military Strategy. February 1995 National Security Strategy. January 1995 DoD Directive S-3600.1. Information Warfare Joint Vision 2010 "C4I for the Warrior." The Joint Staff Pamphlet. J6. 12 June 1993 USAF Horizons "Copernicus...Forward: C4I for the 21st Century," U.S. Navy Public Affairs Library, June 1995 Army Enterprise Strategy Implementation Plan. Office of the Secretary of the Army. 8 August 1994 JCS Pub 3-13. Joint Command and Control Warfare (C2W) Operations (final draft). September 1995</p>

Table 5.1 (continued)

Level (Authority)	Role Description	Representative U.S. Documents
Operations (commander)	Establish organizations; plan resources; develop and test capabilities (e.g., human competencies, legal, technical means); create concepts of operations (CONOPS) to implement the strategy. Oversee development of doctrine.	<p>DoD Directive 5200.1, DoD Information Security Program</p> <p>DoD Directive 5205.2, DoD Operations Security Program</p> <p>TRADOC Pam 525-69. Concept for Information Operations. 1 August 1995</p> <p>TRADOC Pam 525-70. Battlefield Visualization Concept. 1 October 1995</p> <p>JCS Pub 3-58, Joint Doctrine for Operational Deception</p> <p>JCS Pub 2-01, Joint Tactics, Techniques, and Procedures for Intelligence Support to Joint Operations</p> <p>JCS Pub 3-53. Doctrine for Joint Psychological Operations. 30 July 1993</p> <p>JCS Pub 3-56. Command and Control Doctrine for Joint Operations. 3 May 1995</p>
Tactics (war fighter)	Equip, train for, and deploy the technical means and tactical doctrine for application of those means to conduct information operations.	<p>U.S. Army FM 100-6, Information Operations 27 August 1996</p> <p>U.S. Army FM 33-1. Psychological Operations. 18 February 1993</p> <p>Other field manuals, training manuals, and detailed tactical documents for intelligence, electronic warfare, network attack and exploit operations, special operations, and other operations.</p>

not include human life, although human suffering may be brought on by collateral effects.

2. *New vulnerabilities*—Past security due to geographic and political positions of a nation no longer applies to information threats, in which geography and political advantages are eliminated. New vulnerabilities and threats must be assessed because traditional defenses may not be applicable [4].
3. *Security objective*—The desired levels of information security must be defined in terms of integrity, authenticity, confidentiality, nonrepudiation, and availability.

4. *Intent and willingness*—The nation must define its intent to use information operations and its willingness to apply those weapons. Questions that must be answered include the following:
 - What actions against the nation will constitute sufficient justification to launch information strikes?
 - What levels of information operations are within the Just War Doctrine? What levels fall outside?
 - What scales of operations are allowable, and what levels of direct and collateral damage resulting from information strikes are permissible?
 - How do information operations reinforce conventional operations?
 - What are the objectives of information strikes?
 - What are the stages of offensive information escalation, and how are information operations to be used to de-escalate crises?
5. *Authority*—The security of highly networked infrastructures like the NII requires shared authorities and responsibilities for comprehensive protection; security cannot be assured by the military alone. The authority and roles of public and private sectors must be defined. The national command authority and executing military agencies for offensive, covert, and deceptive information operations must be defined. As in nuclear warfare, the controls for this warfare must provide assurance that only proper authorities can launch offensive actions.
6. *Limitations of means*—The ranges and limitations of methods to carry out the policy may be defined. The lethality of information operations, collateral damage, and moral/ethical considerations of conducting information operations as a component of a just war must be defined.
7. *Information weapons conventions and treaties*—As international treaties and conventions on the use (first use or unilateral use) of information operations are established, the national commitments to such treaties must be made in harmony with strategy, operations, and weapons development.

The recognized essential elements of security policy, developed to an art in the Cold War, that may now be applied to information warfare by analogy include the following:

- *Defense or protection*—This element includes all defensive *means* to protect the NII from attack: intelligence to assess threats, indications and warning to alert of impending attacks, protection measures to mitigate the effects of attack, and provisions for recovery and restoration. Defense is essentially passive—the only response to attack is internal.
- *Deterrence*—This element is the *threat* that the nation has the will and capability to conduct an active external response to attack (or a preemptive response to an impending threat), with the intent that that the threat alone will deter an attack. A credible deterrence requires (1) the ability to identify the attacker, (2) the will and capability to respond, and (3) a valued interest that may be attacked [5]. Deterrence includes an offensive component and a dominance (intelligence) component to provide intelligence for targeting and battle damage assessment (BDA) support.

The organization of a policy-to-operations structure is provided in Figure 5.1, illustrating the technical operations performed at the tactical level that may be developed to implement policy.

Security Strategy

National strategy is the art and science of developing and using the political, economic, and psychological powers of a nation, together with its armed forces, during peace and war, to secure national objectives. The national military strategy extends this to apply the armed forces to afford the maximum support to policies in order to increase the probabilities and favorable consequences of victory and to lessen the chances of defeat [6]. Strategists, both military and business alike, debate the precise content, development, and implementation of strategy, but all recognize it must be a dynamic process, ever changing to adapt to the external environment to meet even a static policy position [7].

Strategy is articulated in a plan, defining the means to implement policy. The strategic process (Figure 5.2) includes both strategy developing activities and a complementary assessment process that continuously monitors the effectiveness of the strategy [8].

Strategy development activities progress in the following stages:

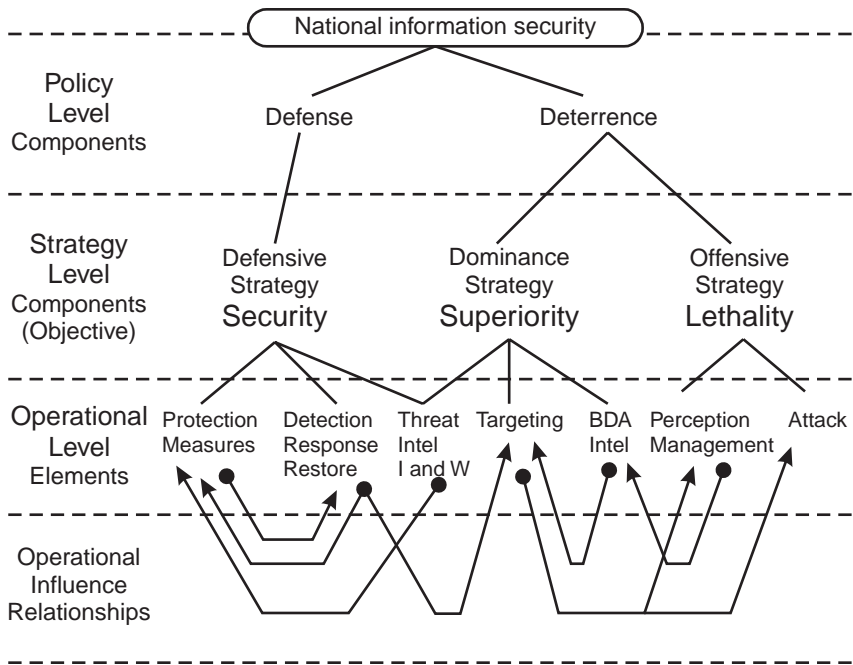


Figure 5.1 Fundamental hierarchy and components of a national information security strategy.

1. Situational analysis is performed to assess the current and predicted threat to the NII, and the technological factors that influence the vulnerability of the NII and lethality of threats.
2. Strategic objectives based upon the national security policy are established. The objectives qualify and quantify the levels of security (defense and deterrence) to be achieved and the dates of achievement.
3. Alternative approaches to meet the objectives are developed, based upon the shortfalls in security and uncertainty regarding the threats.
4. The alternatives are weighed, and specific plan elements (e.g., protection strategy, indications and warning strategy, response strategy) are selected on the basis of effectiveness, feasibility, cost benefits, and risk. The elements of the plan are integrated into a coherent strategic plan.
5. An approach to measure and manage risks to the strategy implementation plan is also developed, quantifying risks, likelihood of occurrence, and consequences. Abatement plans are developed for each risk area.

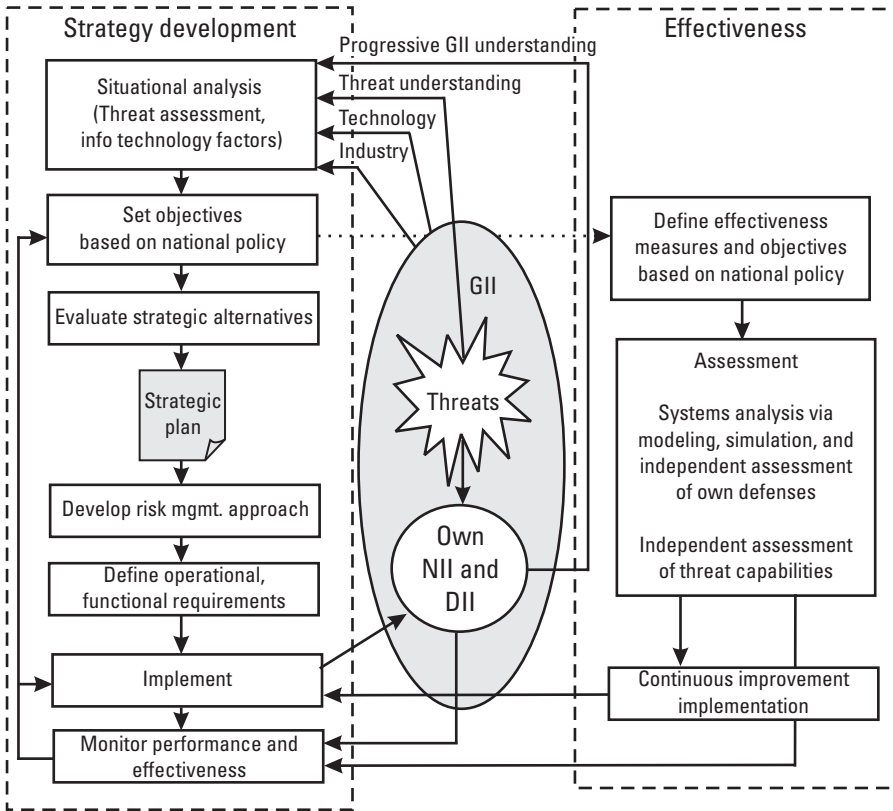


Figure 5.2 The strategic process includes strategy development and assessment elements.

6. Based upon the strategic plan, operational requirements are derived to implement the plan, including the following components:
 - Organization structure, roles, and missions;
 - Required R&D and test and evaluation (T&E) activities;
 - Development of operational concepts, doctrine, and training.
7. Throughout the implementation of the plan, the performance of implementing activities is monitored, and progress may be used to revise elements of the plan.

The effectiveness assessment includes the following stages throughout the implementation of the strategy:

1. Based upon the strategic objectives, effectiveness metrics (and time lines) are established to monitor progress as the strategy is implemented.
2. Ongoing assessment is conducted by an independent organization (e.g., computer emergency response teams, IW centers of excellence) to perform modeling, simulation, and analysis of operational tests, intelligence, and other threat data. The assessments are regularly reported to the policymaking authority.
3. Shortfalls, determined in the assessment process, are used to improve the operational implementation process and, if necessary, to reconsider the strategic plan approach.

The components of a strategic plan will include, as a minimum, the following components:

- Definition of the missions of information operations (public and private, military and nonmilitary);
- Identification of all applicable national security policies, conventions, and treaties;
- Statement of objectives and implementation goals;
- Organizations, responsibilities, and roles;
- Strategic plan elements:
 1. Threats, capabilities, and threat projections;
 2. NII structure, owners, and vulnerabilities;
 3. Functional (operational) requirements of IW capabilities (time phased);
 4. Projected gaps in ability to meet national security objectives, and plan to close gaps and mitigate risks;
 5. Organizational plan;
 6. Operational plan (concepts of operations);
 7. Strategic technology plan;
 8. Risk management plan;
- Performance and effectiveness assessment plan.

Before moving to offensive and defensive operations that result from strategy, we consider the development of an operational (or functional) model of information warfare that may be used to develop operations and to perform modeling and simulation to assess the effects and effectiveness of IW concepts.

5.2 An Operational Model of Information Warfare

Information operations are performed in the context of a strategy that has a desired objective (or end state) that may be achieved by influencing a target (the object of influence). In this section, a simple functional model is developed to form the basis for future discussions of operations and the techniques employed.

Information operations are defined by the U.S. Army as

Continuous military operations within the Military Information Environment (MIE) that enable, enhance and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; information operations include interacting with the Global Information Environment (GIE) and exploiting or denying an adversary's information and decision capabilities [9].

The model is an extension of the basic conflict model introduced in Chapter 1, and includes concepts adapted from Johnson [10] that recognize three conceptual domains of information operations activity. The model recognizes that targets exist in (1) physical space, (2) cyberspace, and (3) the minds of humans. The highest level target of information operations is the human perception of decision makers, policymakers, military commanders, even entire populations. The ultimate targets and the operational objective are to influence their perception to affect their decisions and resulting activities.

The model (Figure 5.3) distinguishes three levels or layers of functions on both the attacker and the target sides [11]. The layers are hierarchical, with influence flowing downward on the attacker side and upward on the target side. The objective of the attacker is to influence the target at the perceptual level by actions that may occur at all levels of the hierarchy. The three layers follow the cognitive model introduced earlier in Chapter 1, dealing with knowledge at the highest level, information at the intermediate level, and data at the lowest level.

The first layer is at the *perceptual* or psychological level, which is abstract in nature and is aimed at management of the perception of a target audience. At this level, the strategic objective defines the desired actions of the target and the perception(s) that will most likely cause those actions. If the desired action is

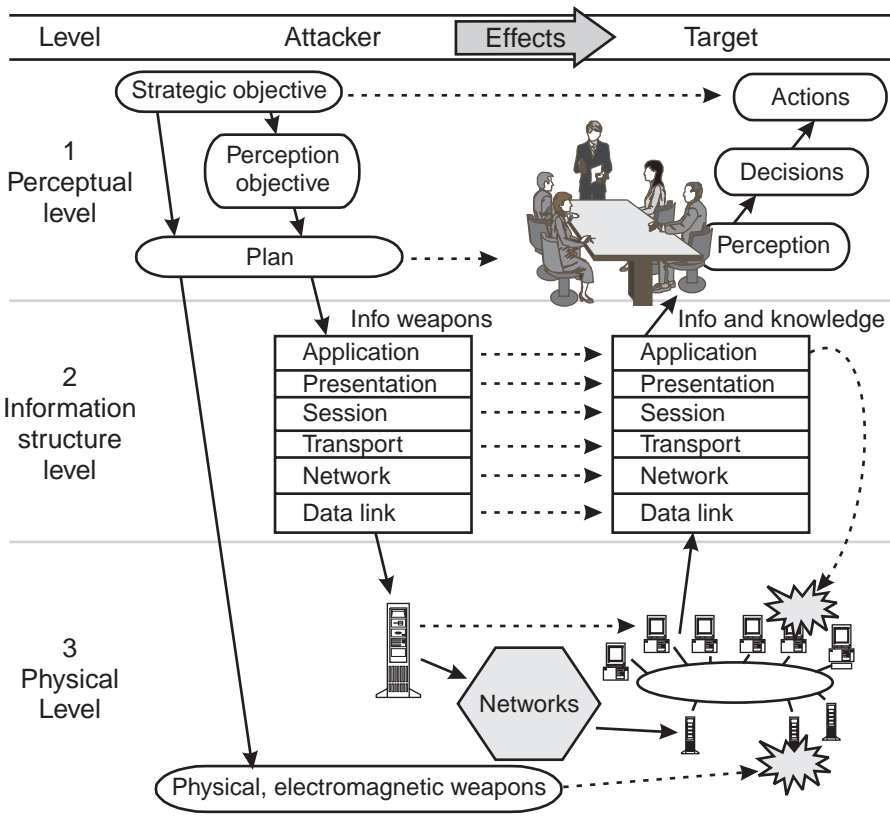


Figure 5.3 Operational model of information operations.

termination of aggression, for example, the objective perception for targeted leaders may be “overwhelming loss of control, disarray, and loss of support from the populace.” If the desired action is disengagement from a military action, the objective perception for targeted military commanders may be “lack of logistic support to sustain operations.” These perception objectives may be achieved by a variety of physical or abstract (information) means, but the ultimate target and objective is at the purely abstract perceptual level, and the effects influence operational behavior. The influences can cause indecision, delay a decision, or have the effect of biasing a specific decision. The abstract components of this layer include objectives, plans, perceptions, beliefs, and decisions [12].

The next layer is the information *infrastructure* layer, which includes the abstract information infrastructure that accepts, processes, manages, and stores

the information. The figure applies the Open System Interconnection (OSI) architecture model for information layers to illustrate how attacks may occur at sublayers within the three layers of the top-level model [13]. This is the layer that is most often considered to be the “cyberspace” dimension at which malicious software and infrastructure exploitation (hacking) attacks occur. The effects at this layer influence functional behavior of the system, and the components of this layer include data, information, and knowledge processes and structures. Notice in the model that the application layer delivers information and knowledge to humans to influence their perception, and it also controls objects in the physical domain (e.g., computers, communications, industrial processes). Attacks on this intermediate layer can have specific or cascading effects in both the perceptual and physical layers.

The third and lowest layer is the *physical system* level, which includes the computers, physical networks, telecommunications, and supporting structural components (e.g., power, facilities, environmental control) that implement the information system. Also at this level are the human administrators of the systems, whose physical influence on the systems is paramount. The effects at this level are technical in nature, influencing the technical performance of the system. Attacks at this layer are also physical in nature.

Attacks may occur directly across the perceptual layer (e.g., a direct meeting between leaders in which human discourse is used to influence the perception of a target, or to collect intelligence), or they may target lower layers with the intent of having consequent influences on other layers. Figure 5.3 illustrates the flow down from the attacker strategy to multiple layer attacks, which are orchestrated to bring about operational effects at the target’s perceptual level. Consider three representative examples chosen from several offered by Johnson [10].

- Communication jamming targets the physical layer, causing the technical effect of signal blockage, the functional effect of loss of information, and a detrimental operational effect on decision making due to lack of intelligence.
- A network worm targets the information infrastructure layer causing no technical effects, but the functional effect of degraded network performance, resulting in the operational effect of delayed decisions.
- A military deception operation targets the decision process and may have no technical or functional effect (the deception is presented through these layers, but the layers are not detrimentally affected). The desired effect of the deception is operational, causing an incorrect decision on the part of the targeted military command.

Table 5.2 contrasts the characteristics of these three layers and illustrates the distinct roles for security at each layer.

The model illustrates how operational elements (listed earlier in Figure 5.1) must consider each level of the model. Consider, for example, how intelligence collection for indications and warning, targeting, and battle damage assessment must consider all three levels.

Table 5.2
Characteristics of the Operational Model of Information Operations

Model Layer (Level of Abstraction)	Characteristics and Components	Attacker's Operations	Defender's Operations	Desired Effects
1 Perceptual (knowledge)	Knowledge and understanding in human decision space: <ul style="list-style-type: none"> • Perception • Beliefs • Reasoning 	PSYOPS Diplomacy Civil and public affairs	Psychological security Objective aids	Cognitive—influence decisions and behavior
2 Infrastructure (information)	Information maintained in cyberspace: <ul style="list-style-type: none"> • Data structures • Processes • Protocols • Data content 	Network attack, support measures Electrical power attack	INFOSEC information security	Functional—influence the effectiveness and performance of information functions supporting perception and controlling physical processes
3 Physical (data in physical form)	Data managed in physical space: <ul style="list-style-type: none"> • Computers • Storage • Networks • Electrical power 	Physical electronic attack Intrusion Theft Wiretapping Destruction	OPSEC physical security	Technical—affect the technical performance and capacity of physical systems

- *Layer 1*—Intelligence should include an estimate of the target’s current perception, uncertainties, concerns, critical decisions, decision-making processes and authorities, and decision time lines. The perceived courses of action available to the target, and decision constraints, should be understood.
- *Layer 2*—Intelligence must describe the information infrastructure: information structures, protocols, communication and computing network structures, switching and fusion nodes, decision points, power grids, security characteristics, and so forth, with an assessment of vulnerabilities.
- *Layer 3*—Finally, intelligence must detail the physical characteristics of systems, computers, telecommunications, power, facilities, personnel, and security support barriers to the targeted physical systems.

The attack threads through the IW model for three categories of information warfare are illustrated in Table 5.3. Exploitation of the physical and information layers purely for purposes of perception management, or psychological warfare (PSYWAR), is illustrated at the top of the figure. Command and control warfare (C2W), in which attacks occur at all three layers, is depicted at the bottom of the figure. These distinctions are representative only, recognizing that in real-world conflict, attacks will occur at all levels to varying degrees. Large-scale netwar, for example, may be supported by small-scale but crucial physical attacks on infrastructure or personnel to accomplish overall objectives.

5.3 Defensive Operations

The U.S. Defense Science Board performed a study of the defensive operations necessary to implement IW-defense at the national level, and in this section we adapt some of those findings to describe conceptual defensive capabilities at the operational level [14]. The board noted the rationale and urgency for implementing defensive operations against potential offensive threats:

Offensive information warfare is attractive to many [potential adversaries] because it is cheap in relation to the cost of developing, maintaining, and using advanced military capabilities. It may cost little to suborn an insider, create false information, manipulate information, or launch malicious logic-based weapons against an information system connected to the globally shared telecommunication infrastructure. The latter is particularly attractive; the latest information on how to exploit many of the design attributes and security

Table 5.3
Attack Threads for Three Warfare Forms

Warfare Form	Characteristics	Attack Threads in IW Model
<p>NETWAR</p> <ul style="list-style-type: none"> • Pure PSYWAR • Political Warfare 	<p>All effects target the perception of the target audience. Physical and information layers only provide the conduit to conduct perception management. These layers are exploited, not attacked.</p>	
<p>NETWAR</p> <ul style="list-style-type: none"> • PSYWAR • Economic Warfare • Denial of Service 	<p>All effects target the perception of the target audience—and include attacks on the information infrastructure to access the target audience. Some elements of information infrastructure are exploited, others attacked, and others used to convey perception themes.</p>	
<p>Command and Control Warfare (C2W)</p>	<p>All three layers of the infrastructure are exploited, attacked, and used to convey the perception themes. Targets are military and national leaders (decision makers).</p>	

flaws of commercial computer software is freely available on the Internet. In addition, the attacker may be attracted to information warfare by the potential for large nonlinear outputs from modest inputs [15].

As illustrated earlier in Figure 5.1, the defensive operational categories include threat intelligence with indications and warnings (I&W), protection measures, and attack response and restoration.

Threat Intelligence, I&W

Essential to defense is the understanding of both the external threats and the internal vulnerabilities that may encounter attack. This understanding is provided by an active intelligence operation that performs external assessments of potential threats [16] and internal assessments of vulnerabilities.

The external threat assessment component performs the following activities:

- *Identify potential threats*—Candidate threats are categorized into non-state and state-supported individuals or groups (Table 5.4) with either motives or capability. A threat matrix is created to accumulate intelligence gathered about these threats (hypothesized, potential, and verified) and their activities [17]. In this phase, motives must be

Table 5.4
Categories of Potential Information Warfare Threats

Sponsorship	Threat Category	Motivations	Representative Threat Activities
Non-state sponsored	Individual criminals, hackers, insiders, and unauthorized users	Challenge Harassment Revenge	Database destruction, modification Theft of information Denial of service attacks
	Organized criminal groups	Greed	Capture of access data, electronic commerce data, or monetary instruments
	Political dissidents and terrorists	Ideology Psychological terror Bring attention to cause Influence policy	Broadcast of propaganda on pirated services Random attacks on visible infrastructure targets
State sponsored	Terrorists	Influence policy Overthrow government	Random or sequenced attacks on visible infrastructure targets
	Foreign intelligence services Tactical units	Disrupt military mission Overthrow government	Multiple-level attack on elements of a defense information infrastructure
	Strategic units	Aggression Disrupt military missions Overthrow government	Orchestrated multiple-level attack on many elements of a national information infrastructure

hypothesized, characterized, and verified to understand the threat potential.

- *Determine capability*—The capabilities and structure of threats are determined, using the all-source intelligence methods described earlier in Chapter 4. Technical R&D activities, statements (public and private), and intelligence-gathering operations (which may be targeting ventures) provide insight into the maturity of a threat: technical capability, development or “weaponization” of technical capabilities, operational testing status, and level of readiness to conduct operations. A threat projection is also estimated, projecting the time scale for development of future capabilities.
- *Establish I&W criteria*—Based upon the motives and technical capability, characteristics that indicate or warn of imminent operations (intelligence collections or attack) are developed to provide I&W templates that characterize expected behaviors that indicate preparations and sequencing of attacks.

Internal vulnerability assessments determine the potential areas of operational or technical security (OPSEC and INFOSEC, respectively) that may allow access to potential attackers. The vulnerability assessment can be performed by analysis, simulation, or testing. Engineering analysis and simulation methods exhaustively search for access paths during normal operations or during unique conditions (e.g., during periods where hardware faults or special states occur). Testing methods employ “red teams” of independent evaluators armed with attack tools to exhaustively scan for access means to a system (e.g., communication link, computer, database, or display) and to apply a variety of measures (e.g., exploitation, disruption, denial of service, or destruction).

The combined external (threat) and internal (vulnerability) assessments are necessary to perform a risk assessment, which also considers the impact or adverse *consequences* of attacks, if successful. Risk is described by the notional relationship:

$$\text{Risk} = \left[\frac{\text{Threat} \times \text{Vulnerabilities}}{\text{Protective Countermeasures}} \right] \times \text{Impact} \quad (5.1)$$

This primitive relationship forms the basis for quantifying values of risk for real systems, where arguments and appropriate scale factors may be used to provide a variety of risk parameters to control or manage the risk to a specific system. The tradeoff between benefits of information access and the

consequences of attacks by imposing threats requires a management of the level of risk imposed upon a system.

Risk management (as opposed to risk avoidance) acknowledges that successful attacks will occur (access, penetration, information or service compromise, even destruction) but that the likelihood of occurrence and degree of consequence will be limited and controlled to a small, statistically quantified value. The contrast in risk avoidance and management is summarized in Table 5.5, illustrating how risk requirements may be layered and quantified.

Table 5.5

Risk Management Tolerates but Controls Penetration To Gain the Benefits of Information Access.
(Adapted from: Sutherland [18].)

Approach:	Risk Avoidance	Risk Management
Basic Principles	Confidentiality	Integrity, availability, confidentiality
Implementation Approach	Rigidity Security versus operation High cost Protect Technology dependent "Prevention-only" countermeasures Separate classified and unclassified structures	Flexibility Integrated protection-operation Incremental improvements Detect-contain-recover Quantified risk Security process metrics
Solution	Full TEMPEST protection for electromagnetic radiation	Integrated and multilevel classified and unclassified structures Multilevel TEMPEST
Example Requirements, Measures of Effectiveness (Relative Response to Attacks)	Prevent > 99% Residual risk < 1%	Prevent > 80% Residual detected: Detect 20% Detect and contain 19% Detect, contain, recover 1% Residual unrecovered: Residual risk < 1%

- *Prevent*—Prevent access to 80% of attacks.
- *Detect*—Detect the presence of the remaining 20% of attacks that are not denied access; this residual includes those attacks that are contained (19%) and those that are not contained, but from which recovery is achieved (1%).
- *Residual*—The residual risk (1%) includes all attacks that are neither prevented, detected, contained, nor recovered and that incur the adverse consequences projected.

The risk management process requires a thorough analysis of specific risks for the targeted system and their likelihoods, a determination of the adverse consequences, and an analysis of the effect of planned mitigation approaches.

Protection Measures (IW-Defense)

Based on assessments of threats and vulnerabilities, operational capabilities are developed to implement protection measures (countermeasures or passive defenses) to deny, deter, limit, or contain attacks against the information infrastructure. All of these means may be adopted as a comprehensive approach, each component providing an independent contribution to overall protection of the infrastructure [19]. The prevention operations deploy measures at three levels, summarized in Table 5.6.

- *Strategic-level* activities seek to deter attacks by legal means that ban attacks, impose penalties or punishment on offenders, or threaten reprisals.
- *Operational security* (OPSEC) activities provide security for physical elements of the infrastructure, personnel, and information regarding the infrastructure (e.g., classified technical data).
- *Technical security* (INFOSEC) activities protect hardware, software, and intangible information (e.g., cryptographic keys, messages, raw data, information, knowledge) at the hardware and software levels.

OPSEC and technical INFOSEC measures are the subject of Chapter 8, and the reader is referred to that chapter for more detail on these measures.

Attack Response and Restoration

The capability to detect, respond to, and restore from information attacks completes the set of defensive operations. Figure 5.4 links the three defensive operations elements, showing the relationships between the elements and the

Table 5.6
Protection Measure Operations (IW-Defense)

Protection Level	Measure	Approach	Example Measures
Strategic measures	Ban capability, deployment, testing, or use	Establish multilateral agreements to ban the development, deployment, testing, use, or first use of offensive information operations	Convention (no use, no first use, no testing) Treaty
	Legal punishment	Establish national or international laws governing offensive operations and criminal penalties	Enacted laws with criminal penalties Agreements for international and interagency cooperation to pursue offenders
	Reprisal	Establish guidelines for reprisals against information aggressors	Economic sanctions Information blockades Military reprisal
Operational security (OPSEC)	Physical security	Establish physical barriers to protect personnel, hardware, and software from physical (kinematic, radiological, chemical, or biological); electromagnetic; or internal attacks by unauthorized access	Facility protection Access control Air conditioning, filtering, and control Power source protection and backup Access, use, protection processes, and procedures
	Personnel security	Establish controls and clearance for all personnel associated with design, testing, operation, and maintenance of infrastructure components	Personnel screening and clearance processes Investigation and periodic assessment Training Ongoing effectiveness assessment
Technical information security (INFOSEC)	Secure software	Establish procedural barriers and software/hardware barriers to access	Software encryption Firewalls Biometrics, tokens, and passwords
	Harden hardware	Design hardware to resist kinematic, radiological, electromagnetic, chemical, and biological attacks	Electromagnetic shielding Power source protection Radiation hardening Chemical-biological hardening

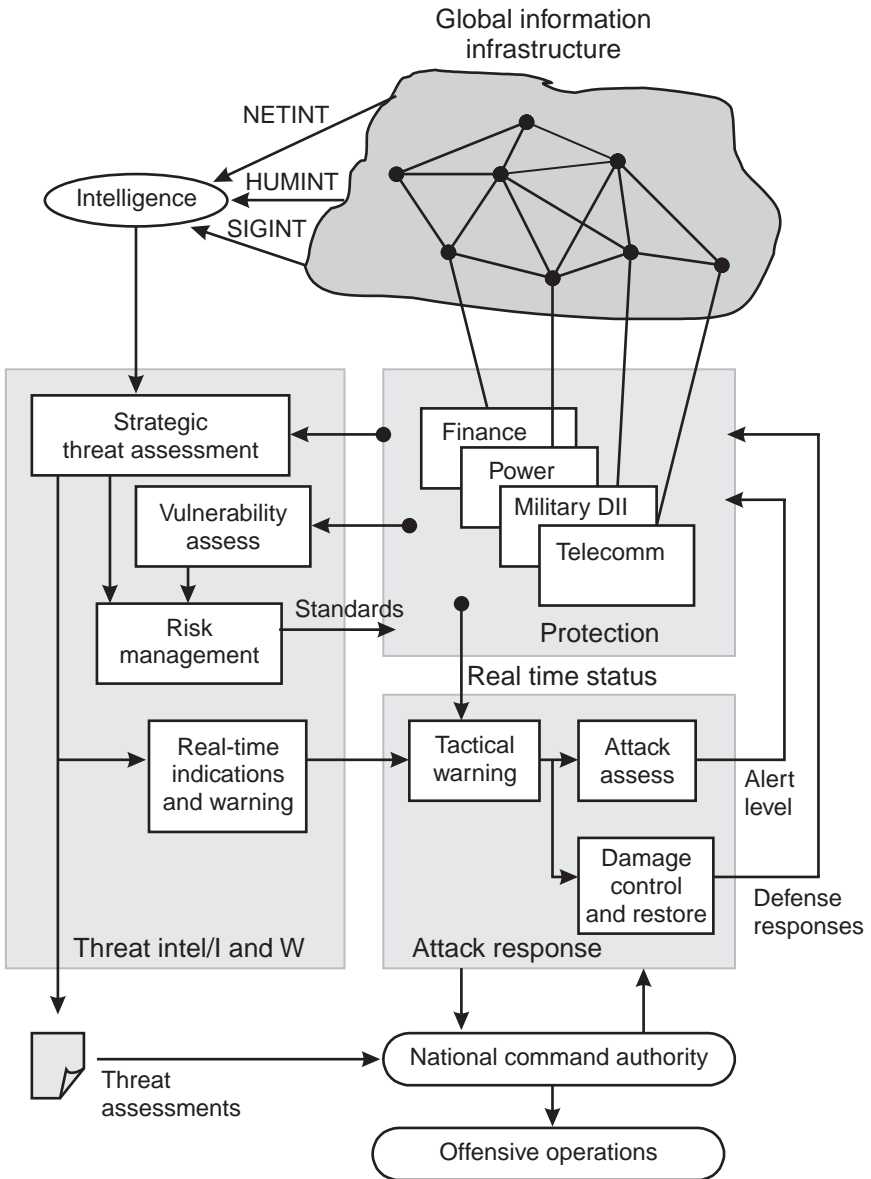


Figure 5.4 Defensive operational elements provide proactive and reactive protection of the information infrastructure.

infrastructure being defended. This real-time capability, depicted in the figure, can produce two reactions.

- *Defensive responses*—Detection of an attack can be used to generate alerts, increase the level of protective restrictions to access, terminate vulnerable processes, or initiate other activities to mitigate potential damage.
- *Offensive responses*—Detection can also be used to initiate deterrent-based offensive responses when the source of the attack can be determined. The detection process may also support targeting and response alternatives.

The figure describes the components of a tactical warning and attack assessment function as envisioned by the U.S. Defense Science Board and the President's Commission on Critical Information Infrastructure Protection in separate reports [20,21]. One of the functions of tactical warning and assessment is the generation of an alert level that identifies the state of the infrastructure at any given time. Five conceptual infrastructure-wide alert levels developed by the Defense Science Board (see Table 5.7) provide a progressive sequence of expected activities and defensive responses. The alert conditions follow the defense condition (DEFCON) model developed for strategic nuclear attacks, including the deployment of a minimum essential information infrastructure (MEII) and implementation of “wartime modes” of operation.

The functions of tactical response include the following:

- *Surveillance*—Monitor overall infrastructure status and analyze, detect, and predict effects of potential attacks. Generate alert status reports and warn components of the infrastructure of threat activity and expected events.
- *Mode control*—Issue controls to components to modify protection levels to defend against incipient threat activities, and to oversee restoration of service in the postattack period.
- *Auditing and forensic analysis*—Audit attack activity to determine attack patterns, behavior, and damage for future investigation, effectiveness analysis, offensive targeting, or litigation.
- *Reporting*—Issue reports to command authorities.

These tactical response concepts are described at the national information infrastructure level, but are functionally applicable to all levels of information

Table 5.7

Conceptual Progressive National IW Alert Levels, Corresponding Threats, and Responses. (*Adapted from: Report of the U.S. Defense Science Board Task Force on Information Warfare-Defense (IW-D), Office of Secretary of Defense for Acquisition and Technology, Washington, D.C., November 1996.*)

Alert Condition:	I	II	III	IV	V
Situation:	Normal Activity	Perturbation	Heightened Defensive Posture	Serious	Prewar
Level of Attack	Unstructured attacks	Surgical attacks	Tactical attacks	Major disruptive attacks	Strategic attacks
Typical Attackers	Amateur, experienced hackers Insiders Criminals	Well-funded nonstate sponsored attackers Criminals	State-sponsored IW attack unit Highly structured nonstate sponsored unit	State-sponsored IW attack unit	State-sponsored IW attack units, supported by insiders
Activity	Normal threat attempts and incidents	10% increase in incidents, 15% increase all incidents	20% increase all incident reports Condition II plus special contexts	Major regional or functional events that threaten national interests Condition II/III plus special contexts	Widespread incidents that undermine national ability to function Condition III/IV plus special contexts
Responses	Normal responses at individual target sites	Increase incident monitoring Analyze for patterns of larger attack activity Alert all agencies to increase awareness Initiate selective monitoring of critical elements	Disconnect unnecessary functions Initiate real-time audit for critical systems Begin mandatory reporting to central control	Implement mandatory central control Implement alternate routing Limit connectivity to minimal states Begin aggressive forensic investigations	Disconnect critical elements from public infrastructure Deploy minimum essential information infrastructure Implement war modes Declare state of emergency Prepare for response

components. Tactical response functions may be implemented at the facility level (e.g., a single power station), the system level (e.g., a regional power grid network), or at higher levels of networking.

5.4 Offensive Operations

Offensive operational capabilities require the capability to identify and specify the targets of attack (*targeting*) and then to *attack* those targets. These two capabilities must be able to be performed at all three levels of the operational model, as presented earlier in Section 5.2. In addition to these two, a third offensive capability is required at the highest (perceptual) level of the operational model: the ability to *manage the perceptions* of all parties in the conflict to achieve the desired end. Here, we describe these three elements of offensive operations, while the techniques of the operations are reserved for following chapters.

Perception Management

Four categories of traditional military operations (Table 5.8) provide the means to monitor and manage the perception of target audiences to meet objectives consistent with overall operations objectives [22]. In the operational model presented in Section 5.2, these disciplines perform top-level perceptual planning and management, while the messages are delivered directly (via human conversation or diplomatic discourse) or through lower level layers in the model. (It should be noted that although perception management is treated in this section on offensive operations, public and civil affairs activities can also be considered to be defensive countermeasures against an opponent's perception attacks.)

Public and civil affairs operations are open, public presentations of the truth (not misinformation or propaganda) in a context and format that achieves perception objectives defined in a perception plan. PSYOPS also convey only truthful messages (although selected "themes" and emphases are chosen to meet objectives) to hostile forces to influence both the emotions and reasoning of decision makers. PSYOPS require careful tailoring of the *message* (to be culturally appropriate) and selection of the *media* (to ensure that the message is received by the target population). The message of PSYOPS may be conveyed by propaganda or by actions. (Basic U.S. Joint PSYOP doctrine and historical examples of PSYOP implementations are provided in [23–25].)

In contrast to the first three means, military deception operations are performed in secrecy (controlled by operational security). These operations are designed to induce hostile military leaders to take operational or tactical actions that are favorable to, and exploitable by, friendly combat operations [26,27].

Table 5.8
Disciplines Involved in Perception Management

Perception Disciplines	Target Audience	Perception Objectives and Means
Military affairs	Public affairs Media Friendly populations	Objectives: To provide a consistent presentation of accurate, balanced, and credible information that achieves confidence in forces and operations Means: Press releases, briefings, and broadcasts (radio, TV, net)
	Civil affairs Foreign civil authorities and population in areas of conflict	Objectives: To provide a consistent presentation of position and credible information that supports friendly objectives Means: Civil meetings, press releases, briefings, broadcasts (radio, TV, net)
Military perceptions management	Psychological operations (PSYOPS) Hostile foreign forces Hostile or neutral foreign populations	Objectives: To convey selected information and indicators to foreign audiences to influence emotions, motives, objective reasoning, and, ultimately, to induce behavior to meet objectives Means: Projection of truth and credible messages via all media
	Military deception Hostile foreign military leaders Hostile foreign forces	Objectives: To confuse or mislead enemy leaders to make decisions that cause actions that are exploitable by friendly forces Means: Deceptive operations, activities, or stories to conceal, distort, or falsify indications of friendly intentions, capabilities, or actions

They have the objective of conveying untruthful information to deceive for one of several specific purposes.

1. *Deceit*—Fabricating, establishing, and reinforcing incorrect or pre-conceived beliefs, or creating erroneous illusions (e.g., strength or weakness, presence or nonexistence);
2. *Denial*—Masking operations for protection or to achieve surprise in an attack operation;

3. *Disruption*—Creating confusion and overload in the decision-making process;
4. *Distraction*—Moving the focus of attention toward deceptive actions or away from authentic actions;
5. *Development*—Creating a standard pattern of behavior to develop preconceived expectations by the observer for subsequent exploitation. (For historical accounts of classic deceptive strategies and operations, see [28,29].)

All of these perception management operations applied in military combat may be applied to netwar, although the media for communication (the global information infrastructure) and means of deceptive activities are not implemented on the physical battlefield. They are implemented through the global information infrastructure to influence a broader target audience.

Intelligence for Targeting and Battle Damage Assessment

The intelligence operations developed for defense also provide support to offensive attack operations, as intelligence is required for four functions.

1. *Target nomination*—Selecting candidate targets for attack, estimating the impact if the target is attacked;
2. *Weaponeering*—Selecting appropriate weapons and tactics to achieve the desired impact effects (destruction, temporary disruption or denial of service, reduction in confidence in selected function); the process targets vulnerability, weapon effect, delivery accuracy, damage criteria, probability of kill, and weapon reliability;
3. *Attack plan*—Planning all aspects of the attack, including coordinated actions, deceptions, routes (physical, information infrastructure, or perception), mitigation of collateral damage, and contingencies;
4. *Battle damage assessment (BDA)*—Measuring the achieved impact of the attack to determine effectiveness and plan reattack, if necessary.

Consider a hypothetical network attack on a military command and control node “Alpha Warrior HQ,” which relies on both wireless data links and fiber-optic land lines for communication with the forces that it commands. The attack objective for Operation BRAVO is to incapacitate the node from forwarding I&W information to division HQ during a 14-hour period, to cover a special forces insertion. In order to perform this function, the network (“ABC”) must be mapped to describe the local area network (LAN) and

external communication links. The commercial equipment at the node must be identified and potential vulnerabilities enumerated. The plan includes four components.

1. Distraction from the ABC network by attacking the more vulnerable DEF net with nuisance denial of service attacks;
2. Initiation of denial of service attacks on the network via covert access to the landline network (“Noma45”), applying spoofing techniques known to be effective on the commercial router on the net;
3. Attack on electrical power (destroying a transformer grid) to disrupt primary power to Alpha Warrior, supported by a concurrent attack on support facilities to mask the primary action;
4. Follow-up attack (timed after emergency power is initiated to allow thermal signature to develop high contrast) on the motor generator supporting Alpha Bravo and the uninterruptable power system (UPS).

The wireless network line will be monitored throughout the attack to perform real-time battle damage assessments in support of the BRAVO insertion operation. These assessments monitor the effectiveness of the denial of I&W (of the insertion) to division HQ.

Figure 5.5 illustrates a simplified example targeting folder format for the hypothetical BRAVO operation, describing the planned actions and the intelligence required both to carry out the attack and to conduct the postattack BDA.

Attack (IW-Offense) Operations

Operational attack requires planning, weapons, and execution (delivery) capabilities. The weapons include perceptual, information, and physical instruments employed to achieve the three levels of effect in the operational model. Table 5.9 summarizes the three levels of attack alternatives (IW-offense), following the same format as Table 5.6, which earlier categorized the alternatives for IW-defense operations. Offensive operations are often distinguished as direct and indirect means.

- *Indirect* attacks focus on influencing perception by providing information to the target without engaging the information infrastructure of the target. This may include actions to be observed by the target’s sensors, deception messages, electronic warfare actions, or physical attacks. External information is provided to influence perception, but the target’s structure is not affected.

TARGET SUMMARY FOLDER		
OPERATION: <u> BRAVO </u>		Plan Date: <u> </u>
Operation Date: <u> 03 Jan 1999 </u>		Prepared: <u> </u>
		Approved: <u> </u>
Item	Plan	Intelligence
Target Description	Alpha Warrior HQ Computer net #ABC Communication server A	52-453 ABC network model and description of server and LAN
Attack Objective	Deny targeted server operation on 03 Jan 99, from 0100 until at least 1500 to support BRAVO insertion operation by denying indications and warnings to division	52-400 Alpha Warrior indications and warning net
Attack Actions and Weapon(s)	Special force attack on primary power transformer at grid #1243 (explosive) Special force attack on motor generator and UPS on north end of building (mortar) Denial of service attack via local network-method #24 Denial of service attack via net Noma45-method #32a	52-315 Alpha Warrior strategic power system 52-289 Alpha Warrior HQ facility 52-453 Noma45 network model and description of server and LAN
Attack Timing	03 Jan 99 0100 03 Jan 99 0130 02 Jan 99 2200 02 Jan 99 2350	—
Coordinated Actions	Distraction—prior day 1400 begin/1900 end denial of service attacks on network #DEF Masking—Special force helo attack on Alpha Warrior bldg. B concurrent with attack 1), above	Conduct BDA via network monitor using methods #325, #432

Figure 5.5 Example target summary folder illustrates the components of an attack plan with supporting intelligence required.

Table 5.9
Categories of IW Attack Alternatives (IW-Offense)

Attack Level	Measure	Approach	Example Measures
Perception attack	PSYOPS	Perform actions or send messages to convey selected information and indicators to influence human emotions, motives, and objective reasoning	Radio, TV, or public network broadcasts Press releases Physical messages (leaflets)
	Deception	Employ deceptive operations, activities, or stories to conceal, distort, or falsify information	Deceptive network sites, messages, e-mail, or activities Physical messages (leaflets)
Operational attack	Systems attack	Apply methods to compromise integrity of information system	Organizational disruption Security disruption to downgrade trust in operation
	Personnel attack	Apply methods to compromise integrity or effectiveness of key personnel	Compromise system administrators Degrade effectiveness of operating or support personnel
Technical attack	Software attack	Apply software or information structural effects to exploit, disrupt, deny, or destroy data, information, or knowledge in information infrastructures	Software intercept "sniffing," exploitation of intercepted information Denial of service flood attacks Malicious software pathogens (viral, bacterial, worm code) Hacked access and destruction of information
	Hardware attack	Apply kinetic, radiological, electromagnetic, chemical, and biological effects to exploit, disrupt, deny, or destroy physical information systems, supporting systems (e.g., power, air conditioning, facilities structure), or personnel support systems	Physical (kinetic) destruction or theft ("break it, or take it") Physical or electromagnetic intercept of information Electromagnetic jamming (denial of service) Power source denial Radiological attack (on semiconductor circuitry) Directed electromagnetic energy attack (on semiconductor or other vulnerable circuitry) Chemical-biological attack on personnel or susceptible materials

- *Direct* attacks specifically engage the target's internal information, seeking to manipulate, control, and even destroy the information or the infrastructure of the target.

Offensive information warfare operations integrate both indirect and direct operations to achieve the desired effects on the target. The effectiveness of attacks is determined by security (or stealth), accuracy, and direct and collateral effects.

5.5 Implementing Information Warfare Policy and Strategy

This chapter has emphasized the flow-down of policy to strategy, and strategy to operations, as a logical, traceable process. In theory, this is the way complex operational capabilities must be developed. In the real world, factors such as the pace of technology, a threatening global landscape, and dynamic national objectives force planners to work these areas concurrently—often having a fully developed capability (or threat) without the supporting policy, strategy, or doctrine to enable its employment (or protection from the threat). This is the state of operational developments for information warfare as of the writing of this book. Technological developments have provided tools and techniques that may be “weaponized” to *conduct* an information war, even though the *concept* of this new class of warfare has not been fully developed.

Policymakers, strategists, and developers of doctrine must concurrently develop and continually refine the framework of these layers that will articulate *what* information warfare is, *who* will be responsible to conduct it, and *how* it will be conducted. In the next chapters, we move to the layer below operations, the tactical layer at which information technology is employed in the form of weapons and shields of warfare.

Endnotes

- [1] “Analysts Advise Caution on Pentagon’s Use of Info Warfare,” *Inside the Pentagon*, Oct. 2, 1997, p. 20.
- [2] Morris, C., J. Morris, and T. Baines, “Weapons of Mass Protection: Nonlethality, Information Warfare and Airpower in the Age of Chaos,” *AirPower Journal*, Spring, 1995.
- [3] For example, the U.S. Defense Department Quadrennial Review (QDR), May 1997, reoriented the military services from a narrow combat focus for information operations

toward an expanded strategy for managing information in cooperation with other federal agencies.

- [4] Round, W. O., and E. L. Rudolph, Jr., "Defining Civil Defense in the Information Age," National Defense University *Strategic Forum*, No. 46, Sept. 1995.
- [5] Wheately, G., and R. Hayes, *Information Warfare and Deterrence*, Washington, D.C.: National Defense University Press, 1996.
- [6] Joint Pub 1-02. Definitions for *national strategy* and *strategy*, respectively. Department of Defense, Washington, D.C., U.S. Government Printing Office, 1997.
- [7] Two texts that illustrate the many views of strategy are Williamson, M., K. M. Knoz, and A. Bernstein, *The Making of Strategy: Rulers, States and War*, Cambridge, NY: Cambridge University Press, 1994, and Pfeiffer, J. W., (ed.), *Strategic Planning—Selected Readings*, San Diego, CA: Pfeiffer and Co., 1992. For an overview of the issues related to the strategic planning process, see Mintzberg, H., "The Fall and Rise of Strategic Planning," *Harvard Business Review*, Jan./Feb. 1994, pp. 107–114.
- [8] The United States and several other European nations performed strategic assessments in the period from 1995 to 1997 and have initiated strategic developments. The United States has openly published general assessments, policy requirements, and strategic concepts developed by the Defense Science Board in 1995 and 1996 studies. As of this writing, other nations have not been as open in reporting the results of assessments and strategic plans.
- [9] *Information Operations*, U.S. Army FM-100-6, Headquarters Department of Army, Washington, D.C., Aug. 27, 1996, Chapter 2.
- [10] Johnson, L. S., "Toward a Functional Model of Information Warfare," *Studies in Intelligence*, Vol. 01, No. 1, 1997. Unlimited distribution version published at www.odci.gov/csi/studies/97unclass/warfare.html on Sept. 19, 1997.
- [11] For an alternative layered model concept, see Mussington, D., "Throwing the Switch in Cyberspace," *Jane's Intelligence Review*, July 1996, pp. 331–334.
- [12] Some authors have suggested a fourth level, above the perception level. Such a level would deal with the "will" rather than perception and reasoning alone, and is based in philosophy and theology. Christian theology has well-developed doctrine on such a level where the "will" or "soul" deals at a spiritual level with deception, denial, disruption, and destruction. That model, developed from the Pauline Epistles, follows the analogy of the three layers below it and is attacked via physical, information, and perceptual layers. For a classic treatment of this subject, see: Edwards, J., "A Treatise Concerning Religious Affections" in *The Works of Jonathan Edwards*, Edinburgh, Banner of Truth Trust, 1974 ed., Vol. I, p. 234 ff.
- [13] "Open System Interconnection Model Standard for Information Processing Systems—OSI Reference Model," ISO/IEC 7498-1: 1994(E) and ITU-T Rec. X.200 (1994 E), Section 6, "Introduction to the Specific OSI Layers."
- [14] Report of the U.S. Defense Science Board Task Force on Information Warfare-Defense (IW-D), Washington, D.C., Office of Secretary of Defense for Acquisition and Technology, Nov. 1996.

- [15] Ibid. Section 2.2, p. 22.
- [16] Threats are entities that are verified to possess both intent and capability.
- [17] Ibid. The DSB Report contains (Appendix A) a simple threat matrix identifying nation states (dimension 1) and current estimate of netwar capability (dimension 2).
- [18] Adapted from presentation by Lee Sutherland of USAF Information Warfare Center at *InfoWarCon 95*.
- [19] Lukasik, S. J., "Public and Private Roles in the Protection of Critical Information-Dependent Infrastructure," Stanford, CA, Stanford Center for International Security and Arms Control, May 1997. This paper discusses the alternative measures and implications for public and private sector roles and responsibilities at the national level.
- [20] Report of the U.S. Defense Science Board Task Force on Information Warfare-Defense (IW-D), Section 6.2.1.
- [21] "Critical Foundations: Protecting America's Infrastructures," President's Commission on Critical Infrastructure Protection, Washington, D.C., Oct. 13, 1997.
- [22] These categories are from the military perspective and are adopted from *Information Operations*, U.S. Army FM-100-6, Headquarters Department of Army, Washington, D.C., Aug. 27, 1996, Chapter 3. Note that the DoD definition of perceptions management includes only "foreign audiences": "Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations."
- [23] "Joint Pub 3-53 Doctrine for Joint Psychological Operations," U.S. Joint Chiefs of Staff, Washington, D.C., July 30, 1993.
- [24] Pease, S. E., *Psywar: Psychological Warfare in Korea, 1950-1953*, Harrisburg, PA: Stackpole, 1992.
- [25] Radvanyi, J., (ed.), *Psychological Operations and Political Warfare*, Westport, CT: Greenwood, 1990.
- [26] "Battlefield Deception," U.S. Army FM 90-2, Headquarters Department of Army, Washington, D.C., Oct. 3, 1988.
- [27] "Joint Doctrine for Military Deception," Joint Pub 3-58, U.S. Joint Chiefs of Staff, Washington, D.C., 1996.
- [28] Breuer, W., *Hoodwinking Hitler: The Normandy Deception*, Westport, CT: Praeger, 1993.
- [29] Dunnigan, J., and A. Nofi, *Victory and Deceit: Dirty Tricks at War*, New York: William Morrow, 1996.

6

The Elements of Information Operations

Information operations are the “continuous military operations within the military information environment that enable, enhance, and protect the friendly force’s ability to collect, process, and act on information to achieve an advantage across the full range of military operations; information operations include interacting with the global information environment and exploiting or denying an adversary’s information and decision capabilities” [1].

Information warfare is the application of information operations (1) against a specific adversary, and (2) in a time of crisis or war. These two conditions in the United States define information warfare as almost wholly within the purview of the Department of Defense (DoD). Information operations provide the integrating strategy to coordinate the disciplines that are required to conduct information warfare. These operations are performed throughout the continuum from network warfare to command and control warfare. They are both defensive and offensive in nature, and are commanded by authorized defense organizations that control the technical disciplines applied.

The integration of some elements of deception, electronic combat, and special operations were effectively orchestrated in the Second World War by the Allies, though not called “information operations.” The joint British-American operations to conceal the Normandy landing and create belief in second landing at the Pas-de-Calais are excellent examples of the early implementation of large-scale deception by integration of physical, electronic, and psychological means [2]. That effort also illustrated the careful strategic development of a perception objective (deceive German command on the plan of

attack) and the implementing means (deceptive radio traffic, psychological operations, agents, and force activities).

As electronic sensing, telecommunications, and processing technologies developed, electronic combat operations (electronic warfare) were developed to attack and protect the electromagnetic spectrum, expanding the possibilities for information operations. As dedicated computer networks (e.g., integrated air defenses) and integrated global computer networks (e.g., Internet and telecommunication nets) expanded through the late 1980s and early 1990s, even so information combat operations were developed for network attack and protection.

As early as the 1970s the United States initiated efforts to study and develop the capabilities now known as information operations. Information operations, or “info ops” (IO), were openly initiated in the United States in the mid-1990s, after more than a decade of study, development, and preparation. The recent and open IO development activities included the following:

- Establishment of information warfare centers within each of the military services to lead training and doctrine development, to define R&D needs, and to provide support to operational commands [3];
- Preparation of IO doctrine, defined in documents such as the U.S. Army Field Manual for Information Operations, FM 100-6 [4–6];
- Establishment of operational units (e.g., the U.S. Air Force 9th Information Warfare Squadron [7]) with sole responsibility for the conduct of IO;
- War gaming conceptual information attacks to understand the range and character of these operations, their impact on conventional military capabilities, and shortfalls in defenses and responses. These studies have highlighted the effectiveness of offensive-IW threats and the potential targeting of commercial information infrastructure in space and on the ground [8,9].

The issues in developing IO capabilities include defining infrastructure targets and their vulnerabilities (for both defense and offense); organizing existing independent capabilities (e.g., electronic attack, PSYOPS, deception, intelligence) into an integrated IO capability; developing orders of battle structures to quantify capability; and understanding how orchestrated information operations will be performed.

Some information operations are inherently “fragile” because they are based on subtle or infrequent system vulnerabilities, or because they rely on

transient deceptive practices that if revealed, render them useless. Certain elements of IO have therefore been allocated to the operational military, while others (the more fragile ones) have been protected by OPSEC within the intelligence communities to reduce the potential of their disclosure. Like the traditional tension between the often mutually exclusive objectives of military intelligence (“listen to it”) and operational forces (“destroy it”), the fragile aspects of IO must be properly allocated and planned to be effective when needed [10,11].

This chapter introduces IO by first describing the information infrastructure targets (and delivery vehicles) of operations (Section 6.1) and the basic war forms based on these infrastructures (Section 6.2). Next, the operations for net warfare (Section 6.3) and military C2W (Section 6.4) are described using representative operational scenarios, followed by the basic operational elements (Section 6.5). In these sections, we develop the basic disciplines at the operational level while reserving electronic and network tactics and technical measures (both offensive and defensive) for the two subsequent chapters.

The three-layer warfare model introduced in the last chapter (perception, information, and physical layers) will remain the organizing model throughout this chapter to describe the implementation of operations.

6.1 The Targets of Information Operations

The widely used term *information infrastructure* refers to the complex of sensing, communicating, storing, and computing elements that comprise a defined information network conveying analog and digital voice, data, imagery, and multimedia data. The “complex” includes the physical facilities (computers, links, relays, and node devices), network standards and protocols, applications and software, the personnel who maintain the infrastructure, and the information itself. The infrastructure is the object of both attack and defense; it provides the delivery vehicle for the information weapons of the attacker while forming the warning net and barrier of defense for the defender. Studies of the physical and abstract structure of the infrastructure are therefore essential for both the defender and the targeter alike.

Three infrastructure categories are most commonly identified.

- *The global information infrastructure (GII)* includes the international complex of broadcast communications, telecommunications, and computers that provide global communications, commerce, media, navigation, and network services *between* NIIs. (Note that some

documents refer to the GII as the inclusion of all NIIs; for our purposes, we describe the GII as the interconnection layer between NIIs.)

- *The national information infrastructure (NII)* includes the subset of the GII within the nation, and internal telecommunications, computers, intranets, and other information services not connected to the GII. The NII is directly dependent upon national electrical power to operate, and the electrical power grid is controlled by components of the NII.
- *The defense information infrastructure (DII)* includes the infrastructure owned and maintained by the military (and intelligence) organizations of the nation for purposes of national security. The DII includes command, control, communications, and computation components as well as dedicated administration elements. These elements are increasingly integrated to the NII and GII to use commercial services for global reach but employ INFOSEC methods to provide appropriate levels of security.

Estimates in 1996 placed the value (annual investment) in the GII at \$1 trillion (U.S.) and the U.S. NII at \$500 billion (U.S.) [12]. The global interconnection of these information infrastructures, and the complex pathways they afford to critical national and defense services, have increased the vulnerability of nations highly dependent on their NIIs to information warfare attacks. Figure 6.1 is a Venn diagram of the GII/NII/DII relationships, illustrating the overlapping regions where the infrastructures use common services (e.g., DII military use of commercial GII communication satellites and Internet). The figure also illustrates alternative indirect paths for attacks on a nation state's DII through GII and NII paths.

- The first path passes from the attacking DII (a) through the GII to the target nation (c) NII and on to the targeted asset within DII (c).
- The second path uses the NII of nation (c) as an anonymous surrogate, through which the attack can be passed on to the targeted NII.
- DII (a) may also attack assets within nation (c)'s NII, which may be used to relay the attack into the DII, or the attack may be used to influence the DII indirectly (e.g., denial of electrical power or commercial telecommunications services used by the DII).
- Finally, an agent in place in the NII of country (b) (either human or software agency) may be used to initiate the attack through the GII toward the targeted DII.

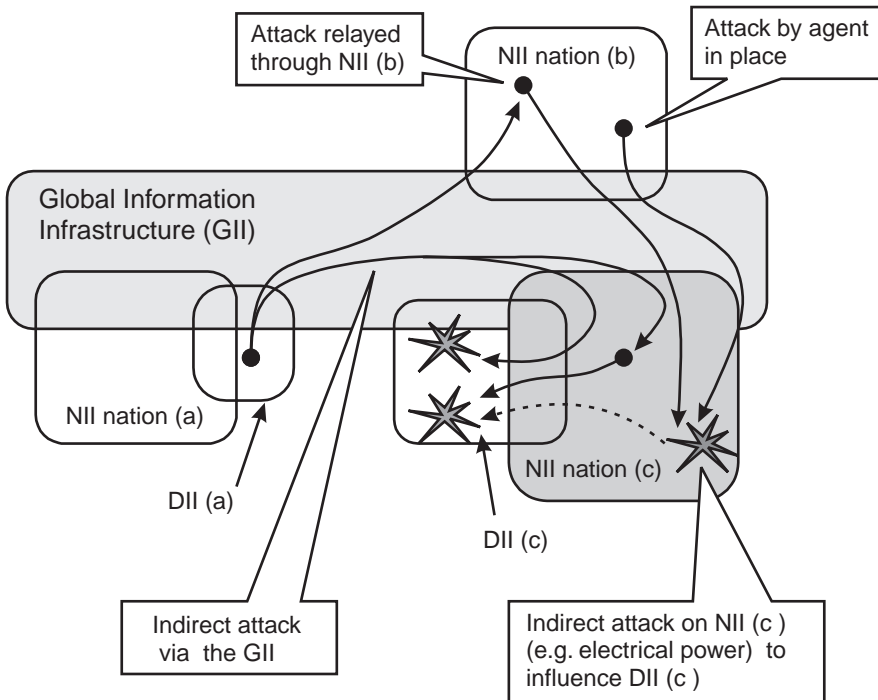


Figure 6.1 Relationship between the information infrastructures and common attack paths across the global, national, and defense complex.

In the following subsections, each of these information infrastructures is described to detail their unique functions, components, and characteristics.

6.1.1 The Global Information Infrastructure (GII)

At the global level, the international telecommunications, computer networking, and command services (e.g. air traffic management, and global navigation services administered by the ICAO [13]) regulated by international laws and treaties and accessible to the international community comprise the GII. The GII is a dynamic, developing infrastructure that is characterized by the following:

- International regulation to control the allocation of spectrum and cooperation to achieve interoperability and management of bandwidth resources;

- International standards and protocols to provide universal interoperability;
- Transnational private (and national) ownership, integration, and operation;
- Open access for both providers and users.

The establishment of the GII with a humanitarian objective to “ensure that the full potential benefit of advances in information and telecommunications technologies are realized for all citizens” is promoted by the group of seven major industrialized nations (G-7) [14]. The G-7 nations promote the GII to create a global information marketplace, encouraging broad-based social discourse within and among all countries to increase economic growth, create jobs, and improve infrastructures [15]. As the GII increases in expanse, connectivity, and complexity, global regulatory issues must also be addressed in the areas of intellectual property rights, censorship, encryption, privacy, and cultural sovereignty. The current global regulatory framework (international law, diversity in national policies, and in social and cultural values) is not prepared for the impact that the emerging GII will introduce [16].

A key backbone of the emerging GII includes intercontinental cables and a future commercial network of layered broadband communication satellites operating at three orbital tiers.

- *Geostationary orbit (GEO)*—Relay and direct broadcast satellites in earth-synchronous orbits at 22,300 miles provide continuous overhead coverage of designated regions on the surface of the Earth while imposing a latency of 250 millisecond (round trip).
- *Medium earth orbit (MEO)*—Operating at 6,000 to 13,000 miles, small constellations of MEO relays provide 50 to 150 millisecond latency and moderate dwell on ground terminal subscribers.
- *Low earth orbit (LEO)*—Larger constellations of satellites operating at 500 to 1,500 miles provide low latency (5 to 100 milliseconds), but require complex intersatellite links and switching to achieve near-continuous coverage to stationary and mobile subscribers.

Layered communication satellite constellations will employ both space- and ground-based switching as well as intersatellite links to achieve high traffic efficiency. The aggregate latency experienced by the user includes the ground-satellite latency (noted above) plus many other switching and routing functions. Immediate global access to data, voice, and video communications

will become available as these networks are integrated with terrestrial fiber-optic links and wireless communication systems within nations. With this increased interconnectivity will come access and vulnerability to functions dependent upon the global network.

6.1.2 The National Information Infrastructure (NII)

The NII includes the information infrastructure controlled by a nation state. It is the controlling component of the more general “critical national infrastructures” of the nation, which are so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security. The critical infrastructures identified by the U.S. President’s Commission on Critical Infrastructure Protection (PCCIP) include five sectors [17,18].

1. *Information and communications (the NII)*—The public telecommunications network (PTN), the Internet, and millions of computers in home, commercial, academic, and government use. These include the networks and systems that support the transmission and exchange of electronic communications among and between end users and electronic or mechanized devices, such as networked computers.
2. *Banking and finance*—Banks, nonbank financial service companies, payment systems, investment companies and mutual funds, and securities and commodities exchanges. These include all the associated operational organizations, government operations, and support entities that are involved in all manner of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loans and other financial instruments.
3. *Energy*—The industries that produce and distribute electric power, oil, and natural gas. This includes generation stations, transmission, and distribution networks that create and supply electricity to end users so that end users achieve and maintain nominal functionality, including the transportation and storage of fuel essential to that system. Also included are production and holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels; the refining and processing facilities for these fuels; and the pipelines, ships, trucks, and rail systems that transport these commodities from their sources to systems that are dependent upon gas and oil in one of their useful forms.

4. *Physical distribution*—The vast interconnected network of highways, rail lines, ports and inland waterways, pipelines, airports and airways, mass transit, trucking companies, and delivery services that facilitate the movement of goods and people.
5. *Vital human services*—Those operations and services of governments at the federal, state, and local levels critical to the functioning of the nation's systems; that is, public health, safety, and welfare, including water supply systems; emergency services (police, fire, rescue and emergency medical services); and government services (nonemergency services, including Social Security payments, unemployment and disability, and management of vital records). This includes continuity of government preparedness planning for the identification of functions that would have to be performed during an emergency, the identification of personnel for performing those functions, the development of plans, and the capability to execute those plans and elements in support of them.

Attackers may seek to achieve numerous policy objectives by attacking these infrastructures. In order to achieve these policies, numerous intermediate attack goals may be established that can then be achieved by information infrastructure attacks. Examples of intermediate goals might include the following:

- Reduce security by reducing the ability of a nation to respond in its own national interest;
- Weaken public welfare by attacking emergency services to erode public confidence in the sustainment of critical services and in the government;
- Reduce economic strength to reduce national economic competitiveness.

Various information operations must be planned and allocated, and units tasked to achieve each of these intermediate goals. For example, attacks on banking and stock markets and coordinated embargoes might be planned to achieve the “reduce economic strength” goal.

Of the five critical sectors, the information component is the common element that connects all of the infrastructures and is the element that is increasingly accessible through the GII. The U.S. NII has developed because of overwhelming commercial investment due to potential economic benefits, and civil applications have also increased throughout the 1990s as the Internet grew

exponentially [19–21]. The increased usage and dependency for government, commerce, and even national security applications has driven the numerous concerns about the accompanying vulnerability. Characterized as an “electronic Pearl Harbor,” an envisaged preemptive attack on critical national infrastructure through the NII has become a U.S. concern [22]. A detailed enumeration of the critical infrastructure and related information infrastructure components are presented in Table 6.1. (See [23] for extensive surveys of the infrastructure of public switched telephone networks (PSTNs), computer networks, commercial/industrial networks, and financial/banking networks in major regions of the world.)

Figure 6.2 depicts the major elements of the critical infrastructure necessary for U.S. national and economic security as viewed by a comprehensive study performed by the U.S. Joint Staff to assess the complexity and structure

Table 6.1
Five Sectors of the National Critical Infrastructure Identified by the U.S. PCCIP

Critical Infrastructure Category	Major Infrastructure Elements	Interdependencies on Category 1 Information Infrastructure Elements
1. Information	Telecommunications (e.g., PTN) Computer networks (e.g., Internet) Media services	—
2. Banking and finance	Stock and financial markets Commodities markets Banking and credit Investment institutions Exchange boards, trading houses, reserve systems	Electronic commerce networks Electronic financial transaction nets Financial records storage
3. Energy	Raw material resources Coal mining, processing Gas production Oil refining Resources storage (coal, oil, gas) Electrical power production Nuclear power production Electrical distribution	Production monitor and control (energy management system [EMS]) Storage monitoring Status and emergency alerting

Table 6.1 (continued)

Critical Infrastructure Category	Major Infrastructure Elements	Interdependencies on Category 1 Information Infrastructure Elements
4. Physical distribution	Water supply Sewage removal, treatment Oil and gas pipeline distribution Highways, rail lines Airports and airways Mass transit	Process monitor and control (supervisory control and data acquisition [SCADA]) Power distribution monitor and control Pipeline monitor and control
5. Vital human services	Basic government operations Executive leadership Legislative leadership Judicial activities National security Emergency services Education Health care Transportation Environmental monitor/protect Public safety (law enforcement)	Telecommunication and computer networking for data and information collection, reporting, management, and control Data storage for archive of records Delivery of information and physical services

of the U.S. NII and its vulnerabilities [24]. The study distinguished two capabilities required for the NII.

- Infrastructure *protection* requires defenses to prevent and mitigate the effects of physical or electronic attack.
- Infrastructure *assurance* requires actions to ensure readiness, reliability, and continuity—restricting damage and providing for reconstitution in the event of an attack.

The Joint Staff study detailed the environmental (legal, regulatory, policy, technology) considerations and defined the role to achieve assurance using

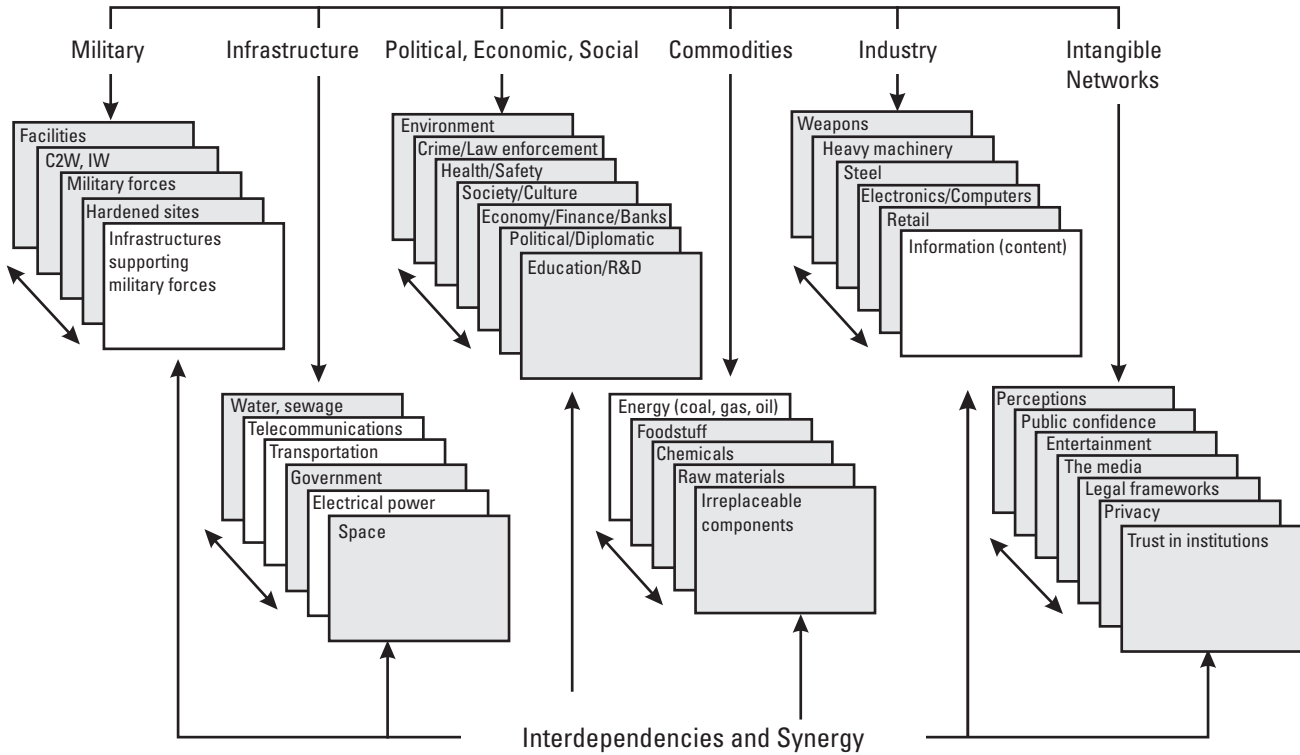


Figure 6.2 The NII provides the control and communications that provide interdependence and synergy among the elements of national and economic security. (Source: [15].)

the infrastructure assurance model shown in Figure 6.3. The conceptual model provides for the following basic roles and responsibilities:

- *Protected information environment*—The private sector maintains protective measures (INFOSEC, OPSEC) for the NII supported by the deterrent measures contributed by the government. Deterrence is aimed at influencing the perception of potential attackers, with the range of responses listed in the figure. The private sector also holds responsibility for restoration after attack, perhaps supported by the government in legally declared emergencies.
- *Attack detection*—The government provides the intelligence resources and integrated detection capability to provide indications and warnings (strategic) and alerts (tactical) to structured attacks.
- *Attack response*—The government must also ascertain the character of the attack, assess motives and actors, and then implement the appropriate response (civil, criminal, diplomatic, economic, military, or informational).
- *Legal protection*—In the United States, the government also holds responsibility (under the Bill of Rights, 1791, and derivative statutes

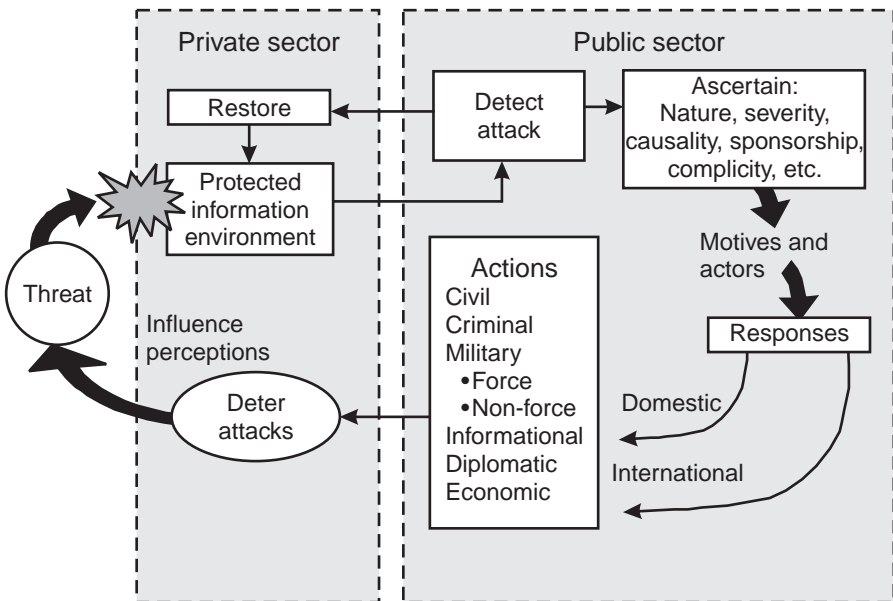


Figure 6.3 The U.S. NII assurance model source. (Adapted from: [25].)

cited below) for the protection of individual privacy of information, including oral and wire communications [26]; computers, e-mail, and digitized voice, data, and video [27]; electronic financial records and the transfer of electronic funds [28,29]; and cellular and cordless phones and data communications [30]. This is the basis for civil and criminal deterrence to domestic and international criminal information attacks on the NII.

It is important to recognize that this model is conceptual, but does not represent the current state of affairs. While the government has defined the NII, the private sector protects only private property, and there is no coordinated protection activity. Individual companies, for example, provide independent protection at levels consistent with their own view of risk, based on market forces and loss prevention. These companies are often market competitors who have not yet developed policy or standards for joint protection at industry-wide or nationwide (NII) levels.

Three functional layers characterize the technical architecture of an advanced electronic NII (Table 6.2) that emphasizes the information services and applications [31,32]. At the lowest level are *bitways*, the physical information pathways made up of network computers, landlines (coaxial and fiber-optic cables), satellite links, and wireless cellular links. The table compares the seven layers of the Open System Interconnection (OSI) reference model, which emphasizes the network sublayers, with the three NII functional layers.

The *services* level integrates the bitways into a functional NII architecture, providing common utilities to integrate the bitways, to route, retrieve and store information, and provide seamless operation. The NII services provide the equivalent of the operating system to the computer. At the highest layer are *applications* that provide specific functions for users, such as secure electronic data exchange for electronic commerce.

Notice that this NII model applies to advanced nations, whereas the NII of less advanced nations look quite different. For some nations, runners, radios, and couriers replace bitways; cells of experts with limited (nonnetworked) computer support perform services; and applications use hardcopy records.

There exist natural *interdependencies* between the critical infrastructure sectors that can be exploited in information warfare attacks across the elements. Figure 6.4 illustrates several obvious interdependency threads between several critical sectors. The diagram demonstrates how the three-layer information warfare model introduced earlier applies to each of the sectors, which can be attacked at any of the three levels. The controlling leadership of each critical sector, and its perception of the situation, may be a target of attack through the

Table 6.2

Functional Layers of the National Information Infrastructure Compared to the OSI Reference Model

NII Layer	Description	Representative Components	OSI Model Layers
Applications	Tools and applications programs that perform specific functions for a variety of disciplines, using the GII and NII	Electronic commerce Energy management Health care Law enforcement Environmental monitoring	
Services	The basic capabilities that form the building blocks for applications, including I/O, basic processing, displays, and data fusion/mining	Data storage and retrieval Data exchange, protocol translation Metaknowledge (indexes) Multilevel security Electronic transactions Information agents Collaboration support Data fusion and mining	7 Application layer
Bitways	The physical infrastructure that provides the means of transmission of information, including controlling software	Fiber-optic and cable landlines	6 Presentation layer
		Satellite links	5 Session layer
		Satellite direct broadcast	4 Transport layer
		Cellular wireless telecommunications	3 Network layer
		Network nodes (switches, routers, exchanges)	2 Link layer 1 Physical layer

lower information or physical levels of the infrastructure. The figure also highlights the effectiveness of information-based attacks, which have the ability to rapidly spread influences *across* sectors. The figure includes the following general influences:

- Electrical power production and distribution is required to sustain long-term telecommunications and computer networks. (Emergency backup power generation sustains operation throughout short-term outages.)

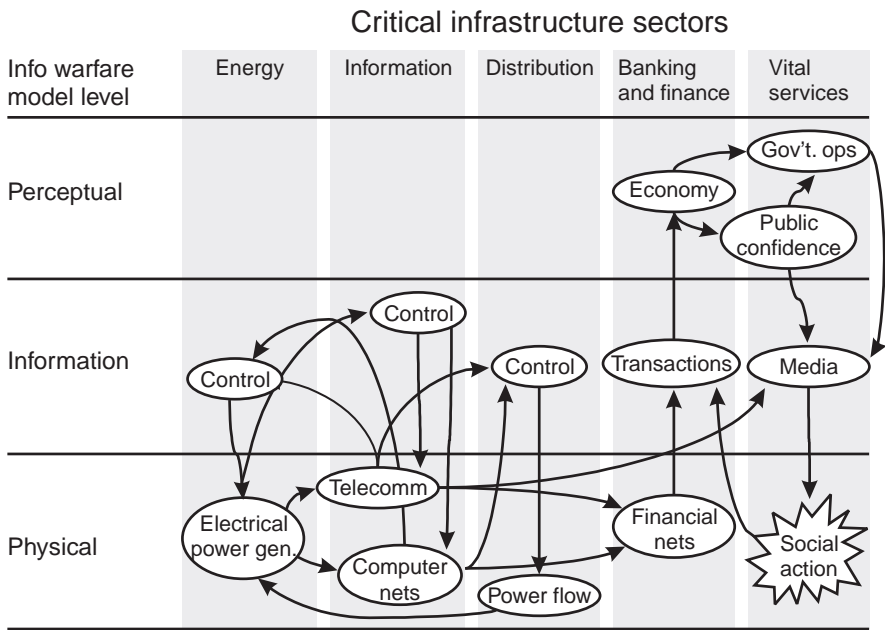


Figure 6.4 Influences across the critical infrastructures cross the three IW model layers.

- Telecommunications and computer networks are required to maintain assured power production and distribution.
- Telecommunications and computer networks are also required to provide electronic transactions in the banking, securities, and market infrastructure.
- Proper operation of the banking and finance infrastructure is necessary to maintain the perception of economic stability, which directly influences public confidence in the economy and in government operations. A cascading attack on a fractional banking system, for example, need not attack all banks. A successful attack on only the *most vulnerable*, followed by effective widespread publication of that success, may be all that is necessary to destabilize *all* banks in the system.
- Government operations, and public confidence in them, are reported by the media, which is dependent upon the information infrastructure to produce and distribute media messages.
- Physical social actions (e.g., commerce and economic decisions, and influence on governments) are influenced by the media and further influence financial transactions and the economy.

These relationships, simplified for this figure, illustrate the complex interdependencies between infrastructure elements and the critical role that information plays in the network. IO attacks, integrated across all elements of critical infrastructure and targeted at all three levels of the NII, will attempt to destabilize the balance and security of these operations. The objective and methodology is to:

- Achieve perception objectives at the perceptual level, causing leadership to behave in a desired manner.
- This perception objective is achieved by influencing the components of the critical infrastructure at the application level.
- This influence on the critical infrastructure is accomplished through attacks on the information infrastructure, which can be engaged at the physical, information, and perceptual layers.

It should be noted that while the GII extends to virtually all nation states, the NIIs of first- and second-wave nations are significantly different from those of third-wave nations (described here). Broadcast AM/FM radio rather than the Internet, neighborhood runners and motorcyclists rather than tactical radios, and land lines rather than mobile subscriber communications may be the “networks” of these nations. The “thickness” of the information infrastructure layer and the composition of the physical layer in the information warfare model are significantly different in first-, second- and third-wave NIIs and must be considered in planning information operations.

The U.S. PCCIP study recommended allocating to the private sector the responsibility for infrastructure protection and incident reporting, while allocating to government the responsibilities for providing information about security capabilities (tools), intelligence and warnings regarding threats and intent, and R&D leadership in the area of countermeasures. Figure 6.5 summarizes specific responsibilities identified by the PCCIP [33].

6.1.3 Defense Information Infrastructure (DII)

The DII implements the functional “information grid” described earlier in Chapter 4 for military information operations, as well as providing all related noncombat administrative and support functions. In the United States, the structure is maintained by the Defense Information Systems Agency (DISA), which established the following definition:

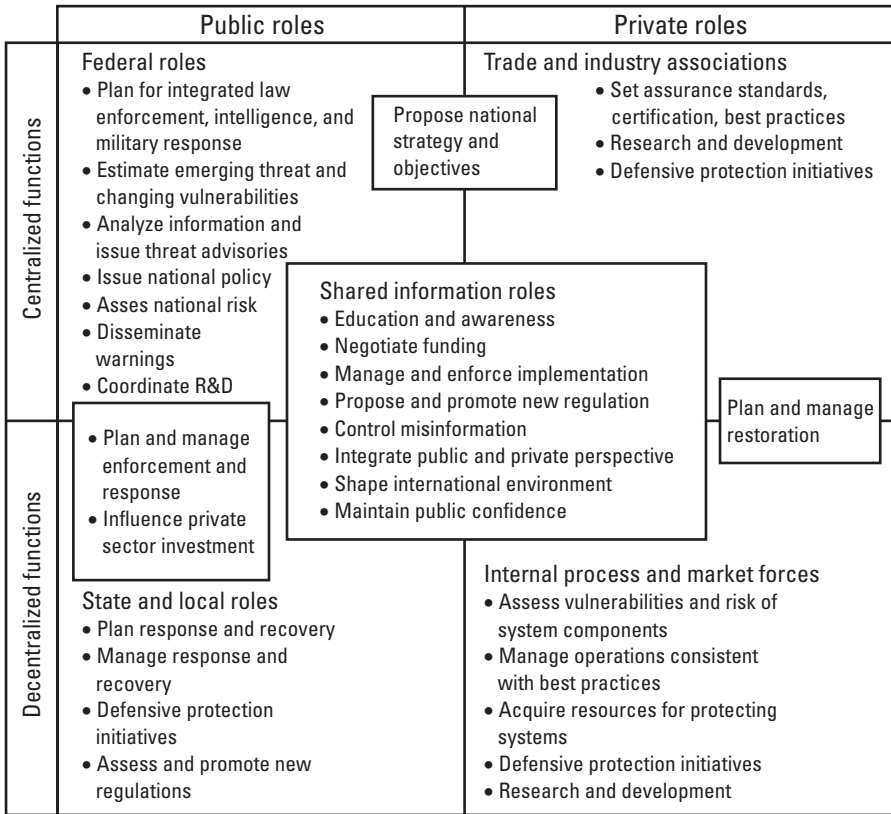


Figure 6.5 PCCIP recommended allocation of roles to provide protection and assurance for the U.S. NII. (Adapted from: PCCIP Briefing “Critical Foundations,” November 14, 1997.)

The DII is the web of communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet the information-processing and transport needs of DoD users across the range of military operations. It encompasses the following:

1. Sustaining base, tactical, and DoD-wide information systems, and command, control, communications, computers, and intelligence (C4I) interfaces to weapons systems.
2. The physical facilities used to collect, distribute, store, process, and display voice, data, and imagery.

3. The applications and data engineering tools, methods, and processes to build and maintain the software that allow command and control (C2), intelligence, surveillance, reconnaissance, and mission support users to access and manipulate, organize, and digest proliferating quantities of information.
4. The standards and protocols that facilitate interconnection and interoperation among networks.
5. The people and assets that provide the integrating design, management, and operation of the DII, develop the applications and services, construct the facilities, and train others in DII capabilities and use [34].

Three distinct elements of the U.S. DII are representative of the capabilities required by a third-wave nation to conduct information-based warfare.

Program and technical activities include the operating policy, technical requirements, and standards developed and maintained by DISA. This also includes the organizations that model, simulate, and perform testing and evaluation of the computers and communication systems in the DII. This activity has responsibility for security requirements and standards.

Communications and computer infrastructure include the physical and information components and operations that process and transport information (Table 6.3). The Defense Information System Network (DISN) integrates all military branches and services, both combat and noncombat applications, with multiple levels of security. DISN integrates all U.S. defense communications assets, MILSATCOM, commercial SATCOM leased links, leased telecommunications services, dedicated networks, and mobile/deployable networks. The Defense Messaging Service (DMS) provides unclassified but sensitive and secure (encrypted) classified message services in separate virtual networks (NIPRNET and SIPRNET, respectively) over an unclassified network structure. The Global Command and Control System (GCCS) provides interoperable connectivity for command and control of forces in foreign theaters of operation. The GCCS provides the common operational picture to all forces, based upon the fusion of all-source intelligence sources and distribution in-theater by secure networks and immediate broadcast media (Figure 6.6). GCCS communication pathways include the following:

- DISN forms the wideband backbone connecting national sources and all supporting commands.
- Direct broadcast satellite downlink provides real-time intelligence feeds and critical information (alerts, warnings, synchronizing messages, timing) to fighting forces.

- Satellite secure and local (ground) secure nets provide secure communication for messages, data exchange, and conferences.
- Theater links provide surveillance, intelligence, and reconnaissance data to in-theater processing.
- Sensor-to-shooter links deliver real-time warning and targeting information to weapon systems.

Table 6.3
Components of the U.S. DII Objective Architecture

Component		Function	Elements Included
Enterprise Services	Defense information systems network (DISN)	Information transport services both within the DII and across DII boundaries on a fee-for-service basis. Provide dynamic routing of voice, text, imagery (still through full motion), and bandwidth services	DMS (defense messaging service)—provides electronic mail services GCCS (global command and control system)—provides command and control (C2) and combat support communications and processing
	Defense megacenters	Information-processing services in support of DoD functional communities on a fee-for-service basis	Centralized and distributed on-line and batch processing support, scheduling, and secure computing Data storage and retrieval Management of applications software and operating systems releases, and computer products distribution
	DII control centers	Performs end-to-end management of the DII technical infrastructure	Global operations and security center (GOSC)—executive control of the DII Regional operations and security centers (ROSCs)—systems and network management and operational control for a specific geographic area Local control centers—the LCCs (base-level control centers and consolidated local area control centers)

Table 6.3 (continued)

Component		Function	Elements Included
Sustaining Base	Intelligence support facilities	Provides objective and timely intelligence to both national and tactical consumers at multiple levels of security access	Intelligence processing, fusion, and dissemination elements delivering processed intelligence products and preprocessed intelligence reports Intelligence broadcast streams Intelligence databases
	Mission and base support facilities	Provides management, administrative, and logistics support to personnel, material, and operations	Management, personnel, and administration systems Logistics support systems Training support systems
Deployed/ Afloat Joint Tactical Forces (JTF)	JTF communications	Provide joint forces communications and processing nets at the theater and tactical levels below theater	Joint services theater networks Satellite ground stations Tactical radios, relays, and landlines Tactical information distribution Dedicated data links
	JTF network management	Manage joint forces communication, allocate bandwidth	Real echelon nodes Deployed forces nodes Broadcast nodes
	Combat information systems	Acquire and distribute near-real-time combat information and situation assessment information to weapons	ISR sensors, dedicated links, and processing ISR ground processing Tactical data systems Sensor-to-shooter links Battlefield identification

DII applications include both common (shared among multiple functional areas) and functional area-unique applications (Table 6.4) within a common operating environment (COE) [35]. The GCCS is the DII C4I system, which is built on the COE. The COE and applications are implemented in all processing and workstation computers throughout the GCCS, providing interoperability for the most fundamental information operations.

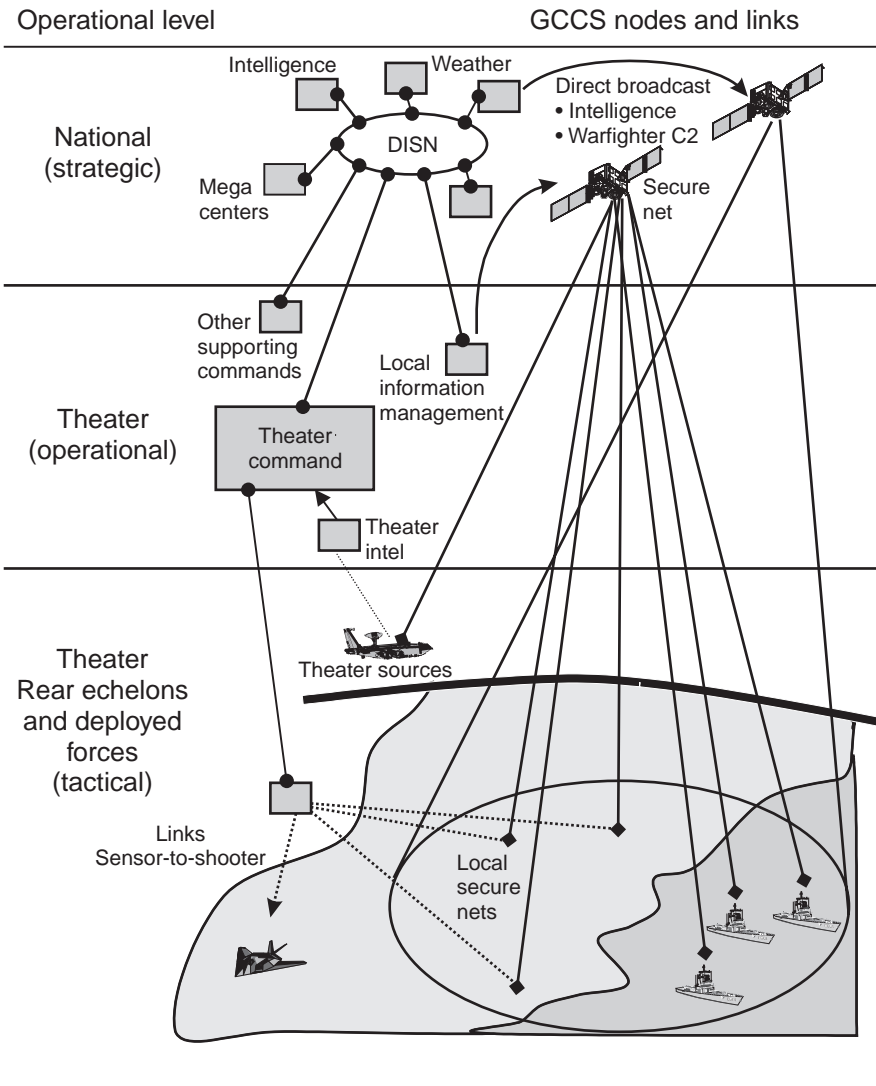


Figure 6.6 Communication infrastructure for the U.S. Global Command and Control System (GCCS).

6.2 Information Infrastructure War Forms

As the GII and connected NIIs form the fundamental interconnection between societies, it is apparent that this will become a principal vehicle for the conduct of competition, conflict, and warfare. The concept of network warfare was

Table 6.4
DII COE Common and Functional Area Applications

Layer	Application	Functions Performed
Kernel	Common operating system and extensions	Common desktop and printer services Software installation tools Security extensions
Infrastructure services	Common data exchange services for all applications	Relational database management Network management WWW servers/clients Communications PC services
Shared data environment (SHADE)		Shared data and joint shared data servers Shared access across applications
Common support applications	Defense messaging service (DMS)	Electronic message (e.g., e-mail, file transfer) Receipt, input and output filtering, logging, parsing, correction, and routing
	Office automation	Word-processing, spreadsheet, graphic drawing tools, briefing/slide presentation tools, and electronic mail
	Information assurance	Encryption, authentication, audit, intrusion detection
Functional area-unique applications	C2 applications	Correlation and fusion Decision support
	Combat support	Logistic analysis and tracking
	Intelligence, surveillance, and reconnaissance	Mapping, charting, and geodesy Imagery processing

introduced and most widely publicized by RAND authors John Arquilla and David Ronfeldt in their classic think piece, “Cyberwar is Coming!” [36] The

authors distinguished four categories of warfare that are based on the expanded global development of information infrastructures (Table 6.5).

The war forms are organized in the table in increasing levels of abstract, ideological conflict. These forms were introduced in Chapter 1, and we now focus on the two categories of information-intense conflict on the global scale—network warfare (netwar) and command and control warfare (C2W). (Ronfeldt and Arquilla used the terminology *cyberwar*, where we adopt the U.S. DoD term *command and control warfare* for consistency.)

The relationships between these forms of conflict may be viewed as sequential and overlapping when mapped on the conventional conflict time line that escalates from peace to war before de-escalation to return to peace (Figure 6.7). Many describe netwar as an ongoing process, with degrees of intensity moving from daily unstructured attacks to focused net warfare of increasing intensity until militaries engage in C2W. Netwar activities are effectively the ongoing, “peacetime”-up-to-conflict components of IO.

In the next sections, we describe netwar and C2W and the operations applied in each.

Table 6.5
Comparison of Major War Forms According to Arquilla and Ronfeldt

War Form	Objective	Means	Targets
Net warfare	Manage the perception of the target population to bring about a desired influence on national behavior	Perception management by means of networked communications, and control of information to influence the full range of potential social targets	Society at large (political, economic, military)
Political warfare	Influence national government leadership decisions and policy	Measures that influence national political systems and institutions of government	Political systems
Economic warfare	Influence national government leadership decisions and policy	Measures that influence national economy via the production and distribution of goods: sanctions, blockades, technology theft, etc. (for a description, see [37])	Economic systems
C2W (cyber warfare)	Achieve military objectives by conducting operations against military targets	Military operations are conducted on information-based principles that integrate knowledge exploitation, PSYOPS, deception, and electronic warfare	Military systems

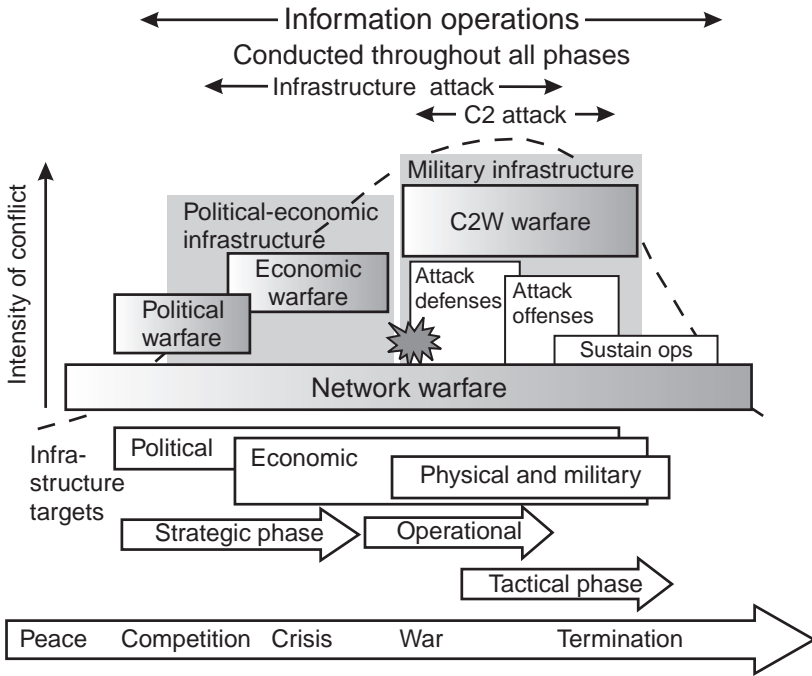


Figure 6.7 Networkwar and C2W on the escalation time line. (After: [38].)

6.3 Information Operations for Network Warfare

Ronfeldt and Arquilla define *netwar* as a societal-level ideational conflict at a grand level, waged in part through Internetted modes of communications. It is conducted at the perceptual level, exploiting the insecurities of a society via the broad access afforded by the GII and NIIs. Netwar is characterized by the following qualities that distinguish it from all other forms:

- *Target*—Society at large or influential subsets are targeted to manage perception and influence the resulting opinion. Political, economic, and even military segments of society may be targeted in an orchestrated fashion. The effort may be designed to create and foster dissident or opposition groups that may gain connectivity through the available networks.
- *Media*—All forms of networked and broadcast information and communications within the NII of a targeted nation state may be used to

carry out information operations. The GII may be the means for open access or illicit penetration of the NII.

- *Means*—Networks are used to conduct operations, including (1) public influence (open propaganda campaigns, diplomatic measures, and psychological operations); (2) deception (cultural deception and subversion, misinformation); (3) disruption and denial (interference with media or information services); and (4) exploitation (use of networks for subversive activities, interception of information to support targeting).
- *Players*—The adversaries in netwar need not be nation states. Nation states and nonstate organizations in any combination may enter into conflict. As networks increasingly empower individuals with information influence, smaller organizations (with critical information resources) may wage effective netwar attacks.

In subsequent studies, Arquilla and Ronfeldt have further developed the potential emergence of netwar as dominant form of societal conflict in the twenty-first century [39] and have prescribed the necessary preparations for such conflicts [40]. A 1994 U.S. Defense Science Board study concluded that “A large structured attack with strategic intent against the U.S. could be prepared and exercised under the guise of unstructured activities” [41]. The same study found evidence of over 50 nations with an emerging structured netwar capability (including NETINT targeted at the U.S.) and over 25 states with unstructured but organized computer underground organizations with potential threatening capabilities. A representative scenario is provided in the next section to illustrate the range of elements of a netwar conflict.

6.3.1 A Representative Netwar Scenario

The U.S. defense community, futurists, and security analysts have hypothesized numerous netwar scenarios that integrate the wide range of pure information weapons, tactics, and media that may be applied by future information aggressors. We illustrate a netwar attack (not a two-sided conflict) in the following scenario. It is a highly fictionalized but illustrative representation of the context and events of a well-financed and highly structured net attack. (This scenario is but one of many forms of potential net warfare; see other example scenarios and concepts in [42–44].) The scenario follows the general format developed by Schwartz for envisioning and characterizing possible futures in *The Art of the Long View* [45].

SCENARIO TITLE: Netwar Deterrence of Military Support

ABSTRACT: Organized criminal organization (“ARGRESS”) within the developing and newly democratic nation Burzan has gained low-level influence in the government and has corrupted state security to assure that transnational crime operations can be sustained. Burzan national leaders have requested military support from a coalition of G-7 nations to restore security and justice. The indigenous ARGRESS launches a net attack to deter the implementation of military support to Burzan.

SITUATION:

1. *Driving forces (why)*—Societies in the G-7 nations are enjoying relative economic security, and the effects of the ARGRESS crime net, though known, are not significant factors. ARGRESS is considered a distant threat, and a problem to Burzan. The G-7 nations are involved in sensitive trade and economic policy negotiations that are strained by global economic competition. It is during this period that the coalition of G-7 nations initiates the formation of a medium-scale military force to support the unstable, legitimate leadership of Burzan.
2. *Rationale (how)*—ARGRESS cannot withstand a military confrontation with the G-7 coalition, so it wages an *asymmetric* attack against the coalition in the information domain to (1) create mistrust within the coalition, (2) create a public and government perception that interference in Burzan will bring unacceptable risk, and (3) reduce national will of the G-7 nations to support the Burzan government. The ARGRESS attackers use commercial information technology, network intelligence procured from a regional rogue nation, and five separate ten-person attack cells operating in the three coalition nations. The attack consists of the following actions:
 - Penetration of industry computers, and corruption and exploitation of information;
 - Penetration and disruption of supervisory control computers in public utilities;
 - Physical penetration and terrorist-class destruction of critical infrastructure nodes;



- Creation of a PYSOP campaign using the Internet, and precision manipulation of public media;
 - Deception activities to mask ARGRESS as the perpetrator, and generation of misinformation to create plausible mistrust within the G-7 coalition.
3. *Scenario narrative (what happens)*—The coalition of three G-7 nations prepares for economic negotiations (including telecommunication rates and tariffs) while independently initiating military plans for a medium-scale operation to provide military support to the democratic Burzan government. ARGRESS, the transnational criminal organization headquartered in Burzan, launches a net attack with the intent of stopping the G-7 support to Burzan. With one week until troop deployment, and two weeks before the economic summit, the following activities occur:
- *Day 1*—Throughout the night, the computers at headquarters or subsidiaries of key telecommunications industries in two of the three G-7 nations are penetrated, and telecommunication market data (possibly related to negotiations) is destroyed. Viruses are deposited at some targets. Other targets with stronger firewalls are left with message threats and claims that malicious code has been installed—enough to place operations in very limited capacity while exhaustive recovery actions are implemented.
 - *Days 2 and 3*—Private telecommunication data captured in the previous night's attack is posted on the Internet by an anonymous organization "G-7 Libertarians" (by capturing a university computer as host for the site). Messages are transmitted via e-mail to the media and 400 G-7 leaders to point attention to the site. Data at the site includes real captured and bogus data, purporting to show unfair pricing tactics. Concurrently, anonymous e-mail traffic to the news media discredits Burzan leadership with claims of corruption and a promise of evidence "to surface in a few days."
 - *Day 4*—G-7 commissioners hold an emergency meeting in Paris, and in midmorning, the telecommunication and electrical power grid is attacked, causing a brownout in several suburbs and reduction of phone services. Attacks include electronic disruption of supervisory controls and bombing of critical transformers and grid

circuits. G-7 Libertarians claim responsibility in anonymous e-mail messages to the media.

- *Days 4 to 6*—Electrical power and transportation infrastructure in at least two major cities of each of the three G-7 coalition nations are attacked, with varying degrees of effectiveness. The financial markets in those nations are also attacked by destruction of local telecommunications switches and computer attacks on exchange computers (physical terrorist attacks with minor but sufficient surgical precision to close markets for 48 hours). The nations declare a state of emergency and delay preparation meetings for the summit. G-7 Libertarians' sites increase in number on captured university computers, expanding the hostile tone and intensity of threats. Public fear in all G-7 nations rises, and military forces are placed on alert. Virtual communities of protesters form on the Internet, demanding a "hands off" policy toward Burzan.
- *Days 7 to 9*—A purposed surveillance video showing the prime minister of Burzan conducting clandestine negotiations with a known drug cartel leader is distributed to international news nets. (The video is a "morphed" creation of sufficient quality to be feasible.) Anonymous messages to news organizations claim that the prime minister has transferred \$2 million (U.S.) to foreign accounts. Bank officials verify the account and transactions. Public protests, promoted by leaders of emerging Internet "communities" that support a "hands off Burzan" policy, are held at government facilities in Burzan and in several G-7 cities. All are heavily promoted on the G-7 Libertarian Internet site, and media coverage is also provided due to effective press releases and media orchestration.
- *Day 10*—The G-7 coalition military command meets in emergency session and initiates contacts with Burzan leadership. Burzan government cannot be effectively contacted due to attacks on the telecommunications in that country. The coalition command is unable to report status to the G-7 commission for the following day's decision meeting.
- *Day 11*—The G-7 high commissioners meet in Geneva and resolve to defer economic negotiations, establish a joint panel to investigate infrastructure attacks, and maintain surveillance of Burzan, but terminate plans to mobilize a supporting force.

4. *Scenario time line (when)*—The three-phase attack launched by ARGRESS is illustrated in Table 6.6, which includes the intended perception objectives developed by ARGRESS to be achieved in the G-7 coalition countries and in Burzan.

Table 6.6
ARGRESS Netwar Attack Strategy Matrix

Attack Phase:	1 Diversion 			2 Confusion 					3 Conclusion		
Day:	1	2	3	4	5	6	7	8	9	10	11
ARGRESS Perception Objectives	G-7 nations believe another nation has committed economic espionage, sabotage G-7 nations believe military coalition is contaminated by economic intentions of one G-7 nation			G-7 nations believe infrastructure attacks may be related to economic competition activity (feasible, although not likely) Burzan government is corrupt and cannot be trusted G-7 nations rate Burzan crisis priority from high to “deferred”					G-7 nations perceive Burzan coalition support as low priority; high-risk action to be deferred or disregarded		
Information Attacks Against G-7	Net attacks occur in coalition nations’ “key industries” (industries in competition between G-7 coalition nations)			Infrastructure attacks focused on impact on “key industries” of public services and finance					Pause in attacks		
Information Attacks Against Burzan	Anonymous e-mail traffic discredits Burzan leadership with claims and rumors of corruption			Deceptive evidence of Burzan corruption produced					Burzan telecommunications disrupted		
Desired Political Effects	Create tension and competitive distrust within G-7 coalition Reduce Burzan problem priority			Reduce G-7 interest in coalition military adventure—due to internal problems, and distrust of Burzan government Public outcry against Burzan					G-7 coalition retracts offer of support to Burzan		

6.3.2 Taxonomy of Netwar Elements and Supporting Disciplines

The elements and disciplines necessary to conduct net warfare IO are organized in Figure 6.8. The taxonomy organizes the functional areas of capabilities (in boxes), and the supporting disciplines or areas of operational expertise (under each box). There certainly exists overlap between netwar and C2W activities, and this taxonomy is similar to the taxonomy for C2W in the next section. Section 6.4 describes each of the disciplines integrated by IO to conduct these activities and the activities of C2W.

6.4 Information Operations for Command and Control Warfare (C2W)

Information operations, escalated to physical engagement against military command and control systems, enter the realm of C2W. C2W is “the integrated use of operations security (OPSEC), military deception, psychological operations (PSYOPS), electronic warfare (EW), and physical destruction, mutually

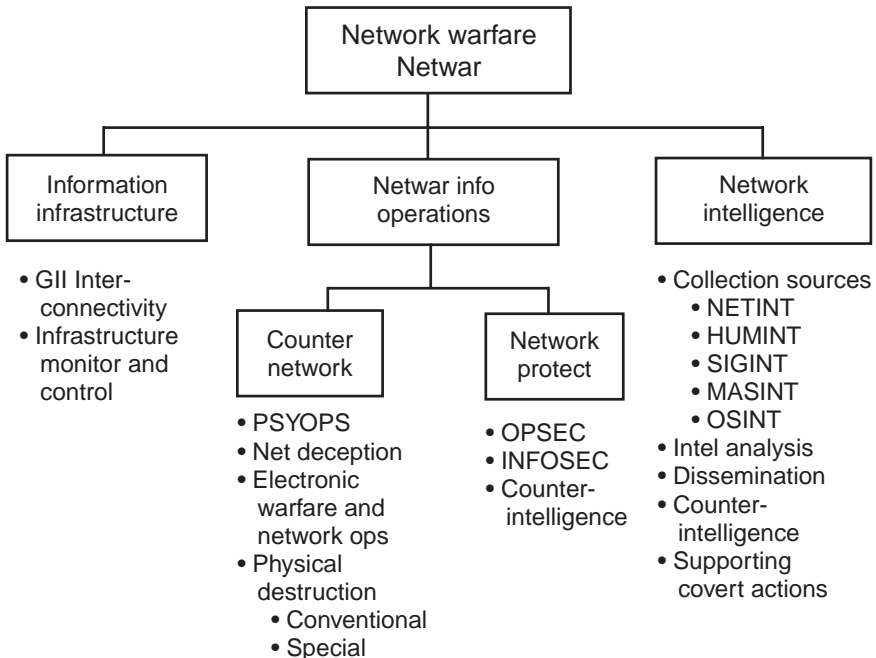


Figure 6.8 Taxonomy of functional elements and supporting disciplines for structured netwar.

supported by intelligence to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions” [46].

C2W is distinguished from netwar in the following dimensions:

- *Target*—Military command and control is the target of C2W. Supporting critical military physical and information infrastructures are the physical targets of C2W.
- *Media*—While the GII is one means of access for attack, C2W is characterized by more direct penetration of an opponent’s airspace, land, and littoral regions for access to defense command and control infrastructure. Weapons are delivered by air, space, naval, and land delivery systems, making the C2W overt, intrusive, and violent. This makes it infeasible to conduct C2W to the degree of anonymity that is possible for netwar.
- *Means*—C2W applies physical and information attack means to degrade (or destroy) the OODA loop function of command and control systems, degrading military leaders’ perceptual control effectiveness and command response. PSYOPS, deception, electronic warfare, and physically destructive means are used offensively, and OPSEC provides protection of the attack planning.
- *Players*—The adversaries of C2W are military organizations of nation states, authorized by their governments.

Ronfeldt and Arquilla emphasize that future C2W will be characterized by a revision in structure, as well as operations, to transform the current view of command and control of military operations:

Waging [C2W] may require major innovations in organizational design, in particular a shift from hierarchies to networks. The traditional reliance on hierarchical designs may have to be adapted to network-oriented models to allow greater flexibility, lateral connectivity, and teamwork across institutional boundaries. The traditional emphasis on command and control, a key strength of hierarchy, may have to give way to emphasis on consultation and coordination, the crucial building blocks of network designs [47].

The Gulf War revealed the U.S. baseline for C2W operations, emphasizing the integration of intelligence, surveillance, and reconnaissance (ISR);

command and control; and electronic/conventional combat to counter Iraqi command and control [48]. (This is similar to the radioelectronic combat [REC] doctrine of the former Soviet Union, developed in the 1970s.) Future C2W will be distinguished from this baseline by greater precision, speed, and depth of infrastructure attack, leading many to believe that C2W will also be conducted by smaller, stealthier networked forces who gain victory in much shorter periods of time. (See U.S. Joint Vision 2010 [49] and U.S. Air Force 2025 studies [50] for representative views of future C2W.)

6.4.1 A Representative C2W Scenario

This scenario illustrates a C2W conflict similar to the Gulf War, but waged over a decade later with more advanced weaponry and delivery systems designed to counter command and control of conventional forces. The scenario is purposely one-sided to favor the attackers for the purpose of illustrating C2W tactics and weapons.

SCENARIO TITLE: Operation SWIFT JUSTICE

ABSTRACT: The mineral rich and newly democratic nation Cintra has conducted national elections. On the day of inauguration, the neighboring rogue country Gadique launches a conventional attack, which swiftly moves against limited resistance into the capital within 48 hours. Contrary to worldwide opposition to the aggression, the dictator of Gadique declares Cintra a province of Gadique and begins establishing defensive positions around the capital and key mines, oil refineries, and ports. The United States and European and regional nations form a coalition to restore democratic rule to Cintra in an operation named SWIFT JUSTICE.

SITUATION:

1. *Driving forces (why)*—Since the end of the Cold War and the 1991 Gulf War, the G-7 and other nation states remained major actors in human affairs. As Huntington generally predicted, the dominating source of conflict in the world transitioned from global-scale ideology to regional conflict over cultural differences [51]. Continued economic and social pressures in the Third World nations have caused ambitious dictatorial leaders to seek regional control, especially over mineral-rich neighbors viewed as threats because of increased

democratization and involvement with democratic nations. Both interstate and intrastate conflicts arise over cultural tensions [52]. The spark of conflict over Cintra (and the rationale that Gadique uses overt and violent aggression) is the rapid change in Cintra's culture; Western culture's rapid introduction into Cintra brings the concurrent diminution of non-Western cultural values of the region.

2. *Rationale (how)*—The dictatorial regime in Gadique maintains a significant standing military and, over a period of a decade, has procured state-of-the-art air defense systems. Unable to procure a capable air force, it has invested in theater ballistic missiles as a means to deliver weapons of mass destruction on enemy ground forces. Anticipating engagement with Western coalition forces, Gadique has also developed a “pilot-scale” capability to produce limited but threatening quantities of the biological agent *clostridium botulinum* (the agent causing botulism) [53]. It has also developed political ties with regional rogue nations and other non-Western nations in an attempt to limit the assembly of future coalitions against its military adventures.
3. *Scenario narrative (what happens)*—The period of this scenario lasts approximately one month, from the attack on Cintra until it is restored to sovereignty. The sequence of events from predeployment until reconstitution follows. From the beginning, diplomatic and nonlethal network operations are initiated (e.g., e-mail broadcasts and computer attacks on the Gadique foreign and defense ministries) to attempt to force a withdrawal by Gadique, to no avail. Throughout the following operations in Cintra, an escalating net warfare attack is sustained against critical infrastructures in Gadique's capital and developed cities.
 - *Predeployment operations (days 1 to 15)*—Upon commitment to restore Cintra, the coalition positions a battle group offshore and initiates intensive surveillance and reconnaissance to map Gadique's positions in Cintra. High-altitude unmanned air vehicles (HAE UAVs), launched from bases 1,000 km distant, maintain constant surveillance of military buildup across the country as the coalition prepares to deploy. Constellations of special PSYOPS UAVs, dubbed “Commando Trio” broadcast television programming over Cintra VHF frequencies with the coalition demand for Gadique to restore Cintra and images of non-Western cultural leaders accusing Gadique's leaders of shaming the culture. The

coalition pre-positions an information operations cell, with automated planning tools, aboard the flagship of the battle group, with support from two IO units at home bases. Aware of Gadique's procurement of UHF and L-band jammers capable of limited jamming of certain satellite links for navigation and communications, the coalition reroutes several links and applies wartime modes to deny Gadique the ability to attack communications and information systems. At midnight on the fourth day, a dozen cruise missile attacks degrade (but do not destroy) electrical power by spreading carbon-fiber materials across transformer grids. In the resulting brownouts and confusion, special forces are inserted into the country to install unattended exploitation/attack packages to selected communications lines.

- *Deployment operations (days 10 to 20)*—Combat maneuver units are positioned in two neighboring countries and offshore. As an element of deception, all units are artificially “doubled” by communication traffic and call signs to imitate the equivalent of three full divisions. Constant air sorties probe SAM missile radar acquisition volumes. Nightly air attack runs are initiated, only to be broken off as the SAMs prepare to fire.
- *Entry operations (days 20 to 25)*—Deep penetrating air decoys are launched to force SAM batteries to reveal their radar positions, which are attacked by unmanned combat air vehicles (UCAVs) and cruise missiles, targeted in-flight by precision locations secured by SIGINT UAVs. As SAMs are suppressed, the communication traffic monitored by SIGINT UAVs and unattended network sensors reveal reconnaissance, intelligence, surveillance, and target acquisition (RISTA) assets, and C2 intelligence fusion centers. Initial combat, airborne, and special forces are inserted to physically attack the located fusion centers. The unattended exploitation/attack packages previously installed on selected lines insert malicious code into the computers of some C2 systems, when accessible over the network. Commando Trio missions broadcast demands for surrender (and assurances of restoration to Cintra's populace) over the national TV frequency, as the prime TV broadcasting station is silenced.
- *Decisive operations (days 25 to 28)*—SWIFT JUSTICE operational tempo expands as attacks move from the core fusion nodes to communication nodes, where special UCAVs attack sites with directed

energy weapons that destroy the front ends of receivers and transmitters. With air superiority achieved, continuous precision bombing of troop leadership posts (complemented by PSYOP messages from Commando Trio and leaflet drops) is initiated. Gadique's troops face increasing loss of control, leadership, and knowledge of the situation in the theater. The coalition implements navigation warfare tactics to deny Gadique the use of precision navigation by jamming differential data links employed to exploit GPS navigation. Airborne units are inserted and ground maneuver forces move immediately toward Gadique's troop concentrations, now unable to communicate or perceive the situation other than by Commando Trio reports, which include real UAV video of initial troop surrenders. Relentless attacks on theater ballistic missile garrisons take away Gadique's ability to attack the small, rapidly moving coalition maneuver forces with biological agents. Network attacks on communications at military bases in Gadique stifle logistics and attempts to reinforce the troops in the Cintra theater. First encounters between opposing forces are scheduled at Gadique's weakest units, reinforcing the Commando Trio threats. Gadique's forces begin retreat toward Gadique and neighboring countries, and over 85% surrender on contact with coalition troops.

- *Termination and post-conflict (days 28 to 30)*—Information operations support the formal surrender by Gadique and requirements for payment of war reparations to Cintra. Information operations conducted against Gadique's government throughout the month-long encounter provide the intelligence and evidence for international courts to bring Gadique's leadership to justice.
 - *Redeployment and reconstitution operations (days 31 to 45)*—Commando Trio and their manned counterparts, commando solo aircraft, continue broadcast to Cintra and neighboring countries to support regional stability until ground TV stations are restored. Military forces remain in Cintra until the authorized democratic government is reinstated and Gadique begins reparations.
4. *Scenario time line (when)*—The time line of SWIFT JUSTICE operations objectives and of attack activities initiated by coalition forces (Figure 6.9) illustrates the sequence of activities and allocation of responsibilities over the five phases of the operation. The time line

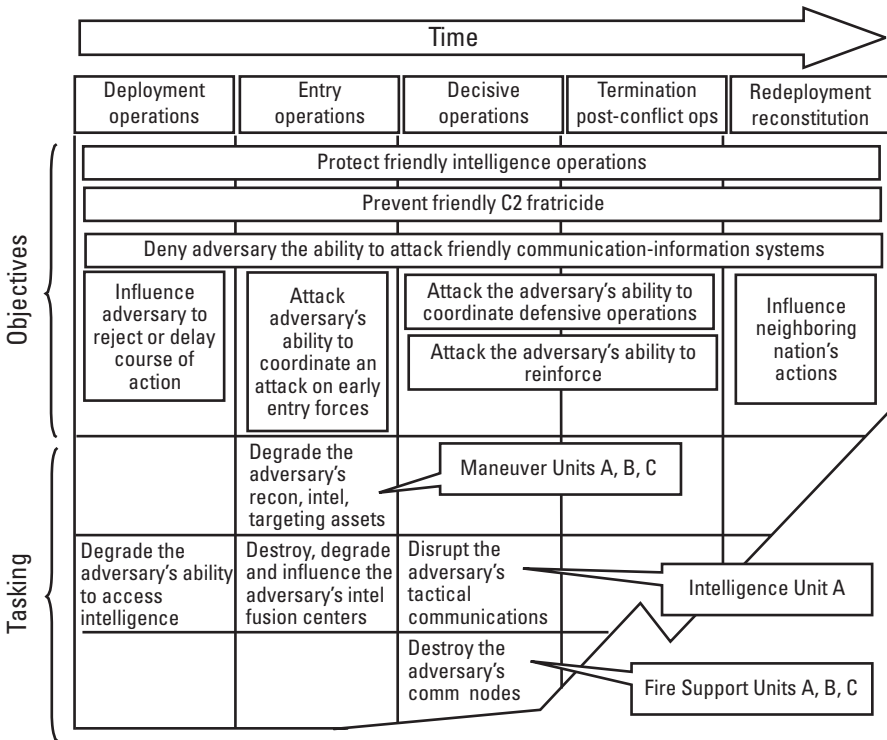


Figure 6.9 Synchronization time line matrix for Operation SWIFT JUSTICE. (Source: FM 100-6, Chapter 6.)

is presented in synchronization matrix format, adapted from FM-100-6 for military information operations [54].

6.4.2 Taxonomy of C2W Functional Elements and Supporting Disciplines

The elements and disciplines necessary to conduct C2W IO are organized in Figure 6.10. The taxonomy organizes the functional areas of capabilities (in boxes) and the supporting disciplines or areas of operational expertise (under each box) [55]. Information operations require the coordination of the supporting disciplines to achieve effective physical, information, and perceptual impact on the target. The information-based warfare elements, command and control (C2), and intelligence that deliver battlespace awareness and enable effective force management were presented earlier in Chapter 4.

The following section describes the characteristics of the common disciplines to conduct both C2W and net warfare information operations.

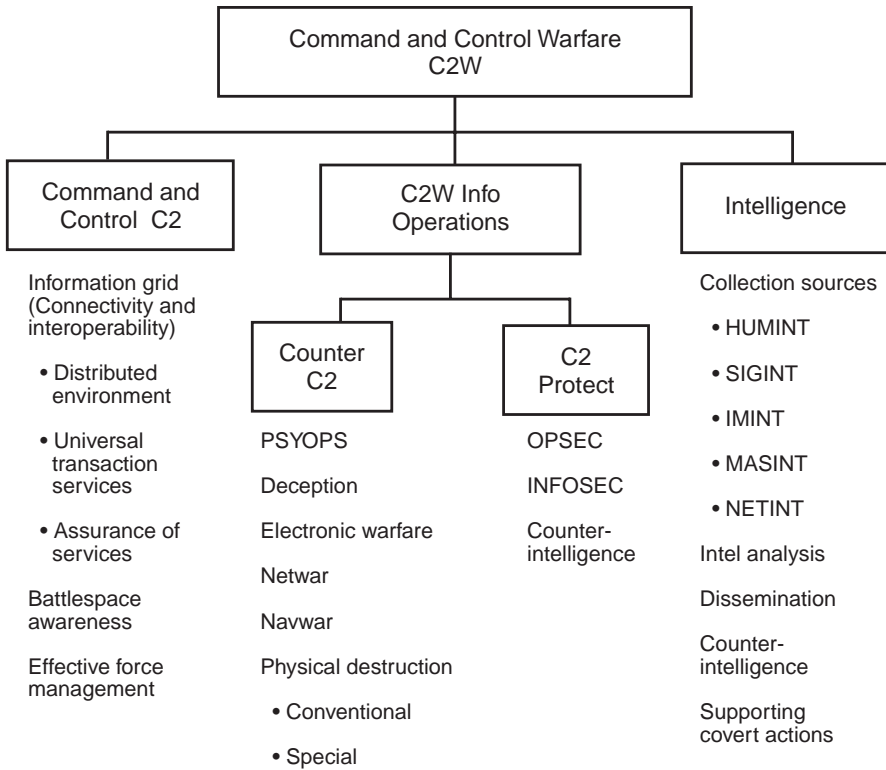


Figure 6.10 Taxonomy of C2W functional elements and supporting disciplines.

6.5 The Component Disciplines of Information Operations

The fundamental offensive and defensive activities common to both C2W and netwar can be mapped to the three levels of the IW model (perceptual, information, physical) to organize six basic operational categories of activities, as shown in Table 6.7.

The table identifies the disciplines that were illustrated in the scenarios earlier in this chapter while distinguishing the differences between netwar and C2W technical operations at the information level for both offense and defense. The definitions of information warfare (and its operations) earlier in this book included five fundamental disciplines: PSYOPS, deception, electronic warfare, destruction, and OPSEC. The table and following sections describe these five, and we have added intelligence and counterintelligence (critical supporting disciplines) for completeness. INFOSEC (a subdiscipline of OPSEC) is treated separately because of its importance in IO, and electronic

Table 6.7
Information Operational Elements Mapping

IW Model Layer		Function	NETWAR (Targets society at large via political and economic infrastructure)	C2W (Targets national will and resolve via military infrastructure)
Offense	Perceptual	Manage perception and disrupt decision processes	PSYOPS (6.5.1) Deception (6.5.2)	
	Information	Dominate info infrastructure Dominate electromagnetic spectrum	Network operations (6.5.3.2) Net attack (NA) Net support (NS)	Electronic warfare operations (6.5.3.1) Electronic attack (EA) Electronic support (ES)
	Physical	Break things Incapacitate or kill people	Physical destruction (6.5.4)	
Defense	Perceptual	Protect perceptions and decision-making processes	Intelligence (6.5.5) Counterintelligence (6.5.6)	
	Information	Protect info infrastructure Protect electromagnetic spectrum	Information security INFOSEC (6.5.7) Net protect (NP) Net support (NS)	Electronic warfare operations (6.5.3.1) Electronic protect (EP) Electronic support (ES)
	Physical	Protect operations Protect things Protect people	Operational security OPSEC (6.5.8)	

warfare is divided into electronic and network components. Therefore, the subsequent sections describe nine disciplines that are essential for IO.

The following sections (referenced in the figure) introduce the basic principles of each of the nine disciplines, reserving details that focus on the information layer for Chapters 8 (offense) and 9 (defense).

6.5.1 Psychological Operations (PSYOPS)

PSYOPS are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behaviors of foreign governments, organizations, groups, and individuals [56]. The objective of PSYOPS is to manage the perception of the targeted population, contributing to the achievement of larger operational objectives [57]. Typical military objectives include the creation of uncertainty and ambiguity (confusion) to reduce force effectiveness, the countering of enemy propaganda, the encouragement of disaffection among dissidents, and the focusing of attention on specific subjects that will degrade operational capability. PSYOPS are not synonymous with deception; in fact, some organizations, by policy, present only truthful messages in PSYOPS to ensure that they will be accepted by target audiences.

The use of mass communication as a perception management tool for “public diplomacy” and “low-intensity conflict” has long been analyzed and developed to influence, persuade, or even coerce targeted populations. The development of communication studies and public opinion research formed the foundation for PSYOPS concepts now employed by the military [58]. The U.S. military has established doctrine to conduct PSYOPS and maintains special operations units with this specialty [59].

PSYOPS are based on two dimensions: the communication of a *message* via an appropriate *media* to a target population (e.g., enemy military personnel or foreign national populations). Table 6.8 summarizes representative forms of messages and the major media avenues used.

PSYOP activities begin with creation of the perception objective and development of the message theme(s) that will create the desired perception in the target population (Figure 6.11). Themes are based upon analysis of the psychological implications and an understanding of the target audience’s culture, preconceptions, biases, means of perception, weaknesses, and strengths. Theme development activities require approval and coordination across all elements of government to assure consistency in diplomatic, military, and economic messages. The messages may take the form of verbal, textual messages (left brain oriented) or “symbols” in graphic or visual form (right brain oriented).

Next, the media for communication of the message are chosen, and the unique messages for each channel are tailored to be culturally appropriate for the component of the target audience that will be reached. Finally, the effects

Table 6.8
The Two Dimensions of PSYOPS

PSYOP Dimension	Type	Specific Examples
Message (Articulation or symbology of a theme or position)	Policy Attitude Intent	Representative themes (and perception goals): Resolve and determination (cease hostilities) Open for discussion (initiate dialogue) Diplomacy (possible compromise) Threaten force (surrender is necessary)
	Press (the media)	Formal statement of policy or position Policymaker statement to press Government agency comments to press Planned "leaks"
Media (Method of delivery of the message)	Broadcast means to groups (government, individuals, military forces)	Direct broadcast radio (AM/FM/SW), military broadcast Direct broadcast television Internet Posters, leaflets, radios, video/audio cassettes delivered by individuals, air drops, or other means Indirect broadcast means (intended for intercept) Loudspeakers
	Communications to individuals	Telephone conversations e-mail messages Letters "Inadvertent" messages
	Actions	Diplomatic actions Government actions Military actions Coalition actions

or impact of PSYOPS activities must be monitored through intelligence to refine and adapt both the message and media to achieve the desired effects.

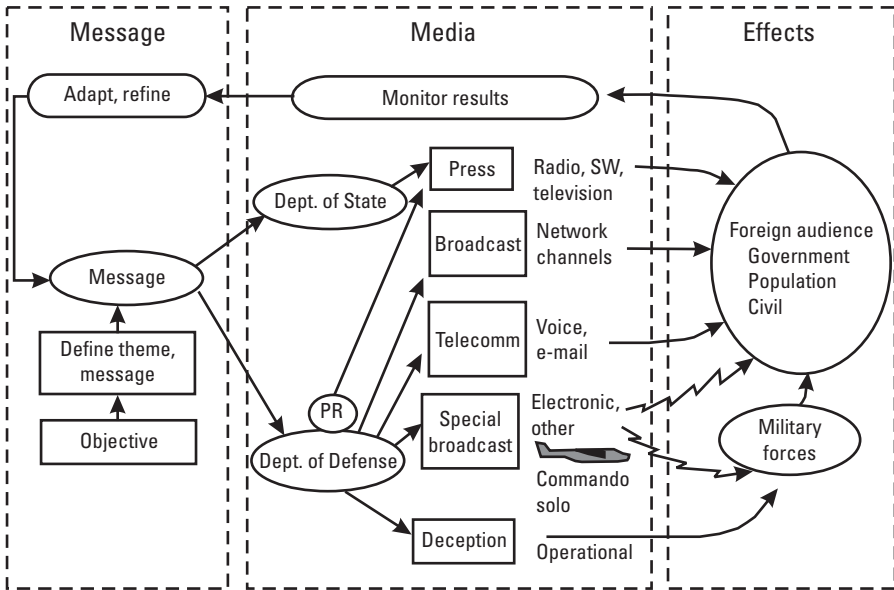


Figure 6.11 Functional flow of a PSYOPS campaign.

6.5.2 Operational Deception

Military deception includes all actions taken to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of a friendly mission [60]. Deception operations in netwar expand the targets to include society at large, and have the objective of inducing the target to behave in manner (e.g., trust) that contributes to the operational mission. Deception contributes to the achievement of a perception objective; it is generally not an end objective in itself.

Two categories of misconception are recognized: (1) *ambiguity* deception aims to create uncertainty about the truth, and (2) *misdirection* deception aims to create certainty about a falsehood. Deception uses methods of distortion, concealment, falsification of indicators, and development of misinformation to mislead the target to achieve surprise or stealth. Feint, ruse, and diversion activities are common military deceptive actions.

Deception operations include the following activities:

- Based upon perception management goals, deception objectives are defined.

- A “deception story” is created to achieve the deception objective (e.g., surprise).
- A deception plan is prepared to present the story to and condition the target (e.g., adversary intelligence system or Internet audience) in the sequence and composition of events that would be expected from the story events. The events can include generation of reports, signatures (e.g., physical or electronic signatures), and messages.

Because deception operations are fragile (their operational benefit is denied if detected), operational security must be maintained and the sequencing of deceptive and real (overt) activities must be timed to protect the deception until surprise is achieved. As in PSYOPS, intelligence must provide feedback on the deception effects to monitor the degree to which the deception story is believed.

Deception operations are based on exploitation of bias, sensitivity, and capacity vulnerabilities of human inference and perception (Table 6.9) [61]. These vulnerabilities may be reduced when humans are aided by objective decision support systems, as noted in the table.

The erroneous decisions aboard the USS Vincennes in 1988 that resulted in the tragic destruction of a commercial airliner were partially attributed to psychological conditions in which the combat information center team (1) had a preconceived attack scenario based on intelligence; (2) accepted data that reinforced the preconceived scenario, while rejecting evidence to the contrary (“scenario fulfillment”); and (3) had to make decisions in the presence of stress, overload, and an incomplete set of information [62]. (This was not a case of deception, but illustrates the conditions that are created and exploited to cause misdirection deception.) Strategic and operational military deception principles and historical examples can be found in [63,64].

Electronic deception is a component of electronic warfare operations, described in Section 6.5.3.1, and includes the deception of electronic sensors and human operators. For example, techniques that duplicate adversary voices (by intercept, modification, and retransmission) are used for ambiguity deception targeted at radio operators and combat crews [65]. The morphological modification (“morphing”) of video imagery can be used similarly to create deceptive video information. The audio and video fakes may not stand up to detailed scrutiny, but may be sufficient to achieve deception objectives under the conditions of bias, overload, and insensitivity.

Deception has been applied on the Internet for purposes of fraud to seduce individuals to provide information, believing they were interacting securely over the World Wide Web. One representative deception, called “web

Table 6.9
Deception Principles, Exploited Human Behaviors, and Counterdeception Measures

Deception Principles	Human Inference and Perception Behaviors Exploited	Potential Counterdeception Decision Aids
<p>Reinforce the target’s existing beliefs to achieve greater acceptance, while actual operations perform the unlikely.</p>	<p>Human decision making maintains biases that apply greater confidence and accept information that reinforces preconceived or pre-established beliefs, and places less confidence in or rejects information that it believes unlikely.</p>	<p>Provide objective quantitative assessment of all feasible possibilities: Display positive, negative evidence; Display long-term changes.</p>
<p>Condition (desensitize) the target over time to reduce sensitivity to subtle, real indicators. Conditioning may include repeated false alarms prior to a real event.</p>	<p>Human inferential decision making is limited in terms of sensitivity. Sensitivity levels are established on the basis of baselines of belief established by repetition.</p>	<p>Detect possible conditioning activities.</p>
<p>Overload human inference capacity to bias the target to make decisions on the basis of a small, incomplete set of facts.</p>	<p>Human inferential decision making is limited in terms of capacity and perception may be biased to a small set of reinforcing data, rather than integrating a complete set including contradictory data.</p>	<p>Provide assessment support to reduce overload, allow human to focus on most the important information, not the most demanding data.</p>

spoofing,” is of the misdirection type, in which a victim first must be lured to a spoof site [66]. The spoof site initiates a “man-in-the-middle” position by “rewriting” URLs on the spoof Web page to point back to the attacker’s server. The attacker’s server creates a shadow of the entire World Wide Web, in which all of the victim’s browser requests are forwarded to the attacker server, and that server obtains the requested (legitimate) page and rewrites all links to return to the attacker’s server. Once captured, the attacker’s server observes all transactions of the victim, which may include the disclosure of passwords, account numbers, or other security-related data.

6.5.3 Electronic Operations

Electronic operations include military *electronic warfare* (EW or electronic combat) that attacks targets over the radiated electromagnetic spectrum, and

network operations that focus on access to targets via the GII, NII, or DII network infrastructure. While some may include all electronic operations under the discipline of electronic warfare, we distinguish traditional EW (long associated with military C2W) from net operations (associated with netwar) for clarity in this text.

6.5.3.1 Electronic Warfare Operations

The use of electromagnetic radiation for communications, target detection (radar), navigation, and identification has made it the premiere medium for information warfare since the Second World War. Numerous texts chronicle the development of military electronic warfare [67], catalog the numerous systems [68], and describe the numerous techniques involved [69–71]. The discipline includes radio frequencies (RF) through the optical regions of the electromagnetic spectrum and is divided into three subdisciplines—electronic attack, electronic protect, and electronic support—as shown in Table 6.10.

Table 6.10
The Three Branches of Electronic Warfare

EW Segment	Function	Application
Electronic attack (EA)	The use of electromagnetic or directed energy to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability	Directed RF energy, or laser energy against radar, communications, navigation, or other systems employing electromagnetic reception or radiation
Electronic protection (EP)	Actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of EW (that degrade, neutralize, or destroy friendly combat capability)	Passive measures inherent in reception equipment to look through jamming, or protect against directed energy Self-protection jamming Dispensable RF chaff or electro-optical (EO) flares as decoys Decoy vehicles, towed or expendable (dropped) decoy emission sources
Electronic support (ES)	Actions tasked by, or under the direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy	Threat recognition Threat avoidance Immediate EA or EP operations decisions Targeting information collection Tactical actions

Electronic support (ES) collects real-time data to support both the attack (EA) and protection (EP) functions.

- EP is supported by providing real-time information on adversary's EA activities, providing warnings to conduct emissions control (EMCON), to change targeted frequencies, to protect sensitive receivers from directed energy, or to provide counterdeceptive or disruptive attacks.
- EA is supported by delivering targeting information (location, operating modes, and temporal-spectral vulnerabilities) on threat systems.

Electronic attack can be further subdivided into four fundamental attack categories: exploitation, deception, disruption or denial, or destruction (Table 6.11). These categories are arranged in order of increasing intrusiveness and violence; they range from passive intercept of signals (exploitation) to permanent physical destruction.

Ground, shipboard, and airborne platforms are employed to conduct electronic warfare, with airborne platforms offering the most attractive line of sight and dwell on targets for both ES and EA operations penetrating denied areas.

The time synchronism of ES and EA is critical and must be dynamically managed to provide necessary intelligence while conducting IO attacks. The tactical needs to both listen to (ES) and disrupt (EA) a source are conflicting, and the timing of each activity must be synchronized with all other information operations.

EA, EP, and ES electronic suites include both onboard and expendable system components. Passive expendables (e.g., radar chaff and electro-optical/IR flares) are complemented by active RF and laser emission source packages that may be used for deception (decoys) or disruption (jammers).

Navigation Warfare

Navigation warfare (navwar) is a form of EW that attacks navigation systems (e.g., tactical radio navigation aids or global positioning system [GPS]) and has the objective of denying the enemy the utility of accurate and timely navigation information while maintaining accurate navigation for friendly forces. Recent global reliance (both military and civil) on GPS has increased the potential, and interest in, countermeasures to keep individual platforms or entire regions of the Earth from acquiring accurate navigation. Herskovitz [72] has described the vulnerability of navigation by GPS due to the susceptibility of the received signal (L1 frequency at 1,575.42 MHz delivers approximately -160 dBW at

Table 6.11
The Fundamental Categories of Electronic Attack

Attack Category	Functional Operation	Representative Techniques	Representative Systems
Exploitation	Extract information from the opponent's sensor or communication system, and exploit the knowledge gained for deception, disruption, denial, or destruction	Radar warning receiver (RWR) Electronic support measures (ESM)	Radar intercept (ELINT) for attack targeting (disrupt, deny, or destroy) Communications intercept (COMINT) Network intercept
Deception	Insert false information into the opponent's sensor or communication system	Decoy signals False messages Spoofing or masquerading as a friend	Radar deception to eliminate targets, insert false targets Communication insertion of false synchronization or messages
Disruption or denial	Degrade the information performance (e.g., detectability, accuracy, intelligibility, tracking rate, identification, error rate, throughput, capacity) of the opponent's sensor or communication systems	Jamming (many types): Broadband Swept Reactive Follow-on Continuous Look-through Signal repetition Saturation	Radar jamming Communications jamming Communications delay and repeat
Destruction	Eliminate the information collection, processing, or distribution capability of an opponent's sensor or communication system	Soft kill: temporary or functional, possibly non-physical elimination Hard kill: permanent or physical elimination	Antiradiation missile Directed energy: RF energy Laser energy

the Earth's surface, L2 frequency at 1,227.6 MHz delivers -166 dBW) to denial or disruption by jamming (see also [73,74]).

A sequence of measures, countermeasures (CM), and counter-countermeasures (CCM) involved in navwar against the GPS system are summarized in Figure 6.12. Notice that each of the basic operations of electronic warfare used by both attackers and defenders of GPS appear in the tree—exploitation, denial, deception, destruction. The tree is representative

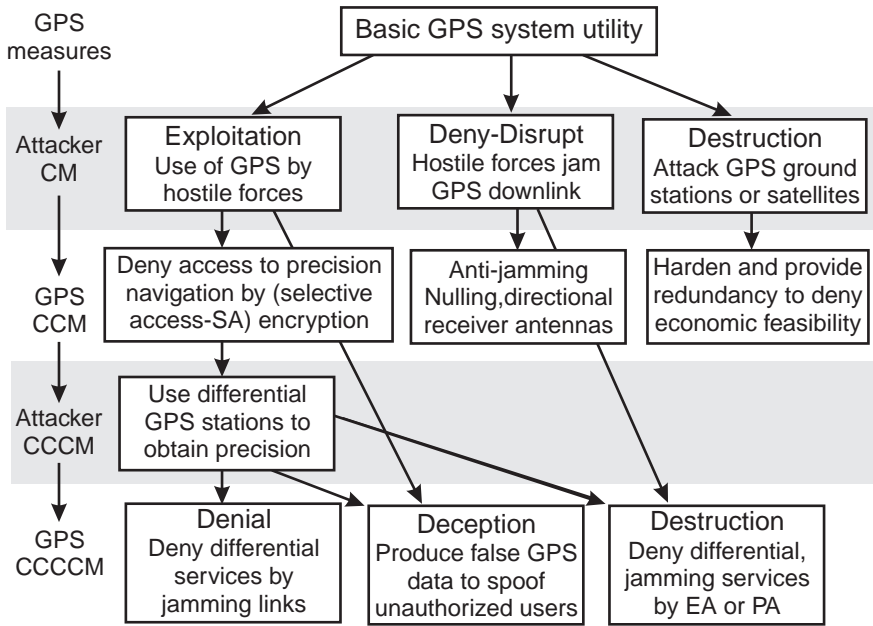


Figure 6.12 Basic countermeasure sequence tree for GPS.

and does not include the myriad of possible operations, such as spoofing of the GPS direct or differential signals to cause a target victim to receive erroneous navigation data [75].

6.5.3.2 Network Operations

Network operations include pure information attacks *through* the information infrastructure. Chapter 8 provides a thorough overview of these offensive operations, which may be organized (Table 6.12) to parallel their counterparts in electronic warfare operations.

6.5.4 Physical Destruction

In addition to the pure information engagements of net attack operations, the physical components of the information infrastructure (and supporting functions, such as electrical power, air conditioning, and human operators) may be subject to physical attacks to disable (soft kill) or destroy (hard kill) the targeted components. Physical attacks range from lethal or nonlethal attacks on critical people (e.g., system administrators) to attacks on critical components (e.g.,

Table 6.12
The Three Branches of Network Operations

Segment	Function	Application
Network attack (NA)	The use of information weapons delivered over the information infrastructure with the intent of penetrating security and exploiting, acquiring, degrading, neutralizing, or destroying infrastructure processes or information	Theft of security information Theft of electronic commerce financial instruments Disruption of computer services, corruption of data, deception via computer Destruction of infrastructure components
Network protection (NP)	Actions taken to protect the information infrastructure from network attacks	Control of computer access (information and physical access) Protection of integrity of computer processes and information
Network support (NS)	Actions taken to search for, map, identify, characterize, and locate information infrastructure elements, or actions to intercept and exploit information	External network scanning, analysis Capture security access information (e.g., passwords) Cryptoanalysis and cryptoattacks

hardware, software, communication links, and databases) that will achieve the desired functional effect on the infrastructure.

The Gulf War applied physical destruction of information infrastructure by surgical physical attacks on critical nodes of integrated air defense systems, telecommunications, and command systems. To perform effective operations, physical targets must be located, identified, and functionally associated with the information infrastructure, and the effects of physical attacks on information functions must be determined. Weapons categories capable of physical destruction include the following:

- *Kinetic energy*—Explosion, impact, or shock effects of explosives, bombs, or missiles are the most conventional means of destruction.
- *Directed energy*—High-power lasers, high-power microwave transmitters, or electron beam generators may be used to transfer electromagnetic energy onto targets over a distance. When sufficient energy is

transferred, sensitive electronic and electro-optical components are vulnerable to these weapons.

- *Chemical-biological*—Chemical and biological agents may attack human operators or sensitive materials associated with electronic components (e.g., insulation, plastics, and metals).
- *Radiological*—Nuclear radiation (in the form of charged particles) can damage unhardened electronic circuitry due to the effects of ionization (generation of electron-hole pairs) in semiconductor materials. Two categories of effects are manifested:
 1. Total dose effects due to cumulative ionization damage caused by charged particles passing through a semiconductor device;
 2. Single event effects (SEE) in which a single high-energy ion causes temporary upsets, latch-ups, or other destructive effects on semiconductors.

Physical weapons and effects will be summarized in Chapter 8 with their corresponding offensive operations.

6.5.5 Intelligence

Intelligence operations contribute assessments of threats (organizations or individuals with inimical intent, capability, and plans); preattack warnings; and postattack investigation of events.

Intelligence can be viewed as a defensive operation at the perception level because it provides information and awareness of offensive PSYOPS and deception operations. Proper intelligence enables clear perception and decision making: cognizance of threats and perception attacks, objective discernment of the situation, and sensitivity to subtle indicators. Intelligence on information threats must be obtained in several categories:

1. *Organization threat intelligence*—Government intelligence activities maintain watches for attacks and focus on potential threat organizations, conducting counterintelligence operations (see next section) to determine intent, organizational structure, capability, and plans.
2. *Technical threat intelligence*—Technical intelligence on computer threats and technical capabilities are supplied by the government, academia, or commercial services to users as services. For example:

- The Computer Emergency Response Team (CERT) Coordinating Center, a federal government-funded activity of the Carnegie Mellon University, identifies vulnerabilities to systems, logs reported attacks, and provides advisories for identified security problems.
- The National Computer Security Association (NCSA) maintains an “underground reconnaissance” activity to monitor and report the state of the art in hacker capabilities, tactics, and activities for NCSA’s constituents.
- Commercial suppliers of antivirus software provide continuous monitoring of viral strains and deliver on-line warnings (and antigen data to update their commercial packages).

6.5.6 Counterintelligence

Structured attacks require intelligence gathering on the infrastructure targets, and it is the role of counterintelligence to prevent and obstruct those efforts. Network counterintelligence gathers intelligence on adversarial individuals or organizations (threats) deemed to be motivated and potentially capable of launching a network attack. Traditional activities include the following [76]:

- *Surveillance*—Threat activities are monitored, including development of capabilities, areas of interest, and focus of attention. Network attack reports are monitored, hypothesized to be reconnoitering efforts, and associated with potential threats in an effort to infer threat activities and interests.
- *Penetration*—Threat organizations may be penetrated by the insertion of agents (human or software agents) to acquire knowledge of intent, capabilities, and plans.

Because counterintelligence supplies information on a threat activity’s targeting perception, it is considered a perception-level defensive measure.

6.5.7 Information Security (INFOSEC)

We employ the term *INFOSEC* to encompass the full range of disciplines to provide security protection and survivability of information systems from attacks, including the most common disciplines, defined here [77].

- *INFOSEC*—Measures and controls that protect the information infrastructure against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of information infrastructure components (including data). INFOSEC includes consideration of all hardware and/or software functions, characteristics and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the infrastructure and for the data and information contained in the infrastructure. It includes the totality of security safeguards needed to provide an acceptable protection level for an infrastructure and for data handled by an infrastructure.
- *COMSEC*—Measures taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security material and information.
- *TEMPEST*—The study and control of spurious electronic signals emitted by electrical equipment.
- *COMPUSEC*—Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks [78].
- *System survivability*—The capacity of a system to complete its mission in a timely manner, even if significant portions of the system are incapacitated by attack or accident [79].

These security activities protect the information infrastructure with emphasis on personnel security (assuring trustworthiness and access of people), process security (assuring security of processes), physical security (assuring security of facilities and equipment), and signals (assuring security of intentionally transmitted and unintentionally radiated signals).

Chapter 9 provides a thorough summary of the technical aspects of INFOSEC operations.

6.5.8 Operational Security (OPSEC)

Operations security denies adversaries information regarding intentions, capabilities, and plans by providing functional and physical protection of people, facilities, and physical infrastructure components. OPSEC seeks to identify potential vulnerabilities and sources of leakage of critical indicators [80] to adversaries, and to develop measures to reduce those vulnerabilities. While INFOSEC protects the information *infrastructure*, OPSEC protects information *operations* (offensive and defensive).

The OPSEC process begins with an analysis of critical indicators and an assessment of threats to derive potential vulnerabilities to information operations. Based on the identified vulnerabilities, a risk analysis is performed to develop OPSEC measures to assure that acceptable risk levels are maintained [81]. Increased INFOSEC, deception, or revised operations may be required to assure OPSEC is achieved.

6.6 Summary

In this chapter, we have described the activities related to net and command and control warfare from an operational viewpoint. We have followed the distinctions of Arquilla and Ronfeldt, showing C2W as escalation to military operations from the nonlethal yet powerful conflict of netwar. Before moving on, it is important to pause and recall that these are only two of the twelve forms of conflict introduced in the first chapter. Information operations also apply to the remaining ten forms: the two low-technology global forms (ideological and terrorist), the four forms of corporate conflict, and the four forms of personal conflict.

While we highlight the high-technology aspects of IO in this and subsequent chapters, the distinctions between high and low technology will increasingly become blurred as information technology becomes a global commodity. Widespread information access and distribution will enable adversaries at levels of conflict to apply aspects of information operations.

We now move from the operational level to detail the technical tactics and countermeasures that implement the operations we have covered in this chapter.

Endnotes

- [1] "Information Operations," FM 100-6, Department of the Army, Washington, D.C., U.S. Government Printing Office, Aug. 27, 1997, Glossary.

-
- [2] Brown, A., *Bodyguard of Lies*, New York: William Morrow and Co. 1991.
 - [3] The three centers include the Air Force Information Warfare Center (Kelly AFB, San Antonio, TX), the Navy Fleet Information Warfare Center (Norfolk, VA), and the Army Land Information Warfare Activity (Ft. Belvoir, VA).
 - [4] "Information Operations," FM 100-6, Department of the Army, Washington, D.C., U.S. Government Printing Office, Aug. 27, 1997.
 - [5] OPNAVINST 3430.26, Implementing Instruction for Information Warfare/Command and Control Warfare.
 - [6] AFI 33-207, Information Protection Operations.
 - [7] "IW Squadron To Evaluate Offensive Tactics," *Aviation Week and Space Technology*, Nov. 27, 1995, p. 54.
 - [8] Anderson, R. H., and A. C. Hearn, "An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: The Day After... in Cyberspace II, MR-797-DARPA," Santa Monica, CA, RAND, 1996.
 - [9] Scott, W. B., "Wargame Raises New Space Policy Dilemmas," *Aviation Week and Space Technology*, Feb. 23, 1998, pp. 98–101.
 - [10] Fulghum, D., "Computer Combat Rules Frustrate the Pentagon," *Aviation Week and Space Technology*, Sept. 15, 1997, pp. 67–68.
 - [11] Fulghum, D., "Cyberwar Plans Trigger Intelligence Controversy," *Aviation Week and Space Technology*, Jan. 19, 1998, pp. 52–54.
 - [12] *Information Warfare Legal, Regulatory, Policy and Organizational Considerations for Assurance*, The Joint Staff, Washington, D.C., 2d ed., July 4, 1996, pp. 2–15.
 - [13] International Civil Aviation Organization (ICAO) is an organization of the United Nations that provides oversight and regulation of international air traffic control operations.
 - [14] The G-7 nations include Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States.
 - [15] The G-7 nations convened an Information Society Conference (ISC), hosted by the European Commission, in Brussels, Belgium, on Feb. 25–26, 1995, to initiate the study and development of the GII. The G-7 ISC initiated "pilot projects" with international cooperation to demonstrate social, economic, and cultural benefits of an information society enabled by a GII. GII projects included the areas of education, inventory healthcare, resources management, emergency management, and maritime navigation.
 - [16] Kahin, B., and C. Nelson, (eds.), *Information Policy and the Global Information Infrastructure: Borders in Cyberspace*, Cambridge, MA: The MIT Press, 1996.
 - [17] "Critical Foundations: Protecting America's Infrastructures," Report of the President's Commission on Critical Infrastructure Protection, Oct. 1997.

- [18] President's Commission on Critical Infrastructure Protection (PCCIP), Executive Order 13010, original July 15, 1996 with amendments on Nov. 13, 1996 by EO 13025, Apr. 3, 1997 by EO 13041, and Oct. 11, 1997 by EO 13064.
- [19] "The Global Information Infrastructure: Agenda for Cooperation," U.S. Information Infrastructure Task Force, Version 1.0, N.D.
- [20] Kahin, B., (ed.), *Building Information Infrastructure*. New York: Primis-McGraw-Hill, 1992.
- [21] Kahin, B. and E. Wilson, (eds.), *National Information Infrastructure Initiatives: Vision and Policy Design*, Cambridge, MA: MIT Press, 1996.
- [22] Munro, N., "The Pentagon's New Nightmare: An Electronic Pearl Harbor," *The Washington Post*, July 16, 1995.
- [23] Black, S. K., (Lt. Col., USAF), *A Sobering Look at the Contours of Cyberspace*, Pittsburgh, PA: Ridgeway Center for International Security Studies and the University of Pittsburgh, Viewpoints 96, June 3, 1996.
- [24] *Information Warfare Legal, Regulatory, Policy and Organizational Considerations for Assurance*, The Joint Staff, Washington, D.C., 2d ed., July 4, 1996.
- [25] CJCSI 6510.01A, Defensive Information Warfare Implementation, as cited in [24] above.
- [26] Domestic Wiretap Act of 1968.
- [27] Omnibus Crime Control and Safe Streets Act of 1978.
- [28] Right to Financial Privacy Act of 1978.
- [29] Electronic Funds Transfer Act of 1980.
- [30] Electronic Communications Privacy Act of 1968, and Communications Assistance for Law Enforcement Act of 1994.
- [31] DePaula, R. P., and R. Bobometti, "NII/GII Overview," *AIAA Colloquium 16th ISCSC*, Feb. 25, 1996.
- [32] For a technical reference architecture model for the U.S. NII, see also "An Architectural Framework for the NII," Cross-Industry Working Team of the President's Information Infrastructure Task Force, Aug. 1994.
- [33] "Critical Foundations," Briefing of the President's Commission on Critical Infrastructure Protection, Briefing 0155, Nov. 17, 1997.
- [34] "Defense Information Infrastructure Master Plan," Version 6.0, Defense Information Systems Agency, Section 2.3 Definition, June 27, 1997.
- [35] "GCCS Common Operating Environment Baseline," LL-500-04-03, Defense Information Systems Agency, Nov. 1994.
- [36] Arquilla, J., and D. F. Ronfeldt, "Cyberwar is Coming!," *J. Comparative Strategy*, Vol. 12, No. 2, Apr.–June, 1993, pp. 141–165.
- [37] Fialka, J. J., *War by Other Means*, New York: W.W. Norton, 1997.

-
- [38] Caldarella, R. J., (Capt., USN), "Information Warfare: the Vision," *Proc. of TMSA Information Warfare Conference*, Washington, D.C., June 12–13, 1995, p. 32.
- [39] Arquilla, J., and D. F. Ronfeldt, *The Advent of Netwar*, Santa Monica, CA: RAND MR-789-OSD, 1996.
- [40] Arquilla, J., and D. F. Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, CA: RAND MR-880-OSD/RC, 1996.
- [41] *Information Architecture for the Battlefield*, U.S. Defense Science Board, Oct. 1994, p. 24.
- [42] Arquilla, J., "The Great Cyberwar of 2002," *Wired*, Feb. 1998, pp. 122–127, 160–170.
- [43] Molander, R. C., A. S. Riddile, and P. Wilson, *Strategic Information Warfare: A New Face of War*, San Diego, CA: RAND, MR-661-OSD, 1996.
- [44] Libicki, M., *The Mesh and the Net*, Washington, D.C., McNair paper 28, National Defense University, 1994, Chapter 6.
- [45] Schwartz, P., *The Art of the Long View*, New York: Doubleday, 1991.
- [46] "Electronic Warfare (EW) and Command and Control Warfare (C2W) Countermeasures," U.S. Department of Defense, DODD 3222.4, Jan. 28, 1994.
- [47] Arquilla, J., and D. F. Ronfeldt, "Cyberwar is Coming!," *J. Comparative Strategy*, Vol. 12, No. 2, Apr.–June, 1993, pp. 141–165.
- [48] Campen, A., "Iraqi Command and Control: The Information Differential," in *The First Information War*, Fairfax, VA: AFCEA International Press, 1992, pp. 171–177.
- [49] "Joint Vision 2010," U.S. DoD Joint Chiefs of Staff, U.S. Government Printing Office, 1977.
- [50] Stein, G. J., "Information Attack: Information Warfare in 2025," *White Papers: Power and Influence*, Vol. 3, Book 1, Maxwell AFB, AL: Air University Press, Nov. 1996.
- [51] Huntington, S. P., "The Clash of Civilizations," *Foreign Affairs*, Summer 1993, Vol. 72, No. 3, pp. 22–49.
- [52] Vickers, M. B., and R. C. Martinage, *The Military Revolution and Intrastate Conflict*, Washington, D.C.: Center for Strategic and Budgetary Assessments, 1997.
- [53] Three production capacities are recognized: laboratory, pilot, and production scales. Pilot scale is considered able to produce biological weapon agents in vessel sizes ranging from 50 to 500 liters.
- [54] *Information Operations*, FM 100-6, Department of the Army, Washington, D.C.: U.S. Government Printing Office, Aug. 27, 1997, Chapter 6, Figure 6-2.
- [55] Hutcherson, N. B., (Lt. Col.), *Command and Control Warfare*, Maxwell AFB: Air University Press, AU-ARI-94-1, Sept. 1994. The figure is adapted from Figure 8, p. 22.
- [56] AFDD 2-5.5, "Psychological Operations," U.S. Air Force Doctrine Document, Feb. 22, 1997.

- [57] Perception management includes PSYOPS, truth projection, cover and deception, and operations security.
- [58] Simpson, C., *Science of Coercion: Communication Research and Psychological Warfare 1945-1960*, Oxford: Oxford University Press, 1994.
- [59] For the U.S. military doctrine on PSYOPS principles and employment, refer to U.S. Joint Pub 3-53, "Doctrine for Joint Psychological Operations," July 30, 1993, and U.S. Army FM 33-1, "Psychological Operations," Feb. 18, 1993.
- [60] AFDD 2-5.5, p. 34.
- [61] FM 90-2, "Battlefield Deception," Washington, D.C., Headquarters Department of Army, Oct. 3, 1988.
- [62] "Formal Investigation into the Circumstances Surrounding the Downing of a Commercial Airliner by the USS Vincennes (CG 47) on 3 July 1988," U.S. Navy Investigation Report 1320, Unclassified Version, July 28, 1988.
- [63] Dewar, M., *The Art of Deception in Warfare*, London: David & Charles, 1989.
- [64] Handel, M. I., (ed.), *Strategic and Operational Deception in the Second World War*, Essex, U.K.: Frank Cass & Co., 1987.
- [65] Fulghum, D. A., "Duplicating Enemy Voices Becoming a Combat Skill," *Aviation Week and Space Technology*, July 8, 1996, p. 48.
- [66] Felten, E. W., et al., "Web Spoofing: An Internet Con Game," *Proc. of 20th National Information Systems Security Conference*, Oct. 1997.
- [67] Munro, N., *The Quick and the Dead: Electronic Combat and Modern Warfare*, New York: St. Martins Press, 1991.
- [68] Blake, B., (ed.), *Jane's Radar & Electronic Warfare Systems, 1997-98*, (9th ed.), London: Jane's Information Group, 1997.
- [69] Schleher, D. C., *Introduction to Electronic Warfare*, Norwood, MA: Artech House, 1990.
- [70] Chrzanowski, E. J., *Active Radar Electronic Countermeasures*, Norwood, MA: Artech House, 1990.
- [71] Neri, F., *Introduction to Electronic Defense Systems*, Norwood, MA: Artech House, 1991.
- [72] Herskovitz, D., "And the Compass Spun Round and Round: The Coming Era of Navigation Warfare," *J. Electronic Defense*, May 1997, pp. 35-39, 65.
- [73] Alterman, S. B., "GPS Dependence: A Fragile Vision for US Battlefield Dominance," *J. of Electronic Defense*, Sept. 1995, pp. 52-54.
- [74] Hardy, S. M., "Will the GPS Lose Its Way?," *J. of Electronic Defense*, Sept. 1995, pp. 56-60.
- [75] "GPS Experts Suggest Way to Avoid Terrorism," *Aviation Week and Space Technology*, Oct. 9, 1995, p. 56.

-
- [76] Herman, M., *Intelligence Power in Peace and War*, Cambridge, NY: Cambridge University Press, 1996, pp. 173–176.
 - [77] Definitions, unless noted otherwise, adapted from *Glossary of Computer Security Terms*, NCSC-TG-004, NSA “Aqua Book,” Version 1, Oct. 21, 1988.
 - [78] Howard, J. D., “An Analysis Of Security Incidents On The Internet 1989–1995,” Dissertation, Carnegie Mellon University, Apr. 7, 1997, Section 5.4., URL: <http://www.cert.org/research/JHThesis/index.html>.
 - [79] Lipson, H. F., and T. A. Longstaff, “Coming Attractions in Survivable Systems,” CERT Coordination Center, Carnegie Mellon University, 1997. URL: http://www.cert.org/research/start_page.html
 - [80] Critical indicators are specific facts about friendly intentions, capabilities, limitations, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.
 - [81] “Joint Doctrine for Operational Security,” Joint Pub 3-54, Apr. 15, 1994.

7

An Operational Concept (CONOPS) for Information Operations

Units or cells of information warriors will conduct the information operations that require coordination of technical disciplines to achieve operational objectives. These cells require the support of planning and control tools to integrate and synchronize both the defensive and offensive disciplines introduced in the last chapter.

This chapter provides a baseline concept of operations (CONOPS) for implementing an offensive and defensive joint service IO unit with a conceptual support tool to conduct sustained and structured C2W. We illustrate the operational-level structure and processes necessary to implement information operations—in support of overall military operations—on a broad scale in a military environment.

The CONOPS provides a conceptual architecture (at the functional level) for providing planning tools to implement the 16 essential capabilities identified in the U.S. Joint Warfighter Science and Technology Plan (1997) as necessary to achieve an operational information warfare capability [1].

1. *Information consistency* includes the integrity, protection, and authentication of information systems.

2. *Access controls/security services* ensures information security and integrity by limiting access to information systems to authorized personnel only. It includes trusted electronic release, multilevel information security, and policies.
3. *Service availability* ensures that information systems are available when needed, often relying upon communications support for distributed computing.
4. *Network management and control* ensures the use of reconfigurable robust protocols and control algorithms, self-healing applications, and systems capable of managing distributed computing over heterogeneous platforms and networks.
5. *Damage assessment* determines the effectiveness of attacks in both a defensive capacity (e.g., where and how bad) and an offensive capacity (e.g., measure of effectiveness).
6. *Reaction* (isolate, correct, act) responds to a threat, intruder, or network or system disturbance. Intrusions must be characterized and decision makers must have the capability to isolate, contain, correct, monitor surreptitiously, and so forth. The ability to correct includes recovery, resource reallocation, and reconstitution.
7. *Vulnerability assessment and planning* is an all-encompassing functional capability that includes the ability to realistically assess the joint war fighter's information system(s) and information processes and those of an adversary. The assessment of war-fighter systems facilitates the use of critical protection functions such as risk management and vulnerability analysis. The assessment of an adversary's information system provides the basis for joint war-fighter attack planning and operational execution.
8. *Preemptive indication* provides system and subsystem precursors or indications of impending attack.
9. *Intrusion detection/threat warning* enables detection of attempted and successful intrusions (malicious and nonmalicious) by both insiders and outsiders.
10. *Corruption of adversary information/systems* can take many diverse forms, ranging from destruction to undetected change or infection of information. There are two subsets of this function: (1) actions taken on information prior to its entry into an information system, and (2) actions taken on information already contained within an information system.

11. *Defeat of adversary protection* includes the defeat of information systems, software and physical information system protection schemes, and hardware.
12. *Penetration of adversary information system* provides the ability to intrude or inject desired information into an adversary's information system, network, or repository. The function includes the ability to disguise the penetration—either the fact that the penetration has occurred or the exact nature of the penetration.
13. *Physical destruction* of adversary's information system physically denies an adversary the means to access or use its information systems. Actions include traditional hard kills as well as actions of a less destructive nature that cause a physical denial of service.
14. *Defeat of adversary information transport* defeats any means involved in the movement of information either to or within a given information system. It transcends the classical definition of electronic warfare by encompassing all means of information conveyance rather than just the traditional electrical means.
15. *Insertion of false station/operator* into an adversary's information system provides the ability to inject a false situation or operator into an adversary's information system.
16. *Disguise of sources of attack* encompasses all actions designed to deny an adversary any knowledge of the source of an information attack or the source of information itself. Disguised sources, which deny the adversary true information sources, often limit the availability of responses, thereby delaying correction or retaliation.

The chapter is organized in typical military CONOPS format, although it provides much less detail than a specific CONOPS document generally contains. The format is intended to provide the nonmilitary reader with insight into the approach by which information warfare technology concepts are transitioned to military operations, and the range of implementation issues that must be addressed. The CONOPS is presented for a conceptual information operations support system (IOSS) that operates at multiple echelons to plan, develop, and conduct information operations as developed in the previous chapter.

Concept of Operations (CONOPS) for Information Operations Support System (IOSS)

Section 1 General

1.1 Purpose

This CONOPS describes an information operations support system (IOSS) comprised of integrated and automated tools to plan and conduct offensive and defensive information operations. The CONOPS describes methodology and identifies associated roles and responsibilities for implementing basic information operations such as those defined in the U.S. Army Field Manual for Information Operations, FM-100-6. This CONOPS is a guidance document, does not specify policy, and is intended for audiences who need a quick overview or orientation to information operations (IO).

1.2 Background

Information operations provide the full-spectrum means to achieve information dominance by: (1) monitoring and controlling the defenses of a force's information infrastructure, (2) planning activities to manage an adversary's perception, and (3) coordinating PSYOPS, deception, and intrusive physical and electronic attacks on the adversary's information infrastructure. This CONOPS provides an overview of the methodology to implement an IO cell supported by the semiautomated and integrated IOSS tools to achieve information dominance objectives. The following operational benefits are accrued:

- *Synchronization*—An approach to synchronize all aspects of military operations (intelligence, OPSEC, INFOSEC, PSYOPS, deception, information, and conventional attack) and to deconflict adverse actions between disciplines;
- *Information sharing*—The system permits rapid, adaptive collaboration among all members of the IO team;
- *Decision aiding*—An automated process to manage all IO data, provide multiple views of the data, provide multiple levels of security, and aid human operators in decision making.

1.3 Threats

The IO support system provides critical support to overall operations and is an important target of potential threats. Potential threats to the IOSS include

conventional, space-based, and electronic warfare (EW); nuclear, biological, and chemical (NBC) contaminants; terrorism; and counterinformation operations (Table 1.3.1).

Section 2 Information Operations Cell System Description

2.1 Mission

The IO support system provides an integrated, semiautomated tool to support the IO unit to conduct the planning, execution, and monitoring of

Table 1.3.1
Threats to the IO Support System

Threat Category	Threat Objectives	Means or Weapons
Conventional	Physical damage or degradation Physical destruction	Theater ballistic missiles Tactical aircraft Special operations forces
Space-based	Locate IOSS	Reconnaissance IMINT or SIGINT
Electronic warfare	Electronically damage information, processing, or communications	Airborne and ground-based electronic attack (EA) including electromagnetic pulse (EMP) and electronic warfare support measures (ESM)
Nuclear	Electronically or radiologically damage electronic equipment	Electromagnetic pulse (EMP) or radiation from nuclear weapons
NBC contaminants	Impair or degrade personnel health or viability of operators	Chemical or biological contaminants delivered by air or ground
Terrorism	Threaten personnel security	OPSEC penetration Suborn system administrators
Counterinfo operations	Disrupt, dominate, or deceive the flow of information between IO cells and associated decision-making command elements or forces	Network intrusion, exploitation, deception, disruption, or denial Network penetration (direct) or external sensor influence (indirect)

IO (offensive and defensive) activities to conduct command and control warfare (C2W). The capabilities of the support system include the following:

- Full integration of IO units between echelons;
- Near-real-time planning for IO;
- Analysis of all-source intelligence relevant to IO;
- Strategic IO indications and warnings (I&W), and tactical alerts;
- Monitoring offensive and defensive activities;
- Simulation of the effects of planned events across IO disciplines;
- Development and distribution of information operations tasking orders (ITO) to forces.

The structure of the IOSS integrated within a typical military operation is depicted in Figure 2.1.1, which illustrates the application of IOSS at two echelons. The joint force IOSS performs theater-level IO planning and allocation of IO objectives to divisions. Multiple-division-level IOSS units perform planning and assignment of mission tasks to individual war-fighting units.

The operations staff for a typical IO cell includes the following members:

- *C2W battle staff officer*—Commands the IOSS unit. Responsible to the force commander to define, plan, and execute information operations. Receives orders (allocated IO plans and strategy) from higher level echelons, and coordinates the collaborative development of IO plans with the subordinate staff. Disseminates approved operational orders (OPORDS) for information operations to task appropriate forces.
- *IO coordinator/supervisor*—Operates IO coordination workstation to parse high-level IO plans and supervise collaborative development by all clients of an integrated local plan.
- *Intel analyst*—Receives local and theater intelligence and manages semiautomated correlation of IO-relevant intelligence into common view. Maintains situation database for use by all IOSS clients. Provides I&W alerts to all IOSS users.
- *OPSEC officer*—Supervises operational security for the IO unit. Maintains physical and perimeter security for the IOSS.
- *INFOSEC officer*—Supervises information security for communications, computation, and information storage for the IOSS.
- *C2W officer*—Leads the planning, development, tasking and battle damage assessments of offensive information operations. Performs

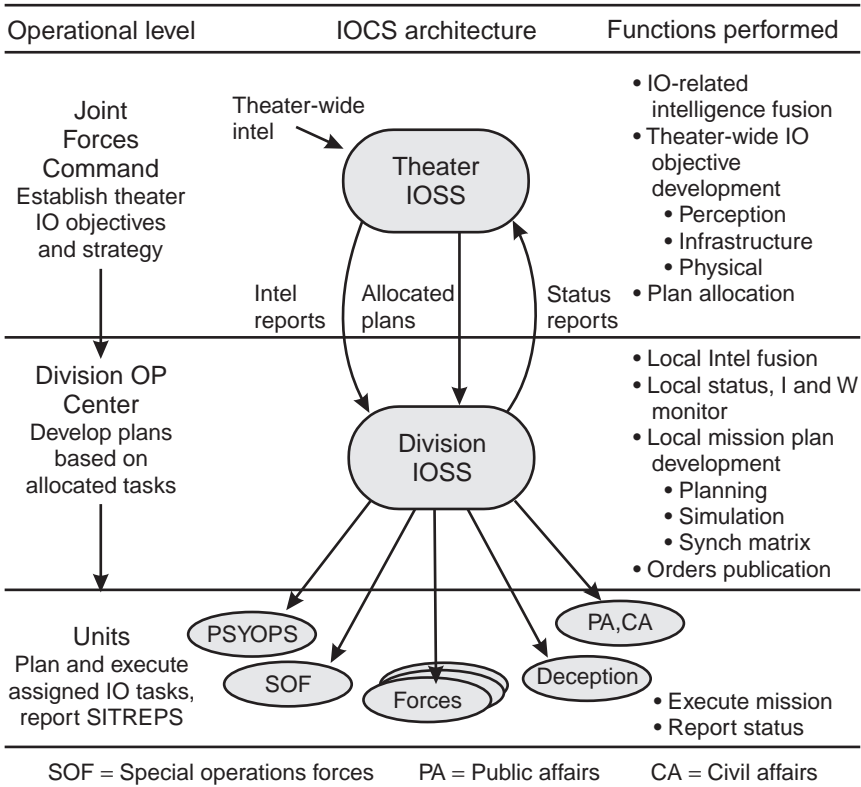


Figure 2.1.1 IOSS top-level functional architecture.

simulated attacks to evaluate alternative tactics and countermeasures; performs weapon-to-target pairings and prepares ITOs.

- *PSYOP officer*—Leads the development of PSYOP plans, coordinating themes, messages, and media to achieve the perception objectives for target audiences designated in the operational objectives. Coordinates, tasks, and assesses the performance and effects of perception management activities.
- *Deception officer*—Leads the development of military deception operations that support PSYOP, offensive IO, and intelligence collection activities. Coordinates, tasks, and assesses deception operations.
- *Public affairs and civil affairs officers*—In operations other than war (OOTW), these officers develop messages and select media for presentation to national and foreign audiences, respectively, to deliver

reliable reports (truthful and accurate). They support IO by overcoming adversary attempts to distort the truth.

- *Special operations representative*—Advises on special operations, availability, and feasibility of planned special targeting actions.

2.2 Physical Description

The task of the IOSS is to support the mission commander by planning, coordinating, and conducting information operations. IOSS is a client/server software system, hosted on computer hardware, connected through networks and long-haul communications, and sheltered within fixed or deployable facilities.

2.3 Technical Architecture

The IOSS network architecture (Figure 2.3.1) partitions IO mission analysis and planning activities from tactical planning and tasking. Operator workstations (clients) coordinate activities on a secure local network that includes three servers.

- *Situation server*—Maintains a dynamic database of a group's own and enemy force's critical infrastructure and information infrastructure based upon current intelligence. Maintains network maps, performance characteristics, vulnerability information, geographic information system (spatial and geophysical maps), and other intelligence data. The associated intelligence workstation performs the automatic correlation of multisource intelligence to create and maintain the current tactical database regarding the targeted infrastructure (networks, nodes) and situation (perception, infrastructure effectiveness, and functional capability).
- *Mission server*—Maintains a database of current mission activities, tasking, resources status, and indications and warnings.
- *Integrated simulation server*—Maintains defensive simulations to assess the risk to the group's own information infrastructure. Maintains offensive simulations to analyze tactics, countermeasures, and weapons applied to targeted information networks. The simulations provide performance and effectiveness metrics to quantify the functional effects, collateral damage, and risk associated with information operations.

The system accepts operational orders (OPORDS) and intelligence data from higher level echelons, and provides output to flow-down OPORDS,

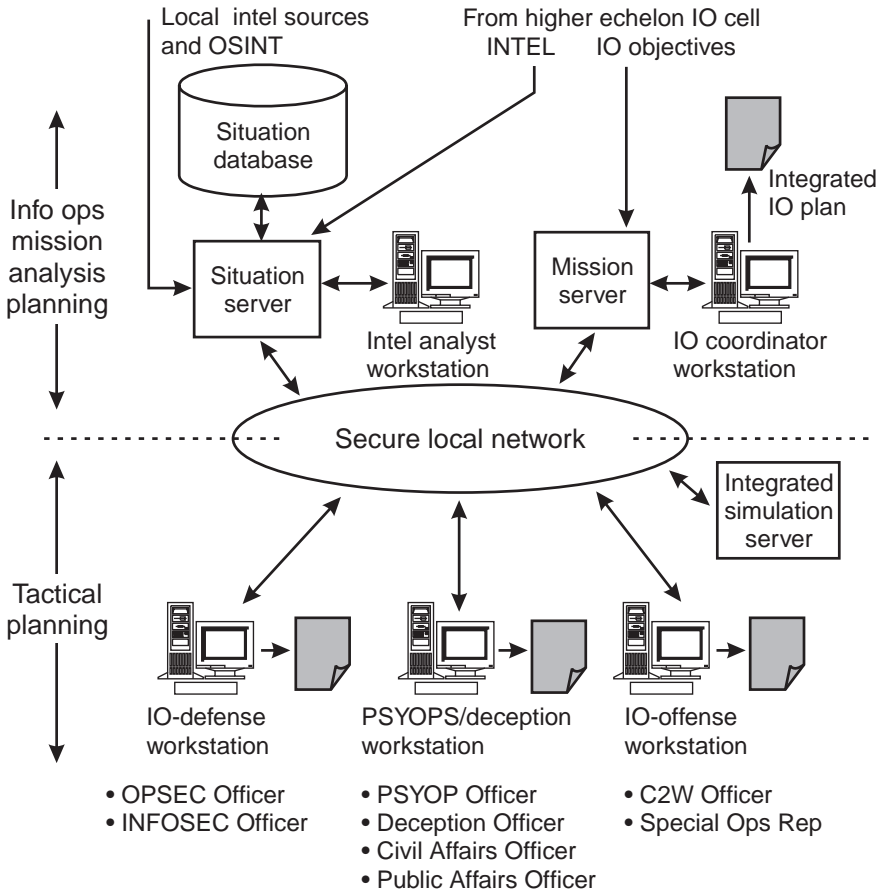


Figure 2.3.1 IOSS network configuration.

ITOs, and intelligence to lower level echelons. Table 2.3.1 enumerates the components (client workstations and servers) and processing functions of the IOSS.

Section 3 Operations

3.1 General

The IOSS prepares and disseminates ITOs to multidisciplinary forces in a fashion similar to the air tasking order (ATO) process for tasking aircraft sorties. The ITO process is continuous and dynamic, with cycle times (from planning

Table 2.3.1
IOSS Components and Processing Functions

IOSS Element	Functions	Inputs	Outputs
Mission server and mission workstation	<p>Accept allocated mission objectives and plans from higher level echelons</p> <p>Create local plans and synchronization matrices via collaborative development across all workstations</p> <p>Display current situation, indications, and warnings alerts</p> <p>Display results of simulated actions for alternative plans</p> <p>Display assessments of actual and simulated results of IO actions</p> <p>Disseminates plans to lower level echelons and/or units</p>	<p>Allocated mission objectives and plans from higher level echelons</p> <p>Plan inputs from local workstations</p> <p>Results of integrated simulations</p>	<p>Integrated IO plan</p> <p>IO task orders (ITOs)</p> <p>Operational orders (OPORDS)</p> <p>Synch matrix</p> <p>Real-time IO status</p> <p>Absolute</p> <p>Relative to plan</p> <p>I&W display</p>
Situation server and workstation	<p>Accept local and theater intelligence source data</p> <p>Correlate and combine (fuse) IO-related intelligence</p> <p>Maintain current situation database</p> <p>Display situation and drill-down displays for IO data</p> <p>Provide intelligence correlation and mapping tools</p>	<p>All-sources of intelligence</p> <p>Local OSINT</p> <p>Local map and GIS data layers</p> <p>Targeted network and decision-making models</p>	<p>Correlated intelligence display</p> <p>IO activities display</p> <p>Battle damage assessments (BDAs)</p>
Integrated simulation server	<p>Support client-requested simulation of effects of information operations on targeted systems</p> <p>Perform perception, infrastructure, and physical-level simulations</p> <p>Score results of simulated attack effects</p>	<p>Simulation parameter baselines and updates</p> <p>Simulation input data</p>	<p>Simulation results</p>
IO-defense workstation	<p>Set up, run, and display results of net attack, electronic attack, and physical attack simulations</p> <p>Develop OPSEC, INFOSEC plans</p>	<p>Situation data</p> <p>Threat data</p> <p>Vulnerability data</p> <p>I&W filter parameters</p>	<p>Risk analyses</p> <p>Defense plan</p> <p>I&W alerts</p>

Table 2.3.1 (continued)

IOSS Element	Functions	Inputs	Outputs
PSYOPS/ deception workstation	Develop perception management plan Set up, run, and display results of perception-level simulations	Perception objectives Force plans OSINT	Perception plan Perception status (versus plan)
IO-offense workstation	Provide decision support for target analysis, target-weapon pairing Create target nomination list and targeting materials (folders) Set up, run, and display results of net attack, electronic attack, and physical attack simulations	Weapon and delivery (physical, EA, and net means) availability data	Attack and effect analyses Attack plan Target folders

through attack assessment) ranging from seconds to 24 hours depending upon the weapons and tactics employed in offensive strikes.

3.2 Organization

The IOSS may be operated in a hierarchical organization, with higher level echelons issuing ITOs for distribution to lower level IO units for assignment and distribution of detailed tasks to combat units.

3.3 Operational Process

Defensive planning is performed by the OPSEC and INFOSEC officers, who maintain a complete model of friendly networks and status reports on network performance. Performance and intrusion detection information is used to initiate defensive actions (e.g., alerts, rerouting, service modification, initiation of protection or recovery modes). The defensive process is continuous and dynamic, and adapts security levels and access controls to maintain and manage the level of accepted risk established at the operational level.

The flow of offensive planning activities performed by the IOSS is illustrated in Figure 3.3.1, which is organized by the three levels of planning.

- *Perceptual level*—The operational plan defines the intent of policy and operational objectives. The operational and perception plans, and

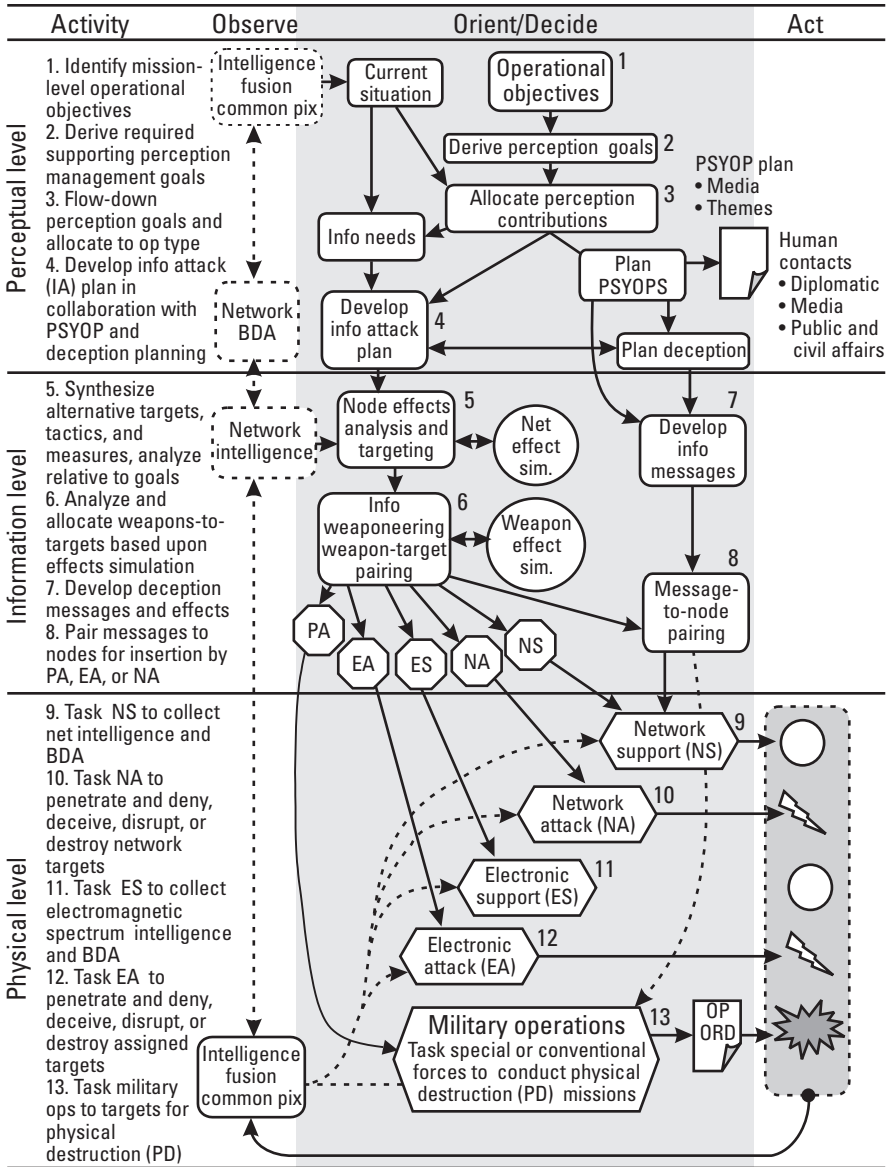


Figure 3.3.1 IOSS activity sequence for offensive operations.

desired behaviors of the perception targets (audiences), are defined at this level.

- *Information infrastructure level*—The functional measures for achieving perception goals, in the perception target's information infrastructure, are developed at this level.
- *Physical level*—The specific disciplines that apply techniques (e.g., physical attack, network attack, electronic support) are tasked at this level.

The IOSS performs the decide function of the OODA loop for information operations, and the functional flow is organized to partition both the observe/orient function that provides inputs and the operational orders (OPORDS) that initiate the attack actions. The sequence of planning activities proceeds from the perceptual to the physical level, performing the flow-down operations defined in the following subsections.

It is important to recognize that IO does not stand alone—it supports overall military operations (not the other way around). This process flow identifies only the IO activities and their integration with non-IO operations. The operational objective (function 1 in the flow) and information attack plan (function 4) are linked to overall operations planning cells. Likewise, the weapon-target pairing functions within weaponeering (function 6) and tasking of forces is also coordinated. The diagram shows a single logical flow for purposes of illustration, although the IOSS performs fully interactive planning, targeting, weaponeering, and tasking between all functions and deconflicts mutually exclusive courses of action.

3.3.1 Perception Operations The operational objectives and current situation are used to develop the desired perception objectives, which are balanced with all other operational objectives. A C2W concept of operations and intelligence-supplied C2 architecture and order of battle (of the adversary) are provided by operations at this level. The IOSS develops IO plans (for information attack, PSYOPS, and deception activities) that are synchronized with theater operational plans. Public and civil affairs officers and diplomats are provided the perception-level plan to coordinate perception messages. Truthful PSYOPS plans and deception plans (intended for different audiences) are then flowed down to the information level for generation of compatible messages for broadcast and insertion, and the information attack plan is flowed down for targeting.

3.3.2 Information Infrastructure Operations At this level, the targeted information infrastructure (II) (at all ISO levels) is analyzed and tactics are developed to achieve the attack objectives by selecting the elements of the II to be attacked (targeted). The product is a prioritized high-value target (HVT) list.

Using nodal analysis, targets are nominated for attack by the desired functional effect to achieve flowed-down objectives: denial, disruption, deceit, exploitation, or destruction. Collaborative evaluation of alternative countermeasures and target nominations is performed by simulation. In all cases, the availability of access to the target (at any level) is a critical factor in the feasibility of alternatives. Accessibility is therefore a determinant in the selection of a course of action. The HVT is further prioritized by payoff and contribution to operational objectives.

Once the analysis develops an optimized functional model of an attack approach that achieves the objectives, weapons (techniques) are selected to accomplish the functional effects. This weaponeering process pairs the techniques (weapons) to targets (e.g., links, nodes, processing, individual decision makers). It also considers the associated risks due to attack detection and collateral damage and assigns intelligence collection actions necessary to perform BDA to verify the effectiveness of the attack. Attack disciplines of physical attack (PA), electronic attack (EA), electronic support (ES), network attack (NA), and network support (NS) are issued tasking to perform the techniques against designated targets.

3.3.3 Physical Level At the physical level, the attacking disciplines plan and execute the physical-level attacks.

- *Physical attack (PA)*—Operational units (e.g., special operations, conventional forces, attack aircraft wings) are assigned physical destruction tasks. They also plan and conduct PSYOPS and deception operations in harmony with plans flowed down from higher levels.
- *Electronic attack (EA)*—Electronic warfare units (space, air, ground, and sea) perform electromagnetic spectrum attacks using directed energy to deny, disrupt, and soft or hard kill targets.
- *Electronic support (ES)*—Electronic warfare units conduct supporting operations to monitor, intercept, and exploit the electromagnetic spectrum for real-time precision targeting and intelligence. This includes SIGINT collections and tactical electronic support measures (ESM).
- *Network attack (NA)*—Network warfare units perform attacks over a computer network infrastructure, contacting, penetrating, and/or accessing targeted information systems. This activity may require coordination with special or air forces to gain some degree of physical access to support network access.

- *Network support (NS)*—Network warfare units conduct supporting operations to monitor and analyze targeted information systems over the GII.

3.4 Target Sets

The IOSS targets all elements of the command and control infrastructure, including those categories identified in Table 3.4.1.

3.5 Deployment

The IOSS can conduct operations from an existing base outside the theater of operations, from an afloat location, or at a bare-base location in the theater of operations. Until advance support units (intelligence, command and control) arrive in the theater, the IOSS may plan information operations with information from reach-back sources or threat information derived from early-deployed systems.

3.6 Employment

As the phase of readiness in the theater and level of conflict change, the demand for ITOs will change, and the IOSS will adapt to operations in initial, buildup, and sustainment phases (Table 3.6.1).

Section 4 Command Relationships

4.1 Command Relationship

The IO unit employing the IOSS conducts C2W under the authority of the joint force commander, and in accordance with rules of engagement (ROE) established for peace and wartime states.

4.2 Organizational Structure

As the situation evolves and transitions to wartime ROE, the IOSS may delegate some aspects of IO execution to lower, more time-responsive levels.

4.3 Intelligence Support

IOSS requires intelligence support to detect, locate, characterize, and map the threat-critical infrastructure at three levels, using the sources identified in Table 4.3.1.

Table 3.4.1
IOSS Target Set Matrix

Target Categories		Representative Targets	IO Targeting Applications	
			Vulnerabilities Targeted	Representative Attack Applications
Complex net-worked systems	Strategic and operational command and control	Strategic and theater C2 nets	Network relay nodes	PA—Strategic attack on sensors, nodes (processing), communications, and electrical power NS—Exploit accessible networks
		I&W networks	Commercial electronic components	
	National air traffic control	National telecommunications, electrical power	Commercial telecommunication links and nodes	Supporting electrical power grids Active sensor emissions Passive sensor apertures Traffic on tactical broadcasts
National telecommunications, electrical power				
Limited linked systems	Tactical command and control	Tactical data and communication links (microwave relays, land line, and SATCOM)		
		Integrated air defense (IADS) sensors and nets		
		Navigation and timing systems		
Limited linked systems	Tactical weapon systems	Tactical broadcasts		
		Weapon platforms	Navigation and communication C2 processing Weapons electronics	ES locate platforms and active sensors EA deceive navigation EA and NA disrupt sensing, links, and processing PA destroy
		Fire control systems	Sensors Guidance links Electronic processing	
Limited linked systems	Tactical weapon systems	Guided missiles	Radar and EO sensors Data links Guidance electronics	ES locate, identify state EA disrupt and destroy via DEW
		Precision guided munitions	Links (EO, laser, RF) Electronics	ES provide warning EA disrupt and destroy via DEW

Table 3.6.1
IOSS Employment Phases

Phase	Initial	Buildup	Sustainment
Operations	Rapid assessment of threats and network mapping—initial targeting	Critical threat assessments and initial node targeting with limited forces	Sustained and continuous IO with ITO tasking to full complement of forces
Deployment	Existing bases	Bare-base location in-theater, supported by re-motes at existing base	Locations in-theater fully linked between echelons
Capacity	Standard staff (10–15) IO sorties: 1,000/day	Standard staff (20–25) IO sorties: 5,000/day	Standard staff (25–35) IO sorties: 10,000/day

Table 4.3.1
IOSS Intelligence Support

Intelligence Level	Intelligence Needs	Typical Sources
Perceptual	Perception and decision-making processes Decision authorities Perception situation	HUMINT OSINT SIGINT
Information infrastructure	Infrastructure network maps Performance models Information states and battle damage assessments Information vulnerabilities Functional battle damage assessments	Net support Electronic support SIGINT
Physical	Location and composition of decision-making process elements Locations of network nodes and lines of communication Physical vulnerabilities and support dependencies (e.g., power, water) Physical states and battle damage assessments	SIGINT Electronic support IMINT

Section 5 Security

5.1 *General*

IO staff operations will be implemented and operated at multiple levels of security (MLS). Security safeguards consist of administrative, procedural, physical, operational, and/or environmental, personnel, and communications security; emanation security; and computer security (i.e., hardware, firmware, network, and software), as required.

5.2 *Physical Security*

The components of IOSS are deployed to a variety of operational environments, ranging from secure vaults in the continental United States (CONUS) to overseas bare-base locations, and connected by a range of communications systems. Security for the system will depend on physical, administrative, personnel, and procedural controls.

5.3 *Emanations Security (EMSEC) and EMP Hardening*

The IOSS equipment, shelters, and facilities will meet applicable requirements to prevent compromising electromagnetic emanations (both radiated and conducted) that would reveal traffic, activities, or internal information on IO. The equipment, shelters, and facilities will also maintain electromagnetic shielding, grounding, and other measures to protect from electromagnetic pulse attacks in accordance with applicable threat documents.

5.4 *Information Security (INFOSEC)*

All classified information will be protected according to the requirements contained in appropriate information security program regulations. Encryption, key distribution, access controls, and trusted network security will be implemented in accordance with applicable INFOSEC requirements for joint C4I systems. The INFOSEC officer (or computer systems security officer [CSR]) is responsible for operational security.

5.5 *Operations Security (OPSEC)*

The IOSS critical elements, threats, and vulnerabilities for any deployment will be identified. OPSEC procedures will be applied to protect the system throughout its life cycle. Operations and computer systems security officers (OPSEC and CSR) are responsible for operational security.

Section 6 Training

6.1 General

Training is the key to successful integration of IO into joint military operations. Training of IO battle staff personnel is required at the force and unit levels, and is a complex task requiring mastery of the related disciplines of intelligence, OPSEC, PSYOPS, deception, electronic warfare, and destruction.

6.2 Formal Training

The fielding and operation of an IO cell or battle staff may require formal courses or unit training for the diverse personnel required. Training audiences include instructors, IO operators, IO battle staff cadre, system support, a broad spectrum of instructors in related disciplines, and senior officers.

6.3 Simulation Training

IO units must conduct routine training with simulation tools that realistically simulate effects at the perceptual, information infrastructure, and physical levels. Effectiveness of IO activities, both defensive and offensive, will be scored, and simulation debriefings will provide assessments of training effectiveness.

6.4 Exercise Participation

IO units should participate in formal and informal exercises to develop and evaluate skills and interoperability with combat units. Exercise training should be as realistic as possible, including accurate time constraints, system errors, information flow rates, and time delays inherent in an operational environment.

Section 7 Policy, Doctrine, and Instructions

7.1 General

The operations described in this CONOPS are performed within the policy and doctrinal guidance provided by military documents referenced below.

7.2 Select Bibliography

Command and Control Warfare Policy

CJCSI 3210.01, Joint Information Warfare Policy, Jan. 2, 1996.

DOD Directive S-3600.1, Information Warfare.

CJCSI 3210.03, Joint Command and Control Warfare Policy (U), Mar. 31, 1996.

JCS Pub 3-13.1, Joint Command and Control Warfare (C2W) Operations, Feb. 7, 1996.

Information Operations

“Information Operations,” Air Force Basic Doctrine (DRAFT), Aug. 15, 1995.

FM-100-6, Information Operations, Aug. 27, 1997.

TRADOC Pam 525-69, Concept for Information Operations, Aug. 1, 1995.

Intelligence

Joint Pub 2-0, Doctrine for Intelligence Support to Joint Operations, May 5, 1995.

AFDD 50, Intelligence, May 1996.

FM 34-130, Intelligence Preparation of the Battlefield, July 8, 1994.

PSYOPS, Civil and Public Affairs

JCS Pub 3-53, “Doctrine for Joint Psychological Operations,” AFDD 2.5-5, Psychological Operations, Feb. 1997.

FM 33-1, Psychological Operations, Feb. 18, 1993.

FM 41-10, Civil Affairs Operations, Jan. 11, 1993.

FM 46-1, Public Affairs Operations, July 23, 1992.

Operational Deception

CJCSI 3211.01, Joint Military Deception, June 1, 1993.

JCS Pub 3-58, Joint Doctrine for Operational Deception, June 6, 1994.

AR 525-21, Battlefield Deception Policy, Oct. 30, 1989.

FM 90-2, Battlefield Deception [Tactical Cover and Deception], Oct. 3, 1988.

FM 90-2A (C), Electronic Deception, June 12, 1989.

Information Attack

FM 34-1, Intelligence and Electronic Warfare Operations, Sept. 27, 1994.

FM 34-37, Echelon Above Corps Intelligence and Electronic Warfare Operations, Jan. 15, 1991.

FM 34-36, Special Intelligence Forces Intelligence and Electronic Warfare Operations, Sept. 30, 1991.

Operational Security (OPSEC)

DOD Directive 5205.2, Operations Security Program, July 7, 1983.

Joint Pub No. 3-54 Joint Doctrine for Operations Security.

AFI 10-1101, (Air Force), Operational Security Instruction.

AR 530-1, (Army) Operations Security, Mar. 3, 1995.

Information Security (INFOSEC)

DoD 5200.1-R, Information Security Program Regulation.

AFPD 31-4, (Air Force) Information Security, Aug. 1997.

AR 380-19, (Army) Information System Security, Aug. 1, 1990.

Endnotes

- [1] “Joint Warfighter Science and Technology Plan,” U.S. DoD Office of Secretary of Defense, 1997, Section I “Information Warfare,” <http://www.fas.org/spp/military/docops/defense/jwsp> on Dec. 12, 1997.

8

Offensive Information Operations

This chapter introduces the functions, tactics, and techniques of malevolence against information systems. Offensive information operations target human perception, information that influences perception, and the physical world that is perceived. The *avenues* of these operations are via perceptual, information, and physical means.

Offensive information operations are malevolent acts conducted to meet the strategic, operational, or tactical objectives of authorized government bodies; legal, criminal, or terrorist organizations; corporations; or individuals. The operations may be legal or illegal, ethical or unethical, and may be conducted by authorized or unauthorized individuals. The operations may be performed covertly, without notice by the target, or they may be intrusive, disruptive, and even destructive. The effects on information may bring physical results that are lethal to humans.

Offensive operations are uninvited, unwelcome, unauthorized, and detrimental to the target; therefore, we use the term *attack* to refer to all of these operations.

For these reasons, this chapter must be considered within the context of understanding offense to prepare for defense: security design must be preceded by an understanding of the attacks it must face. This chapter necessarily precedes the chapter on defensive operations, developing the spectrum of attacks, while the next provides the complementary elements of protection and reaction.

Offensive information attacks have two basic functions: to capture or to affect information. (Recall that information may refer to processes or to data/information/knowledge content.) These functions are performed together

to achieve the higher level operational and perceptual objectives. In this chapter, we introduce the functions, measures, tactics, and techniques of offensive operations.

- *Functions*—The fundamental functions (*capture* and *affect*) are used to effectively gain a desired degree of control of the target's information resources. Capturing information is an act of theft of a resource if captured illegally, or technical exploitation if the means is not illicit. The object of capture may be, for example, a competitor's data, an adversary's processed information, another's electronic cash (a knowledge-level resource with general liquidity), or conversations that provide insight into a target's perception. Affecting information is an act of intrusion with intent to cause unauthorized effects, usually harmful to the information owner. The functional processes that capture and affect information are called *offensive measures*, designed to penetrate operational and defensive security measures of the targeted information system.
- *Tactics*—The operational processes employed to plan, sequence, and control the countermeasures of an attack are the attack tactics. These tactics consider tactical factors, such as attack objectives; desired effects (e.g., covertness; denial or disruption of service; destruction, modification, or theft of information); degree of effects; and target vulnerabilities.
- *Techniques*—The technical means of capturing and affecting information of humans—their computers, communications, and supporting infrastructures—are described as techniques.

In addition to these dimensions, other aspects, depending upon their application, may characterize the information attacks.

- *Motive*—The attacker's motive may be varied (e.g., ideological, revenge, greed, hatred, malice, challenge, theft). Though not a technical characteristic, motive is an essential dimension to consider in forensic analysis of attacks.
- *Invasiveness*—Attacks may be passive or active. Active attacks invade and penetrate the information target, while passive attacks are noninvasive, often observing behaviors, information flows, timing, or other characteristics. Most cryptographic attacks may be considered passive

relative to the sender and receiver processes, but active and invasive to the information message itself.

- *Effects*—The effects of attacks may vary from harassment to theft, from narrow, surgical modification of information to large-scale cascading of destructive information that brings down critical societal infrastructure.
- *Ethics and legality*—The means and the effects may be legal or illegal, depending upon current laws. The emerging opportunities opened by information technology have outpaced international and U.S. federal laws to define and characterize legal attacks. Current U.S. laws, for example, limit DoD activities in peacetime. Traditional intelligence activities are allowed in peacetime (capture information), but information attacks (affect information) form a new activity (not necessarily lethal, but quite intrusive) not covered by law. Offensive information operations that affect information enable a new range of nonlethal attacks that must be described by new laws and means of authorization, even as blockades, embargoes, and special operations are treated today. These laws must define and regulate the authority for transitional conflict operations between peace and war and must cover the degree to which “affect” operations may access nonmilitary infrastructure (e.g., commercial, civilian information). The laws must also regulate the scope of approved actions, the objective, and the degree to which those actions may escalate to achieve objectives. The ethics of these attacks must also be considered, understanding how the concepts of privacy and ownership of real property may be applied to the information resource. Unlike real property, information is a property that may be shared, abused, or stolen without evidence or the knowledge of the legitimate owner.

This chapter describes the technical elements of offensive information operations, beginning with a matrix of the fundamental offensive actions (Section 8.1) that may be targeted at each of the three layers of the IW model introduced in Chapter 5. Next, available weapons are defined (Section 8.2), and the attack tactics are developed for net and C2 warfare (Sections 8.3 and 8.4, respectively). Targeting and “weaponizing” processes are described in Section 8.5 before describing information-level weapons (Section 8.6) and physical-level weapons (Section 8.7).

The chapter concludes with an overview of the concepts for modeling and measuring the performance of offensive information operations and their effects (Section 8.8).

8.1 Fundamental Elements of Information Attack

Before introducing tactics and weapons, we begin the study of offense with a complete taxonomy of the most basic information-malevolent acts at the functional level. This taxonomy of attack countermeasures may be readily viewed in an attack matrix formed by the two dimensions:

- Target level of the IW model: perceptual, information, or physical;
- Attack category: capture or affect.

The attack matrix (Figure 8.1) is further divided into the two avenues of approach available to the attacker:

1. *Direct, or internal, penetration attacks*—Where the attacker penetrates [1] a communication link, computer, or database to capture and exploit internal information, or to modify information (add, insert, delete) or install a malicious process;
2. *Indirect, or external, sensor attacks*—Where the attacker presents open phenomena to the system's sensors or information to sources (e.g., media, Internet, third parties) to achieve counterinformation objectives. These attacks include insertion of information into sensors or observation of the behavior of sensors or links interconnecting fusion nodes.

In C2W, indirect attacks target the observation stage of the OODA loop, while direct attacks target the orient stage of the loop [2]. The attacker may, of course, orchestrate both of these means in a *hybrid* attack in which both actions are supportive of each other. An indirect attack may, for example, divert the attention of a sensor so a direct attack can successfully penetrate a targeted system (indirect supports direct attack). Alternatively, a direct attack on a network may force a command system to rely on a single sensor that is deceived by an indirect attack (direct supports indirect attack).

Two categories of attacks that affect information are defined by the object of attack.

- *Content attacks*—The *content* of the information in the system may be attacked to disrupt, deny, or deceive the user (a decision maker or process). In C2W information operations, attacks may be centered on changing or degrading the intelligence preparation of the battlefield (IPB) databases, for example, to degrade its use in a future conflict.

Objective Effect:	CAPTURE		AFFECT					
	Privacy is breached		Integrity of data is invalidated Availability of services is degraded					
Security Property Attacked:	<i>Indirect</i> Observe, Model, Infer	<i>Direct</i> Penetrate and Observe	<i>Indirect</i> Cause effects through the sensors or over the open network without penetration of the target			<i>Direct</i> Penetrate and affect targeted infrastructure and affect		
Avenue:								
Offensive Act:	Capture Information Resource		Deceive	Disrupt, Deny	Destroy	Deceive	Disrupt, Deny	Destroy
Level of Attack (IW Model)								
Perceptual	Observe open behaviors, statements, cultural influences, and biases to infer decision processes and perception	Observe closed conversations, decisions, actions by HUMINT access	PSYOPS activities provide information to manage human perception (Messages may be delivered by direct human discourse, or via the information infrastructure, such as the broadcast media or Internet)			Counterintelligence and covert operations manage perception by penetration of target audience with human agencies to convey perception themes – and to implement lower-level countermeasures (e.g. suborned systems administrator with access)		
Information Infrastructure	Passive intercept of message traffic Non-intrusive mapping of network topology Cryptographic analysis	Network attack and penetrate to secure unauthorized access to data Trojan horse program Install sniffer	Issue deceptive e-mail message Conduct deceptive network behavior	Deny network data collection service by flood attack that disrupts access to public sources Insert open message traffic and data that diverts attention and processing resources Insert sensor data that upsets guidance or control process	Insert Trojan horse with deception action Modify, corrupt data by viral agent	Insert malicious code (e.g., virus or worm) to deny or disrupt service in single host computer or across an entire network		
Physical	Intercept van Eck radiation from CRT monitor Inductive wiretap Search open trash	Capture (theft) of equipment, cryptographic keys, physical keys, storage media Wiretap	Deceive user to capture security relevant data ("Social Engineering")	Theft or capture of critical components Make available erroneous data Masquerade or spoof user to induce disruptive actions	Penetrate physical security to capture security relevant data	Physical bombing of facilities or supporting infrastructure Electronic attack (EA) on system components		

Figure 8.1 Attack Matrix categorizes information countermeasures by affect and IW attack level.

During conflict, content attacks are focused on real-time data and the derived information and knowledge.

- *Temporal attacks*—The information process may be affected in such a way that the *timeliness* of information is attacked. Either a delay in receipt of data (to delay decision making or desynchronize processes) or deceptive acceleration by insertion of false data characterizes these attacks.

8.2 The Weapons of Information Warfare

As well as perceptual-level attacks described earlier, information operations may apply physical or information-level weapons [3], using physical or information-level weapon systems to deliver them. The information weaponeer can cause the desired functional effects (capture or affect) described in the last section by a variety of means at the physical or the pure information levels [4].

A simple weapon matrix (Table 8.1) illustrates a representative variety of non-nuclear weapons and available delivery systems that may be considered by weaponers. The matrix, while not enumerating all weapon types, illustrates the dimensions of attack approaches (physical, electronic, or network) and delivery systems that must be considered. The matrix indicates the subsequent sections in this chapter that describe each weapon category.

8.3 Network Attack Tactics

Distributed, networked computer systems form the heart of emerging information infrastructures, and attacks on these networks, are of the “direct” form—seeking to penetrate security to achieve their objective. In this section we introduce the vulnerabilities of complex networks, the tactics that exploit these vulnerabilities, and the tools that carry out those attacks. At the close of the section, representative attacks on Internet services are summarized to illustrate the range of attacks that have been observed.

8.3.1 Network Attack Vulnerabilities and Categories

Howard has developed a basic taxonomy of computer and network attacks for use in analyzing security incidents on the Internet [5]. The taxonomy structure is based on characterizing the attack *process* (Figure 8.2) by five basic components that characterize any attack.

Table 8.1

Information Weapon Matrix Illustrates Several Representative Weapon Categories and Associated Delivery Alternatives

Weapon category:	Kinetic energy	Chemical-biological (CBW)	Directed energy	Pure information
Chapter section:	Section 8.7.1	Section 8.7.2	Section 8.7.3	Section 8.6
Attack category:	Physical	Physical	Electronic	Network
Surface delivery: Human insertion Robotic insertion Artillery	Kinetic package bomb Mortar-, artillery-delivered munition	Package CBW weapon Mortar-, artillery-delivered CBW munition	EMP, HPM package bomb Ground jammer Dispensable jammer	Manufactured logic flaw, trap door, logic weapon Suborned system administrator Saboteur
Air delivery: Missile Aircraft Submunition	Precision guided kinetic munitions Antiradiation missiles	Precision guided counterelectronics CBW Antipersonnel CBW	Airborne HPM, HEL beam Missile, artillery EMP, HPM bomb	
Space delivery: Reentry Energy beam	Reentrant non-nuclear weapons Kinetic kill vehicle against space communications	Reentrant CBW weapons	Space-based HPM, HEL, or particle beam Space-based jamming of space communications	
Network delivery: Manual attack Software agent attack				Logic weapon (Software, hardware, firmware)

Note: This table does not include nuclear weapons. Delivery complexity increases in descending rows (e.g., surface delivery is the least complex, and network the most).

CBW—chemical-biological weapon

HPM—high power microwave

EMP—electromagnetic pulse

HEL—high-energy laser

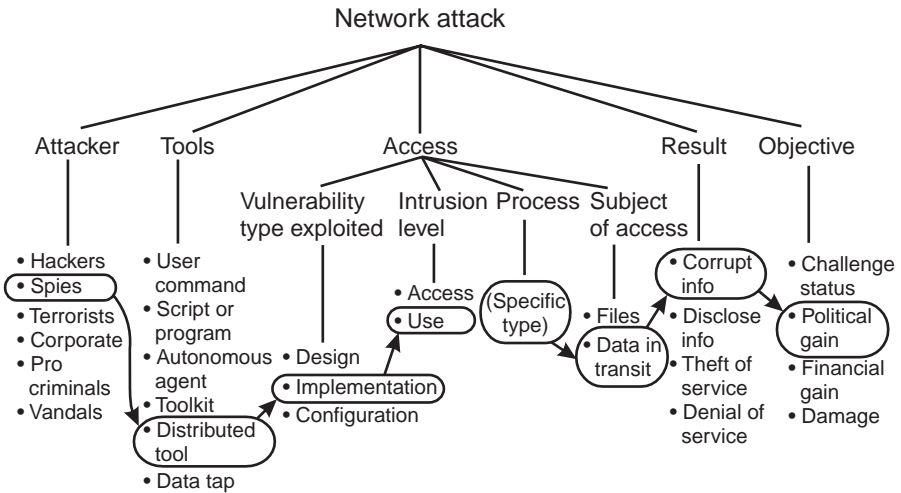


Figure 8.2 Process-based taxonomy (developed by Howard [6]).

1. *Attackers*—Six categories of attackers are identified (and motivations are identified separately, under objectives): hackers, spies, terrorists, corporate, professional criminals, and vandals.
2. *Tools*—The levels of sophistication of use of tools to conduct the attack are identified.
3. *Access*—The access to the system is further categorized by four branches.
 - *Vulnerability exploited*—Design, configuration (of the system), and implementation (e.g., software errors or bugs [7]) are all means of access that may be used.
 - *Level of intrusion*—The intruder may obtain unauthorized *access*, but may also proceed to unauthorized *use*, which has two possible subcategories of use.

Use of processes—The specific process or service used by the unauthorized user is identified as this branch of the taxonomy (e.g., SendMail, TCP/IP).

Use of information—Static files in storage or data in transit may be the targets of unauthorized use.

4. *Results*—Four results are considered: denial or theft of service, or corruption or theft (disclosure) of information.
5. *Objectives*—Finally, the objective of the attack (often closely correlated to the attacker type) is the last classifying property.

(This taxonomy is limited to network attacks using primarily information layer means, and can be considered a more refined categorization of the attacks listed in the information-layer row of the attack matrix presented earlier in Section 8.1.)

Howard has constructed the taxonomy such that any simple attack can be categorized as a process, composed of the flow through the elements in the taxonomy. Illustrated in the figure is the process thread of a network attack (state-supported agents are attackers) in which distributed (multiple-site) tools are used to exploit implementation vulnerabilities to gain use of the system. A specific system process is used to corrupt information in data packets in transit through the targeted computer to achieve a political objective of the supporting nation state.

This taxonomy clearly distinguishes the source (who), the objective (why), and the result (what) from the means (how). Each of these components is required to effectively detect, understand, and respond to attacks. The taxonomy is useful for real-time detection systems (discussed in Chapter 9) and is necessary for investigation and prosecution of attackers.

The intrusion-level and access subject activities can be further defined for any given process, such as the more detailed categorization of attacks against messaging systems adapted from Sadeghiyan (Table 8.2) [8].

8.3.2 Network Attack Processes

We have identified a wide variety of attack categories in the attack matrix in Section 8.1, which are implemented by tactical sequences of operations. The tactics of typical network attack operations reported by the CERT coordination center include a general sequence.

1. Survey and “map” the topology of the computer network (described as NETINT in Chapter 4, and the process of intelligence preparation of infospace);
2. Select targets and gain access to the networked system, and expand surveillance;
3. Increase or expand access;
4. Launch the objective action.

Table 8.2
Primary Active Threats to Network Messaging

Intrusive Action	Functional Objective	Description
Access	Unauthorized access	Invalid user gains access to system, unauthorized user gains access at a level higher than authorized
Denial	Denial of service	Disruption of message system, rendering it completely inoperable or reduced in operating capacity to some degree
Intermessage	Masquerade (spoofing)	Invalid user impersonates valid user to gain access, then misuses facility, pretends to originate message, or falsely acknowledges receipt of message
	Message modification	Message integrity (e.g., a component, address, content, labeling) is compromised while in transit
	Message replay	Valid message is repeated for purposes of exploitation
	Information leakage	Transmission monitoring to measure traffic level, traffic source destination, or content while in transit
Intramessage	Repudiation	Message system denies origin, submission, or delivery
	Security context violation	Security context is broken and message is submitted, delivered, or transferred in breach of security policy
Data storage	Routing modification	Corruption of a routing directory
	Message preplay	Delivery of a deferred message prior to authorized delivery
	Information corruption	Message integrity is compromised while in storage

A functional description of the general network attack tactics is now provided, rather than the hundreds of specific platform (e.g., SUN, DEC, HP,

IBM) or operating system-specific (e.g., UNIX, Windows NT) details that are described in CERT coordinating center alerts [9] or in a variety of texts on network system security [10–12].

The basic pattern for attacking relatively unsecured networked UNIX computers in the 1980s was revealed in a widely publicized case described in some detail in *The Cuckoo's Egg* [13]. Those early manual attacks consisted of (Figure 8.3) two general phases.

In the first phase (initial intrusion), attackers in Hannover, Germany, used a modem to establish direct connection to a network computer, exploiting simple GUEST login facilities by guessing passwords or using default passwords (e.g., “GUEST”) on computers where defaults were not changed. Once logged onto a vulnerable machine on the network, accounts and structure of the system could be quickly explored using UNIX facilities (e.g., “finger” operations) to search for unused accounts and vulnerabilities for use in subsequent intrusions. A covert account would be established for subsequent access.

The second (exploitation) phase used the proven penetration method to gain access, and checked for current users logged onto the system (to determine if administrators were on-line and capable of detecting the intrusion). If clear of surveillance, administrative-level access was gained by exploiting a UNIX vulnerability, and then the attacker’s version of control software was installed. Once in control, the intruder searched directories, located information of

Two phase attack strategy

Phase 1—Penetrate

- Search for passwords
- Gain access
- Find unused accounts
- Establish covert access account

Phase 2—Penetrate and act

- Gain entry
- Check for surveillance
- Gain system control
- Attack
 - Search directories
 - Acquire useful data
 - Search e-mail (evidence of detection)
 - Destroy surveillance, evidence
- Replace control and logoff

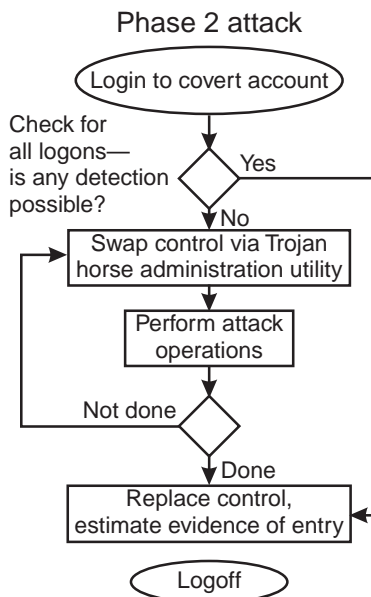


Figure 8.3 A simple network attack strategy.

interest, and transferred it for storage. From this vulnerable host, the intruder could also launch attacks on other network computers that had established access and “trust” with the system. At frequent intervals, system status was checked to monitor whether an administrator might have logged onto the system. Upon completion of the attack, system activity logs were modified to eliminate evidence of activities, and control was restored to normal control software.

The major vulnerabilities exploited in early UNIX attacks were lax security (e.g., use of simple passwords, retaining manufacturer default configurations and settings, and lack of complexity in password selection) and known system security flaws that had not been repaired. Since that time, many of the most basic security flaws have been corrected, but attack sophistication increased with the discovery of more intricate exploitable system vulnerabilities and the development of tools that automate the search for weaknesses and implementation of attacks [14].

The general functional paths and tactics employed for more complex network system attacks are illustrated in Figure 8.4 in five general stages. Each stage in this functional flow indicates a greater level of penetration of the target system and greater potential for malicious action. (See [15] for an actual account of a typical red team attack on a corporate networked system following this general procedure.)

Probing and Network Mapping

The attacker may seek to intrude on the targeted system via the Internet or via modems accessible by public telecommunications (remote login). The following penetration efforts are usually supported by prior intelligence collection efforts that provide insight into the target (e.g., physical system types, general structure, and telephone exchanges.):

1. *Internet access mapping*—Using the publicly available information on the Network Information Center (NIC) to locate the target domain, and the Domain Naming Service (DNS) to gain subnet information (e.g., IP addresses), a likely structure can be deduced to plan probing of the target. System function ports (UNIX access channels) can be “scanned” by interrogating each potential address; status responses to these “pings” provide confirmation to the attacker of potential attack paths. Similarly, test messages (e.g., e-mail addressed to likely addresses) may be issued in an attempt to identify system pathways based on the system information contained in the “bounced” returns.

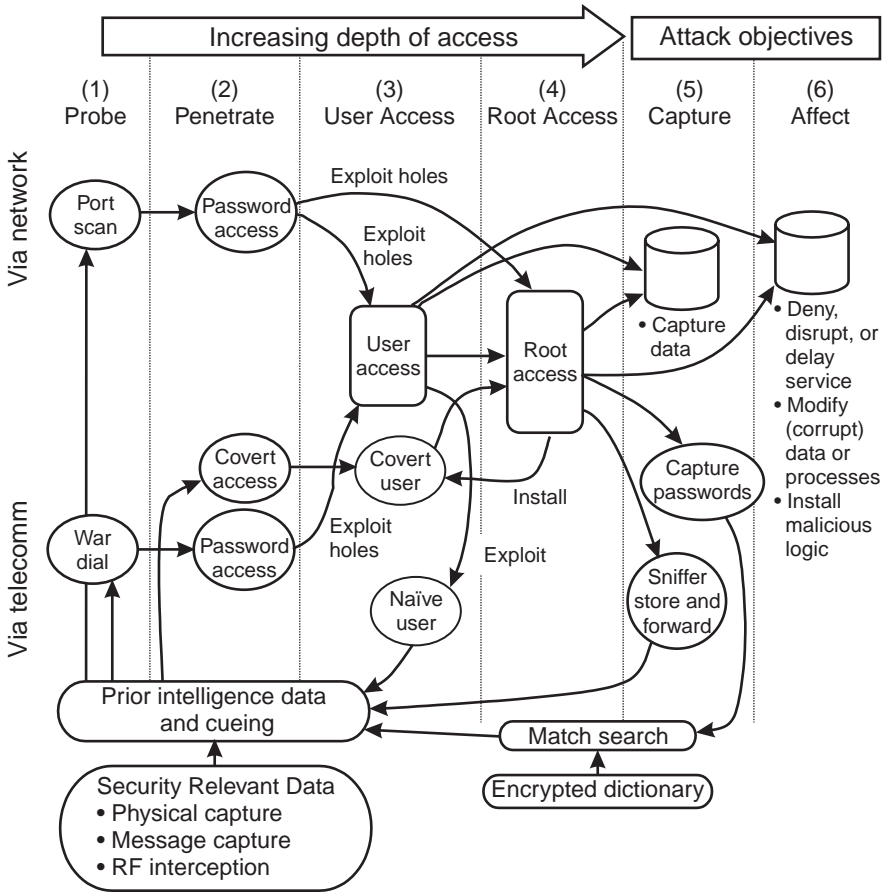


Figure 8.4 Typical access sequences for network attacks.

2. *Telecommunication access mapping*—Using prior knowledge of probable phone exchanges used by the target, a “war-dialing” program exhaustively (but in random sequence) dials exchange numbers and tests for modem responses to locate potential modem access to the target. Located modems are tested to determine access control protocols employed.

Penetration

Accessing available network ports or modems, attempts to breach log-on access controls are initiated. At this level, automated tools (such as the classic UNIX tools widely available on the Internet in the mid-1990s: Security Administrator

Tool for Analyzing Networks [SATAN], and Rootkit) can explore and probe the network for all known potential vulnerabilities. Login tactics include simple password testing, more sophisticated guessing using prior information, or direct access via previously captured passwords. Efforts are made to log on as a user (with low levels of privilege) or to achieve full-privileged administrative “root” or “superuser” access to the system. Note in the figure the feedback paths from prior penetrations (prior to security improvements) that may contribute to future access: (1) passwords may have been captured directly, or (2) encrypted password files may have been captured. In either case, simpler passwords, though encrypted, may be “cracked” by exhaustive comparison with an encrypted dictionary to locate matches.

User Access

Once user-level access is obtained, a greater range of system resources can be explored and mapped, including names of users, services, and network structures. From this level, vulnerabilities in multilevel security are exploited to gain higher access levels (system accounts) or to explore information beyond the user’s normal access (this is referred to as “stair-stepping” to higher access).

Root Access

At the highest levels of access, the attacker has significant control to immediately perform malevolent actions, to capture security-relevant data for future attacks (even after current vulnerabilities have been corrected), or to install “trap-door” capabilities for future covert access. At both this level and the user level, all activities are performed in a manner to avoid detection (real time or future) by system administrators. Authentication and logging programs are modified where possible to remove traceability of actions, and internal data and applications installed by the attacker are encrypted or otherwise disguised to prevent discovery.

Exploit System Resources

From a root-level privilege, the attacker may exploit information within the system for future attacks on this or other networked systems. Common exploitation actions include (1) installation of “sniffer” programs to collect message traffic or security-relevant data (e.g., user IDs and passwords) as they pass through the system, (2) capture of administrative files on system structure, (3) capture of encrypted password files, (4) capture of application information of interest, and (5) establishment of a new user identity with access to provide a future backdoor entry path for the attacker. The captured data may be transferred to the attacker at the time of initial attack or stored and forwarded at a future time.

Affect System Resources

Finally, the attacker may (from user or root-privilege levels) install malicious logic to deny, disrupt, or destroy information or processes within the system.

Additional supporting activities may be required to accomplish the system penetration activities above, such as seducing users or administrators to take specific actions; securing access to a separate but trusted host system; securing local access to a user account; tapping (intercepting) electromagnetic radiation from monitors, keyboards, or system cabling; or even obtaining brief physical access to the host system. Any of these actions can provide cues or complete information on passwords or other security-relevant data.

Gosselin has detailed a representative sequential access attack to a commercial network (for red team security analysis purposes) and defined five levels of “determinations” of knowledge (or depth of penetration achieved) about the target system that may be gained (Table 8.3) [16]. Kabay has clearly described the first-generation penetration techniques and the statistical characteristics of brute force attacks [17].

8.3.3 Internet Service Attacks

The tactics described above attempt access to resources by achieving user or administrator status, but do not include access attempts via Internet servers using services such as File Transfer Protocol (FTP) or Hypertext Transfer Protocol (HTTP).

Vulnerabilities in Common Gateway Interfaces (CGI) or routers, FTP, and HTTP services can also be exploited to gain privileged access to targeted systems. Table 8.4 enumerates some of the more common vulnerabilities of the Internet that have been widely attacked. (Note that these are historical, well-documented vulnerabilities still exploited on weak systems at the time of writing, but all are addressed in the future Internet protocols that will introduce increased security and by current protective measures described in the next chapter [18].)

Additional tactics include exploitation of the users of the targeted host system by inducing them to, for example:

- View a specific remote WWW site that provides active or executable content (e.g., ActiveX or JavaScript) to the target’s browser [19]. The active application (or “applet”) may exploit vulnerabilities in the browser security to capture security-relevant data from the host that may be useful for future attacks.

Table 8.3
Five Levels of Intelligence Determination

Level of Determination About Networked System	System Knowledge Obtained	Methods of Acquisition
1. Intended for public	IP addresses Domain names Telephone numbers	InterNIC and DNS services Phone directories Bulletin boards
2. Accessible to public without authentication	Network type and protocols Operating systems, server names, and gateway addresses User logons	Access to a public account on the networked system
3. Accessible to public, but not intended for public use	Server details Network services User account lists File systems	Physical access to a nonpublic networked computer; search and locate, or guess simple user account password
4. Acquired from sources intended to be secure and protected	Detailed lists of addresses, services, configurations, and software versions (to identify exploitable vulnerabilities) Located security holes	Access to public account and use of attack or security analysis tools to explore for means to "stair-step" from user to root access
5. Penetration of security, ID, and authentication	Security-relevant data to permit access	Physical access to secured areas; force, seduction, or coercion of users or administration

- Download data that contains executable content (e.g., word processing documents with macros that perform malevolent actions).
- Download application programs that include exploitation or malevolent logic.

All of these network tactics apply equally to the offensive network (or cyber) operations of command and control warfare, but they are enhanced (or supplemented) by the more intrusive military operations.

Table 8.4

Common First-Generation Internet Vulnerabilities and Representative Attacks

Internet Service	Vulnerabilities	Representative Attacks
Simple Mail Transport Protocol (SMTP)	No authentication of address headers and source	Spoofing e-mail messages with false "from" headers Unauthorized rerouting of mail Flooding a system ("barrage") with mail to deny service from anonymous sources
Transmission Control Protocol/ Interconnect Protocol (TCP/IP)	Insecure and unauthenticated transmission of IP addresses Inadequate boundary protection	Easily captured packets expose source and destination IP addresses, revealing active channels and traffic activity Spoofing connection source address ("IP masquerading") to appear to be a trusted or privileged computer "SYN attack" floods target server with SYN requests, but does not reply to the target's acknowledge requests—to crash the target "Ping of death" sends data properties that exceed allowable boundaries to crash the target "Session stealing" captures an established legitimate session by "IP splicing"—allowing the attacker to assume the role of the authenticated user
File Transfer Protocol (FTP)	Allows anonymous or guest (public) login Allows attacker limited access to facilities	Anonymous FTP allows initial-level access to system resources, which can be leveraged to expanded access Attacker may break in to ongoing legitimate FTP activities
World Wide Web (WWW) services	Nonsecure Hypertext Transfer Protocol (HTTP) modes accept active content	Active content (e.g., executable JavaScript or ActiveX) can be used to initiate malicious effects "Cookie" data collected by an observed site monitors activities at that site "Man-in-middle masquerading" seduces a visiting browser into viewing the WWW through the spoofer's software-in-middle

8.4 Command and Control Warfare Attack Tactics

In military C2W, the desired attack effects are degradation of the opponent's OODA loop operations (ineffective or untimely response), disruption of decision-making processes, discovery of vulnerabilities, damage to morale, and, ultimately, devastation of the enemy's will to fight.

Command and control warfare has often been characterized as a war of OODA loops where the fastest, most accurate loop will issue the most effective actions [20]. The information-based warfare concepts introduced in Chapter 3 (advanced sensors, networks, and fusion systems) speed up the loop, improving information accuracy (content), visualization and dissemination (delivery), and update rates (timeliness). The basis for investments in unmanned air vehicles, ground sensors, and other sensor networks has been justified on their contributions to content, delivery, and timeliness. With greater dependence (on the information gained) also comes greater vulnerability; and with vulnerability comes the greater likelihood of these systems becoming targets. C2 warfare can also be viewed as a competition for information dominance or superiority (as discussed in Chapter 4) in which the attacker is reducing the opponent's knowledge.

8.4.1 Command and Control Network Vulnerabilities

The targets of C2W attacks are decision makers, *through* weapons, and command, control, communications, computation, and intelligence (C4I) systems that are planned to rely on sources, sensors, and networked communications [21]. C2W attacks exploit all of the vulnerabilities described in Section 8.3.1, and expand those attacks to include sensors and fusion nodes that perform the observe and orient functions. Offensive information operations exploit the vulnerabilities described here and in Section 8.3.1.

Attacks exploit vulnerabilities in complex C4I systems to counter security and protection measures, as well as common human perceptual, design, or configuration vulnerabilities that include the following:

- Presumption of the integrity of observations and networked reports;
- Presumption that observation conflicts are attributable only to measurement error;
- Presumption that lack of observation is equivalent to nondetection rather than denial;

- Absence of measures to attribute conflict or confusion to potential multisource denial and spoofing.

Because C4I information systems, by their nature, include network dependence on multiple sensors, communication channels, and computers to acquire knowledge, and often use dispersed sources that utilize a communication link to report observations, these are the most natural dimensions for evaluating vulnerability. A vulnerability space (Figure 8.5) defined by these ordinates illustrates three general categories or levels of vulnerability.

The origin represents multiple sensor systems with the lowest vulnerability—they have multiple, redundant sensors that are collocated and do not rely on communication links to pass the source information to the fusion node. These are inherently strong—invulnerable to link attacks and able to withstand a degree of sensor attacks.

The first category (*sensor tight*) includes systems close to the origin. They are not dependent on all sources to make decisions and even may have a degree of redundancy in their use of sensors. They do not have exposed communication links. Dual-mode weapon seekers, for example, fall in the sensor-tight category. The attacker must focus on the seeker aperture alone.

The second category (*efficient*), moving outward from the origin, is characterized by increased dependence on either a single source or multiple sources to achieve consensus and includes mixed sensors—some local and some remote (reporting via communication links). The most vulnerable category (*dependent and distributed*), of course, includes those systems that *require* all sources and have completely remote sensors and sources.

Figure 8.5 also illustrates the most likely attack strategies produced by an attacker. Systems with local or mixed sensors are most vulnerable to sensor attacks, while mixed and distributed systems will be attacked on the links.

Table 8.5 summarizes the characteristics of these general categories and provides representative examples of each case. It is important to note that these categories imply *inherent* vulnerability properties, which must be recognized, characterized, and addressed. It is possible to make category 1 and 3 systems equally secure, but the category 3 system is inherently more vulnerable.

8.4.2 Attack Categories for Data Fusion Systems

The specific categories of attacks to the general C4I data fusion architecture (introduced earlier in Chapter 3) are now identified in Figure 8.6, where the flow of the closed loop fusion process is depicted along with the potential attack points (identified numerically with arrows.) The fusion model follows the U.S.

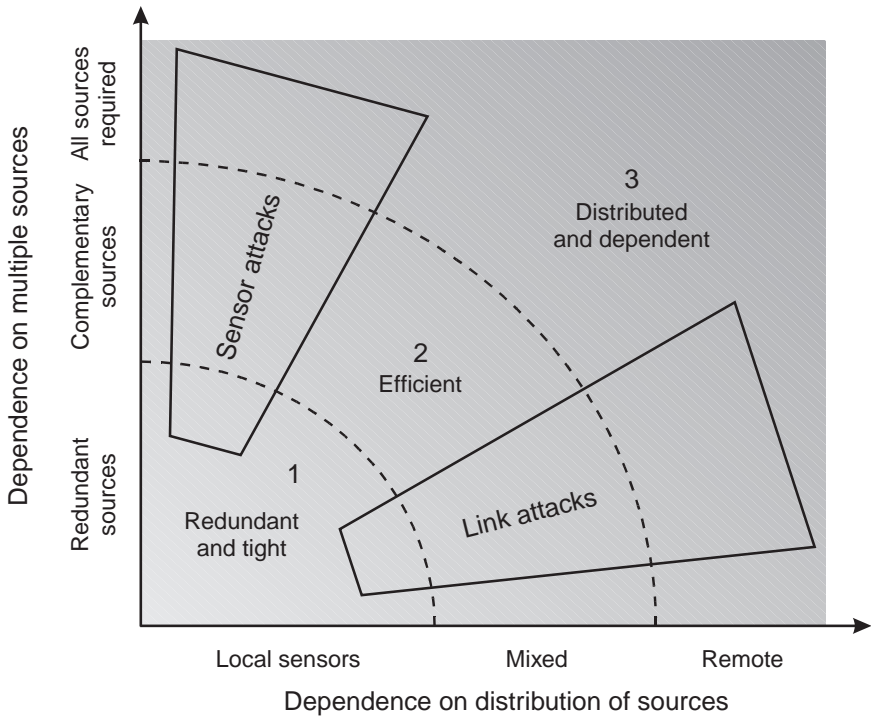


Figure 8.5 C4I network vulnerability may be characterized by the degree of dependence on multiple sources and the distribution of those sources.

DoD Joint Directors of Laboratories Data Fusion Subpanel model introduced earlier in Chapter 3 [22]. The four-level model has been organized to illustrate the relative place in the information chain and to depict the upward flow of the fusion process (data to information, then knowledge) and the downward flow of control.

Six major attack points are identified in the figure to illustrate the critical types and entry points for an IW attack. These also give insight into the areas of protection that must be considered for fusion systems.

The six attack points (numbered to correspond to points on Figure 8.6) are as follows:

1. Sensor and link attacks attempt to influence the sensing or report links, either to inhibit correct information or to insert false information. Sensor attacks can be performed by traditional electronic warfare means, by physically deceptive acts (openly detected) or by other means such as camouflage, concealment, and deception (CC&D)

Table 8.5
Vulnerability for Each of Three Categories of Weapons and C4I Systems

Vulnerability Category	Characteristics	Example Weapons and C4I Systems
1. Redundant and tight	<p>Redundant and complementary sensors</p> <p>All sensors local and only local links to fusion node</p> <p>Attacks directly to sensor or to supporting information systems (e.g., data links, threat programming)</p>	<p>Redundant multimode seekers for precision guided munitions (PGMs)</p> <p>Common aperture surveillance sensors</p>
2. Efficient	<p>Single or multiple sensors with little or no redundancy</p> <p>Not all sources are local—mixed local and remote sensors</p> <p>Both sensor and link attacks may be required to be effective</p>	<p>Local netted intelligence surveillance and reconnaissance (ISR) systems</p> <p>Theater intelligence systems</p> <p>Theater and below command and control systems</p>
3. Distributed and dependent	<p>High dependence on multiple sources (or dependent on all sources) to make decisions</p> <p>Sources widely and remotely distributed, requiring exposed communication links and network</p> <p>Either sensor or link attacks may be effective</p>	<p>Theater ISR systems</p> <p>Global intelligence systems</p> <p>Global command and control systems</p>

practices. Link attacks include conventional countermeasures as well as more complex network attacks on communication nets (including commercial links used widely by the military).

2. Object refinement attacks attempt to degrade the ability to align, correlate, track, or identify individual objects. These can be achieved *through the sensors* (by, for example, jamming or deception) or by direct penetration attack on the level 1 fusion process.
3. Situation and threat refinement attacks seek to degrade or deceive the processes that infer aggregate behavior. To attack this level *through the sensors*, deceptive events must be orchestrated for many individual objects, which are then properly detected by level 1 processes and passed to the higher level. The deception attempts to match a situation template (at level 2 or 3) to provide erroneous assessments of

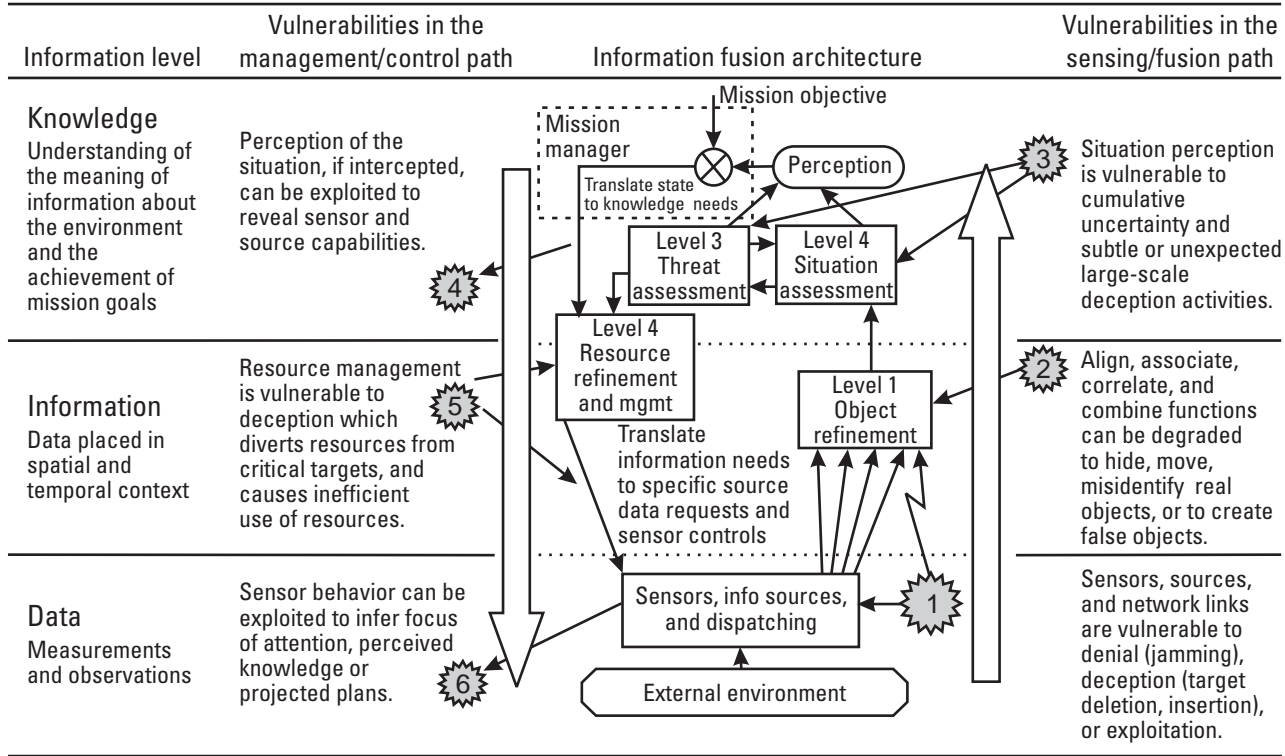


Figure 8.6 Vulnerabilities of and candidate attack tactics for all elements of the general fusion architecture. (Source: [21].)

opponents' true actions. Again, the attack may also directly attack the level 2 and 3 process or the databases they maintain.

4. Attempts to secure the knowledge of the fusion system (e.g., capturing access to the fused databases or operational displays) may reveal the performance of the sensors and fusion system for future IW attack purposes. In a simple fusion system, this may be inferred by observing the behavior of the use of the knowledge. For example, the behavior of a missile may reveal the performance of a fused seeker if the target characteristics are also observed.
5. Countermeasures may also attack the *control* of the sensors or sources, as well as the sensors or sources themselves. An attack on sensor controls may disable or degrade the effectiveness of a sensor just as efficiently (and, perhaps more easily) than an attack against the sensor aperture. A sensor looking in the incorrect direction at a critical time period is just as useless as one that is disrupted (jammed) or deceived.
6. Finally, sensor behavior can be monitored (especially active sensors) to observe the behavior of the fusion system to infer its focus of attention, its information needs and deficiencies, and its collection planning cycles and patterns.

The attacks in each of these areas can range from momentary nuisance threats (e.g., point jamming, broadcast floods) to orchestrated system-wide tactics aimed at widespread disruption and destruction. The exploitation attacks are coordinated to collect information to plan deception and disruption attacks. Exploitation is also used to monitor the effect of these attacks and to plan further attacks.

8.4.3 Attack Matrix for C4I Data Fusion

We can now map the preliminary set of counterinformation techniques (internal or external) that can be employed against fusion systems *at each level* of the data fusion process by type of attack effect.

A representative matrix is provided in Table 8.6, identifying specific attack types (including both external attacks to sensor inputs and subtle internal attacks to links and databases).

The vertical columns distinguish the four fundamental areas of attack that pose threats to systems containing data fusion elements. In each area, four fusion-specific threat mechanisms can be defined to focus information on the fusion process.

Table 8.6
Representative C4I Counterinformation Attack Matrix

		Counterinformation Attack Categories		
JDL Level	Fusion Functions	Denial, disruption	Deception	Exploitation
		Manipulation of data to prevent the efficient or accurate fusion and use of derived knowledge by the primary user	Creation and insertion of false data or information, which (once fused) will present an incorrect perception to the user	Manipulation of a data fusion system to extract knowledge about its use or the information it has obtained for its primary user
L1	Object detection	Deny multiple sensor detection, confusion Overload detect process	Synchronous insertion of deception objects in multiple sensors	L1, L2, and L3 require exploitation of internals or direct interception of data link information using network attack techniques described in Section 8.3
	Correlation and tracking	Create spatial or temporal mismatch Create track divergence	Cause track walk-off in separate sensors Insert false tracks	
	Identification classification	Deny multiple sensor identification, confusion Create synchronous false identification	Synchronous insertion to cause false identification Multisensor spoofing	
L2, L3	Aggregate situation and threat assessment	Deny standard patterns Overload inference operations (fill many templates simultaneously)	Create belief in deception plots, themes, and stories Create deceptive (unreal) threats	
		Deny linkages and relationships	Create deceptive tactical opportunities	
L4	Process refinement	Overload sensor management by creating divergent tasking patterns Overload processes and links, timed to deny selected critical knowledge	Insert incorrect cues to reduce sensor inefficiency Insert incorrect data models to disrupt L1, 2, 3, or 4 processes	

- *Exploitation* threats seek to utilize the information obtained by fusion systems or the fusion process itself to benefit the adversary. Information that can be captured from the system covertly can be used to attack the system, to monitor success of IW attacks, or to support other intelligence needs.
- *Deception* threats to fusion systems require the orchestration of multiple stimuli and knowledge of fusion processes to create false data and false fusion decisions, with the ultimate goal of causing improper decisions by fusion system users. Deception of a fusion system may be synchronized with other deception plots, including PSYOPS and military deceptions to increase confidence in the perceived plot.
- *Disruption* of sensor fusion systems denies the fusion process the necessary information availability or accuracy to provide useful decisions. Jamming of sensors, broadcast floods to networks, overloads, and soft or temporary disturbance of selected links or fusion nodes are among the techniques employed for such disruption.
- Finally, soft- and hard-kill *destruction* threats include a wide range of physical weapons, all of which require accurate location and precision targeting of the fusion node.

The matrix provides a tool to consider each individual category of attack against each element of the system. Many fusion systems employ a hierarchy of fusion nodes, and each node must be considered individually, taking into account the unique functions, timing, architecture, and interfaces of the node.

The matrix also provides a means of exploring all possible points of entry, vulnerabilities, and tactics that may be applied. On the basis of this matrix, vulnerabilities can be assessed and ranked, and the degree of impact (adverse consequence) of a successful attack can also be determined.

This general matrix contains only functional attack actions to illustrate the general tactics or end objectives that are desired in each matrix element. For any specific system, the matrix will include tactics tailored to the unique architecture and timing of the system targeted. The matrix for a dual-mode seeker, for example, will be significantly different from a complex theater ISR system. A comprehensive analysis may be required at each block of the matrix to conceive all potential attacks.

Note that the exploitation of levels 1, 2, and 3 fusion require penetration of the fusion nodes to capture operating information from internal databases, unless this information can be inferred from operating behavior (e.g., sensor tasking or actions) or the behavior of weapons or forces that use the system.

8.5 IW Targeting and Weaponeeing Considerations

Structured information strikes (netwar or C2W) require functional planning before coordinating tactics and weapons for all sorties at the perceptual, information, and physical levels. The desired effects, whether a surgical strike on a specific target or cascading effects on an infrastructure, must be defined and the uncertainty in the outcome must also be determined. Munitions effects, collateral damage, and means of verifying the functional effects achieved must be considered, as in physical military attacks.

The IW targeting process can be depicted in the typical six-phase cycle applied to offensive air operations [23]. Unlike air operations, however, the cycle time of information operations may require semi and full automation of the cycle to perform sorties and reattack sequences in periods of seconds. IW planning and targeting process tools (as developed in Chapter 7) must account for the differences in cycle times for information-level and physical-level attacks (seconds and hours, respectively) to achieve synchronized effects. Table 8.7 summarizes the targeting cycle phases and considerations for information operations.

8.6 Information-Level (Network) Attack Techniques

The tools of information-level attack can be partitioned into the typical components of traditional weapon systems:

- *Intelligence and targeting*—Subsystems to collect intelligence to understand targeted information systems (operations, status, vulnerabilities) and to develop targeting materials;
- *Weapon delivery*—Subsystems to provide access to the target (message, computer, communication link, database, facility) and to deliver munitions;
- *Information weapon*—Specific information (in the form of hardware, software, or abstract data) that affects the target system.

The following subsections (Table 8.8) introduce each of these categories of techniques.

8.6.1 Intelligence and Targeting

The general intelligence process, introduced earlier in Chapter 4, provides a wide range of means to collect knowledge about targeted information systems,

Table 8.7
Notional Targeting Cycle for Offensive Information Operations

Targeting Phase	Targeting Functions Performed	Special Considerations for Info Ops
1. Objectives and guidance	Define operational objectives Derive functional objectives	Issue rules of engagement (ROE) for information targets
2. Target development	Nominate targets Prioritize targets Prepare target description (e.g., network topology, port utilization, software structure)	Assess intelligence needs and task collectors Analyze information effects for prioritization
3. Weaponizing assessment	Define target attack objectives (e.g., functional effects, level of stealth required) Define information aim points Recommend attack level (perceptual, info, physical) and weapons Recommend BDA intelligence	Deconflict attacks between all objectives (e.g., operational, deception, PSYOPS) Assess likelihood of adverse collateral damage effects Analyze potential for cascading effects on information and physical infrastructure Analyze timing of sorties
4. Develop info tasking orders	Analyze resources and risks Evaluate allotment of tasks Allocate tasks to physical and information resources Prepare task orders	Assess rules of engagement for nominated targets Deconflict tasks against common targets (e.g., exploit versus deny) Synchronize sorties
5. Attack execution	Issue authorization for attack Conduct attack, monitor progress	Real-time synchronization of physical and network attacks
6. Attack assessment	Integrate intelligence Assess and compare achieved functional effects to objectives Issue reattack recommendations	Relate physical and information damage assessment to functional impact achieved

from their information properties (via SIGINT, NETINT, and OSINT) to the physical security of their facilities (via HUMINT). In addition to these direct

Table 8.8
Components of an Information-Level Weapon System

	Information-Level Weapon System		
Function	Intelligence and targeting	Weapon delivery	Information weapons
Section	Section 8.6.1	Section 8.6.2	Section 8.6.3
Elements	Cryptographic attacks	Perceptual delivery	Information weapons
	Network exploitation	Network delivery	
		Physical delivery	

and even intrusive observation methods, cryptographic and net exploitation attack techniques are the most long-standing methods to penetrate fundamental information security.

Cryptographic Attacks

The analysis and “breaking” of encryption is performed to penetrate cryptographic information security in order to:

- Gain one-time access information that has been encrypted (this information may represent knowledge, electronic funds, certification, or many other information representations);
- Commit one-time security forgery (e.g., to create a secure authentication);
- Spoof a user by presenting a valid authentication intercepted and copied from a valid user;
- Fully understand an encryption and keying process to permit repeated and full access to traffic on the targeted system.

Cryptanalysis attacks seek to locate vulnerabilities of the general cryptographic system. (See Figure 8.7. More details on cryptography as a principal defensive security mechanism are reserved for Chapter 9.) A fundamental tenet of cryptographic algorithm design is that a strong algorithm’s security rests entirely in the key and not the design details of the algorithm. (A general rule of encryption security—*Kerchoff’s principle*—is to assume that the encryption/decryption algorithms may be known by the attacker, but the system must remain secure by the strength of the method and security of the key. This does not mean, in practice, that the algorithms are made public.) Cryptographic

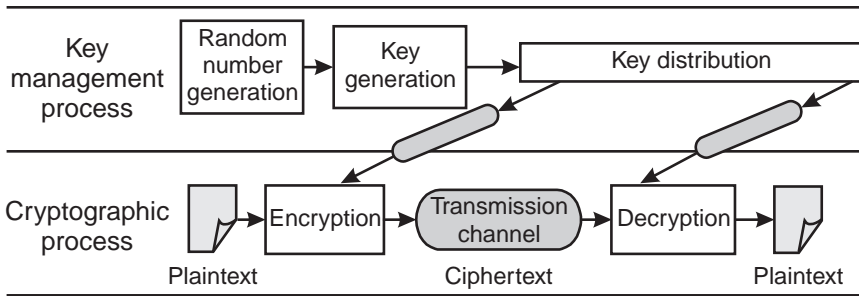


Figure 8.7 Basic elements of a cryptographic system.

attacks against strong, known cryptosystems, therefore seek to acquire or guess keys and understand the algorithms of unknown cryptosystems. Attacks generally fall into in one of the following areas:

1. Key management systems are attacked to acquire keys or reduce the search space for brute force key searches.
2. Key generators that format key variables and the distribution systems may be exploited if weaknesses occur in their design, implementation, or security.
3. Random number generators that randomly select seed numbers to generate keys may be exploitable if they are pseudorandom and a repetitive (deterministic) characteristic can be identified. If deterministic sequences can be identified, key sequences can be predicted.
4. Encryption system may be attacked if any portion of the path (plaintext or ciphertext) can be intercepted to perform an analysis.

Table 8.9 provides a simple taxonomy of the most basic cryptographic attack techniques, which include cryptanalysis and deception methods. The methods for attacking symmetric and asymmetric encryption approaches differ somewhat, and details of these methods may be found in [24–26]. The table does not include more complex timing analyses that estimate key information given the timing (number of clock cycles) of a legitimate decryption unit [27] and destructive methods that are applied to captured equipment.

Net Exploitation Attacks

In Section 8.3, the basic tactics for network exploitation were introduced, alluding to the following major information-level tools and techniques for collecting security-related data and gaining access to networked systems:

Table 8.9
Basic Cryptographic Attack Methods

Attack Approach	Data Used to Perform Attack	Attack Technique (Assumes knowledge of the algorithm)
Cryptanalysis	Ciphertext only	<i>Brute force</i> —Using a string of ciphertext and assumptions about the encryption method, decrypt all possible keys in the key space until plaintext is revealed <i>Guessed plaintext</i> —Guess at plaintext message, encrypt, and compare to known ciphertext to search for matches
	Known plaintext, corresponding ciphertext	<i>Brute force</i> —Search key space for encryption of known text that produced known ciphertext; even if not known, portions of plaintext may be guessed
	Chosen plaintext	<i>Brute force</i> —Obtain access to encryption process and encrypt a chosen plaintext using the keyed encryption device and analyze (symmetric system) or encrypt all possible private keys in key space (asymmetric system) <i>Differential cryptanalysis</i> —Obtain access to encryption process and encrypt chosen plaintext from a specially selected subset of the key space and analyze
	Chosen ciphertext	Obtain access to decryption process and insert chosen ciphertext string, obtain the decrypted plaintext and analyze
	Partial key	<i>Brute force</i> —In asymmetric (public key) cryptosystems, the public key must be factored into its prime number components to derive the secret (private) key
Deception	Ciphertext only	<i>Replay</i> —Replay unknown but valid recorded ciphertext within key interval for deceptive purposes
	Key	<i>Key theft</i> —Steal key via attack on key management
	Spoof key	<i>False key insertion</i> —Impersonate key distributor to target and present a key for use by target
	Known secure party pair	<i>Man-in-middle</i> —Secure a position between two secure parties (A and B) and provide keys (by spoofing both to believe that attacker is A or B); intercept and decrypt traffic in-transit and maintain masqueraded key distribution

1. *Agents*—Software processes that are endowed with the capability to execute operations autonomously and perform independent reasoning within a certain domain or environment (e.g., a network) may be applied to attack activities. Agents possess perception, reasoning (inferencing), and goal-directed independent execution authority [28]. “Mobile” agents capable of traveling through a network (e.g., a “worm,” described in Section 8.6.2) may be used to conduct goal-directed searches on a network to search for vulnerabilities, or to carry and insert trapdoor or Trojan horse processes to collect (store and forward) security-related data.
2. *Scanners*—Tools for exhaustively (or intelligently) scanning (or “pinging” for response) IP addresses, computer ports, telephone numbers, and other channels of access are fundamental tools of exploitation. These tools may be integrated with interception tools to perform convergent searches for channels.
3. *Interception tools*—Signal interception via RF capture (e.g., intercept inadvertent “van Eck” emissions from CRT monitors, RS-232 connections, or keyboards, or intentional radiation from wireless transmissions), wiretapping, or covert software or hardware (“sniffers” installed within the target information system [29]) provides the capability to monitor message traffic or network process activities to collect data. Store-and-forward or direct transmission methods may be employed to exfiltrate the collected data from the interceptor.
4. *Toolkits*—Automated software tools, including distributed tools for synchronized attacks from multiple locations, provide an array of techniques to test all possible vulnerabilities (design, implementation, and configuration) of a targeted system. (These tools are also used by defense “red teams” to evaluate security.)

In addition to these means, of course, security-related data and targeting information may be secured by HUMINT at the perceptual and physical levels (e.g., coercion, subversion, or deception of humans with useful knowledge, or by human observation, respectively). These HUMINT methods are referred to as “social engineering” in the hacker and nonprofessional literature.

8.6.2 Weapon Delivery

Following the three-layer model, weapons (and intelligence-collecting tools, above) may also be delivered to the target by three levels of delivery means. Table 8.10 summarizes the most common methods available at each level.

Table 8.10
Information Weapon Delivery Means

IW Model Level	Delivery System	Representative Examples
Perceptual	Via perceptual means	Coerce or suborn an authorized user or administrator to physical- or information-level action (below) Seduce or deceive an authorized user to action
Information	Via the network	Deliver via security holes identified by NETINT using toolkits or agents Deliver via autonomous agent worms
Physical	Via physical means	Covertly install (trap door, Trojan horse, etc.) in physical equipment hardware logic prior to delivery Covertly install in software prior to delivery Electronically insert via wiretap access Electronically insert via RF energy transmission Covertly install software or hardware during maintenance or special operation

8.6.3 Information Weapons

Information-level weapons perform malicious functions within the targeted information system. Malicious logic, also referred to as “logic contagion,” “bad code,” or “info bombs,” may be implemented in software, firmware, or hardware logic to perform the functions of disruption, denial, or destruction. As in conventional munitions, these are invasive, requiring insertion into or delivery in proximity to the target information system. (Recall that if the target is a network computer, information weapons delivered to supporting controls of electrical power, fire suppression, or a facility air conditioning system may be sufficient to affect the target.) Unlike conventional kinetic munitions that have the general objective function to release energy (“explode”) to cause physical damage, the objective function of malicious logic is very dependent upon the target, and effects cannot be measured in as single, common performance metric (e.g., equivalent tons of TNT or overpressure). Information weapons must *logically* be tailored to affect the information target.

The general taxonomy of malicious logic (Figure 8.8) includes both independent and dependent programs that are attached to legitimate programs. The taxonomy includes the following basic categories:

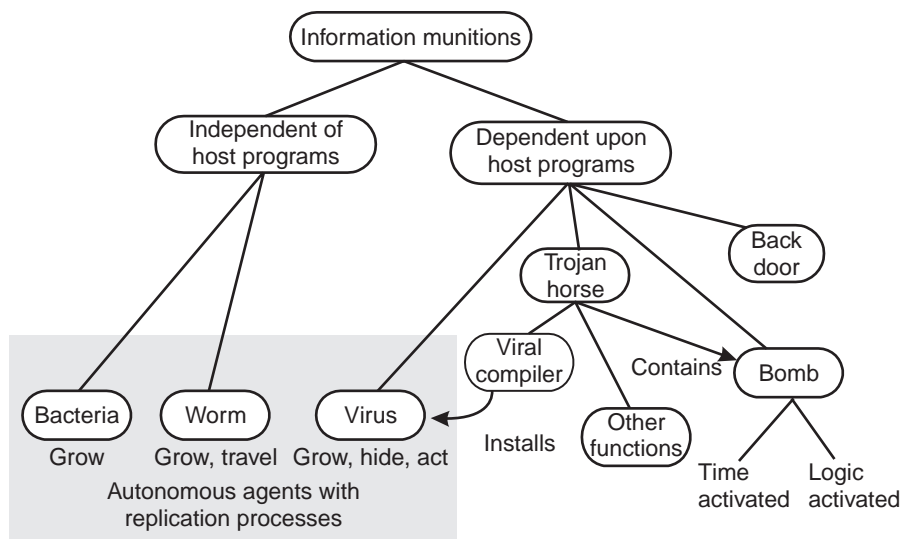


Figure 8.8 Basic taxonomy of information weapons.

1. *Bacteria*—A bacterium is an independent, self-replicating agent program that creates many versions of itself on a single machine, and as the multiplying versions are executed, increased storage space and processing time are acquired. Its geometric growth and resource capture properties enable it to deny service to legitimate users. Unlike a virus, bacteria programs do not attach to a host program.
2. *Worm*—The worm is also an independent self-replicating agent program that seeks to “travel” to spread from computer to computer on a network. From a beginning computer, it searches for other host computers, establishing a communication link and transferring the worm to the new computer. Like the bacterium, the worm can exhibit geometric growth on a network and consume resources to conduct a denial of service attack [30].
3. *Virus*—The virus is a dependent self-replication agent program that requires a “host” program to which it attaches (and within which it hides). The program is introduced to a “clean” system attached to a host program, which, once executed, “infects” (inserts a copy of itself to) another host program. In subsequent paragraphs, we describe the virus in greater detail as a weapon.
4. *Trojan horse*—Like the wooden horse delivered to the city of Troy, containing a secret cargo (in Virgil’s classic *Aeneid*), a Trojan horse

- program is any apparently legitimate program that contains a hidden hostile function. These may be inserted directly into application programs or into the compilers that transform source to object code. The program usually contains a conditional test to activate the malicious function.
5. *Bomb*—Deceptive, disruptive or destructive functions may be performed by “bomb” logic that is activated by time or logical conditions.
 6. *Back door (or trap door)*—This “door” is installed logic that provides a covert channel of information, or covert access to the system, that is uniquely useable by and only known to the attacker. The “scanners” that store and forward security-relevant data (described in Section 8.3.2) are Trojan horse programs.

The virus is perhaps most well known because of the widespread growth of this affliction by vandals who have developed, released, and continue to improve strains, especially on personal computers. The pathology, fundamentals, and security measures have been well documented in an ongoing campaign to eradicate new strains released into the networked computer environment [31–34]. The most basic virus operation (Figure 8.9) includes the following replicating (infecting) steps, easily implemented in less than 1,000 bytes of object code (pseudocode illustration from Frederick Cohen [35]):

1. When the virus program “V” is executed, it initiates subroutine infect-executable, a search at random for an executable file that is not already infected (i.e., programs that do not contain the “1234567” marker signature at the beginning of “V”).
2. When an uninfected executable file is located, “V” is inserted (adds a copy of itself) at the beginning of that program (the “host” program).
3. Next, the main program performs the test in subroutine trigger-pulled to determine if a condition exists (e.g., time, logical condition), and if true, the subroutine do-damage is executed.

Since the introduction of malicious viruses in the 1980s, the complexity and competition between attackers and defenders have increased through three basic generations (Figure 8.10). Viruses, like penetrating aircraft or missiles, must avoid observation or they can be detected and removed before they complete their mission. The basic competition is between viral stealth and antiviral detection and disinfection. The first generation of static viruses, affecting boot programs, directories, and application programs, were relatively static and

```

Program V :=
{1234567;

Subroutine infect-executable:=
  {loop: file-random-executable;
   if (first-line of file = 1234567)
     then goto loop;
   else prepend V to file;}

Subroutine do-damage:=
  {insert malicious action code}

Subroutine trigger-pulled:=
  {insert triggering condition test}

Main-program-of-virus:=
  {infect executable;
   if (trigger-pulled)then do-damage
   goto next;}

next:
}
    
```

Figure 8.9 Basic virus program “V” structure. (Source: Cohen, F. B., *A Short Course on Computer Viruses*, 2d. ed., © 1994, John Wiley & Sons, Inc. Reprinted by permission of John Wiley & Sons, Inc.)

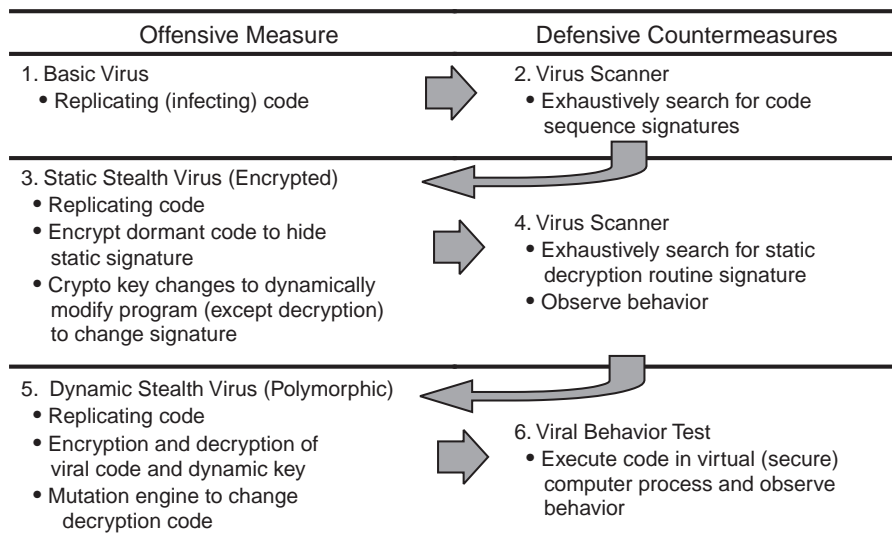


Figure 8.10 Three generations of virus development.

could be countered by detection of the signature of their executable object code at the beginning of programs. Also, their effect on programs (e.g., program code length, or checksum value of the program binary code) can be detected. A “scanner” performed this search for known signatures and unexpected program changes to indicate infection. This led to “encrypted” viruses, which attempted to reduce their signature by encrypting the object code while stored, and decrypting the code before execution. Using a random key each execution of the code, the dynamic encrypted version changes signature each execution. Only the decryption code must remain static, reducing the signature of the overall program but still leaving a small signature for detection by scanners. The third generation of “polymorphic” viruses attempts to eliminate even this static signature by changing the form of the unencrypted decryption code each cycle. Antiviral detection of this strain of viruses is performed by more complex analysis of the viral *behavior* (which is relatively static) rather than its object code structure while dormant.

The stealthy polymorphic mechanisms described here for viruses may also be applied to Trojan horses, back doors, and other malicious code that must remain unobservable within the targeted host until detonation.

All of these classes of logic (programs) and the many hybrids that can be derived from them for specific targets form the basis for pure information-based weapons that threaten targets if they can be delivered by attackers via physical or network means, or by authorized personnel acting on their behalf.

8.7 Physical-Level Attack Techniques

Direct attacks on the physical infrastructure (information and supporting elements) by physical means provide temporary denial, disruption, or long-term destruction. The following subsections summarize the major kinetic and directed energy weapon options. These intrusive and violent means are primarily military weapons used in C2W but, to a limited degree, may be applied in netwar as well as in terrorist war forms as weapons of mass destruction or disruption.

8.7.1 Kinetic Energy Weapons

In conventional warfare, critical strategic military targets have included physical “lines of communication” such as bridges, roads, railroads, ports, and airfields to prohibit physical traffic. These attacks are generally carried out by

penetrating air strikes (by manned aircraft or cruise missiles) and require conventional precision guided munitions (PGMs). Information operations focus attacks on information nodes and lines of communication (communication traffic, processing, and decision making) that control physical infrastructure. Studies on strategic attacks on telecommunications [36] and electrical power [37] have examined the implications of infrastructure attacks for effects on leaders, civilian morale, war materiel production, and military operations.

The implications of these studies for military C2W include the following:

1. Military benefits of attacking electrical power are limited to short period confusion and reduction in war production. Potential for negative political effects of collateral damage (to civilian populations) usually outweigh military effects (because the military has priority access to the grid and alternate means of generating power).
2. Military benefits of attacking telecommunications are high, but collateral effects on civilian population cannot be controlled because of the increasing use of common (commercial) carriers by civil and military users alike.

While these implications hold for C2W, attacks on power and telecommunications offer benefits for low-intensity conflicts and terrorists (unlike military planners) seeking high-impact sociopolitical effects on civilian populations (disruption). Although terrorists cannot mount military-scale attacks, small-scale attacks on critical infrastructure nodes (e.g., financial centers) may achieve this objective with low-technology bombs (delivered by individuals, cars, or air). Communication lines, satellite terminals, pipelines and pumping stations, electrical power transformer grids, and financial centers are targets for disruptive physical attacks, although most have survivability plans for recovery from physical disruptions (e.g., utility plans for natural disasters). The disruptive effects of these attacks can also be supportive in the conducting of netwar, inflicting damage on targets difficult to attack through the network or creating confusion or degradation in service to open vulnerabilities to network attacks.

8.7.2 Chemical and Biological Weapons (CBW)

Chemical and biological weapons, generally targeted at human subjects, may provide selective capabilities to affect material properties of vulnerable components of information technology systems: plastics and rubbers, sealants, electrical connectors, and so forth. The military employment of CBW for counterinformation applications would have significant political obstacles

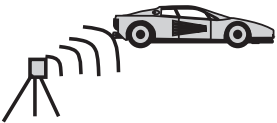
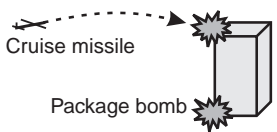
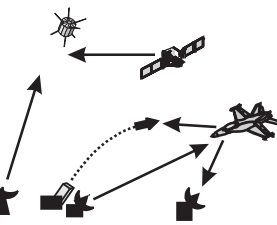
because of the CBW conventions and the difficulty in identifying agents that are both human-safe and counterinformation effective (presuming they would not be classed as weapons of mass destruction).

8.7.3 Directed Energy Weapons (DEW)

Directed high-energy weapons (DEW) offer the potential to damage sensitive electronic and electro-optical components from extended ranges. Speculations on the feasibility and state of such weapons developments have existed for a decade, and even though the United States has acknowledged research and development in the area, sparse technical information has been released. Three categories of DEW weapons (considered electronic attack weapons of electronic warfare) are generally recognized by the energy spectrum employed: radio frequency energy (RF), lasers, and energetic particles.

Table 8.11 depicts the major operational concepts for implementing weapons based on the ability to create and direct electromagnetic energy. Reported short-range civil applications include nonlethal arresting of fleeing

Table 8.11
Conceptual DEW Weapon Deployments

	Employment scenario	Representative applications
Civil law enforcement (short range)		Short-range disruption of automotive electronics (HPM) Nonlethal disruption of electro-optical sensors, humans
Electronic attack (medium range)		Non-nuclear electromagnetic pulse (EMP) disruption of computer, network, and telecommunications electronics Delivered by air, artillery, or ground
Military weapons (long range)		Satellite-to-satellite laser or EMP directed beam Aircraft defensive countermeasure to radar, missiles Anti-aircraft attack on avionics Antimissile countermeasure to disrupt sensors and guidance electronics

vehicles by disrupting engine control electronics by pulsed RF energy [38,39], and disabling electro-optical sensors and disorienting humans by laser radiation [40]. Medium-range applications include higher power non-nuclear explosive devices that radiate electromagnetic energy (isotropic radiation) in the form of a bomb capable of disruption of semiconductor electronics. Longer range laser and electromagnetic directed beams have potential offensive and defensive applications, including several reported developments.

- Aircraft self protection from missiles using ultrawideband (UWB) electromagnetic and IR laser emissions to counter surface to air (SAM) and air to air (AAM) missiles [41];
- RF energy weapons suitable for man-portable, submunition, or air delivery to attack command and control electronics [42].

The susceptibility of targeted electronics and effects of these weapons are dependent on many factors (range to target, frequencies and bandwidths, atmospheric conditions, target shielding and electrical interconnection configuration, and target physical characteristics), making the effectiveness of these weapons a complex function of the employment. It is expected that significant testing will be required before these weapons achieve reliable operational capability. The United States has acknowledged an extensive program to model susceptibility of systems to DEW and to develop modeling and simulation tools to understand effects [43,44]. Because of their proximity to targets (in end game) and dependence on sensitive seekers and electronics, precision guided munitions (PGMs) are vulnerable to suppression by DEW countermeasures. Since the early 1990s, U.S. PGMs have been designed with considerations for laser and RF DEW countermeasures [45]. In the following paragraphs, we refer to “conceptual weapons” that may be feasible once technology developments permit safe, effective, and deployable implementations. (Weapon design issues of beam direction, electromagnetic compatibility [EMC], survivability of the weapon’s own electronics, energy magazine capacity, reliability, maintainability, logistics, and physical size all must be solved before deployable weapons are fielded.)

RF Energy Weapons

RF energy weapons radiate directed electromagnetic fields in an effort to couple energy (induced electrical currents that are converted to electrothermal energy in semiconductor junctions and passive elements) into a target’s sensitive electronics. The destructive intent of this coupling is to radiate or conduct energy to the target’s electronics with functional effects ranging from temporary

“upset” to complete damage and failure. Coupled energy induces an electrical overstress on semiconductor junctions, resulting in heating, alloying, metallization, and, ultimately, irreversible junction failure [46]. Passive components (resistors, capacitors, and inductors) are also susceptible to voltage breakdown and failure.

A more subtle disruption/deception use of this coupling has been conceived by some who suggest the RF weapon may be used to remotely insert data or malicious executable code into a target system. Dubbed remote “microwave programming,” such concepts have been both technically described and refuted as infeasible. (See, for example, [47,48].)

Two categories of conceptual RF energy weapons have been reported. The first category includes high-power microwave (HPM) weapons that radiate narrowband, narrow beamwidth microwave energy, like high-power radar, operating in frequencies ranging between 10 MHz and 100 GHz with power outputs ranging from megawatts to tens of gigawatts. Magnetrons capable of delivering megawatt power levels for HPM demonstrators have been reported for shipboard antimissile applications [49]. Klystrons, gyrotrons, and a variety of other sources have been developed and evaluated as candidates to provide HPM beams capable of delivering a 1- μ sec pulse at one or more gigawatt power levels [50]. (This pulse provides $10^9 \times 10^{-6} = 1,000$ W/sec = 1,000 kilojoules of energy, a threshold for practical weapon applications.) Basic HPM technologies are described by Beneford and Swegle [51], and technology advances in this area may be monitored in proceedings of the IEEE International Pulse Power Conferences.

The second category of RF weapons employs electromagnetic pulse (EMP) effects. These effects are naturally created by lightning, giving rise to broadband (impulse) energy, with pulse durations on the order of milliseconds and energy densities on the order of 5-10 of J/meter. Generated EMP providing shorter but more intense effects can be created by three general means (Table 8.12), each with unique challenges and potential applications as weapons. Nuclear EMP (NEMP) or high-altitude EMP (HEMP) are recognized threats to space electronic systems [53] and pose a threat to electronics, especially those interconnected to long lines capable of inducing currents on the Earth’s surface over large geographic regions. A single 10-kiloton nuclear device detonated at 300 miles is capable of affecting a region the size of the continental United States [54]. The use of HEMP as a weapon, of course, transcends to a nuclear attack level, with additional nuclear effects that make it much more than an information weapon. The United States has acknowledged the existence of a nuclear directed energy weapon (NDEW) program to develop nuclear means of generating a wide range of output with potential for strategic defense [55]. EMP may also be created by a variety of nonnuclear means,

Table 8.12
Electromagnetic Pulse Generation Categories

	High Altitude Nuclear EMP (HEMP)	System-Generated and Switching EMP	Generated EMP
Method of EMP Generation	Generated by high altitude (30 miles) nuclear detonation Gamma rays interact with atmospheric molecules to produce Compton electrons, which create the EMP field	System-generated EMP (SGEMP) caused by ionizing rays and interaction with equipment to create electrons Switching EMP (SEMP) caused by switching transients and electric fast transients repeated bursts of SEMP (EFT/burst)	Switched-pulse compression amplifies, then inductively stores and discharges the pulse Explosive magnetic flux compression uses explosives to release pulse
EMP Characteristics [52]	Peak – 50 kV/m Duration ~10–200 ns	Peak – 100 kV/m Duration ~5–100 ns	Peak ~ 30 kV/km Duration –0.1 sec to 100 sec

including transient switching surges in systems and the use of generators, which may be applied as weapons. Numerous store/discharge techniques for pulsed power generation have been reported, including electronically switched and explosive discharge methods [56]. The high energy densities of explosives offer practical means of one-time discharge for EMP “bomb” applications. Explosive methods use the explosive charge to compresses a magnetic flux, creating the pulsed energy discharge that is applied to a pulse conditioner to match the pulse duration and impedance of the raw pulse to the high power source. Practical EMP weapons are expected to apply microyield nuclear (2 kiloton), conventional explosives, or plasma technologies [57,58]. U.S. DoD MIL-STD-461D/462D provides detailed requirements and testing procedures to harden electronic equipment to EMP effects.

High-Energy Laser (HEL) Weapons

Chemically-driven lasers capable of generating hundreds of kilowatts of average power offer potential as laser weapons to target sensitive photonic devices of electro-optical sensors (e.g., seekers, range finders, target-designators, surveillance, and other electro-optical sensors) over long ranges. Even higher power lasers, such as the chemical oxygen iodine laser (COIL) in the USAF airborne

laser (ABL) program, create thermal heating on a missile target as the destructive mechanism. These weapons are sensitive to atmospheric propagation (absorption, scattering, and turbulence), beam-pointing stability, and target surface characteristics.

Energetic Particle Weapons

Charged and neutral particle beams have been conceived as weapons because of their potential to directly transmit particles (electrons or neutral atomic particles, respectively) to a target, penetrating into the internal structure of target. The transfer of energy is efficient and lethal to both electronic and mechanical components. A proof-of-concept compact charged particle accelerator delivering a 10 Mev beam for in-atmosphere weapon application testing has been reported [59]. Atmospheric applications require multiple-pulse tunneling through the atmosphere and accurate beam steering to maintain the tunnel to the target.

8.7.4 Passive Conductive Measures

The dispersal of conductive materials, in particulate or filament form, has been suggested as a potential passive weapon that can affect sensitive electronic equipment or exposed power wiring or transformer grids. Dense clouds of conductive particles (e.g., metal or carbon particles) can be dispersed to be ingested by air conditioning systems of buildings, resulting in damaging conductive deposits on sensitive electronic components [60]. Some have reported that conductive carbon filaments, dispersed across exposed electrical power components (e.g., transformer farms, power lines), were dispersed by U.S. cruise missiles in the Gulf War to cause power grid disruptions [61].

8.8 Offensive Operations Analysis, Simulation, and War Gaming

The complexity of *structured* offensive information operations and the utility of their actions on decision makers is not fully understood or completely modeled. Analytic models, simulations, and war games will provide increasing insight into the effectiveness of these unproven means of attack. Simulations and war games must ultimately evaluate the utility of complex, coordinated, offensive information operations using closed loop models (Figure 8.11) that follow the OODA loop structure presented in earlier chapters to assess the influence of attacks on networks, information systems, and decision makers.

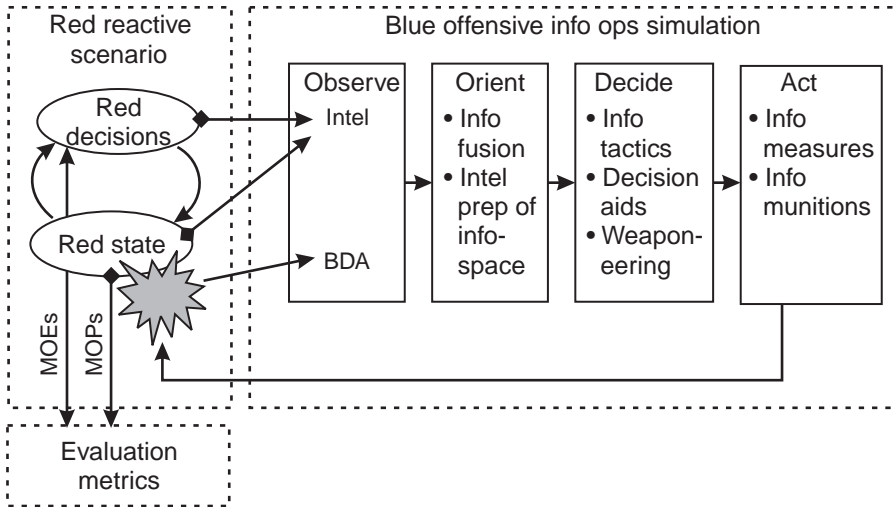


Figure 8.11 Representative offensive information operation simulation.

Measures of performance and effectiveness are used to assess the quantitative effectiveness of IW attacks (or the effectiveness of protection measures to defend against them). The measures are categorized into two areas.

- *Performance metrics* quantify specific technical values that measure the degree to which attack mechanisms affect the targeted information source, storage, or channel.
- *Effectiveness metrics* characterize the degree to which IW objectives impact the mission functions of the targeted system.

Table 8.13 summarizes typical IW measures of performance (MOPs) to measure typical IW attack effects (information degradation and effects) [62]. (Refer back to Chapter 2, Section 2.4, for information gain metrics and [63] for general data fusion metrics.) The table summarizes typical metrics for each of the four categories of effects that have been previously described. In each case, the metrics quantify the effect achieved, often relative to unaffected operation. Effectiveness metrics often apply utility functions (functions of several MOP parameters) defined by operations analysts to describe an aggregate measure of degradation, exploitation, deception, or destruction achieved. The table also lists representative measures of effectiveness (MOEs) for each of the effect areas.

Table 8.13
Typical Measures of Offensive Operations Performance and Effectiveness

Desired Effect		Measures of Performance (MOP)	Measures of Effectiveness (MOE)
Capture	Interception, Exploitation	Number of sources targeted Number of sources identified Sources obtained Intercept probability (P_{int}) Data acquired (volume, by category) Information acquired (volume, by category)	Degree of system penetration (%) Information gained Value of information intercepted (utility function based on use of information) Degree of understanding of opponent's belief achieved Utility of information gained
Affect	Denial, Disruption	Data reduced (%) Information reduced (%) Uncertainty introduced (P) Specific knowledge reduced (specific entities, objects, events) Decision rate reduced Link capacity reduced Link delay added	Decision capacity reduction (%) Decision accuracy reduction (%) Information capacity reduced (%) Coverage or access denied Aggregate delay introduced until decision
	Deception	Degree of belief achieved (in deceptive events) Scale of deception	Degree of belief achieved (in deception scenario) Value of information changed Value of knowledge impact
	Destruction	Items destroyed Items degraded Information destroyed Information degraded	Process capacity destroyed Link capacity destroyed Data, information, knowledge destroyed Effect on overall infrastructure (%) Duration of impairment

Clark and Wallfesh have studied the theater-level implications of offensive information operations on C2W, including the development of high-level

MOEs to measure these influences [64]. Their research has explored the difficulties in isolating the contribution of information operations and quantifying their impact on outcomes. Table 8.14 enumerates several of the representative MOEs that their analysis suggested may have potential for measuring offensive IO impact on C2W.

8.9 Summary

The wide range of offensive operations, tactics, and weapons that threaten information systems demand serious attention to security and defense. The measures described in this chapter are considered serious military weapons. The U.S. director of central intelligence (DCI) has testified that these weapons must be considered with other physical weapons of mass destruction, and that the electron should be considered the ultimate precision guided weapon [65]. One editorialist asks, “Of course the U.S. civilian computer networks have

Table 8.14
Theater Level MOEs That Measure C2W Impact

C2W Contributor	Candidate MOEs
Intelligence	<p>Did Blue locate Red’s center of gravity in a timely manner?</p> <p>Were branches and sequels foreseen? Was there adequate preparation?</p> <p>Did Blue identify Red’s main thrust? If so, was it identified in time to react?</p> <p>Was critical information and intelligence collected and analyzed? Was it disseminated in a sufficiently timely manner to command levels needing the information?</p> <p>Were critical decisions made on faulty reports?</p>
INFOSEC	<p>Was the flow of information traffic impeded?</p> <p>Was priority message traffic subject to saturation?</p>
EW	<p>Was interception of message traffic successful?</p> <p>Were Red’s critical information and communication nodes interrupted significantly? Were interruptions introduced at critical times?</p> <p>Were significant Red C2 modalities defeated?</p>
PSYOPS	<p>Did Blue convince the enemy of defeat?</p>

been contending with hackers for quite a while without any major catastrophe. But is anyone ready for the 100-hacker raid or the 1,000-hacker raid, or the 2,000-hacker raid?” [66].

From offensive information operations, then, we turn to their defensive counterparts. In the next chapter, we address each of the offensive approaches introduced in this chapter to develop security policies and defensive countermeasures that must be applied to mitigate the effects of these weapons.

Endnotes

- [1] Penetration is defined as the successful act of bypassing the security mechanisms of a system.
- [2] Stein, G. J., “Information Attack: Information Warfare in 2025,” *White Papers: Power and Influence*, Vol. 3, Book 1, Maxwell AFB, AL: Air University Press, Nov. 1996, p. 114.
- [3] We adopt terminology for information weaponry to be analogous to usage in conventional warfare, although no standard exists (e.g., adoption in Joint Publication 1-02) at the time of writing. We distinguish *weapon systems* as entire systems (targeting, delivery and munitions), *weapons* as the system’s damaging object (physical “ammunition” or information-level damaging software), and *sorties* as individual information-level attack actions.
- [4] Weaponing is “the process of determining the quantity of a specific type of lethal or nonlethal weapons required to achieve a specific level of damage to a given target, considering target vulnerability, weapon effect, munitions delivery accuracy, damage criteria, probability of kill, and weapon reliability.” Definition from Joint Pub 1-02.
- [5] Howard, J. D., “An Analysis of Security Incidents on the Internet (1989–1995),” Pittsburgh, PA, Dissertation Carnegie Mellon University, Apr. 7, 1997.
- [6] *Ibid.*, See Figure 6.8.
- [7] Common inadvertent software errors include domain errors, reuse of residual objects or data, inadequate authentication, boundary condition violations, and other exploitable logic areas.
- [8] Sadeghiyan, B., “An Overview of Secure Electronic Mail,” Dept. of Computer Science, Australian Defence Force Academy, June 12, 1992 (referencing CCITT Data Communication Networks, [Blue Book] ITU Geneva, 1989).
- [9] CERT Coordinating Center of Carnegie Mellon University provides advisories on vulnerabilities of systems and issues notices of threat activities.
- [10] Knightmare, The, with G. Branwyn, *Secrets of a Super Hacker*, Loompanics unlimited, Port Townsend, WA: 1994.
- [11] Denning, D. E., and J. Peter, *The Internet Besieged*, Reading, MA: Addison-Wesley, 1997.
- [12] Shimomura, T., and J. Mackoff, *Takedown: The Pursuit & Capture of Kevin Mitnick, America’s Most Wanted Computer Outlaw—by the Man Who Did It*, Hyperion, 1995.

-
- [13] Stoll, C., *The Cuckoo's Egg*, New York: Doubleday, 1989.
- [14] "ASDC3I/SEI Reports to PCCIP on Computer Attacks," *Defense Information and Electronics Report*, Apr. 25, 1997, pp. 11–14.
- [15] Behar, R., "Who's Reading Your e-mail?," *Fortune*, Feb. 3, 1997, pp. 57–70.
- [16] Gosselin, R. J., "External Threats to Computer Security in Networked Systems," 1997, pp. 63–80.
- [17] Kabay, M. E., "Penetrating Computer Systems and Networks," Chapter 18 in *Computer Security Handbook*, 3d ed., edited by Hunt, A. E., S. Bosworth, and D. B. Hoyt, New York: John Wiley & Sons, 1995.
- [18] For a technical explanation of major attacks, see, Orvis, W. J., "Hacker Tools: How Do They Do That?," *Proc. of 19th DOE Computer Security Group Training Conf.*, UCRL-MI-127196, May 1997.
- [19] McGraw, G., and E. Felten, "Avoiding Hostile Applets," *Byte*, May 1997, pp. 89–92.
- [20] Orr, G. E., *Combat Operations C3I: Fundamentals and Introductions*, Maxwell AFB, AL: Air University Press, 1983.
- [21] Waltz, E. L., "The Data Fusion Process: A Weapon and Target of Information Warfare," *Proc. of National Sensor Fusion Symposium*, Apr. 1997.
- [22] Most recent version is described in, "Functional Description of the Data Fusion Process," Joint Directors of DoD Laboratories, Nov. 1991. At the time of this writing, the model is in revision and refinement by the JDL Subpanel on Data Fusion.
- [23] Joint Publication JP 3-56.1, *Command and Control for Joint Air Operations*, Chapter 4, "Targeting and Tasking for Joint Air Operations," Nov. 14, 1994.
- [24] Fahn, P., *Answers to Frequently Asked Questions About Today's Cryptography*, Redwood City, CA: RSA Laboratories, (Version 2.0, 1993, See Sections 2.5, 3.9, and 5.2). Also see Version 3.0, 1996.
- [25] Stinson, D. R., *Cryptography: Theory and Practice*, Boca Raton, FL: CRC Press, 1995. See Sections 1.2 and 3.6.
- [26] Purser, M., *Secure Data Networking*, Norwood, MA: Artech House, 1993. See section 2.1 on attacks.
- [27] Kaliski, B., "Timing Attacks on Cryptosystems," *RSA Laboratories BULLETIN*, No. 2, Jan. 23, 1996.
- [28] For an overview of definitions of agents, see Franklin, S., and A. Graessler, "Is It an Agent, or Just a Program?: A Taxonomy for Autonomous Agents," *Proc. of Third International Workshop on Agent Theories*, New York: Springer-Verlag, 1996.
- [29] Sniffers generally collect the initial 128 characters of a new user's logon because this portion of the message block contains the user ID and password.

-
- [30] The Internet worm was released on UNIX systems on Nov. 2, 1988, and demonstrated the extensive network service denial potential of worms, although the weapon did not achieve its full potential before being detected and disinfected.
- [31] Denning, P. J., (ed.), *Computers Under Attack: Intruders, Worms and Viruses*, New York: ACM Press, 1990.
- [32] Hoffman, L. J., *Rogue Programs: Viruses, Worms, & Trojan Horses*, New York: Van Nostrand, 1990.
- [33] Hruska, J., *Computer Viruses and Anti-Virus Warfare*, New York: Viking Penguin, 2d ed., 1993.
- [34] Ferbache, *A Pathology of Computer Viruses*, New York: Springer-Verlag, 1991.
- [35] Cohen, F. B., *A Short Course on Computer Viruses*, New York: John Wiley & Sons, 2d ed., 1994, p. 4.
- [36] Hurst, G. R., (Maj. Gen., USAF), *Taking Down Telecommunications*, Maxwell AFB, AL: Air University Press, Sept. 1994.
- [37] Griffith, T. E., (Maj., USAF), *Strategic Attack of Electrical Systems*, Maxwell AFB, AL: Air University Press, Oct. 1994.
- [38] Kiernan, V., "Stop Now, or the Car Gets It," *New Scientist*, Nov. 9, 1996, pp. 24–26.
- [39] Auto-Arrestor™ Product Description, Jaycor Inc., Dec. 1997,
URL:<http://www.jaycor.com>
- [40] Tapscott, M., and K. Atwal, "New Weapons That Win Without Killing on DOD's Horizon," *Defense Electronics*, Feb. 1993, pp. 41–45.
- [41] "HPM/LASER Aircraft Self-Protect Missile Countermeasures," WE.19.08F, in 1997 U.S. Defense Technology Objectives (DTO).
- [42] "High-Power Microwave C2W/IW Technology," WE.22.09, in 1997 U.S. Defense Technology Objectives (DTO).
- [43] Tatum, J. T., "A New Threat to Aircraft Survivability: Radio Frequency Directed Energy Weapons (RF DEW)," JTCG/AS, *Aircraft Survivability*, Fall 1995, p. 11.
- [44] Marquet, L. C., "Aircraft Survivability and Directed Energy Weapons," JTCG/AS, *Aircraft Survivability*, Fall 1995, p. 7.
- [45] "AMC-SWMO Countermeasures Study," Vol. I, *Guide to How Countermeasures Affect Smart Weapons*, Jan. 1992, pp. 3–6 to 3–7 and 4–21 to 4–25.
- [46] Antinone, R. J., "How To Prevent Circuit Zapping," *IEEE Spectrum*, April 1987, pp. 34–38.
- [47] Cramer, M. L., and S. R. Pratt, "Computer Viruses in Electronic Warfare," *Proc. Fourth Annual Computer Virus Conf.*, NY, 1990.
- [48] Martin C. Libicki has commented, "One of the more outrageous fallacies to have garnered serious research dollars was the concept that U.S. forces could somehow broadcast viruses into enemy computers. It might be possible if the computer systems of the opposition

were designed to accept over-the-air submissions of executable code, but who would design a system to do that?" See, *What Is Information Warfare?*, Washington, D.C., National Defense University, 1995, p. 54.

- [49] "High Power Microwave Sources and Systems Description," Jaycor Inc., Dec. 1997, URL:<http://www.jaycor.com>
- [50] Lehr, M, et al., "Another Path to High Power Microwaves," *J. of Electronic Defense*, June 1997, p. 48.
- [51] Beneford, J., and J. Swegle, *High Power Microwaves*, Norwood, MA: Artech House, 1992.
- [52] "Electromagnetic Pulse (EMP) and TEMPEST Protection for Facilities," Engineering and Design Pamphlet EP 1110-3-2, U.S. Army Corps of Engineers, Dec. 31, 1990, Table 2-1.
- [53] "DoD Study Team Addresses EMP Concerns," *Military Space*, Vol. 14, No. 15, July 21, 1997, p. 1.
- [54] "Electromagnetic Pulse Simulation and Testing," *Compliance Engineering*, Volume XII, No. 2.
- [55] "Draft Public Guidelines to Department of Energy Classification of Information," Office of Declassification, U.S. Department of Energy, June 27, 1994, Section 3.4 paragraph H.
- [56] Weldon, W. F., "Pulsed Power Packs a Punch," *IEEE Spectrum*, Mar. 1985, pp. 59–66.
- [57] Lehr, M, et al., "Explosive Pulsed Power for Driving HPM Loads," *J. of Electronic Defense*, June 1997, pp. 45–50.
- [58] Varni, J., (Lt. Col., USAF), et al., "Space Operations: Through the Looking Glass," USAF 2025 Research paper, Maxwell AFB, AL: Air University Press, Aug. 1996, Chapter 3b.
- [59] Miller, J., E. Nolting, and N. Chesser, "Charged Particle Beam Weapons," JTTCG/AS, *Aircraft Survivability*, Fall 1995, p. 12.
- [60] Fulghum, D. A., "New Weapons Slowed by Secrecy Clamp," *Aviation Week and Space Technology*, Jan. 19, 1998, p. 54.
- [61] Vickers, N. G., R. C. Martinage, *The Military Revolution in Intrastate Conflict*, Washington, D.C., Center for Strategic and Budgetary Assessments, Oct. 1997, p. 34. The authors referred to this weapon as an electrical power distribution munition (EPDM).
- [62] Waltz, E., "Information Warfare: A Systems-Level Introduction," Seminar Notes, Nov. 1995.
- [63] Waltz, E., and J. Llinas, *Multisensor Data Fusion*, Norwood, MA: Artech House, 1990, pp. 404.
- [64] Clark, H. W. and S. K. Wallfesh, "Measuring Effectiveness of Theater IW/C2W Campaigns," *Proc. of Old Crows' FiestaCrow 95*, San Antonio, TX, Apr. 26, 1995.
- [65] Mann, P., "Cyber Threat Expands with Unchecked Speed," *Aviation Week and Space Technology*, July 8, 1996, p. 63.
- [66] Hughes, D., "Cyber Raid, Wall Street: This Is No Drill...", *Aviation Week and Space Technology*, Dec. 22–29, 1997, p. 98.

9

Defensive Information Operations

This chapter provides an overview of the defensive means to protect the information infrastructure against the attacks enumerated in the last chapter. Defensive IO measures are referred to as *information assurance*.

Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities [1].

This definition distinguishes *protection* of the infrastructure by prevention of unauthorized access or attack (proactive measures), and *defense of* the infrastructure by detecting, surviving, and responding to attacks (reactive measures). The assurance includes the following component properties and capabilities:

- *Availability* provides assurance that information, services, and resources will be accessible and usable when needed by the user.
- *Integrity* assures that information and processes are secure from unauthorized tampering (e.g., insertion, deletion, destruction, or replay of data) via methods such as encryption, digital signatures, and intrusion detection.
- *Authentication* assures that only authorized users have access to information and services on the basis of controls: (1) authorization (granting and revoking access rights), (2) delegation (extending a portion of one entity's rights to another), and (3) user authentication (reliable

corroboration of a user, and data origin. (This is a mutual property when each of two parties authenticates the other.)

- *Confidentiality* protects the existence of a connection, traffic flow, and information content from disclosure to unauthorized parties.
- *Nonrepudiation* assures that transactions are immune from false denial of sending or receiving information by providing reliable evidence that can be independently verified to establish proof of origin and delivery.
- *Restoration* assures information and systems can survive an attack and that availability can be resumed after the impact of an attack.

Information assurance includes the traditional functions of information security (INFOSEC), which is defined at two levels. At the policy level, INFOSEC is “The system of policies, procedures, and requirements established under the authority of E.O. 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security” [2]. At the technical level, the U.S. National Computer Security Center (NCSC) has traditionally defined the components of INFOSEC to include the following.

INFOSEC includes measures and controls that protect the information infrastructure against:

- Denial of service;
- Unauthorized (accidental or intentional) disclosure;
- Modification or destruction of information infrastructure components (including data).

INFOSEC includes consideration of:

- All hardware and/or software functions, characteristics, and/or features;
- Operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities;
- Management constraints;
- Physical structures and devices;

- Personnel and communication controls needed to provide an acceptable level of risk for the infrastructure and for the data and information contained in the infrastructure.

INFOSEC includes the totality of security safeguards needed to provide an acceptable protection level for an infrastructure and for data handled by an infrastructure [3].

This broad definition includes four components traditionally included within communications security (COMSEC).

- *Emanations security* (EMSEC)—The control of emanations that may compromise internal information;
- *Electronics security*—The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations (e.g., radar);
- *Transmission security* (*TRANSEC*)—The protection of transmissions (“externals”) from traffic analysis, disruption, and imitative deception;
- *Cryptographic security*—The use of encryption to protect communication content (“internals”).

More recently, the aspect of survivability (the capacity to withstand attacks and functionally endure at some defined level of performance) has been recognized as a critical component of defenses included under the umbrella of INFOSEC and information assurance.

Throughout the 1970s and 1980s, INFOSEC efforts were focused on nonnetworked, trusted computing security evaluation criteria (TCSEC) and communications security (COMSEC) for national and military communications [4]. Classical models for trusted computing were developed in the 1970s [5] and later applied to computer networks, which introduced the “composition problem”—determining the security attributes of the networked system from the analysis of the properties of the system’s components [6]. Foreseeing the need for advanced information security capabilities to provide privacy and security in an increasingly networked world, studies of the issues related to network security were initiated in the early 1980s. (See, for example, the early work of W. H. Ware at RAND [7–10].)

Information assurance and security authorities have proliferated even as information technology has expanded to network applications, and the interest in strong security has moved from the sole realm of the military to the GII.

Current sources of open security standards developed to promote secure networking over the GII include the following:

- National Institute of Standards and Technology (NIST);
- International Standards Organization (ISO);
- Comite Consultatif international de Telegraphie at Telephonie (CCITT, or International Telegraph and Telephone Consultative Committee) a committee of the International Telecommunications Union (ITU);
- Internet Engineering Task Force (IETF).

The U.S. TCSEC and the European Information Technology Security Evaluation Criteria (ITSEC) [11] have formed the benchmark criteria for trusted system development throughout the 1990s. At the time of writing, the governments of North America and Europe are developing common criteria (CC) for information technology security evaluation, expected to be adopted by the ISO for evaluation of security products and protocols for use in public and private sector applications. The U.S. DoD has developed a joint technical architecture (JTA) for C4I systems that applies many of these standards the critical elements of the U.S. DII, ultimately replacing the TCSEC [12].

Interest in security has been raised by widely reported and studied attacks on military (DII) and civil/commercial (NII) networks. A U.S. GOA assessment estimated 250,000 attacks on the U.S. DII in 1996, growing at a rate of 100% per year with a 65% successful penetration rate [13].

Information assurance faces four basic categories of threats (Table 9.1), characterized by the degree of structure in their attack capability and the measure of trust (or access) that the threat enjoys. The approach to security for each category varies; security emphasis for external threats is defense, while the emphasis for internal threats is deterrence.

Much of the focus of attention in the popular press has been on unstructured, external threats. These threats have been single individuals, or small hacker groups with knowledge of network vulnerabilities and access to a complete nation of computers, in which some have certainly not corrected the vulnerable holes. While these asymmetric threats (e.g., lone teenager versus large corporation or DoD) have captured significant attention, they do not pose the more significant threat that comes in two areas.

- *Internal threats (structured or unstructured)*—Any insider with access to the targeted system poses a serious threat. Perverse insiders, be they

Table 9.1
 Defense Emphasis Matches Threat Categories. (Source: Based on Doty [14].)

		Threat Structure	
		Unstructured	Structured
Threat Source	External Attackers that are not a trusted member of the target organization Security focus: defense	Threat Classic “hacker” Attacks targets of opportunity; lacks persistence against difficult targets Defense Access control lists One-time passwords Remote user authentication Firewall	Threat Organized attack cell Higher motivation for access (financial, criminal, industrial espionage or sabotage; political, state-sponsored acts of IW) Defense Access control lists One-time passwords Remote user authentication Firewall Intrusion detection/response
	Internal Attackers that are trusted members of the target organization or a less trusted support worker with some degree of access Security focus: deterrence	Threat Classic “technophile” Lacks persistence Deterrence User education Regular security awareness publications	Threat High motivation, technical capability, and access knowledge Knowledge of vulnerabilities, target Deterrence and defense High-visibility monitoring Frequent activity audits High-level physical security and internal OPSEC

disgruntled employees, suborned workers, or inserted agents, pose an extremely difficult and lethal threat. Those who have received credentials for system access (usually by a process of background and other assessments) are deemed trustworthy. Protection from malicious acts

by these insiders requires high-visibility monitoring of activities (a deterrent measure), frequent activity audits, and high-level physical security and internal OPSEC procedures (defensive measures). While continuous or periodic malicious actions may be detected by network behavior monitoring, the insider inserted to perform a single (large) destructive act is extremely difficult to detect before that act. OPSEC activities provide critical protection in these cases, due to the human nature of the threat. This threat is the most difficult, and its risk should not be understated because of the greater attention often paid to technical threats.

- *Structured external threats*—Attackers with deep technical knowledge of the target, strong motivation, and the capability to mount combination attacks using multiple complex tactics and techniques also pose a serious threat. These threats may exploit subtle, even transitory, network vulnerabilities (e.g., configuration holes) and apply exhaustive probing and attack paths to achieve their objectives. While most computer vulnerabilities can be readily corrected, the likelihood that all computers in a network will have no vulnerabilities exposed at any given time is not zero. Structured attackers have the potential to locate even transient vulnerabilities, to exploit the momentary opportunity to gain access, and then expand the penetration to achieve the desired malevolent objective of attack.

In Chapter 6, we pointed out how intelligence and counterintelligence provide defense for the perceptual level of the IW model, and OPSEC provides defense for the physical level. In this chapter, we focus on the elements of defensive information operations *at the information layer*. We define the basics of INFOSEC (Section 9.1) before introducing the basic security methods in the subsequent sections: trusted computing (Section 9.2), access control (Section 9.3), encryption (Section 9.4), incident detection and response (Section 9.5), survivability (Section 9.6), physical-level hardening (Section 9.7), defense tools (Section 9.8), and security analysis and simulation (Section 9.9).

There are many detailed texts on the theory and application of each of these specific areas, and the intent of this chapter is to provide a system-level overview with a guide to the major sources available in each area for deeper study. Basic references include the *Computer Security Handbook* [15], *Site Security Handbook* [16], *Computer Security Basics* [17], *Computer System and Network Security* [18], and *Secure Data Networking* [19]. The international financial industry has long maintained security for electronic transfer of funds,

and has ongoing efforts to keep pace with information warfare threats. Those developing standards are documented in ANSI X9 standards.

9.1 Fundamental Elements of Information Assurance

The definition of information assurance includes six properties, of which three are considered to be the fundamental properties from which all others derive [20].

- *Confidentiality (privacy)*—Assuring that information (internals) and the existence of communication traffic (externals) will be kept secret, with access limited to appropriate parties;
- *Integrity*—Assuring that information will not be accidentally or maliciously altered or destroyed, that only *authenticated* users will have access to services, and that transactions will be certified and unable to be subsequently repudiated (the property of *nonrepudiation*);
- *Availability*—Assuring that information and communications services will be ready for use when expected (includes *reliability*, the assurance that systems will perform consistently and at an acceptable level of quality; *survivability*, the assurance that service will exist at some defined level throughout an attack; and *restoration* to full service following an attack).

These fundamentals meet the requirements established for the U.S. NII [21] and the international community for the GII.

Following the method to establish the attack matrix in the last chapter, we can identify the categories of measures that can achieve these properties in a defense matrix that distinguishes measures at each level of the IW model (Table 9.2).

The emphasis of this chapter is on technical security measures, but physical and personnel security measures are essential complementary protection for the physical and perceptual layers. Protection of the human users and operators of the information systems (e.g., decision makers, analysts, technicians, maintainers) is required to maintain their integrity (from subornation or influence to contribute to attacks) and objectivity (from deception and PSYOPS regarding the system performance, system integrity, or external environment). These security activities are perceptual security measures in terms of the IW model: protecting the perception of the human element.

Table 9.2

Defense Matrix Categorizes Security Measures by Security Property and IW Security Level

Security Property	Privacy (Confidentiality)	Integrity	Availability
Property Characteristics	Protect data from unauthorized disclosure; includes connection confidentiality, connectionless confidentiality, selective field confidentiality, and traffic flow confidentiality	Prevent and/or detect unauthorized modification, insertion, deletion, or replay of data; protects against false denial of sending or receiving data by providing the receiver or sender with reliable evidence that can be independently verified (nonrepudiation)	Assure that information and communications services will be ready for use when expected—this includes <i>reliability</i> and <i>survivability</i> of services
Level of Security (IW Model): Perceptual	Perceptual Security Measures		
	<p><i>Physical and technical measures</i>—to maintain accurate, objective perception of the security state of the system (e.g., physical and technical intrusion detection monitors that provide reliable status)</p> <p><i>Personnel measures</i>—to maintain personnel security to protect from subornation or other inducement to inside attacks and to provide training and environment to protect from effects of PSYOPS or deception</p>		
Level of Security (IW Model): Information Infrastructure	Technical Security Measures		
	(See Figure 9.1)		
Level of Security (IW Model): Physical	Physical Security Measures		
	<p>Physical access controls and facility protection</p> <p>Personnel management and security</p> <p>Contingency planning and disaster recovery</p> <p>Electromagnetic hardening (EMSEC)</p>		

Physical-level security includes controls for physical access to facilities, protection from local capture (intercept) of information via unintentional electromagnetic radiation, protection from failure of supporting utilities (e.g.,

power, air conditioning, water) and natural disasters, and many other threats. The NIST handbook, *An Introduction to Computer Security*, provides an overview of these physical and personnel security practices [22].

In Figure 9.1, the technical security measures that will be discussed in the following sections are compared to the fundamental information assurance properties they provide and the categories of *technical* security functions (mechanisms) under which they are generally categorized.

		Fundamental Security Properties		
		Privacy (Confidentiality)	Integrity	Availability
Property Characteristics		Protect data from unauthorized disclosure; includes connection confidentiality, connectionless confidentiality, selective field confidentiality, and traffic flow confidentiality	Prevent and/or detect unauthorized modification, insertion, deletion, or replay of data; protect against false denial of sending or receiving data by providing the receiver or sender with reliable evidence that can be independently verified (nonrepudiation)	Assure that information and communications services will be ready for use when expected—this includes reliability and survivability of services
Security Measures				
Technical Methods (Algorithms)	9.3	Authentication and Access Control	<ul style="list-style-type: none"> · Authentication and authorization · Multiple-levels of security (MLS) · Firewall access controls and audits 	
	9.4	Cryptographic Encryption	<ul style="list-style-type: none"> · Data encryption · Key management and escrow 	<ul style="list-style-type: none"> · Digital signatures for nonrepudiation · Digital certificates
		Uniqueness Testing		<ul style="list-style-type: none"> · Time stamping and name binding of data Secure domain naming
	9.5	Integrity Checking		<ul style="list-style-type: none"> · Data integrity checks (change detection)
		Intrusion Detection, Response		<ul style="list-style-type: none"> · Attack detection · Malicious (e.g. virus) logic detection
	9.6	Fault Tolerant Computing		<ul style="list-style-type: none"> · Redundant and clustered architectures · Survivable network with diversity, variability
		Restoration		<ul style="list-style-type: none"> · Data archiving · Recovery · Malicious logic inoculation
	9.7 9.9	Assessment Analysis Simulation	<ul style="list-style-type: none"> · Network access scanner, assessment tools · Audit and tracing tools · Attack diagnosis and vulnerability evaluation · System simulation 	

Figure 9.1 Fundamental elements of information assurance related to security properties and technical security mechanisms.

9.2 Principles of Trusted Computing and Networking

Traditional INFOSEC measures applied to computing provided protection from the internal category of attacks. “Trusted computing” processes were defined in the 1980s in trusted computer security evaluation criteria (TCSEC) defined by the National Computer Security Center (NCSC) guides, known as the “Rainbow Series.” (See the “TCSEC,” the classic document referred to as the “orange book” [23–27].) These criteria establish the requirements against which commercial computers (and networked systems) are evaluated for secure applications. Rather than design requirements, the criteria are structured to provide an evaluation tool to quantify (to discrete levels) the relative level of security achieved by any particular implementation.

For over a decade, the TCSEC standard has defined the criteria for four divisions (or levels) of trust, each successively more stringent than the level preceding it.

- *D: Minimal protection*—Security is based on physical and procedural controls only; no security is defined for the information system.
- *C: Discretionary protection*—Users (subjects), their actions, and data (objects) are controlled and audited. Access to objects is restricted based upon the identify of subjects.
- *B: Mandatory protection*—Subjects and objects are assigned sensitivity labels (that identify security levels) that are used to control access by an independent reference monitor that mediates all actions by subjects.
- *A: Verified protection*—Highest level of trust, which includes formal design specifications and verification against the formal security model.

The TCSEC defines requirements in four areas: security policy, accountability, assurance, and documentation. Figure 9.2 summarizes the security evaluation requirements specified in the TCSEC, and the successive application of those requirements to the C, B, and A levels (and six classes) that rate the degree of security trust. (D, which constitutes the seventh TCSEC class, is not included in the table because no trust criteria apply.) Notice that some criteria (e.g., system testing) increase with every successive class, while others have common criteria across several classes (e.g., identification and authentication requirements are the same for B and A classes).

		Protection Division:		B			A
		C		Mandatory Protection			Verified Protection
<i>Characteristics:</i>		Discretionary Protection		<ul style="list-style-type: none"> Accountability of subjects and their actions by sensitivity labels that identify security level of both subjects and objects (data) Sensitivity labels enforce access controls via a reference monitor 			<ul style="list-style-type: none"> Full B3 protection Formal security design and verification process
		<ul style="list-style-type: none"> Protection by need-to-know basis Accountability of subjects and their actions via audit trails 					
<i>Class:</i>		C1 Discretionary	C2 Control Access	B1 Labeled Protect	B2 Structure Protect	B3 Security Domains	A1 Verified Design
Area	Trust Criteria						
Security Policy Model	Discretionary Access Control	1	2			3	
	Object Reuse		1	2			
	Sensitivity Labels			1	2		
	Label Integrity				1		
	Export Label Info				1		
	Export to Multilevel Devices				1		
	Label Output				1		
	Mandatory Access Controls			1	2		
	Subject Sensitivity Labels			1	2		
Accountability	Device Labels			1	2		
	Identification and Authentication	1	2	3			
	Audit		1	2	3	4	5
Assurance	Trusted Path				1	2	
	System Architecture	1	2	3	4	5	
	System Integrity	1	2				
	System Testing	1	2	3	4	5	6
	Design Spec and Verification			1	2	3	4
	Covert Channel Analysis				1	2	3
	Trusted Facility Management				1	2	
	Configuration Management				1	2	
	Trusted Recovery					1	2
	Trusted Distribution						1
Documentation	Security User Guide	1	2				
	Trusted Facility Manual	1	2	3	4	5	
	Test Documentation	1			2		3
	Design Documentation	1		2	3	4	5

Legend: No Requirement: Requirement Level N: N

Figure 9.2 TCSEC evaluation criteria and trust classes.

Most commercial computer systems achieve C1 or C2 ratings, while A and B ratings are achieved only by dedicated security design and testing with those ratings as a design objective.

The following paragraphs summarize the emphasis of the trust criteria listed in the figure for each of the four areas of security.

Security Policy Model

At the core of the concept of trust is a formal security policy model that mathematically defines a trusted computing base (TCB) as an abstract model. The model includes the notion of a secure state of the TCB, subjects (users that access the TCB), objects (datasets in the TCB), and actions that the TCB performs. The model describes these fundamental actions (e.g., modes by which subjects gain permissions to access objects: read, write, execute, add, modify, and delete) and the state transitions of the TCB. The model permits analysis and provides a means of proof that any given TCB architecture implementation (hardware, software, or firmware in combination) always remains in secure states. The C, B, and A division requirements impose increasing security properties on the policy implemented in the TCB.

Based on the Bell-LaPadula model referenced earlier, the TCB defines “sensitivity labels” that identify the security levels of subjects or objects, and security-level relationships between all subjects and objects based on those labels. An object or subject at one level *A* is *dominated by* another object or subject at another level *B* if the label of *A* is less than or equal to that of *B*. The labels of all objects/subjects are defined and the relation is used to mediate access in the TCB. Fundamental security properties of the model include (1) simple security property (a subject may have read access to an object only if its security level dominates that of the object), and (2) confinement or “star” property (a subject may have write access to an object only if the security level of the subject dominates the object). These properties and other rules that govern other permission modes form the kernel of the TCB (“reference monitor” or “validation mechanism”). This kernel controls *every* access of subjects to objects based on labels, must be immune to tampering, and must be sufficiently small that it is subject to complete analysis and testing to assure that no security holes exist.

The TCB model also allows the construction of complex trusted architectures by ordering TCB subsets in such a manner that overall security properties are assured by maintaining dependencies of higher level components on more primitive components.

Security policy also addresses controls over the reuse of storage objects to assure that any subjects having access to an object (e.g., a storage space on disk) cannot have access to residual information (ciphertext or plaintext) that may remain (e.g., by “magnetic remanence” or residual magnetic flux on storage media) from the object.

Accountability

User identification and authentication (by user ID and password, respectively) is required at all levels, with increasing audit controls at higher classes. Methods

to record all access to the protected objects are required, and at higher classes, increasing monitor functions audit security-relevant events that may indicate the imminent violation of security policy. Response functions are also required to protect the TCB from potential violations. At the B2 and higher levels, a trusted communication path must exist between users and the TCB.

Assurance

The system architecture that implements the TCB must meet design structure requirements (i.e., increasingly restrictive Bell LaPadula model properties by class designation), a means of testing integrity (periodic evaluation), and be subject to comprehensive penetration testing to verify that the implementation enforces the security policy. The architecture must also demonstrate that exploitation or *covert channels* do not exist in the system design. Such channels are any means of communicating information regarding the TCB operation to a subject external to the TCB (in violation of the security policy). Common covert channels, for example, are design flaws in two areas that might provide a mechanism for attackers to gain information from an incomplete TCB.

- *Covert timing channel*—The timing of behavior (e.g., use of resources, accesses) of subject A may, in effect, be modulated to communicate information to a second observing subject, B, at a different sensitivity level.
- *Covert storage channel*—If two subjects (processes A and B with different sensitivity labels) share a memory storage resource (e.g., disk sector) and A leaves residual information (without erasure) in storage, B may gain unauthorized access to that information.

At B and A levels, dedicated security procedures must be defined for management of the facility (user and administrator separation), configuration, and recovery from disruption. For the A1 class, a trusted distribution facility must be maintained to develop, test, and distribute updates (hardware, software, and firmware) to site systems.

Documentation

Increasing levels of documentation of the design, test methods, facility operations, and user operations are also required as the levels of protection class increase.

This overview of the TCSEC illustrates the criteria for a single computer, though the protection principles have been extended to multilevel security for networked computers in the “Ted Book” companion [28] to the orange

book (also abbreviated the “TNI”). Networks pose significant challenges to security.

- *Heterogeneous systems*—The variety of types and configurations of systems (e.g., hardware platforms, operating systems), security labeling, access controls, and protocols make security analysis and certification formidable.
- *Path security*—Lack of control over communication paths through the network may expose data packets to hostile processes.
- *Complexity*—The complexity of the network alone provides many opportunities for design, configuration, and implementation vulnerabilities (e.g., covert channels) while making comprehensive analysis formidable.

Trusted networks require the properties already identified, plus three additional property areas identified in the TNI.

1. *Communications integrity*—Network users must be authenticated by secure means that prevent spoofing (imitating a valid user or replaying a previously sent valid message). The integrity of message contents must be protected (confidentiality), and a means must be provided to prove that a message has been sent and received (nonrepudiation).
2. *Protection from service denial*—Networks must sustain attacks to deny service by providing a means of network management and monitoring to assure continuity of service.
3. *Compromise protection services*—Networks must also have physical and information structure protections to maintain confidentiality of the traffic flow (externals) and message contents (internals). This requirement also imposes selective routing capabilities, which permit control of the physical and topological paths that network traffic traverse.

The concept of “layers” of trust or security is applied to networks, in which the security of each layer is defined and measures are taken to control access between layers and to protect information transferred across the layers. Figure 9.3 illustrates the typical view of multiple layers of network security.

The U.S. National Security Agency has developed a network security model (NSM) methodology for assessing network security using a quantitative evaluation of personnel, operating procedures, architecture, and physical

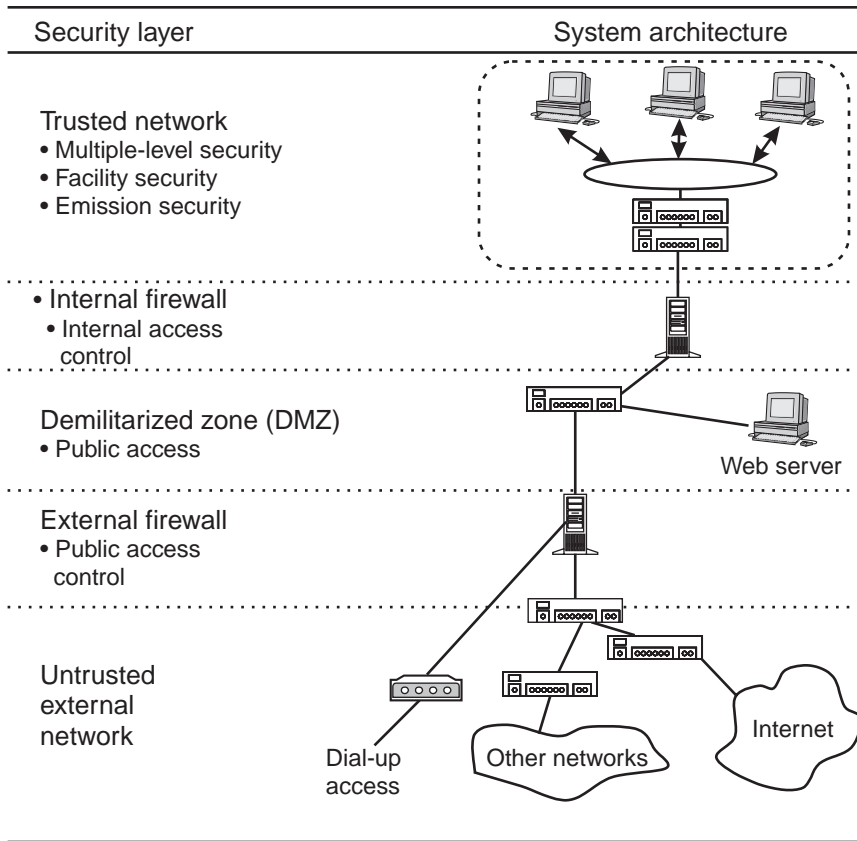


Figure 9.3 Typical commercial multiple-layer network security architecture.

environment for each of four security properties: confidentiality, integrity, availability, and service availability [29]. Scoring of security is based on a hierarchy of evidence, claims, weighted factors, and thresholds that define secure or unsecure.

A trusted system security capability maturity model is also in development to establish ISO-9000 like standards for IA systems developers.

As the effectiveness of strong security authentication and site-to-site encryption approaches have improved, several approaches to conducting secure transactions over the untrusted portion of the GII have emerged. These approaches use the GII (Internet) as the backbone network between sites, as alternatives to dedicated leased lines or frame relay networks with dedicated end-to-end encryption. The direct approach introduces a standard secure Internet Protocol (IPsec) that allows the Internet to be used as a secure wide area

network (S/WAN) [30]. The indirect approach, or “virtual private networking,” uses nonstandard vendor-developed secure protocols to “tunnel” through the open network using the less secure current IP properties.

9.3 Authentication and Access Control

The fundamental security mechanism of single or networked systems is the control of access to authentic users. The process of authentication requires the user to verify identity to establish access, and access controls restrict the processes that may be performed by the authenticated user or users attempting to gain authentication.

9.3.1 Secure Authentication and Access Control Functions

Authentication of a user in a secure manner requires a mechanism that verifies the identity of the requesting user to a stated degree of assurance. The major authentication mechanisms (and the countermeasures employed to attack them) are enumerated in Table 9.3 to summarize the alternatives available to system designers.

Remote authentication and granting of network access is similar to the functions performed by military identification friend or foe (IFF) systems, which also require very high authentication rates. In network systems, as in IFF, cryptographic means combined with other properties provide high confidence and practical authentication. A variety of methods combining several mechanisms into an integrated system is usually required to achieve required levels of security for secure network applications [31].

A relatively complex password authentication system, employed in the MIT-developed Kerberos authentication and key distribution system for UNIX, illustrates the use of sequential authentication steps to perform remote authentication over an unsecured network (this prevents an attacker from capturing a password by wiretapping the net or “sniffing” by software). The Kerberos authentication protocol includes the following steps (all across open channels):

1. *Initial request*—A user (X) seeking to be authenticated issues a request to an authentication server (AS) to be authenticated and to use a network service (a session on server S) by sending ID (but no password).
2. *AS server reply*—The AS looks up the ID of X, verifies access privileges, and uses the secret password of X to encrypt two items into a

Table 9.3
Common Authentication Methods and Countermeasures

Authentication Basis	Authentication Mechanism	Countermeasures
Personal knowledge	Static (reusable) passwords and personal ID number (PIN) known to user	Password may be captured (packet sniffing or intercept) or guessed and reused
	Dynamic (one-time) passwords generated by a sequential dynamic algorithm, dependent upon time or query sequence	Password log or generation sequence must be captured or guessed
Personal ownership or possession, or location	Challenge and response: electronic token or smart card device provides unique response to authenticator's challenge (effectively a one-time password)	Valid challenge-response pair must be captured and replayed within time validity window, or response signature scheme broken Capture token
	Address-based response: callback system establishes connection by calling the requestor to verify source by the telecommunication path	Compromise callback process to route authentication connection to attacker, spoofing the callback process
	Location-based response: user must respond with valid GPS location to verify physical location on earth using location token	Physical location must be captured and GPS data must be spoofed Capture token
	Cryptographic authentication: electronic token or smart card device provides cryptographic exchange (digital signature)	Key management or encryption system must be compromised or broken Capture token
Personal characteristics	Biometric: discrimination of unique human physiological signature Retinal scan Fingerprint Facial thermography Voiceprint	Requires capture of signature and/or physiological forgery
	Physical implant of token device in human body	Requires capture of signature and/or physiological forgery

- package: (1) a ticket-granting ticket, and (2) a session key for subsequent steps. AS sends the encrypted package back to X.
3. *Initial authentication*—User X enters password at the workstation, where it is used to decrypt the package (only the valid user can properly decrypt). The user can now request specific services by using the issued session key to encrypt a service request message including the received ticket-granting ticket with authentication and sending it to a ticket-granting server (TGS).
 4. *TGS server reply*—The TGS, like the AS, decrypts the service request message from X with knowledge of X's identity, password, and session key. TGS examines the contents to authenticate X and the validity of the ticket-granting ticket. The TGS creates and sends a new ticket for the requested service and a new session key to X, encrypted with the old session key.
 5. *Final authentication at server S*—The user may now pass the encrypted service ticket and authentication data to the desired server, S, to gain access to the desired services.

While the Kerberos has been available on the Internet and adopted by numerous organizations as a strong system, vulnerabilities have been reported on early versions. Brute force attacks on the DES encryption used by Kerberos have been demonstrated to allow successful penetration of the network [32].

9.3.2 Secure Access Systems: Firewalls

Firewalls are trusted systems that integrate authentication, connection control, incident-response, encryption, network structure security, and content security into a single secure unit. Located between two networks, all traffic passing between the networks must pass through the firewall, which restricts passage to only authorized traffic allowed by the security policy. The firewall, as a trusted component, must be immune to penetration. The firewall effectively creates a security “domain” or “enclave” by providing a perimeter defense to a network (the secured domain) and may be employed in “nested layers” of increasing restriction of access.

Connection Control

As in any trusted component, at the core of a firewall is the security policy, a detailed technical statement of what transactions may occur across the firewall boundary. Two basic policy alternatives (extremes) exist.

- *Permit any service unless explicitly denied*—In this case, all possible threat attempts must be technically defined (permissive policy).
- *Deny any service unless explicitly permitted*—In this case, all possible valid service access activities must be technically defined (restrictive policy).

In either case, the firewall maintains exhaustive lists of technical descriptions (rules or scripts) that provide the traffic control functions. Traditional firewalls control traffic by several security functions.

1. *Authentication*—Authentication is required to initiate a session of activities, and may be required throughout the session to ensure that an intruder has not “hijacked” a legitimate transaction.
2. *Packet filtering*—Individual packets are inspected for source addresses, destination addresses, and ports to filter out unauthorized traffic based on addresses. (Because packet addresses are not secure, this method is vulnerable to address spoofing.)
3. *Application filtering*—Service requests are filtered on the basis of requested applications, and proxy (surrogate) application programs *within the firewall* perform the requested services, rather than host programs on the protected internal network. The proxy applications are restricted to only service functions that meet security policy and prevent external traffic from requesting access to internal network resources. The proxy acts as a trusted broker for the external requestor, who never has direct access to internal network resources. (Because the firewall has two separate network connections, this configuration may also be referred to as a “dual-homed gateway.”)
4. *State and context analysis*—The most thorough filter process inspects external traffic at all system (ISO) levels to *understand* the requested activities.
 - Communication information is inspected at link, network, transport, and session layers to understand the traffic path and intended type of activity; the complete session is then observed to verify continuity of state.
 - Application and presentation-level states are inspected to verify continuity of authentication, use of authorized services, and encryption activities.

5. *Combination of all methods*—Designers may implement combinations of the above functions to provide appropriate protection for any given application.

Figure 9.4 illustrates the three basic firewall implementations, which offer increasing sophistication in control of network traffic to and from the domain protected by the firewall.

The design of the firewall must follow the principles of trusted computer architectures, developed earlier, to enforce fundamental security policies, accountability, and assurance.

Category	Characteristics	Architecture
Packet-filtering router or gateway	<ol style="list-style-type: none"> 1. Operates at the network level only 2. Inspect source and destination addresses, and ports 3. Maintain list of acceptable addresses and ports; pass or drop packets on basis of rules 	
Application-level gateway or "proxy" server	<ol style="list-style-type: none"> 1. Operates at the application-level and monitors session activities 2. Firewall server maintains independent "proxy" application services with rigid security controls 3. Proxy performs applications and restricts operations to subset of secure operations (proxies do not have root privileges) 	
State and context inspection	<ol style="list-style-type: none"> 1. State of the packets are inspected—addresses, transport methods, users, applications 2. Context of the states of activities are inspected—sequence of packets and application activities 3. Combined state and context rules allow or disallow access 4. Throughput performance is influenced by level of analysis required for all activities 	

Figure 9.4 Basic firewall alternatives provide increasing degrees of inspection of transactions across the wall.

Incident Detection and Response

These inspection functions also identify connection attempts to exploit the system vulnerabilities, and allow the firewall to respond in accordance with defensive security policies. Section 9.5 describes the functions of incident detection and response, some of which may be integrated into firewalls.

Authentication

Using the authentication means described earlier in this section, the firewall can authenticate users over the established connection (in-band) or can establish a separate connection (out-of-band) with the external user's host to secure the authentication. This firewall authentication is independent of the authentication required by the user's workstation and the authentication required by the internal network application accessed by the remote user.

Network Structure Security

The firewall can translate external addresses to internal addresses, maintaining security of the internal network topology and address structure.

Content Security

Application-level filtering, and state/context inspection processes detect and screen potentially harmful content inbound for the secure domain. Malicious code, executable content (e.g., ActiveX and Java), and other hostile incoming content may be blocked, while outgoing content may also be screened to block selected information from leaking to the external network.

Encryption

Encryption can be added to the firewall to provide virtual private networking capabilities between authenticated remote users and the firewall.

A number of texts describe the details of these functions, firewall engineering, the range of commercial products available, and the methods of scripting the detailed technical restrictions of security policy into actual firewall systems [33–36].

Firewall access control applies to security for “internal” attacks (defined in the last chapter) seeking to gain direct access to the targeted information system. External attacks transmit data directly to sensors of some networks (e.g., civil air traffic control radar, military C4I sensors) that are subject to electronic attack, as introduced in Chapter 6. Security must also include conventional electronic warfare sensor counter-countermeasures (CCM) that provide basic protection from these external attacks, including the following:

- Monitors detect jamming and overload patterns using templates that characterize disruption attacks. Certain deceptive inputs can also be detected (with greater uncertainty than disruption) at the sensor.
- Filters can be applied once disruption is detected, filtering the source data by spatial region, mode, type, or temporal characteristics to block the disruption source.
- Limiting or prioritizing functions can assure that disruptive (jamming) sources cannot overload the level 1 fusion processing.

The desired effect of CCM techniques is to provide a gracefully degraded performance (capacity, accuracy, and confidence in information) with an indication to the next level processing that a disruption or deception source is present.

9.4 Cryptographic Encryption Measures

Cryptography provides the mathematical processes for transforming data (by encryption and decryption) between an open, or *plaintext*, format and a secure *ciphertext* format to provide the privacy property. The strength of the encryption algorithm (the *cipher*) is a measure of the degree to which the ciphertext endures cryptanalysis attacks (see Section 8.6.1) that seek to break the cipher and discover the plaintext, eliminating privacy. Because of the inherent security of the processes, cryptographic techniques provide privacy for messages, authentication of users, and assurance of delivery and receipt of messages (non-repudiation).

The ultimate strength and generality of cryptographic processes lies in the mathematical formulation of the underlying transform algorithms. This introduction provides a functional introduction, but mathematical treatments in a number of texts are necessary for further understanding of the cryptosystems described here (see [37–39]).

The general cryptosystem (Figure 9.5) includes the cryptographic message path that includes the encryption, transmission, and decryption process, and a supporting method of distributing a numerical variable, or key, that controls the encryption transformation. The following subsections describe each of these processes for data encryption and the use of encryption to create digital signatures for authentication and nonrepudiation.

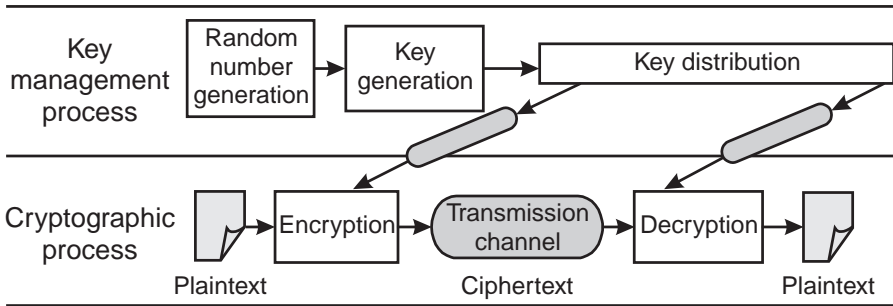


Figure 9.5 Basic elements of a cryptographic system.

9.4.1 Encryption Alternatives

Encryption processes apply substitution, permutation, or number theoretic methods (or combinations of these) to transform plaintext to ciphertext. The key variables that control the transformation algorithms provide the capability to change the transformation, and therefore the number of possible keys (the key space) directly influences the strength of the algorithm against attack. Keying is the process of changing the key variable: as a function of a time schedule (e.g., hourly, daily); each communication session; each individual message; or continuously, synchronized throughout the encryption process (key streaming).

A basic taxonomy of common cryptosystems (Figure 9.6) distinguishes, at the top level, between public and private (secret) algorithms.

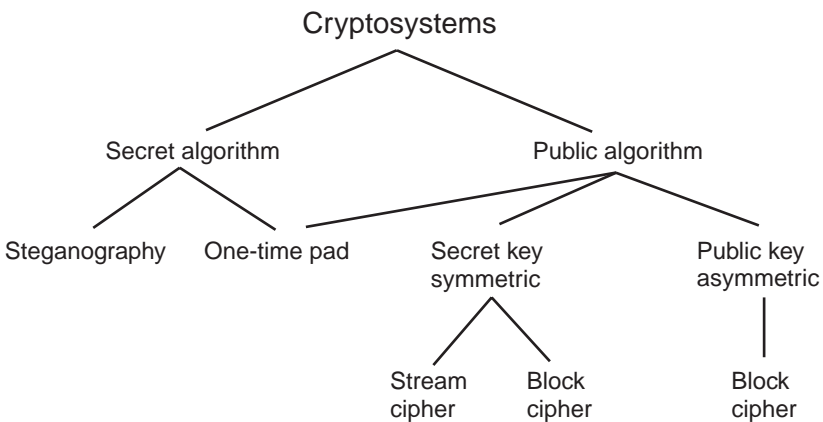


Figure 9.6 Taxonomy of common cryptosystems.

Secret Algorithms

These algorithms maintain security by the covertness of the algorithm or the existence of the communication channel. The classic “one-time pad” provides perfect secrecy (it is mathematically unbreakable at the expense of a large, unique key for each message sent) and can be considered either a secret or public algorithm, depending upon application. The classic formulation of a one-time pad algorithm with a one-time key follows.

Consider a finite set of binary plaintext messages, P , of length n (bits), and a finite set of binary keys, K , of length n (bits). There exists a finite set of ciphertext messages, C , of length n (bits) that can be computed by the encryption rule that computes the vector sum (modulo 2) of a given plaintext message, p , and a randomly chosen key, k . Decryption is performed by computing the vector sum (modulo 2) of a received ciphertext message, c , and k to produce p .

While this cipher appears simple, it requires a key as long as the message and a new random key selection (and/or algorithm) for each message. Useful for critical messages, the one-time pad is not practical for bulk encryption of data.

Steganography (or data hiding) is a branch of cryptography that encrypts data by “hiding” the ciphertext within a covert communication medium. The ciphertext may be hidden *within* a text, audio image, or video data stream in such a way that the data stream appears undisturbed, and it is not apparent that the message even exists.

For example, imagery-based steganographic processes “embed” data within a digital image in such a fashion that the embedded information is encrypted, and the perturbation to the image is not distinguishable to the eye [40]. One such process follows a typical encryption sequence [41].

1. The original image, I , is processed to compute a metric that describes the noise component inherent to I .
2. A secret key, k , is computed as a function of the noise metric.
3. A secret data message, m , (up to 20% of the size of I) is embedded into I by computing an embedded image I' , which is a function of k , I , and m .
4. I' is transmitted to the intended recipient by a public channel, and the secret key is transmitted via a secure channel.
5. The recipient decrypts the embedded message using K and I' , and restores the original image I .

Steganographic processes such as this can provide digital watermarks for digital data, as well as performing secret algorithm cryptography in which data is securely passed across covert channels (e.g., the image, or another digital data channel with sufficient redundancy).

Public Algorithms

The most common need for encryption is for bulk encryption of significant volumes of data that are transmitted over known transmission paths (e.g., satellite links, landlines, wireless links, local or wide area computer networks) Public algorithms provide the practical approach to standardize the wide distribution of cryptosystems for high-volume applications where the public may know the algorithms but the keys maintain the secrecy.

The method of keying the cryptosystem distinguishes the two fundamental approaches to public algorithms (Figure 9.7 illustrates a one-direction path for simplicity). Classical secret-key systems employed by the military provide a means of distributing secret keys to the sender and receiver, and synchronizing the use of the keys for appropriate messages. The architecture, called “symmetric,” makes uniform use of the key at both ends of the system. The U.S. data

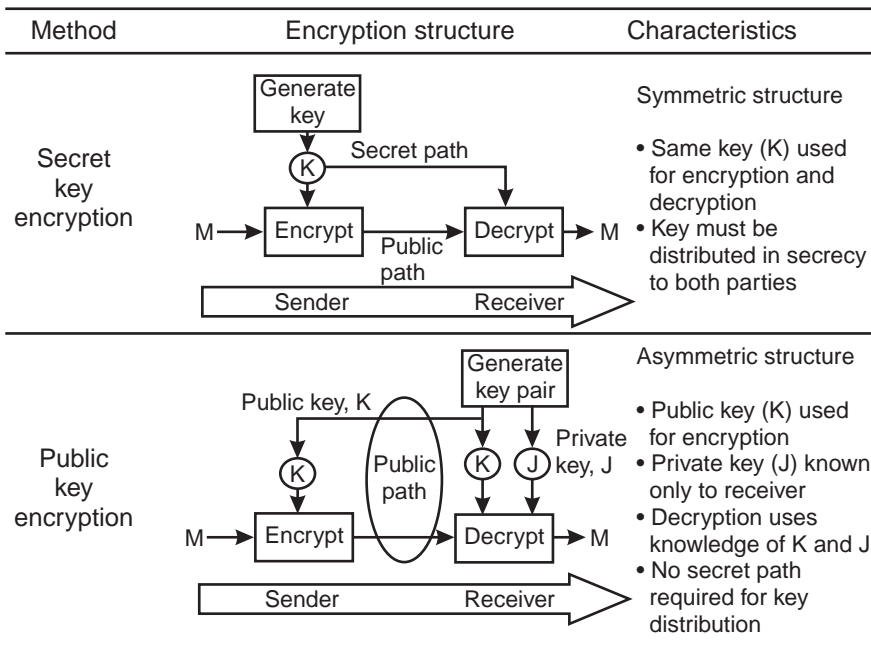


Figure 9.7 Comparison of private- and public-key cryptosystems.

encryption standard (DES) is the best-known secret-key algorithm, which encrypts 64-bit blocks using a 56-bit key.

In contrast, the more recently developed asymmetric or public-key cryptosystem eliminates the requirement for transmission of the secret key to both parties [42]. In the one-way illustration in the figure, the public-key system works as follows:

1. The receiver computes a public- and private-key pair (K and J , respectively), using a key generation algorithm that applies knowledge of the *one-way trap-door property* that is the basis of the ciphers. K allows the sender to compute the function in the forward direction (encryption), J allows the receiver to perform the inverse of the function (decryption, the trap door). Knowledge of K is insufficient to perform the inverse, so even the sender cannot decrypt a known message.
2. The public key (K) is sent to the sender over an open channel.
3. The sender encrypts the plaintext message M with K using the *one-way function* of the encryption algorithm and transmits the message over an open channel to the receiver.
4. Using the private key J (known only to the receiver), the receiver is able to decrypt the ciphertext using the trap-door property of the cipher to produce M .

Notice that the receiver can publish the public key, and anyone can send a secure message to the receiver, but only the receiver is able to decrypt the messages. The security of the system is based on the inability of an attacker to compute the private key from the public key.

Secret-key algorithms are computationally more efficient than public-key systems, and are therefore more suitable for high-rate “bulk” data encryption. (For a given processing rate, a secret-key encryption may run 1,000 to 10,000 times faster than public-key algorithm for equivalent security.)

Table 9.4 summarizes the characteristics of major cryptosystems at the time of writing. The U.S. government controls the export of cryptosystems based on security “strength” or resistance to attack, which is a function of the key length. State-of-the-art computational capabilities (and mathematical factoring capabilities) continue to improve, making the threshold between “weak” and “strong” change with time. At the time of writing, 512- and 56-bit key lengths (public and private key systems, respectively) are considered to be “strong.”

Table 9.4
Summary of Common Cryptosystems

Type	System	Characteristics	Comments
Secret key	Data encryption standard (DES)	56-bit key, 16-round iteration 64-bit block cipher	U.S. standard (1977) for financial and commercial applications Multiple modes of use; triple DES iteration uses 112-bit key
	International data encryption algorithm (IDEA)	128-bit key, 8-round iteration 64-bit block cipher	Similar to DES, applied to some UNIX systems for network security
	SKIPJACK	80-bit key, 32-round iteration Block cipher	U.S. standard implemented in Clipper (telephone) and Capstone (data) chips; integrated with escrowed key encryption standard (EES)
	RC2	Variable 40-, 56-bit key 64-bit block cipher	Proprietary RSA algorithm—exportable replacement for DES
	RC4	Variable size key Stream cipher	Proprietary RSA algorithm
	RC5	Up to 2,048-bit key and 0- to 255-round iteration with 32-, 64-, 128-bit blocks	Proprietary block cipher algorithm
Public key	Diffie-Helman	Basic algorithm with multiple specific implementations	Applicable to key exchange between two parties without prior secret key
	RSA	512-key standard (may be expanded) Provides encryption and authentication	Patented algorithm by RSA, Inc.; widely used for network, Internet applications
	Pretty good privacy (PGP)	Combines techniques from IDEA and RSA	Software algorithm, used for e-mail security to provide integrated privacy and authentication
	El Gamal	Basic algorithm with multiple specific implementations	Based on discrete logarithm one-way function; used for key management

9.4.2 Digital Signatures

In addition to providing privacy, the encryption process provides a means of authentication of a message by an encrypted data item called a digital signature. The digital signature permits proof of identity of the sender, and proof that an attacker has not modified the message. Public-key encryption concepts provide a convenient basis to create digital signatures, as illustrated in the following simplified example operation (which expands on the earlier public-key example):

1. A sender prepares a plaintext message, M , to send to a receiver, whose public key is K .
2. The sender computes a digital signature (unique to the message). A “hash” function computes a short fixed-length “message digest,” D , which is unique to M . D is then encrypted by the sender’s own public key, Q , creating the signature S .
3. The sender appends S to M , creating a “signed message” M' .
4. The sender encrypts M' with K using the *one-way function* of the encryption algorithm and transmits the message over an open channel to the receiver.
5. Using the receiver’s private key, J (known only to the receiver), the receiver is able to decrypt the ciphertext using the trap-door property of the cipher to produce M' . The receiver separates M and S .
6. Using the sender’s public key, Q , the receiver decrypts S , leaving the message digest D .
7. The receiver now applies the hash function to M to compute a derived message digest D' for comparison with the decrypted D . A perfect match validates both the integrity of M and the authenticity of the source.

While this simple example illustrates the basic principle of signatures, many possible implementations exist, either as secret or public algorithms, depending upon the application.

9.4.3 Key Management

The generation, storage, distribution, and overall protection of keys is critical to the security of all cryptosystems—public or private algorithms. Compromised keys provide the most direct means of unauthorized access. For this

reason, physical, information, and perceptual layers of security must protect the key management functions, including those summarized below.

- *Key security policy*—A specific security policy must define the controls for the full life cycle of keys (generation, distribution, activation, destruction, or lifetime escrow storage) and controls for usage.
- *Key layering hierarchy*—Keys may be defined in “layers,” in which higher level keys are used to encrypt lower level keys for distribution.
- *Key separation*—Keys may be separated into components for distribution on separate channels or for retention by separate parties (for added security), with provisions for construction of the complete key by the computing function of the individual components.
- *Keying period control*—The validity period of keys (the “cryptoperiod”) is defined as a function of time, system state, or other variable, and must be distributed with the keys to users.
- *Key escrow*—Some systems provide an escrow capability, in which data is held in historical escrow by a “trusted third party” to permit future recovery of session keys and decryption of messages if legally authorized by a government organization. The U.S. Escrowed Encryption Standard (EES) defines one approach to key escrowing [43].

9.5 Incident Detection and Response

Traditional computer security distinguishes auditing from alarm reporting. Security *auditing* reviews the records of activities to detect security incidents (including changes in operational configuration), to verify compliance with security policy, and to test security controls. Security *alarm reporting* monitors security-related events that may indicate misuse of security controls or configurations, hostile activities against security controls, or behaviors inconsistent with security policy. Automated detection of incidents and immediate alarm reporting and response is required to respond to structured information warfare attacks on networks. The manual audits and analyses of the past have limited the damage from unstructured incidents, but are ineffective for high-speed structured threats.

Automatic detection and reporting is required for a wide range of threatening actions, including the following:

- *External intrusions*—Attempts to gain unauthorized access via firewalls and other external ports (e.g., routers, gateways, dial-up modems). The

U.S. DOE computer incident advisory capability (CIAC) classifies these intrusions as type 1 (remote attacks on network and dial-up services) and type 3 (server attacks on client applications, through executable applets accepted from external sources).

- *Internal security intrusions*—Internal attempts to violate security policy by authorized users (e.g., attempts to access data above level of authorization, insert malicious logic, access to system resources, creation of covert channel). The CIAC refers to these as type 2 intrusions.
- *System failures*—Failure of security mechanisms that affect the integrity of security.
- *Anomalous behavior*—Abnormal behavior of system components or processes that may indicate a security-related incident.

The major categories of security-related incidents (Table 9.5) each have unique system-level response alternatives. In virtually all cases, a pager message and status monitor report alert the security administrator, detailed audit logging is initiated, and reports are issued to other trusted network nodes as appropriate.

As in all alarm systems, false alarm (“false positives”) and detection failure (“false negatives”) rates measure overall detection performance. Extensive studies of network intrusion detection have documented the technical challenge of achieving comprehensive detection on complex networks [44,45]. There are several technical approaches to implementing detection mechanisms including the following:

1. *Known pattern templates*—Activities that follow *specific* sequences (e.g., attempts to exploit a known vulnerability, repeated password attacks, virus code signatures, etc.) of identified threats may be used to detect incidents. For example, Courtney, a detection program developed by the Lawrence Livermore National Laboratory, specifically detects the distinctive scan pattern of the SATAN vulnerability scanning tool.
2. *Threatening behavior templates*—Activities that follow *general* patterns that may jeopardize security are modeled and applied as detection criteria. Statistical, neural network, and heuristic detection mechanisms can detect such general patterns, but the challenge is to maintain an acceptably low false alarm rate with such general templates.
3. *Traffic analysis*—Network packets are inspected within a network to analyze source and destination as an initial filter for suspicious access

Table 9.5
Incident Categories, Types, and Responses

Category	Incident Types	Typical Responses
Network I&W	Normal advisory	Determine own vulnerability Curtail vulnerable services until corrective action
	Network-wide structured attack advisory	Increase alert status Tighten filters and protective measures for similar incidents
External incidents	Scanning, probing	Tighten protective measures
	Intrusion attempts (dial-up or network)	Seduce scanner to "honeypot" or virtual system and monitor Initiate net trace and trap measures Selectively deny address access Terminate offending connections
	Denial of service attacks	Selectively control service responses Attempt source identification
Internal activities	Change in trust state or detection of invalid digital signature	Change security level of system Terminate secure activities Initiate antiviral or system diagnostics
	Malicious code: installation, residence, or activation	Terminate operations Initiate antiviral or other diagnostic
	System fault	Change security level of system Terminate secure activities Initiate system diagnostics
	Insider unauthorized access attempt	Tighten protective measures Seduce insider to "honeypot" or virtual system and monitor Initiate trace and trap measures

activities. If packets are addressed to cross security boundaries, the internal packet contents are inspected for further evidence of intrusive or unauthorized activity (e.g., outgoing packets may be inspected for keywords, data contents; inbound packets for executable content) [46].

4. *State-based detection*—Changes in system states (i.e., safe or “trusted” to unsafe transitions as described in Section 9.2) provide a means of detecting vulnerable actions.

A comprehensive network detection system, modeled after the data fusion architecture (introduced in Chapter 3), combines evidence from a variety of sensors and sources of security-related events. These reports are correlated, combined into a network threat situation, and assessed for impact and response (Figure 9.8). Detection “sensors” monitor packet traffic prior to the firewall, at modems on the internal network, and detection mechanisms within the firewall and trusted computers also supply incident reports.

Responses to incident detections can range from self-protective measures (terminate offending session and modify security policy) to offensive reactions,

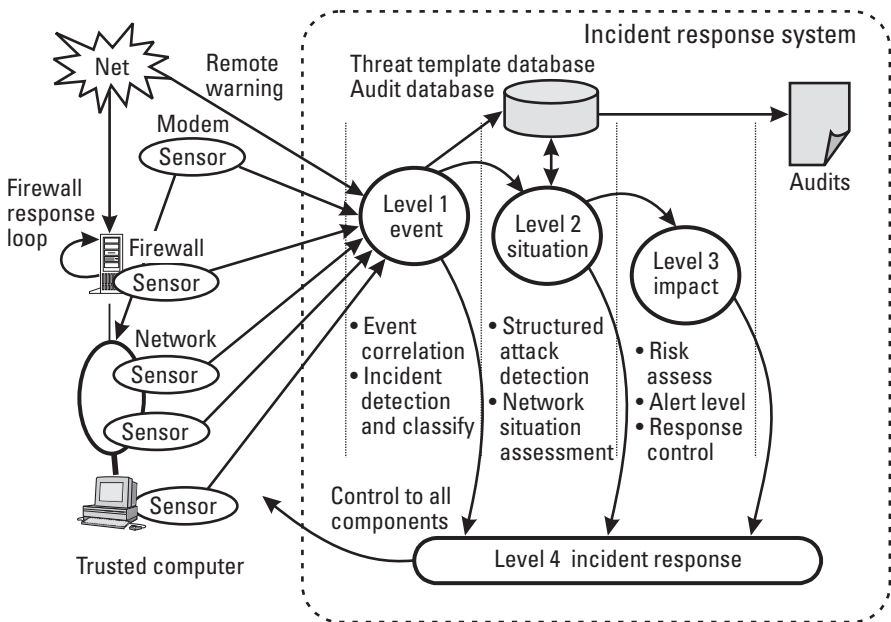


Figure 9.8 Network incident detection architecture follows data fusion model.

if the source of attack can be identified. In order to identify attackers, *entrapment* measures that are used include the deliberate insertion of an apparent security hole into a system. The intruder is seduced (through the entrapment hole) into a virtual system (often called the “honey pot”) that appears to be real and allows the intruder to carry out an apparent attack while the target system “observes” the attack. During this period, the intruder’s actions are audited and telecommunication tracing activities can be initiated to identify the source of the attack. Some firewall products include such entrapment mechanisms, presenting common or subtle security holes to attackers’ scanners to focus the intruder’s attention on the virtual system.

In addition to technical detection and response for protection, conventional investigative responses to identify and locate network or electronic attack intruders are required for deterrence (e.g., to respond with criminal prosecution or military reprisal). Insight into the general methodology for investigating ongoing unstructured attacks on networks is provided by a representative response that was performed in 1994 by the Air Force Computer Emergency Response Team (AFCERT) from the U.S. Information Warfare Center [47].

1. *Auditing*—Analyze audit records of attack activities and determine extent of compromise. The audit records of computer actions and telecommunication transmissions must be time-synchronized to follow the time sequence of data transactions from the target, through intermediate network systems, to the attacker. (Audit tracking is greatly aided by synchronization of all telecommunication and network logging to common national or international time standards.)
2. *Content monitoring*—Covertly monitor the content of ongoing intrusion actions to capture detailed keystrokes or packets sent by the attacker in these attacks.
3. *Context monitoring*—Remotely monitor Internet traffic along the connection path to determine probable telecommunication paths from source to target. This monitoring may require court-ordered “trap and trace” techniques applied to conventional telecommunication lines.
4. *End-game search*—Using evidence about likely physical or cyber location and characteristics of the attacker, other sources (HUMINT informants, OSINT, other standard investigative methods) are applied to search the reduced set of candidates to locate the attacker.

9.6 Survivable Information Structures

Beyond the capabilities to detect and respond to attacks is the overall desired property of information system survivability to provide the following characteristics:

- *Fault tolerance*—Ability to withstand attacks, gracefully degrade (rather than “crash”), and allocate resources to respond;
- *Robust, adaptive response*—Ability to detect the presence of a wide range of complex and subtle anomalous events (including events never before observed), to allocate critical tasks to surviving components, to isolate the failed nodes, and to develop appropriate responses in near real time;
- *Distribution and variability*—Distributed defenses with no single-point vulnerability, and with sufficient diversity in implementations to avoid common design vulnerabilities that allow single attack mechanisms to cascade to all components;
- *Recovery and restoration*—Ability to assess damage, plan recovery, and achieve full restoration of services and information.

Survivable systems are also defined by structure rather than properties (as above), characterizing such a system as one comprised of many individual survivable clusters that “self-extend,” transferring threat and service data to less capable nodes to improve overall health of the system [48]. While the technology to provide these capabilities in an automated fashion is beyond the state of the art, CERT teams of experts perform these functions now to provide system survivability. Recognizing the need for robust automated protection of complex systems (the entire information infrastructure) that have inevitable vulnerabilities, many have turned to the model of the biological immune system to envision adaptive survivable structures. Martin Libicki has summarized the layers (response sequences) of the human immune defense system and enumerated several potential implications to survivability designs for information systems [49]. Libicki concluded a large system of systems must employ distributed agents that can coordinate in both recognition of an intrusion and in development of tailored responses to achieve high levels of systemic security as exhibited in biological immune systems.

The analogy to the human immune defenses includes four layers of response to an attack by a pathogen (a penetrating microorganism), with each layer representing a more serious level of penetration and response (Table 9.6).

Table 9.6

Biological Immune Response Compared to Survivable Information System Response

Layer Sequence	Biological Response Components	Survivable Info System Analogy
Physical barriers ↓	Skin Protective mucus membranes and acids (stomach)	Access control Firewalls
Innate immunity response to infection ↓	Recognition of known pathogens and affected cells Release attack cells PMS cells for antigens Release NK cells for viruses	DEDUCTIVE incident detection based on templates of known attackers and attack patterns, and detection of system failures
Acquired immunity response ↓	Recognition of new hostile pathogens Issue lymphocytes (B cells and T cells) to bind to the pathogen, marking it as an antigen for attack	INDUCTIVE-ABDUCTIVE incident detection based upon anomalous behavior and damage reported
Mobilization and counterattack	Appropriate antibodies are released to destroy marked pathogens, to isolate and destroy infected cells	Inoculation and removal of known malicious logic or creation of tailored response to the newly discovered attack mechanism Isolation of untrusted nodes

Many independent and cooperating cells provide this extremely complex biological security system, which successfully protects against an incomprehensible array of threats (e.g., injuries and diseases). Many have suggested that robust information system survivability must also apply a complex of autonomous software agents rather than a monolithic intrusion detection component (which will be the first target of an attacker) [50].

Conventional approaches to increase the reliability and recovery capabilities of computer networks contribute to fault tolerance, recovery, and restoration. Multiple processors and “clustering” of systems to provide mutual support contribute to survivability properties, especially when the clustered processors exhibit variability. Server clusters may share memory resources and high-speed links to provide scalability (under normal conditions) or fault tolerance (in the face of failure or attack) [51]. The use of “warm” (partially configured) or “hot” (fully configured) backup computer facilities are traditional

survivability solutions, as well as frequent backup of information on storage media to permit resumption of processing.

The U.S. Defense Advanced Research Projects Agency (DARPA) survivability program applies a “public health system” model that applies (1) distributed immune system detection, (2) active probing to diagnose an attack and report to the general network population, (3) reassignment of critical tasks to trusted components, (4) quarantine processes to segregate untrusted components, and (5) immunization of the general network population [52]. The DARPA program is developing the technology to provide automated survivability tools for large-scale systems.

9.7 Defense Tools and Services

System and network administrators require a variety of tools to perform security assessments (evaluation of the security of a system against a policy or standard) and *audits* (tracing the sequence of actions related to a specific security-relevant event). Table 9.7 enumerates the major categories of tools and services applied to security administration.

In the following paragraphs, we describe the general functions of the most common tools and services.

Vulnerability Scanners

A variety of software packages perform exhaustive scans for potential implementation or configuration vulnerabilities to the operating system (from operating system terminals), to intranets, and the firewall or other access to external nets (including enabled Internet services) [53].

Scanner software tools test access via dial-up modems, Internet, or internal connections (Figure 9.9) to evaluate performance against the security policy enforced. An increasing number of such tools are being developed by the government (Ice Pick) and commercial vendors (e.g., Internet Scanner, Pingware, NetProbe, and SATAN) [54]. A database of known security vulnerabilities forms the base for scanning, and updates are continuously provided by advisory services from a CERT or the scanner manufacturer. Excursions about the baseline vulnerabilities are performed to detect and log any existing holes or vulnerabilities in the tested system configuration. Scans can be nondestructive (locate vulnerability) or destructive and obtrusive (locate and exploit denial of service vulnerability, for example, which may crash a system) in nature. In addition to searching for exploitable holes, scanners also search for evidence of prior

Table 9.7
Major Security Tools and Services

Category	Description
Tools	<p><i>Vulnerability scanners</i>—Perform exhaustive internal and external scan for potential implementation or configuration vulnerabilities</p> <p><i>Content scanner and antivirus tools</i>—Scan files, memory, and downloads for evidence of malicious logic, viral infection; check file integrity; and observe behavior for viral activities</p> <p><i>Password scanner</i>—Scans user-selected passwords for vulnerabilities</p> <p><i>Integrity scanner</i>—Scans files to verify digital signatures are intact to assure integrity (nonmodification)</p>
Services	<p><i>Independent risk analysis</i>—Assessment of facility and system risks by independent team</p> <p><i>Scanner updates</i>—Frequent updates to antivirus and vulnerability scanners based on current intelligence</p> <p><i>Security advisories</i>—Deliver advisories on threat activities, discovered vulnerabilities, patches, and holes</p> <p><i>Certification</i>—Conducts independent verification (scheduled and random spot checks) of the implementation of a defined security program, and certifies that a defined level of security is achieved</p>

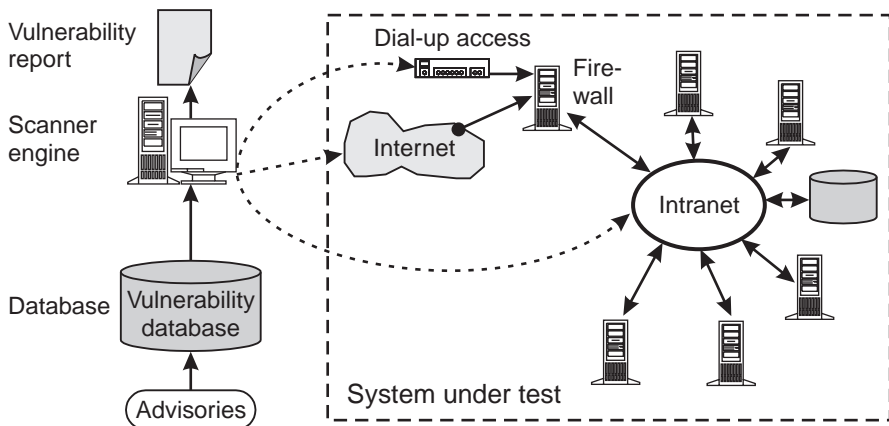


Figure 9.9 Vulnerability scanner evaluates all potential access paths for exposure.

malicious activity: changed modes, changed directories, modified system files, or unauthorized installed applications. A scanner may also integrate user password checking to make sure passwords are not easily cracked. It may also provide integrity scanning by appending digital signatures to critical system files to verify, from scan to scan, that no modifications have occurred.

The output of the scanner is a vulnerability report, with recommendations for changes to mitigate risks and achieve desired levels of security.

Content Scanning Tools

These tools scan the data and programs within a processor or network to search for malicious contents. The most well known are antiviral tools that examine processes, files, memory, and downloads for evidence of viral infection for a variety of viral strains. The following categories of detection methods are applied:

- *Signature scanning*—A scanner searches through all files in storage (static files and memory-resident code) to examine for signatures of viruses. Such scanning can locate the static code sequences of simple viruses or the unchanged components of decryption or mutation engines (see the methods described earlier in Section 8.6.3.). Each file is also scanned as it is accessed during run time.
- *Integrity checking*—The checker performs digital change detection by computing digital signatures for clean files, then performing routine checking to verify that the file remains unmodified. A signature mismatch identifies infected (changed) files with modified contents, because the computed signature does not match the previously stored signature. (Early viruses countered simple checksum and cyclic redundancy check signatures; signatures that are more complex significantly strengthen the value of integrity checking.)
- *Behavior blocking*—Viral behaviors (e.g., attempts to modify boot sectors, system files, perform encryption/decryption and code mutation) are monitored by independent monitors in real time. Suspicious code is executed in “virtual” processors to allow observation of code behavior to detect viruses by their actions.
- *Restoration*—Infected files are disinfected by cleaning (removing viral code) or replacement with a verified backup copy.

Comprehensive integration of antiviral tools use blockers to prevent infection, integrity checkers to detect the presence of an infection, scanners to determine the strain of the virus, and restoration to reinstate the system to a

disinfected state. Selection of appropriate tools depends upon the application to individual computers or networks and the vulnerabilities to viral attack [55].

Independent Risk Analysis Services

Software tools and independent consulting services provide comprehensive assessments of facility and system risks [56]. The analysis tools require the collection of data on assets, potential threats, security safeguards (physical, technical and administrative procedures), and policy. Administrators and users are queried on procedures and use patterns, and all safeguards are exhaustively enumerated in the software tool to compute risk factors across a wide spectrum of threats. The risk analysis may also apply vulnerability scanners in “red team” attacks to measure actual exposure. The service provides an assessment of security posture: vulnerabilities, consequences of those vulnerabilities, deficiencies, and risk (degree of potential losses). The report of the analysis also includes recommendations for changes to meet security policy.

Tool Update Services

Antiviral tool and vulnerability scanner vendors provide frequent technical updates to users based on current intelligence and discovered vulnerabilities from users.

Security Advisory Services

CERT organizations deliver advisories on threat activities, incidents, discovered vulnerabilities, and patches to permit rapid correction of vulnerabilities.

Certification

Independent organizations, such as the International Computer Security Association (ICSA), conduct independent verification (scheduled and random spot checks) of the implementation of an organization’s security program, and certify that a defined level of security is achieved.

9.8 Physical-Level System Security

In addition to the information-level network and electronic assurance measures developed in the last section, physical-level measures must be implemented to prevent the capture and affect types of countermeasures described in the last chapter. Physical security includes measures in two areas.

- *Physical and personnel security* includes protection of the physical equipment, communication paths, and facilities (including supporting

utilities) from physical penetration, protection of personnel, and clearance of personnel to protect from insider attacks. This level of security, while fundamental, is not described here, and the reader is referred to comprehensive security texts and reports (see [57–59]).

- *Electromagnetic hardening* provides protection from the compromise of activities and internal information content due to hostile intercept of signals on intended paths (e.g., network cables) or unintended paths (e.g., unintended radiated signals), while also protecting from damage or disruption due to directed energy attacks.

Table 9.8 compares the defensive measures to the attacker’s physical counterparts (refer back to Section 8.6).

This section focuses on the role and methods of electromagnetic hardening to perform dual functions.

- Abating electromagnetic paths that leak unintentional emanations;
- Blocking paths through which directed energy weapons (DEW) can couple damaging energy into electronic equipment.

From a design standpoint, these functions are closely connected, although we discuss each function separately for clarity.

Table 9.8
Physical-Level Defensive Measures

Attack Objectives	Offensive Measures	Defensive Countermeasures
Capture information	“Wiretap” network signal paths Intercept unintentional signal emanations	Physical security to deny access to pathways, detection methods Electromagnetic hardening (passive) and jamming (active) to reduce emanations to secure levels
Affect information	Kinematic and chemical biological weapons Directed energy weapons (e.g., HPM, HEL, EMP)	Physical security to protect perimeter denies access to cables, antennas, etc. Electromagnetic hardening to reduce vulnerability to pulsed energy

Capture Threats

To prevent the capture of information via physical or electromagnetic intercept, the defender must protect against vulnerabilities along both intentional and unintentional paths of access available to the attacker (Figure 9.10).

Physical facility security must protect internal signal lines (intentional paths) from physical wiretapping (spliced electrical or fiber-optic line, or inductive electrical pickup), which can gain deep access to internal signals. Physical inspections, line impedance monitors, time-domain reflectometry, and RF spectrum analysis (to detect RF transmission of tapped signals to an external source) are the fundamental tools to detect the presence of planted taps. The use of end-to-end encryption on internal paths (e.g., network LANs) provides supporting security to reduce the value of intercepted traffic on facility signal paths.

Electromagnetic security is required to protect from the potential for external intercept of compromising signals on unintended signal paths conducted along signal or power lines, or radiated from equipment or interconnecting lines. The study and specification of far-field signal levels, and methods of their intercept and suppression, have been conducted by several national intelligence organizations, but details have not been released to the public [60]. The U.S. TEMPEST activities, conducted by the National Security Agency have developed emission standards, design, control, and testing procedures for securing information systems from compromising emanations [61]. (See [62] for a historical overview of the TEMPEST program.) TEMPEST requirements are specified in a series of classified National COMSEC Information Memoranda (NACSIM), Instructions (NACSI), and National COMSEC/EMSEC

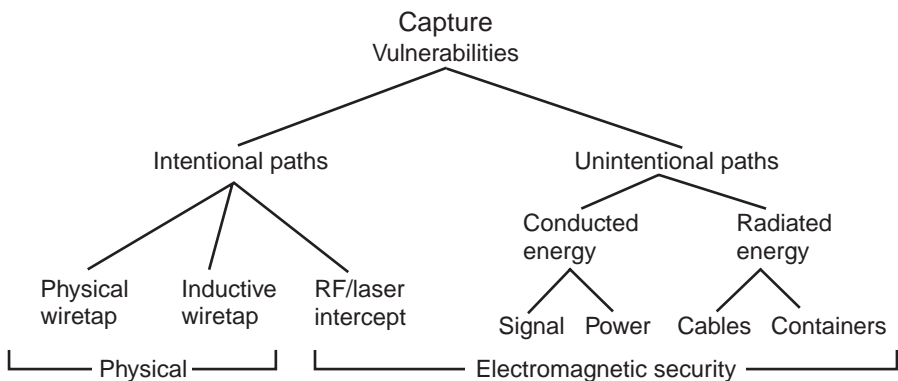


Figure 9.10 Taxonomy of capture vulnerabilities.

documents (NACSEM) [63]. The U.S. Army Corps of Engineers unclassified engineering and design pamphlet, *Electromagnetic Pulse (EMP) and TEMPEST Protection for Facilities*, provides a qualitative overview of TEMPEST guidelines with limited quantitative insight into emission factors for 50 and 100 dB shielded facilities [64]. The NACSIM/NACSEM documents define and quantify at the engineering performance level such items as the following [65]:

- *RED/BLACK separation*—The categorization of internal/plaintext (RED) and external/ciphertext (BLACK) areas of equipment, and the types of coupled signals (leakage) that can cross red/black interfaces and compromise encryption are defined (see cryptographic attacks in Section 8.6.1). RED/BLACK isolation is required to prevent cryptographic attacks that access both plain and ciphertext for a common message.
- *Emanation spectra*—Narrowband and broadband signal spectra levels are specified for conducted and radiated emanation suppression to achieve security.
- *Testing methods*—Radiated and conductive testing procedures and equipment are defined (antennas, conducted sensors, receivers and tuners, spectrum analyzers, line impedance stabilization networks, correlators, and displays).
- *Control techniques*—Design techniques to control the level of signal emanations to achieve security requirements are defined, with guidelines for implementing each technique and calculating expected levels of isolation.

Table 9.9 summarizes the major categories of emanation controls that are required to suppress RED and BLACK radiated and conducted emanations. The major protection controls are numbered in the table and are illustrated by numbered callouts in Figure 9.11 for a typical installation. A comprehensive security program such as TEMPEST requires emanation-level specifications that define levels of security, design guidelines, and specifications, and test methods to certify compliance of any particular component design. In addition, facility-level monitoring may be required to certify the integration of components in a given site configuration. The expense and emanation suppression achieved for any comprehensive emanation protection program must be considered within the overall risk management plan.

The unintentional RF emissions from CRT displays (popularly referred to as “van Eck” emissions [66]) have been widely reported as an extremely

Table 9.9
Electromagnetic Emanation Protection Measures

Unintentional Emanation Category	Target	Fig 9.11 Ref. No.	Electromagnetic Protection Controls
Radiated energy	Facilities	1	Establishment of physical “zones” of susceptible signal levels and secure denied access perimeter around facility at the range of acceptable signal levels
		2	RF shielded glass, screens, and wall materials
		3	RF shielded computing areas, “Screen Rooms”
		4	RF seals, screens, and baffles for utility penetrations (e.g., power, telephone, water, air conditioning) into shielded areas
		5	Grounding and isolation for RF shields
		6	Active broadband jammers for external areas
	Equipment (racks, units, and cards)	7	RF shielded equipment (Faraday cage)
		8	Leakage control for equipment apertures (e.g., slits, slots, cooling filters)
		9	Conductive seals: gaskets, caulk, and epoxies
		10	Grounding for RF shields
	Lines	—	Prevention of control degradation via corrosion
		—	RED/BLACK physical separation
11		RED/BLACK interface filters (electronic) RED/BLACK electro-optical coupling	
12		Fiberoptic cabling and interfaces Electrical cable shielding	
Conducted energy	Signal lines	—	RED/BLACK interface filters (electronic) RED/BLACK electro-optical coupling Fiber-optic cabling and interfaces Ferrite sleeves (“split beads,” torroids) around cables Spurious signal introduction
	Power lines	—	Power supply filtering AC line filtering

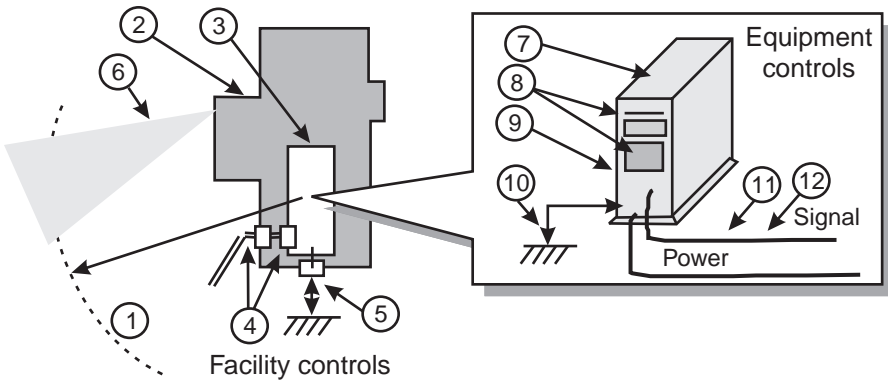


Figure 9.11 Electromagnetic emanations controls (see reference numbers in Table 9.9).

vulnerable RED emanation that may be detected at ranges up to a kilometer. Reports claim that a single CRT can be discriminated from many units and reconstructed to provide the external interceptor a complete view of the targeted video or computer monitor. Keyboard cables and RS-232 serial signal cables also pose the risk of emanating unintentional radiation. Commercial architects are developing procedures to protect commercial office buildings using TEMPEST-like principles due to these vulnerabilities and the threat of corporate-level information warfare activities [67].

Combinations of shielding, filtering, and sealing methods described in the table provide the desired levels of signal suppression (from 50 to 100 dB over frequencies ranging from tens of kilohertz to tens of gigahertz). These levels, when combined with physical protection to prohibit access to hostile monitoring within a defined perimeter or “zone,” provide a high level of security from the intercept of emanations.

Attack Threats

The engineering disciplines that analyze, measure, and establish signal emission standards for electromagnetic compatibility (EMC) and electromagnetic interference (EMI) are applicable to the issues of electromagnetic attack threats. Commercial and military EMI deal with the design controls required to mitigate interference (due to natural radio noise sources, co-interfering sources, and man-made noise due to sources such as generators or motors). EMC maintains operational compatibility among collocated electrical and electronic equipment (e.g., RF transmitters and receivers). U.S. military EMC standards for EMC design and test, [68,69] respectively, provide methods to protect against high-energy pulses from lightning and high-altitude EMP (HEMP)

from nuclear bursts, and are applicable to protection from the DEW threats. EMI/EMC and TEMPEST control methods are similar and complementary.

The effects of EMP attacks (described earlier in Section 8.7.3) can result from electric field energy directly radiated on the targeted system, or by being conducted to the target through electrical power, signals, antennas, or conductive utility feeds.

HEMP (and future DEW weapons) may produce voltage transients on exterior lines on the order of megavolts. The resulting EMP electric and magnetic fields induced on interior conducted paths may produce currents (that may reach thousands of amperes) or voltage transients (thousands of volts, peak) capable of severe damage on unprotected systems. The shielding and isolation methods described to reduce emanations also protect information systems from DEW threats. Hardening measures (Table 9.10) are tailored to the potential paths and coupling mechanism vulnerabilities for any given site.

A series of shielding barriers (concentric “zones”) at the facility, area (room), and equipment levels may be used to provide robust protection for equipment located within the innermost zone. Common grounding, shielded cables, and “vaults” to seal cable penetrations of each barrier are required to prevent leakage and coupling of energy from layer to layer. RFI seals and gaskets are required to protect doors from leakage.

9.9 Security Analysis and Simulation for Defensive Operations

Security analysis and simulation processes must be applied to determine the degree of risk to the system, to identify design, configuration, or other faults and vulnerabilities, and to verify compliance with the requirements of the security policy and model. Depending on the system and its application, the analysis can range from an informal evaluation to a comprehensive and exhaustive analysis. (See [70] for comments from the U.S. Defense Science Board on the need for security engineering.)

Figure 9.12 provides the general process flow that is initiated with the system requirement document that defines the level of security required, the system functions, and the threat. System-level security management requirements, such as those recommended by the Advanced Battlespace Information System (ABIS) Task Force (Table 9.11 [71]), must be translated to specific function requirements which are allocated to system elements (e.g., communication, links, trusted computing bases, sensors, and networks).

The first step in the analysis process includes an assessment of the threats (the existence or predicted existence of means to attack the system, and the objectives of those attacks) to the system, based on intelligence and

Table 9.10
General EMP Hardening Measures

DEW-to-Target Paths	EMP Coupling Mechanisms	Hardening Measures
Radiated paths	Diffusion through RFI shields or leakage through apertures, and cable penetrations through the shield	<p>Conducting facility shield (solid welded metal, screen or rebar-mesh reinforced concrete); RFI shielded doors with “fingerstock” hinges and grounding system</p> <p>Dual-door entries that act as waveguides to cut off interference</p> <p>RFI seals for all utility entries</p> <p>Waveguide cutoff protection for ventilation vents</p>
Conducted paths	Coupling of energy onto external overhead cables, antennas, utility lines (or conductive pipes), buried cables, or internal site cable networks (after diffusing or leaking into site)	<p>On-site electrical generators</p> <p>Isolation from utility mains (power feeds) by uninterruptible power supplies (UPS), motor-generator sets, or hydraulic isolation</p> <p>Physical and dielectric isolation of conducting utility pipes and ducts</p> <p>Electromagnetic isolation of telephone signal lines by electro-optical coupling, electronic filters or waveguide cutoffs</p> <p>Equipment-level protection for:</p> <ol style="list-style-type: none"> 1. Amplitude effects: surge protection (“crowbar” or “clamp” circuits) 2. Frequency effects: lowpass or bandpass filters to provide insertion losses at EMP broadband frequencies

extrapolation of technology capabilities. The vulnerability assessment hypothesizes (at the functional level) the areas of likely access (internal and external) and assesses the relative vulnerability (or security weaknesses) to attack. Vulnerabilities can be attributed to source utilization, distribution and dependency (as

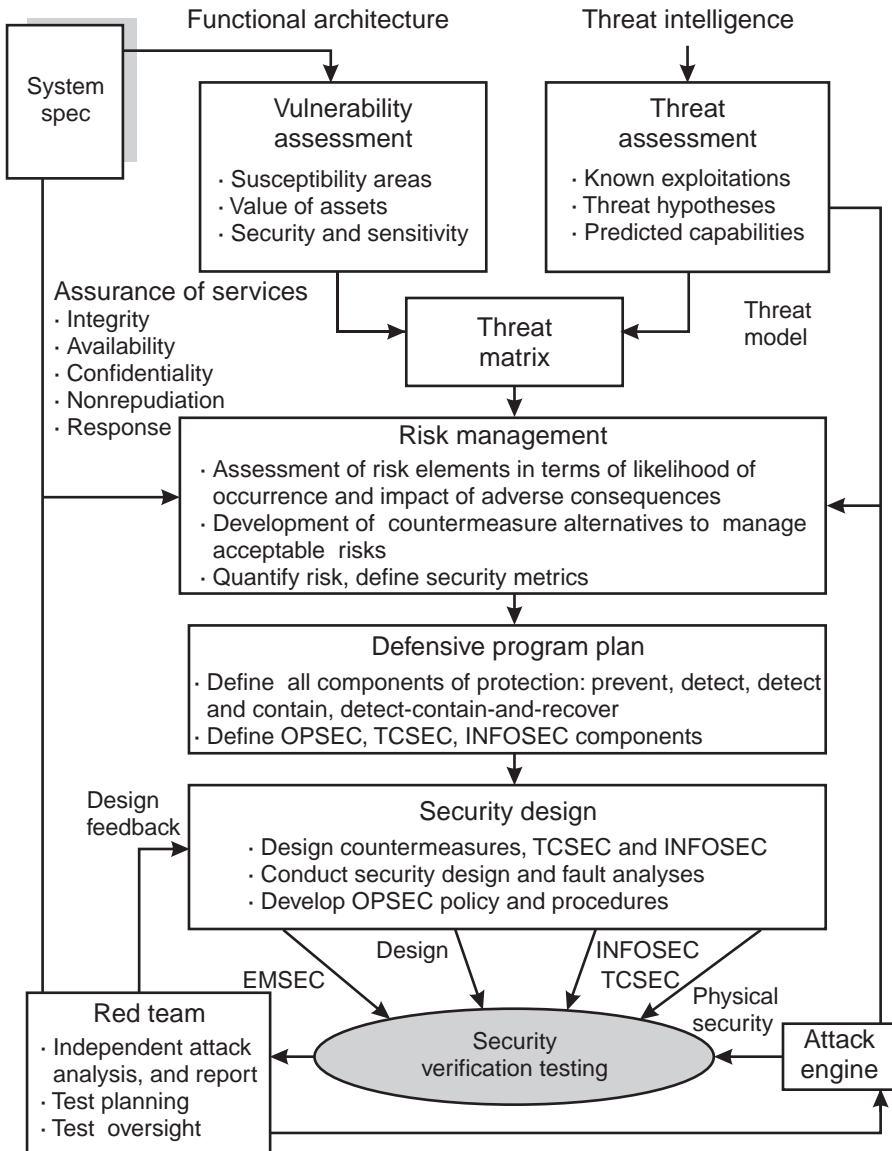


Figure 9.12 Security analysis and design process manages risk, which is a function of both system vulnerability and potential external threats.

shown in Section 8.4.1 for C2 systems), or to failures in analysis, design, implementation, or operation of the network or system.

Table 9.11
ABIS Information Service Assurance Response Goals for Real Time C4I

Information Assurance Area	System-Level Goals
Real-time C4I	Detection, correlation, and characterization of IW events, within 1 second Localization of IW attacks, development of traces, and threat assessment, within 10 sec Coordination across grid management [with other fusion nodes], within 30 sec Response to IW attack, within 1 min Dissemination of IW attack advisories, within 1 min Damage control and restoration of services and information, within 3 min
Unconventional attacks	Protection for EMP, conductive particle clouds Protection from corrosive agents, chemical and biological
Protection for operational circuits	Total protection from nuisance threats: Disposable jammers 10W at 25 to 50 miles Protection for principal circuits from small tactical jammers: ~100 to 200W at 50 miles
Grid status, incident detection, implication assessment, and visualization	Simulated impacts on information ops presented to network managers for management decisions: within 1 min for tactical network within 10 min for operational and strategic backbone

The result of the threat and vulnerability assessment is a threat matrix that categorizes threats (by attack category) and vulnerabilities (by functions). The matrix provides a relative ranking of the likelihood of threats and the potential adverse impact of attacks to each area of vulnerability. These data form the basis for the risk assessment.

The risk management process begins by assessing the risks to the system that are posed by the risk matrix. Risks are quantified in terms of likelihood of occurrence and degree of adverse impact if they occur. On the basis of this ranking of risks, a risk management approach that meets the security requirement of the system is developed. This process may require modeling to determine the effects of various threats, measured in terms of IW MOP or MOEs, and the statistical probability of successful access to influence the system.

Security performance is quantified in terms of risk, including four components: (1) percent of attacks detected; (2) percent detected and contained; (3) percent detected, contained, and recovered; and (4) percent of residual risk.

This phase introduces three risk management alternatives.

- *Accept risk*—If the threat is unlikely and the adverse impact is marginal, the risk may be accepted and no further security requirements imposed.
- *Mitigate (or manage) risk*—If the risk is moderate, measures may be taken to minimize the likelihood of occurrence or the adverse impact, or both. These measures may include a combination of OPSEC, TCSEC, INFOSEC, or internal design requirements, but the combined effect must be analyzed to achieve the desired reduction in risk to meet the top-level system requirements.
- *Avoid risk*—For the most severe risks, characterized by high attack likelihood or severe adverse impact, or both, a risk avoidance approach may be chosen. Here, the highest level of mitigation processes are applied (high level of security measures) to achieve a sufficiently low probability that the risk will occur in operation of the system.

When the threats and vulnerabilities are understood, the risks are quantified and measures are applied to control the balance of risk to utility to meet top-level security requirements, and overall system risk is managed.

The defensive program plan applies the measures developed (and modeled or simulated) in the risk management phase and applies them to the requirements for design, technical, and physical security.

In formal systems design, this effort is performed concurrent with the functional and physical design of the system and derives the security requirement section of flowed-down design specifications. The security design requirements will include items such as the following:

1. Formal model, and INFOSEC and TCSEC hardware and software requirements and restrictions (referencing standard security requirements documents);
2. Indications and warnings that monitor functional requirements;
3. Attack detection, analysis, and tracing of functional requirements;
4. Attack recording, audit trail annotating, and reporting of functional requirements;
5. Backup database storage and data communication link requirements;

6. Restoration and recovery of services functional requirements;
7. Alternate modes of operation (for different levels of security or states of operation during attack and recovery);
8. Functional requirements for “minimum essential services” during attack and recovery from attack.

The design stage then implements the design, which must undergo design analysis and security verification testing. An exhaustive and comprehensive analysis for design errors (omissions, commissions, or oversight of flaws) may be performed using processes such as a detailed security fault analysis to verify compliance with the security model [72]. An independent red team may also be chosen to conduct the security verification testing, which implements the threat model in an attack engine to conduct simulated attacks on the system to evaluate actual security performance.

Red team attacks (also called “penetration testing”) target the physical and operational security as well as the technical aspects of the system. The results of the red team verification may result in design changes to assure compliance with the system security requirements.

9.10 Summary

In this chapter, we have surveyed only the surface of the broad scope of information assurance measures. With the ever-increasing complexity of computer and telecommunication networks (and the software that operates them), control of the potential vulnerabilities makes assurance a daunting challenge. The U.S. Defense Science Board has concluded that fundamental research, on the order of that which led to preeminence in cryptographic theory over past decades, is required to provide credible information assurance in future systems:

The development of robust survivable distributed systems resistant to information warfare attack, as well as other types of failure, requires major advances in theory, modeling and technology, and the combined efforts of a vigorous research community embracing academia, industry, and government. Prior R&D efforts have focused on specific areas, such as computer and network security, encryption, technology, operating system environments with multilevel security features and coping with network outages caused by single node failures, etc. Little attention has been paid to the ab initio design and implementation of systems capable of surviving willful malicious attack, or detecting and tolerating corrupted software.

Even less attention has been paid to the non-*ab initio* case, where the system must incorporate legacy subsystems that are not under the designer's control [73].

As in all forms of defense, information assurance requires vigilance and persistent improvement in the methods of protection at the perceptual, information, and physical levels of information warfare. Technology must support protective measures at all three levels, where vulnerabilities will continually increase even as our networked system complexities increase.

Endnotes

- [1] DoD Directive S-3600.1, "Information Operations," Dec. 9, 1996. (Cited in DARPA Information Assurance Briefing Oct. 8, 1997, URL: <http://www.hokie.bs1.prc.com/ia/ia.htm>.)
- [2] DoD Directive 5200.1, "DoD Information Security Program," Dec. 13, 1996. The Directive prescribes procedures for implementation of Executive Order 12958, "Classified National Security Information," Apr. 20, 1995, within the Department of Defense. Regulation 5200.1-R "Information Security Program," Jan. 1997, implements the directive.
- [3] Definition adapted from *Glossary of Computer Security Terms*, NCSC-TG-004, National Computer Security Center, Version 1, Oct. 21, 1988.
- [4] During this period, the U.S. National Computer Security Center "Rainbow Series" of requirements documents were developed for trusted computing, and in 1987 were expanded to include networked computing with the publication of NCSC-TG-005 *Trusted Network Interpretation of the TCSEC (TNI)*, (Red Book).
- [5] The interested reader is referred to the following classic papers on security modeling:
Bell, D. E., and L. J. La Padula, "Secure Computer Systems: Mathematical Foundations," MTR-2547-I, (AD 770 768), The MITRE Corporation, Bedford, MA, Mar. 1973.
Bell, D. E., "Secure Computer Systems: A Refinement of the Mathematical Model," MTR 2547-III, (AD 780 528), The MITRE Corporation, Bedford, MA, Dec. 1973.
Bell, D. E., and L. J. La Padula, "Secure Computer Systems: Unified Exposition and Multics Interpretation," MTR-2997, (AY/W 020 445), The MITRE Corporation, Bedford, MA, July 1975.
- [6] Tinto, M., "The Design and Evaluation of INFOSEC Systems: The Computer Security Contribution to the Composition Discussion," NCSA Technical Report 32-92, June 1992.
- [7] Ware, W. H., *Security, Privacy, and New Technology*, Santa Monica, CA: RAND, Document P-6606, 1981.
- [8] Ware, W. H., *Security, Privacy, and National Vulnerability*, Santa Monica, CA: RAND, Document P-6628, 1981.

- [9] Ware, W. H., *A Taxonomy for Privacy*, Santa Monica, CA: RAND, Document P-6708, 1981.
- [10] Ware, W. H., *Information Systems, Security, and Privacy*, Santa Monica, CA: RAND, Document P-6930, 1983.
- [11] *Information Technology Security Evaluation Criteria (ITSEC)*, Provisional Harmonized Criteria, Version 1.2, Commission of the European Communities, Office for Official Publications, Luxembourg, June 1991.
- [12] "Joint Technical Architecture," U.S. DISA, Section 6: Information Systems Security Standards.
- [13] "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," U.S. General Accounting Office GAO/AIMD-96-84, U.S. Government Printing Office, May 5, 1996.
- [14] Doty, T., "Internet Security: Vulnerabilities, Threats and Mitigation," ACM Professional Development Seminar, University of Maryland, Nov. 1997.
- [15] Hutt, A. E., S. Bosworth, and D. B. Hoyt, *Computer Security Handbook*, New York: John Wiley & Sons, 3d ed., 1995.
- [16] *Site Security Handbook*, Internet Engineering Task Force, Mar. 1996.
- [17] Russell, D., and G. T. Gangemi, Sr., *Computer Security Basics*, Cambridge, MA: O'Reilly & Associates, 1992.
- [18] White, G. B., E. A. Fisch, and U. W. Pooch, *Computer System and Network Security*, Boca Raton, FL: CRC Press, 1996.
- [19] Purser, M., *Secure Data Networking*, Norwood, MA: Artech House, 1993.
- [20] Various lists of security properties and services have been adopted in standards and definitions. We include the following secondary properties within the three fundamentals:

Basic Property	Included Secondary Properties
Confidentiality	Confidentiality of data and traffic flow
Integrity	Authenticity of users
	Security of access to services
	Certification of origin and reception of data
	Nonreputability of transactions
	Auditability and traceability of transactions
Availability	Reliability
	Survivability

-
- [21] "NII Security: The Federal Role." The U.S. Information Infrastructure Task Force (IITF), June 14, 1995.
- [22] *An Introduction to Computer Security: The NIST Handbook*, National Institute of Standards and Technology, Special Publication 800-12, N.D.
- [23] Department of Defense, "Trusted Computer System Evaluation Criteria," DoD 5200.28-STD [Orange Book], Dec. 1985.
- [24] "A Guide to Understanding Discretionary Access Control in Trusted Systems," NCSC-TG-003, Version 1, Sept. 30, 1987.
- [25] "Trusted Database Management System Interpretation," NCSC-TG-021, Version 1, Apr. 1991.
- [26] "Minimum Security Functionality Requirements for Multiuser Operating Systems," Issue 1, NIST Federal Information Processing Standards, Jan. 28, 1992.
- [27] Department of Defense, "Security Requirements for Automated Information Systems (AISs)," DoD Directive 5200.28, Mar. 21, 1988.
- [28] "Trusted Network Interpretation of Trusted Computer System Evaluation Criteria," NCSC-TG-005, National Computer Security Center, July 1987.
- [29] "The Network Rating Model: Methodology for Assessing Network Security," National Security Agency, Second Draft, Oct. 31, 1996.
- [30] At the time of writing, the Internet Engineering Task Force (IETF) is evaluating next-generation Internet Protocols (IP) that will include expanded address space, flow labeling to identify traffic priority, security for packet-level encryption and authentication, and other features. Packet-level security alone will eliminate many of the current threats.
- [31] Opplinger, R., *Authentication Systems for Secure Networks*, Norwood, MA: Artech House, 1996.
- [32] Violino, B., "Students Find Flaw in Kerberos 4," *Digital Tech Web*, CMP Media, Feb. 26, 1996.
- [33] Cheswick, W. R., and S. M. Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker*, New York: Addison-Wesley, 1994.
- [34] Chapman, B., and E. Zwicky, *Building Internet Firewalls*, Cambridge, MA: O'Reilly & Associates, 1995.
- [35] "Deploying Firewalls in a DII COE Environment Running Distributed Computing Environment (DCE) and Common Desktop Environment (CDE)," Defense Information Infrastructure (DII) Common Operating Environment (COE), DISA, Oct. 22, 1996.
- [36] Hare, R. C., and K. Siyan, *Internet Firewalls and Network Security*, Indianapolis, IN: New Riders Publishing, 1995.
- [37] Stinson, D. R., *Cryptography: Theory and Practice*, Boca Raton, FL: CRC Press, 1995.
- [38] Schneier, B., *Applied Cryptography*, New York: John Wiley & Sons, 2d ed., 1996.

- [39] Menezes, A. J., P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, Boca Raton, FL: CRC Press, 1996.
- [40] Johnson, N. F., and S. Jajodia, "Exploring Steganography: Seeing the Unseen," *IEEE Computer*, IEEE, Feb. 1998, pp. 26–34.
- [41] Sanford, M. T., and T. G. Handell, "Data Embedding," Los Alamos National Laboratory, Oct. 1995.
- [42] Diffie, W., and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. On Information Theory*, IT-22, 1976, pp. 644–654.
- [43] "A Proposed Federal Information Processing Standard for an Escrowed Encryption Standard," (EES), NIST, July 30, 1993. Also, FIPS PUB 185, Escrowed Encryption Standard, Feb. 8, 1994.
- [44] Cohen, F., "National INFOSEC Baseline-Intrusion Detection and Response," Sandia National Laboratory, Oct. 1996.
- [45] Denning, D. E., "An Intrusion Detection Model," *IEEE Transactions on Software Engineering*, Vol. SE-13, No. 2, Feb. 1987, pp. 222–232.
- [46] Donetti, J., and S. Elko, "Network Intrusion Detector," *Proc. 1997 DOE Information Security Conference*, Lawrence Livermore National Laboratory, LLNL CSTC 97-055.
- [47] Testimony of Mr. Jim Christy to U.S. Senate Permanent Subcommittee on Investigations, Appendix A: The Case Study—Rome Laboratory, Griffiss Air Force Base, NY Intrusion, June 5, 1996.
- [48] Browne, R., "Defining Survivability," *Proc. of Information Survivability Workshop 97*, IEEE, Feb. 12–13, 1997.
- [49] Libicki, M. C., "Postcards from the Immune System," Essay 5 in *Defending Cyberspace and Other Metaphors*, Washington, D.C.: National Defense University Press, 1997.
- [50] Crosbie, M., and G. Spafford, "Defending a Computer System Using Autonomous Agents," *Proc. 18th National Information Systems Security Conference*, Oct. 1995.
- [51] Harbaugh, L., "Reliability in Clusters," *Information Week*, Mar. 24, 1997, pp. 49 ff.
- [52] Shrobe, H., "Survivability," *Proc. ARPATech '96 Systems and Technology Symposium*, Defense Advanced Research Projects Agency, Washington, D.C., May 1996.
- [53] "Comprehensive Enterprise Network Security Assessment," Internet Security Systems, Atlanta, GA, 1996.
- [54] Surkan, M., "Daemons Defy Hackers," *PC Week*, Feb. 5, 1996.
- [55] Polk, W. T., and L. E. Bassham, *Guide to the Selection of Anti-Virus Tools and Techniques*, National Institute of Standards and Technology, Special Publication 800-5, Dec. 1992.
- [56] Gilbert, I. E., *Guide for Selecting Automated Risk Analysis Tools*, National Institute of Standards and Technology, Special Publication 500-174, Dec. 1990.

-
- [57] *An Introduction to Computer Security: The NIST Handbook*, National Institute of Standards and Technology, Special Publication 800-12, N.D, Section III “Operational Controls.”
- [58] “Executive Guide: Information Security Management,” U.S. General Accounting Office, Exposure Draft, Nov. 1997.
- [59] See DoD Directives 5200.2 (Personnel Security Program) and 5200.8 (Physical Security Program) for basic elements of physical-level security.
- [60] Emanation security programs have been reported in the United States (TEMPEST) and NATO nations (AMSG 720B, Compromising Emanations Laboratory Test Standard).
- [61] The nomenclature “Transient ElectroMagnetic Pulse Emission STandard” is often cited as the basis for TEMPEST.
- [62] Russell, D., and G. T. Gangemi, Sr., *Computer Security Basics*, Cambridge, MA: O’Reilly & Associates, 1992, Chapter 10.
- [63] The fundamental TEMPEST documents (classified documents available to cleared U.S. government organizations and contractors with need to know only) include the following:
- NACSIM 5000, TEMPEST Fundamentals (U), NSA, Feb. 1, 1982.
- NACSIM 5100A, Compromising Emanations Laboratory Test Requirements, Electromagnetics (U), NSA, July 1, 1981.
- NACSIM 5203, Guidelines for Facility Design and RED/BLACK Installation (U), NSA, June 30, 1982.
- NACSEM 5109, TEMPEST Testing Fundamentals (U), NSA.
- NACSEM 5110, TEMPEST Facility Evaluation Criteria (U), NSA, July 1983.
- NACSEM 5201, TEMPEST Guidelines for Equipment/System Design (U), NSA, Sept. 1978.
- [64] *Electromagnetic Pulse (EMP) and TEMPEST Protection for Facilities*, Engineering and Design Pamphlet EP 1110-3-2, U.S. Army Corps of Engineers, Dec. 31, 1990.
- [65] Based on unclassified TEMPEST training course syllabus by Don White Consultants, Inc.
- [66] van Eck, W., “Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?,” *Computers and Security*, Vol. 4, 1985. Also see the follow-up article: “Electronic Eavesdropping Machines for Christmas?,” *Computers and Security*, Vol. 7, No. 4, 1988.
- [67] Wilson, G. R., “Data Security by Design,” *Progressive Architecture*, Mar. 1995, pp. 82–84.
- [68] MIL-STD-461D, “Requirements for the Control of Electromagnetic Interference Emissions and Susceptibility,” Jan. 11, 1993.
- [69] MIL-STD-462D, “Measurement of Electromagnetic Interference Characteristics,” Jan. 11, 1993.

- [70] “Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D),” Defense Science Board, Office of Secretary of Defense, Appendix F, Nov. 1996, p. 6.
- [71] “Advanced Battlespace Information Systems (ABIS) Task Force Report,” Vol. V, Grid Capabilities and Working Group Results, May 1996, pp. 2-40 to 2-43.
- [72] NSA Data Item DI-R-54458, “Security Fault Analysis for Traditional Contracts,” National Security Agency.
- [73] “Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D),” Appendix F, “Technology Issues,” Nov. 1996, p. 17.

10

The Technologies of Information Warfare

The current state of the art in information operations is based on core technologies whose performance is rapidly changing, even as information technologies (sensing, processing, storage, and communication) rapidly advance. As new technologies enable more advanced offenses and defense, emerging technologies farther on the horizon will introduce radically new implications for information warfare.

The previous chapters have introduced the core technologies that enable IW; the enabling and emerging technologies that will transform information operations in the future—in terms of speed, precision, and effect—are surveyed in this chapter.

The technology changes described in this chapter have broader implications than technical performance improvements for information operations. Consider several related impacts that technological changes are creating.

- *Economic availability*—Expanded availability of information technology to individuals reduces the economic advantage that superpower governments have traditionally held over other nations, terrorist groups, or even individuals. The availability of these technologies to small forces (even individuals) potentially enables them to conduct offensive attacks in the information domain, though offensive actions in the physical domain would be unthinkable due to asymmetry in conventional military force capabilities.
- *Technology ownership*—The balance of technology investment and ownership of many critical technologies is shifting from the government to the private sector. High-end processing, cryptography,

precision satellite imaging, mobile communications, and many other technologies that were once owned (and controlled) by governments are now driven by commercial markets. R&D investments by industry in many of these areas now exceed the investments by governments, and government efforts to control the global transfer of information technologies by export restrictions are being challenged by commercial developers.

- *Information access*—The rapid growth of both the Internet and the next-generation GII is exponentially increasing universal access to data and information sources (due to connectivity, storage, and bandwidth technologies). This access has eliminated previous standards of individual privacy and the security of individuals and government facilities from precision targeting in all information warfare realms (perceptual, information, or physical). Along with access also comes increasing physical “transparency” as commercial remote sensing and global positioning technologies will make available global geophysical data previously available only to high-technology nation states.

The culmination of these technology impacts enables the increase in global conflict and the potential for information warfare. Vickers and Martinage have summarized this cumulative impact of information availability brought on by technological progress:

Information will likely have four dominant effects on future intrastate conflict: it could substantially increase the intensity, transparency, and strategic reach of intrastate conflict; and it could bring intrastate conflict into a new dimension—war in cyberspace [1].

10.1 A Technology Assessment

Information warfare–related technologies are categorized both by their information operations role and by three distinct levels of technology maturity.

- *Core technologies* are the current state-of-the-art, essential technologies necessary to sustain the present level of information operations.
- *Enabling technologies* form the technology base for the next generation of information warfare capabilities; more than incremental improvements, they will enable the next quantum enhancement in operations.

- *Emerging technologies* on the far horizon have conceptual applications when feasibility is demonstrated; they offer a significant departure from current core technologies and hold the promise of radical improvements in capability, and changes in the approach to information operations.

Previous chapters have focused on the core and enabling technologies that have allowed the current generation of information operations now available or becoming operational. In this chapter, we provide a broad overview of the enabling and emerging technologies that will bring incremental and revolutionary changes to information warfare.

A classic element of both national and business intelligence is the surveillance of technology—the technology “watch,” or technology “scanning” [2,3]. This intelligence function monitors the state of the art in critical technologies that have the potential to impact operations (or markets), present new threats (or products), and change the balance of power (or market share).

Developers, strategists, and decision makers who create and conduct information operations must remain abreast of a wide range of technologies to conceive the possibilities, predict performance impacts, and strategically manage development to retain leadership in this technology-paced form of warfare.

Numerous U.S. Department of Defense (DoD) technology studies have evaluated the potential technologies that will impact the many aspects of information warfare.

- *New World Vistas*—This study, documented in a 15-volume report, was conducted for the U.S. Air Force Scientific Advisory Board to project critical technologies for air and space superiority in the next century. The study emphasized that “the entire fabric of Information Warfare should be joined to the fabric of conventional warfare” [4].
- *Air Force 2025*—This series of studies was performed under a directive from the chief of staff of the Air Force to examine the concepts, capabilities, and technologies necessary to remain the dominant air and space force in the future [5].
- *Advanced Battlespace Information System*—This study was chartered by the U.S. DoD Director, Defense Research and Engineering (DDR&E) to explore how emerging information technologies can be used to provide the capabilities sought in Joint Vision 2010. The study provides a comprehensive mapping of operational capabilities, to functions, and then to necessary technologies [6].

- *Military Critical Technologies List (MCTL)*—The U.S. DoD has prepared this document to enumerate technologies deemed critical to maintain superior military capabilities. The MCTL includes directed and kinetic energy weapons (Section 4) and information warfare (Section 9) technologies [7].
- *Defense Science and Technology Plans*—A series of three planning documents define technology areas, objectives budgets, and Science and Technology (S&T) programs, and provide insight into the structure R&D investment process. See [8–10] for near-, mid- and far-term technologies, respectively.
- *Office of Secretary of Defense Studies*—The OSD has directed focused studies by the Defense Science Board [11,12] and special study panels such as the “Highlands Group” on information warfare–related issues and technologies [13].

The U.S. military services have also conducted internal studies of IW-related technologies and have focused R&D investments on the critical technologies that will not be available from commercial information technology developments [14].

In addition, U.S. panels commissioned by the federal government and independent organizations have considered global environment as well as information technology impacts in studies of the intelligence organizational aspects of information-based warfare.

- *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*—An appraisal commissioned by the U.S. White House and Congress [15].
- *IC21—The Intelligence Community in the 21st Century*—A “bottom-up” review of intelligence and future organization options by the U.S. Congress [16].
- *Making Intelligence Smarter: The Future of U.S. Intelligence*—Report of an independent task force sponsored by the Council on Foreign Relations, February 1996 [17].

Figure 10.1 illustrates three conceptual levels of scientific applications, or “technologies.”

Many of the technology areas described in this chapter will require the integration of several critical component technologies. In some cases, Table 10.1 includes technology areas without defining all of the underlying

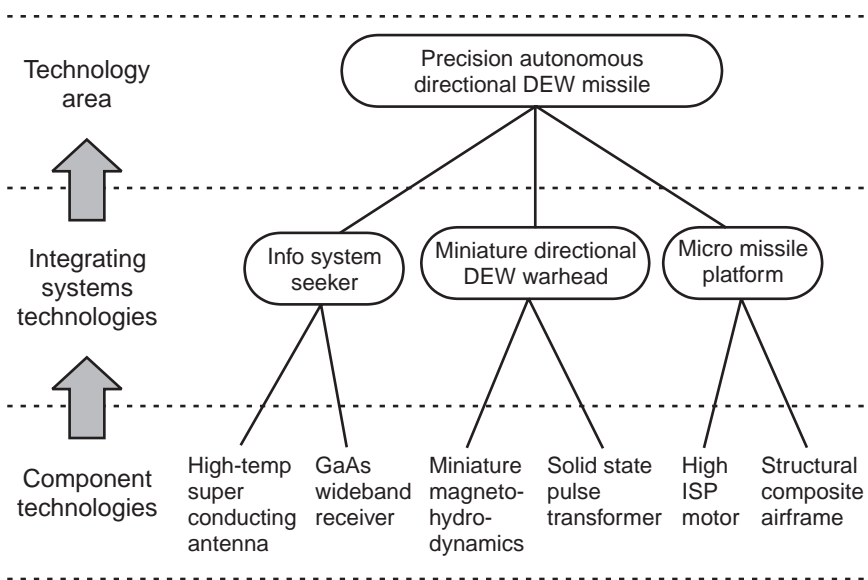


Figure 10.1 Representative illustration of how component technologies are integrated to produce a higher level technology “area” or “capability.”

component technologies (e.g., biological, materials, software, optical). The following sections will identify many of those component technologies to one more layer of depth. This chapter does not cover all possible technology areas; rather, we attempt to maintain a uniform coverage of direct critical areas at a relatively high level.

Indirect technologies that are sometimes included within information warfare (like applicable nonlethal weapons [18], electromagnetic-biological weapons, wearable or implanted computers, weapons of mass destruction, etc.) are not included to allow focus on those technologies with direct involvement in information operations. Numerous technologies are not included, with the intent of highlighting the most critical areas at a top level.

A top-level technology matrix for information warfare, Table 10.1 compares two categories with current baseline of core technologies.

- *Emerging* technologies now in development to provide incremental improvements in information operations;
- *Enabling* technologies on the horizon that will revolutionize current approaches.

Table 10.1
General Technology Categories for Information Warfare

Technology Category	Information Warfare		Information-Based Warfare		
	Attack	Defend	Collect	Process	Disseminate
<p>Core: Required to maintain, sustain current capabilities</p>	<p>Electronic attack based on brute force and precision jamming, deception</p> <p>Manual and semiautomated network attack</p> <p>Dynamic malicious code</p>	<p>Secret- and public-key cryptography</p> <p>Trusted computers, network security augmentations (firewalls, authentication, security tiers)</p> <p>Electromagnetic hardening</p>	<p>Airborne reconnaissance (manned and medium endurance)</p> <p>Space surveillance</p> <p>HUMINT collection aids</p> <p>Global positioning system</p> <p>EO, IR, SAR multispectral sensing</p>	<p>Data warehouses</p> <p>Data fusion (deduction) and automatic target recognition (ATR)</p> <p>Data mining (abduction-induction)</p> <p>Text-based databases, information index and retrieval (IIDR), and hyperlinking</p>	<p>Push/pull dissemination of data and information</p> <p>Data compression</p> <p>Global broadcast</p> <p>3-D visualization</p>

Table 10.1 (continued)

Technology Category	Information Warfare		Information-Based Warfare		
	Attack	Defend	Collect	Process	Disseminate
Enabling: Technological base for next-generation capabilities	Semiautomated network attack and response	Trusted network components (barriers, wrappers, walls)	High-altitude endurance UAVs	High-bandwidth global broadcast	Networks of sensors in space, air, and surface operating as a whole
	Tactical electronic attack directed energy weaponry (DEW)	Network integrated intrusion detection	Unattended intelligent ground sensors (UAGS)	Medium-bandwidth global communication satellite network	Integrated precision tracking, data and network sensing
	High-energy chemical lasers	Bulk encrypting steganography	Commercial high-resolution imaging satellites	Global cellular and microcellular wireless voice, data communications	Semiautonomous integrated collection management and processing of all sources
	Dynamic and autonomous malicious logic	Multiple-type authentication anti-DEW weapons (ADEW)	Integrated sensor networks ground-air-space	N-dimensional visualization—virtual reality	Global near-real-time tailored knowledge delivery
			Integrated precision positioning, telecom, tracking		
			Hyperspectral, integrated aperture sensing		

Table 10.1 (continued)

Technology Category	Information Warfare		Information-Based Warfare		
	Attack	Defend	Collect	Process	Disseminate
Emerging: Beyond next generation, a departure from current practices	Automated network attack and response Tactical precision DEW Micromechanical organisms Digital organisms Precision directed energy weapons Computational sociology (cyber PSYOPS) Quantum computing with large number prime factorization	Trusted universal wrappers, barriers, firewalls Digital organisms operating as trusted agents All-optical networks Quantum cryptography	Barrier-penetrating sensors Ultraspectral all-spectral sensing Micro UAVs Micromachine autonomous ground sensors and nanomanipulators Intelligent autonomous distributed sensor networks	Digital organism information agents Hypermedia object information bases Quantum and DNA molecular computing and storage	High-bandwidth broadcast, multicast, point-cast, and networking Automated bidirectional multilingual natural language translation Direct multidimensional presentation to human brain

It is important to recognize that many of the “technology areas” discussed in this chapter refer to the integrated result of numerous component technologies. The following sections necessarily present technology descriptions in the form of succinct technology “predictions,” stated in the future tense.

This chapter provides the basis for a technology watch for information warfare—enumerating enabling and emerging categories of technologies that must be observed to understand the underlying scientific progress. The following sections review these technology areas at the next level of technology detail and their implications on information operations of the future. The sections include three technology categories: dominance or information-based warfare (Section 10.2), offense (Section 10.3), and defense (Section 10.4). It is important to notice that a number of important categories (e.g., information processing) have impact across all areas, although in different ways.

10.2 Information Dominance Technologies

Three general areas characterize the information dominance technologies: collection of data, processing of the data to produce knowledge, and dissemination of the knowledge to humans.

- *Collection*—The first area includes the technical methods of sensing physical phenomena and the platforms that carry the sensors to carry out their mission. Both direct and remote sensing categories of sensors are included, along with the means of relaying the sensed data to users.
- *Processing*—The degree and complexity of automation in information systems will continue to benefit from increases in processing power (measured in operations per second), information storage capacity (in bits), and dissemination volumes (bandwidth). Processing “extensibility” technologies will allow heterogeneous nets and homogeneous clusters of hardware along with operating systems to be scaled upwards to ever-increasing levels of power. These paramount technology drivers are, of course, essential. Subtler, however, are the intelligent system technologies that contribute to system autonomy, machine understanding, and comprehension of the information we handle. Software technologies that automate reasoning at ever more complex levels will enable humans to be elevated from data-control roles to information-supervision roles and, ultimately, to knowledge-management roles over complex systems.

- *Dissemination*—Communication technologies that increase bandwidth and improve the effective use of bandwidth (e.g., data, information and knowledge compression) will enhance the ability to disseminate knowledge. (Enhancements are required in terms of capacity and latency.) Presentation technologies that enhance human understanding of information (“visualization” for the human visual sense, virtual reality for all senses) by delivering knowledge to human minds will enhance the effectiveness of the humans in the dominance loop.

Table 10.2 details specific technologies that will contribute to information dominance, and the following paragraphs summarize the enabling and emerging technology items in the table by collection, processing, and dissemination functions.

10.2.1 Collection Technologies

Collection technologies include advanced platforms and sensing means to acquire a greater breadth and depth of data. The collection technologies address all three domains of the information warfare model: physical, information, and perceptual variables.

High-Altitude Endurance (HAE) Unmanned Air Vehicles (UAVs)

First-generation HAE UAVs (e.g., U.S. Global Hawk and Darkstar, Table 10.3) will introduce penetrating airborne surveillance with abroad area search capability. HAE UAVs also provide relatively long dwell over designated target areas. HAE vehicles complement short- and close-range UAVs, which do not have deep penetration capability [19,20], and satellite surveillance, which does not have high revisit rates. Follow-on generations of MAE and HAE UAVs will add communication relay capabilities, precision SIGINT, and local precision navigation capabilities, and will operate as a sensor network with autonomous and cooperative behavior in hostile airspace.

Intelligent Unattended Ground Sensors (UAGS)

Expendable and covert UAGS supplement airborne sensors, providing detailed ground-level sensing at identified target areas with acoustic, chemical, imaging, and other sensors. Deployed by UAVs, and relaying sensed data through satellites or UAVs, the UAGS will be able to cooperate in networks and report precise data on tactical events and entities.

Table 10.2
Critical Information-Based Warfare Technologies

	Collect	Process	Disseminate	Implications
Core	Airborne reconnaissance (manned and medium endurance) Space surveillance HUMINT collection aids Global positioning system EO, IR, SAR multispectral sensing	Data warehouses Data fusion (deduction) and automatic target recognition (ATR) Data mining (abduction-induction) Text-based data bases, information index and retrieval (IIDR), and hyperlinking	Push/pull dissemination of data and information Data compression Global broadcast 3-D visualization	State of the art
Enabling	High-altitude endurance UAVs Unattended intelligent ground sensors (UAGS) Commercial high-resolution imaging satellites Integrated sensor networks ground-air-space Integrated precision positioning, telecommunications, tracking Hyperspectral, integrated aperture sensing	Integrated and intelligent inductive (learning) and deductive decision aids Computing networks (distributed op systems) with mediated heterogeneous databases Precision geospatial information systems Autonomous information search agents Multimedia databases (text, audio, imagery, video), index, and retrieval Electro-optical storage, holographic storage	High-bandwidth global broadcast Medium-bandwidth global communication satellite network Global cellular and microcellular wireless voice, data communications N-dimensional visualization—virtual reality	Networks of sensors in space, air, and surface operating as a whole Integrated precision tracking, data and network sensing Semiautonomous integrated collection management and processing of all sources Global near-real-time tailored knowledge delivery

Table 10.2 (continued)

	Collect	Process	Disseminate	Implications
Emerging	Barrier-penetrating sensors	Digital organism information agents	High-bandwidth broadcast, multicast, pointcast, and networking	Universal precision tracking, data and network sensing
	Ultraspectral all-spectral sensing	Hypermedia object information bases	Automated bidirectional	Autonomous data collection, collaborative management
	Micro UAVs	Quantum and DNA molecular computing and storage	multilingual natural language translation	Intelligent real-time global
	Micromachine autonomous ground sensors and nano-manipulators		Direct multidimensional presentation to human brain	dissemination of knowledge
	Intelligent autonomous distributed sensor networks			

Commercial High-Resolution Imaging Satellites

Commercial satellites with 1m resolution (ground sample distance) will make available global precision geospatial data (including stereo-generated digital terrain elevation data, and precision location via the global positioning satellite).

Integrated Sensor Networks Ground-Air-Space

Existing sensor data “stovepipes” will give way to networked sensors that operate as a “system of sensors” to coordinate timing of sensing and focus of attention. Secure networks and distributed data fusion processing are required to develop such nets to provide global precision location, identification, and tracking of targets.

Integrated Precision Positioning, Telecommunications, Tracking

Telecommunications, global positioning (and timing), and tracking will be integrated to provide precision (1m x, y, z) real-time tracking and instantaneous communications with all units (reporting sensors and friendly forces). This will allow the exchange of *appropriate* data (for sensor coordination), information (for reasoning), and knowledge (for presentation to humans and decision making) to *appropriate* nodes on the network.

Table 10.3
U.S. Baseline Medium- and High-Altitude UAVs

Class	Vehicle	Mission Characteristics	Sensor Characteristics
Medium-altitude endurance (MAE)	Predator [21]	Ceiling: 15,000–25,000 ft. 6,000 mi. linear range Typical mission: 500 mi. to target, 24 hours on-station, and return Control via UHF Milsat	SAR: 1m ground resolution EO: Video with 1,000 mm lens X band line-of-sight link Ku band bent-pipe data link relay via SATCOM to control
High-altitude endurance (HAE)	Global Hawk [22]	Ceiling: 50–65,000 ft. Long-range mission: 3,000 mi. to target, 24 hours on station Medium-range mission: 500 mi. to target, 40 hours on station Operating radius : 2–3000 mi. Control via UHF Milsat	Simultaneous SAR and EO/IR sensors SAR: 1m search, 0.3m spot EO/IR: NIIRS 6 EO and NIIRS 5 IR
	Darkstar [23]	Ceiling: Above 45,000 ft. Typical mission: 500 mi. to target, 8 hours on station Operating radius: 500 mi. Radar cross section stealth properties Control via UHF Milsat	Single sensor, interchangeable SAR and EO/IR SAR: 1m search, 0.3m spot EO/IR: NIIRS 6 EO and NIIRS 5 IR

Hyperspectral, Integrated Aperture Sensing

Infrared and multispectral imaging will be supplemented by hyperspectral imaging to detect subtle target signatures using narrow spectral bandwidth signature characteristics, as well as spatial shapes and context [24].

Ultraspectral and All-Spectral Sensing

Integrated electromagnetic sensors with common or integrated apertures will provide all-spectral (radar, MMW, UV, visible, IR) sensing, and ultraspectral

spectrometry. Such precision measurements may require active illumination of targets by synchronized tunable lasers.

Barrier-Penetrating Sensors

Special sensing methods employing active electromagnetic energy (for example, low frequencies for foliage penetration, lasers for other penetration), and energetic particles (for hard barrier penetration) will provide limited surveillance of camouflaged or concealed activities.

Micro UAVs

Extremely small autonomous air vehicles, the size of bird or even insects, will provide short-range sensing capabilities, including urban surveillance and even facility penetration. Small high-density power sources and propulsion technologies are required, as well as microscopic sensors (e.g., imaging, micro-chemical, acoustic), onboard processing and RF link [25]. These vehicles, deployed as expendables from long-range UAVs acting as relays, will provide deep penetrating sensing to ground targets.

Micromachine Autonomous Ground Sensors and Nanomanipulators

Microelectromechanical systems (MEMS) technologies, coupled with autonomous microelectronic control will enable the development of ever smaller expendable ground sensors. These “bugs” will apply nanomanipulation tools capable of crawling, cutting, and inspecting materials and penetrating facilities to perform sensing and relay of data to a deploying platform.

Intelligent Autonomous Distributed Sensor Networks

Networked sensors in the air, on the ground, and in space will coordinate the sensing process through autonomous collaborative and near-real-time networking to achieve knowledge-based sensing goals.

10.2.2 Processing Technologies

Processing technologies address the increased volume of data collected, the increased complexity of information being processed, and the fundamental need for automated reasoning to transform data to reliable knowledge.

Integrated and Intelligent Inductive (Learning) and Deductive Decision Aids

Reasoning aids for humans applying increasingly complex reasoning (integrating symbolic and neural or genetic algorithms) will enhance the effectiveness of humans. These tools will allow individuals to reason and to make decisions on

the basis of projected complex outcomes across many disciplines (e.g., social, political, military, and environmental impacts). Advances in semiotic science will contribute to practical representations of knowledge and reasoning processes for learning, deductive reasoning, and self-organization.

Computing Networks (Distributed Operating Systems) With Mediated Heterogeneous Databases

Open system computing, enabled by common object brokering protocols, will perform network computing with autonomous adaptation to allocate resources to meet user demands. Mediation agents will allow distributed heterogeneous databases across networks to provide virtual object-level database functions across multiple types of media.

Precision Geospatial Information Systems

Broad area (areas over 100,000 km²) geospatial information systems with continuous update capability will link precision (~1m) maps, terrain, features, and other spatially linked technical data for analysis and prediction.

Autonomous Information Search Agents

Goal-seeking agent software, with mobile capabilities to move across networks, will perform information search functions for human users. These agents will predict users' probable needs (e.g., a military commander's information needs) and will prepare knowledge sets in expectation of user queries.

Multimedia Databases (Text, Audio, Imagery, Video) Index and Retrieval

Information indexing discovery and retrieval (IIDR) functions will expand from text-based to true multimedia capabilities as object linking and portable ontology techniques integrate heterogeneous databases and data descriptions. IIDR functions will permit searches and analysis by high-level conceptual queries.

Optical Storage

Optical storage media will increase the capacity of mass information storage and increase immunity to some forms of electromagnetic attacks. Holographic storage methods will provide mass storage for compact applications.

Digital Organisms

Advanced information agents, capable of adaptation, travel, and reproduction will perform a wide range of intelligent support functions for human users, including search, retrieval, analysis, knowledge creation, and conjecture.

Hypermedia Object Information Bases

Object-oriented databases with hyperlinks across all-media sources will permit rapid manipulation of large collections of media across networks.

Quantum and DNA Molecular Computing and Storage

Computation by computers using quantum-mechanical [26] or DNA-biomolecular [27] mechanisms to encode and store numerical symbols and perform computation will permit orders of magnitude increases in processing performance due to parallelism. Quantum computers encode symbols as a quantum bit or *qubit*, which can encode a linear superposition of two states (unlike the binary *bit* that encodes two possible states). Due to superposition and parallelism, the quantum computer can perform many functions exponentially faster than a conventional computer. DNA biomolecular computing, on the other hand, performs combinatoric processing using selected DNA strands whose combinations may be matched to solve specific problems using chemical reaction processes. The complexity of the DNA strands and the parallelism of the matching process provide an extremely powerful search mechanism to perform exhaustive searches in a short period of time.

10.2.3 Dissemination and Presentation Technologies

Dissemination technologies increase the speed with which created knowledge can be delivered, while expanding the breadth of delivery to all appropriate users. Presentation technologies address the critical problems of communicating high-dimensionality knowledge to human users efficiently and effectively, even while the human is under duress.

High-Bandwidth Global Broadcast

Wideband global broadcast of data will provide real-time distribution of secure intelligence and command data to all forces. High-efficiency modulation and data compression techniques will provide bandwidths for transmission of imagery, video, and complex planning data.

Medium-Bandwidth Global Communication Satellite Network

Tiered layers of communication satellites will provide medium-bandwidth tactical interactive networking capabilities of the global grid.

Global Cellular and Microcellular Wireless Communications

Global access to real-time voice, video, and data communication will be enabled by constellations of communication satellites acting as communication networks

with satellite-based switching and routing. Compact all-digital (software) receivers and active-array antenna technologies will continue to miniaturize ground terminals.

High-Dimensional Visualization

Virtual reality technologies will deliver effective multidimensional information to humans in synthetic visualizations (through the eyes, on external flat panel displays, or directly projected into the retina) and to a more limited degree through supportive sound, touch, smell, and taste). This capability will increase human understanding of complex situations and provide dynamic decision support by partially immersing the human in large volumes of structured information and knowledge.

High-Bandwidth Broadcast, Multicast, Pointcast, and Networking

Ground-based communication backbones will employ optical fiber, optical switching, and even optical multiplexing technologies (such as optical wavelength division multiplexing) to exploit near-theoretical bandwidths of fiber optics (terahertz frequencies with picosecond optical pulses). Adaptive switching will efficiently control message flow to match available net bandwidth, delivering high efficiency for all communication modes (broadcast, multicast, pointcast, and highly interactive networking).

Automated Bidirectional Multilingual Natural Language Translation

Processing and storage technologies will expand voice recognition, natural language understanding (across global languages), and speech synthesis to provide highly accurate voice command, dictation, and translation services between multinational forces and command systems.

Direct Multidimensional Presentation to Human Brain

Direct presentation of multidimensional information will be delivered directly to the human brain via electrobiological interfaces, allowing the human to be virtually immersed in the information. Improvements in understanding of human cognition and perception are required before this capability can be developed to achieve near-capacity comprehension of the meaning of complex, multidimensional situations.

10.3 Offensive Technologies

Current offensive technologies (Table 10.4) are essentially manual weapons requiring human planning, targeting, control, and delivery. Enabling

Table 10.4
Critical Offensive Technologies

	Offensive Technologies	Implications
Core	Electronic attack based on brute force and precision jamming, deception Manual and semiautomated network attack Dynamic malicious code	State of the art
Enabling	Semiautomated network attack and response Tactical electronic attack directed energy weaponry (DEW) High-energy chemical lasers Dynamic and autonomous malicious logic	Structured attack of networks (DII, NII) applying semiautomated precision denial of service, network deception and exploitation, electronic attack, and coordinated PSYOPS
Emerging	Automated network attack and response Tactical precision DEW Micromechanical organisms Digital organisms Precision DEW Computational sociology (cyber PSYOPS) Quantum computing with large number prime factorization	Automated and adaptive large-scale (structured) attack of networks; multiple independently targeted network nodes with simultaneous PSYOPS perception management of large population groups

technologies will improve the understanding of weapon effects on large-scale networks, enabling the introduction of semiautomated controls to conduct structured attacks on networks. Integrated tools (as discussed in Chapter 7) will simulate, plan, and conduct these semiautomated attacks. Emerging technologies will expand the scope and complexity of attacks to provide large-scale network control with synchronized perception management of large populations.

The following paragraphs summarize the enabling and emerging technologies in the table.

Tactical Directed Energy Weaponry

Tactical viability of DEW will be achieved when size, weight, and form factors permit EMP weapons to be delivered within conventional ordinance packages, or HPM weapons to be deployed on tactical aircraft or mobile vehicles. To achieve this, component technologies for energy storage, generation, and conversion to electromagnetic form will achieve outputs on the order of 1,000 kilojoules in packages on the order of hundreds of kilograms.

High-Energy Chemical Lasers

High-energy chemical oxygen iodine laser (COIL) technology, integrated with precision beam control technologies will provide lethal tactical DEW capability against IR/EO sensors and vulnerable mechanical structures (e.g., fuel tanks, antenna structures). Performance of these systems will achieve ranges of hundreds of kilometers, when COIL lasers demonstrate over 1 kilojoule pulses in the visible to IR wavelengths and beam control sustains aiming to within less than $1/4 \mu\text{radian}$.

Semiautomated Network Attack and Response

Planning and decision support tools will model network attacks and effects, enabling effective dynamic targeting and initiation of structured attacks. Humans will remain in the loop to perform battle damage assessment and conduct semiautomated responses.

Dynamic and Autonomous Malicious Logic

Advances in autonomous agent technology will enable malicious logic to exhibit self-adaptation for both concealment and malicious effects to match the context of their environment.

Automated Network Attack

Semiautomated attack tools will be integrated with surveillance, simulation, and agent-based BDA support to enable an increase in the level of automation. Intelligent tools will automate and integrate parallel attacks across all disciplines of information operations.

- At the strategic, operational, and tactical levels;
- Against all components of a national “system”: fielded military, population, infrastructure, organic essentials, and leadership [28].

Micromechanical Organisms

Autonomous digitally controlled mechanical organisms will give physical sensing, actuation, and mobility to microscopic devices capable of seeking and disrupting electronic systems. Such mechanisms may be dispersed like chemical agents and may be considered to act as intelligence mechanical-chemical weapons.

Digital Organisms

Fully autonomous digital organisms with intelligent capabilities will perform goal-oriented activities including search (network traveling), self-adaptation, self-defense, offense, and reproduction.

Precision Directed Energy Weapons

The second generation of tactical DEW will further increase energy density, conversion efficiency, and directionality of the directed energy. Precision DEW (both HPM and EMP) will allow tailoring of directed energy to achieve desired effects (disrupt to destroy) for specific target types.

Computational Sociology (Cyber PSYOPS)

Complex models of the behavior of populations and the influencing factors (e.g., perceptions of economy, environment, security) will permit effective simulation of societal behavior as a function of group perception. This capability will permit precise analysis of the influence of perception management plans and the generation of complex multiple-message PSYOPS campaigns. These tools could support the concepts of “neocortical warfare” in which national objectives are achieved without force [29,30].

Quantum Computing with Large Number Prime Factorization

Quantum computing holds the promise to perform highly parallel factorization of large numbers and compute discrete logarithms rapidly, challenging the security of current “strong” cryptographic methods by providing powerful tools for brute-force cryptanalysis.

10.4 Defensive Technologies

Core defensive technologies (Table 10.5) now being deployed by both the military and commercial domains provide layers of security to bridge the gap between the two approaches.

Table 10.5
Critical Defensive Technologies

	Defensive Technologies	Implications
Core	Secret- and public-key cryptography Trusted computers, network security augmentations (firewalls, authentication, security tiers) Electromagnetic hardening	State of the art
Enabling	Trusted network components (barriers, wrappers, walls) Network integrated intrusion detection Bulk encrypting steganography Multiple-type authentication ADEW: anti-DEW weapons	Trusted networks constructed from protected commercial components; semiautomated network survivability based on integrated network warning and response
Emerging	Trusted universal wrappers, barriers, firewalls Digital organisms operating as trusted agents All-optical networks Quantum cryptography	Adaptive and autonomous network trust (multiple levels of network security), survivability, and self-healing

- First generation (and expensive) military “trusted” computers based on formal analysis/testing, and dedicated secure nets with strong cryptography;
- Commercial information technologies (computers, UNIX or Windows NT operating systems, and networks) with augmenting components (e.g., firewalls, software wrappers, smart card authentication) to manage risk and achieve a specified degree of security for operation over the nonsecure GII.

Enabling technologies will provide affordable security to complex heterogeneous networks with open system augmentations that provide layers of protection for secure “enclaves” and the networks over which they communicate. These trusted layers (software wrappers, hardware walls, or barriers) will

provide security to the untrusted databases, operating systems, and other elements under their control.

Emerging technologies will increase security and survivability over large-scale networks with autonomous detection, reaction, and restoration (even self-healing) mechanisms. Trusted agents will perform security assignments.

The following paragraphs summarize the enabling and emerging technologies in Table 10.5.

Network Integrated Intrusion Detection

Intrusion detection will integrate data from distributed sensing agents across networks, and will perform detection on the basis of individual operations and multiple levels of aggregate performance. Protective responses will be adaptive and semiautomated with minimal human intervention.

Bulk Encrypting Steganography

Data-hiding cryptographic methods will achieve high degrees of efficiency and security (both COMSEC and TRANSEC), permitting strong bulk encryption of data for “public access” on networks.

Multiple-Type Authentication

Authentication controls for access to information systems will integrate multiple types of biometric and cryptographic devices to provide secure authentication of individual humans. Biometric systems will achieve high-accuracy identification of humans and their physiological state when attempting to access systems.

ADEW: Anti-DEW Weapons

Active countermeasures to locate and attack DEW weapons or supporting sensors may include special directed energy weapons designed to trigger premature energy release or destruction of the dense energy storage mechanism within the targeted DEW.

Trusted Universal Wrappers, Barriers, Firewalls

Trusted object-oriented software layers will provide high levels of security for a wide range of common object resources.

Digital Organisms Operating as Trusted Agents

Secure autonomous digital agents will perform trustworthy security tasks, including intrusion discovery (learning), detection, response, and restoration. Operating as biological immune system counterparts, these organisms will

conduct collaborative detection and cooperative mobilization to attack malicious logic and restore disrupted services.

All-Optical Networks

Highly optical and all-optical networks and databases will employ laser, fiber-optic, and holographic technologies to provide protection from DEW and physical interception threats.

Quantum Cryptography

The communication of quantum states of particles (e.g., photons, atoms, magnetic moments) provide a potential means of encrypting information for transmission such that both COMSEC (communication security) and TRANSEC (transmission security) properties are integrated. There can be no passive interception of quanta ciphertext messages without disruption of the message itself [31,32].

10.5 Summary

This technology list is by no means complete, but attempts to cover the broad scope of information-related physical technologies that will change the appearance and conduct of information warfare. The operational forms, threats, and risks of information warfare will continually change as these technologies are steadily developed, integrated, and operationally introduced. Many of the technologies and operational implementations will be developed in secrecy to maintain their military value and maintain the margin of utility that is afforded by OPSEC.

Those who study and implement information operations and those who will carry out warfare at the information level must understand these basic technologies and prepare for their impact on future global, corporate, and personal security and conflict.

Endnotes

- [1] Vickers, N. G., and R. C. Martinage, *The Military Revolution in Intrastate Conflict*, Washington, D.C., Center for Strategic and Budgetary Assessments, Oct. 1997, p. i. Intrastate conflict refers to the use of violence to overthrow, force a change, or bring redistribution of political or economic power within a nation state.
- [2] Dussage, P., S. Hart, and B. Ramanantosa, *Strategic Technology Management*, New York: John Wiley & Sons, 1994, pp. 88 ff.

- [3] Ashton, W. B., and G. S. Stacey, "Technical Intelligence in Business: Understanding Technology Threats and Opportunities," *International J. of Technology Management*, Vol. 10, No. 1, 1995, pp. 79–104.
- [4] *New World Vistas: Air and Space Power for the 21st Century*, U.S. Air Force Scientific Advisory Board, Dec. 1995, quotation from p. 42, Summary Volume.
- [5] Air Force 2025 Research Monographs (five volumes), U.S. Air Force, Maxwell AFB, AL: Air University Press, Aug. 1996.
- [6] *Advanced Battlespace Information System, Task Force Final Report*, Mar. 1996. See Volume VI, Annex B, for mapping from operational capabilities to 43 critical technologies.
- [7] *The Military Critical Technology List (MCTL), Part I: Weapon Systems Technology*, Office of Undersecretary of Defense for Acquisition & Technology, Washington, D.C., Nov. 1996.
- [8] "Basic Research Plan (BRP)," Director of Defense Research and Engineering, U.S. DoD, Jan. 1997.
- [9] "Defense Technology Area Plan (DTAP)," Director of Defense Research and Engineering, U.S. DoD, Jan. 1997.
- [10] "Joint Warfighting Science and Technology Plan (JWST)," Director of Defense Research and Engineering, U.S. DoD, Jan. 1997.
- [11] "Report to the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield," Office of Undersecretary of Defense for Acquisition & Technology, Washington, D.C., Oct. 1994.
- [12] "Technology Issues," Appendix F, *Report of the Defense Science Board Task Force on Information Warfare – Defense (IW-D)*, Office of Undersecretary of Defense for Acquisition & Technology, Washington, D.C., Nov. 1996.
- [13] Cooper, P., "Information Whizzes to Advise DoD on Future Wars," *Defense News*, Feb. 26–March 3, 1996, p. 14.
- [14] The U.S. Department of Defense annual R&D budget (R-1) provides a primary source for monitoring investments in IW-related technologies for basic research through advanced concept technology demonstrations (ACTDs).
- [15] "Preparing for the 21st Century: An Appraisal of U.S. Intelligence," Commission of the U.S. Congress, Harold Brown (Chairman), Mar. 1, 1996.
- [16] "IC21—The Intelligence Community in the 21st Century," Washington, D.C., U.S. House of Representatives, Permanent Select Committee on Intelligence, Mar. 4, 1996.
- [17] "Making Intelligence Smarter: The Future of U.S. Intelligence," Report of an Independent Task Force, Washington, D.C., The Council on Foreign Relations, Feb. 1996.
- [18] Scott, W. B. "Panel's Report Backs Non-Lethal Weapons," *Aviation Week and Space Technology*, Oct. 16, 1995, pp. 50–51. *Nonlethal* generally refers to weapons not lethal but temporarily disabling to humans. The term also encompasses some "weapons" capable of disabling physical systems, including electronic systems and their supporting infrastructure (e.g., chemical agents that coat optical sensors, short-circuit electronics, or obstruct mechanical systems).

-
- [19] Close-range UAVs support small unit operations with ranges to 30 km, and short-range UAVs have medium-altitude endurance (30 to 50 hrs with 150 to 300 km range). The U.S. first-generation Predator UAV is an example an MAE currently in service.
- [20] Fulghum, D. A., "International Market Eyes Endurance UAVs," *Aviation Week and Space Technology*, July 10, 1995, pp. 40–42. Also see associated articles.
- [21] Fulghum, D. A., "Tier 2 Endurance UAV Nears First Flight," *Aviation Week and Space Technology*, May 16, 1994, pp. 20–23.
- [22] "Tier II Plus & Tier III Minus High Altitude Endurance UAV Programs," *Inside the Pentagon*, Aug. 25, 1994, pp. 12–15.
- [23] Dornheim, M. A., "Mission of Tier 3—Reflected in Design," *Aviation Week and Space Technology*, June 19, 1995, pp. 52–55.
- [24] The term *multispectral* generally refers to a sensor that measures the IR-visible spectrum, partitioning the measurement into tens of discrete spectral bands (spectral bandwidth 0.1 micrometer), *hyperspectral* is hundreds to a thousand bands (spectral bandwidth 0.01 micrometer), and *ultraspectral* above one thousand bands (spectral bandwidth 0.001 micrometer).
- [25] Evers, S., "U.S. Research on Micro Air Vehicles Design Takes Off," *Jane's Defence Weekly*, June 11, 1997, p. 14.
- [26] Lloyd, S., "Quantum-Mechanical Computers," *Scientific American*, Oct. 1995, p. 145. Also see Brassard, G., "The Computer in the 21st Century," *Scientific American*, Mar. 1995.
- [27] Adleman, L. M., "Molecular Computation of Solutions to Combinatorial Problems," *Science*, Vol. 266, Nov. 1994, pp. 1021–1024.
- [28] Wardon, J. A. III, (Col., USAF), "The Enemy as a System," *Proc. 1997 AFELM*, Ft. Leavenworth, KS, Aug. 1997.
- [29] Szafranski, R., (Col., USAF), "Neocortical Warfare: The Acme of Skill?," *Military Review*, Vol. LXXIV, No. 11, Nov. 1994.
- [30] Wood, R. J., (Lt. Col., USAF), *Information Engineering: The Foundation of Information Warfare*, Maxwell AFB, AL: Air University Press, Apr. 1995.
- [31] Bennett, C. H., "Quantum Information and Computation," *Physics Today*, Oct. 1995, pp. 24–30.
- [32] Spiller, T. P., "Quantum Information Processing: Cryptography, Computation, and Teleportation," *Proc. of IEEE*, Vol. 84, No. 12, Dec. 1996, pp. 1719 ff.

About the Author

Edward Waltz is the manager of Information Science and Technology Programs at ERIM International, a high-technology firm located in Ann Arbor, Michigan. He is responsible for the research and development of advanced information-based technologies to collect, protect, and combine data and to provide visualized knowledge to intelligence, military, and commercial users.

Mr. Waltz joined ERIM in 1993 from the Allied-Signal Communications Systems Division, where he managed the development and production of systems employing radar, electro-optical, information security, and data fusion processing for civil and military applications. Prior to 1992, when he joined the Communications Systems Division, he was a systems engineer at the Bendix Aerospace Systems Division, where he had roles on the space shuttle, Landsat, Seasat, Apollo, and military surveillance programs.

His 30 years of engineering experience have encompassed a wide range of signal and data processing applications, with emphasis on noncooperative and automatic target recognition (NCTR and ATR). In addition to his target recognition background for both imaging and nonimaging sensors, he has broad experience working with command and control systems users and has practical experience in transitioning technology to operational application.

He is internationally recognized for his expertise in multiple sensor processing and has lectured on the subjects of data fusion and information warfare throughout the United States and in Canada, Europe, and the Middle East. He is the author of the text *Information Warfare Principles and Operations* (Artech House, 1998). He is also the co-author of the first textbook on the subject,

Multisensor Data Fusion (Artech House, 1990), and he has authored or co-authored more than 25 other technical publications on advanced sensors, data fusion, and information warfare.

He received a B.S. in Electrical Engineering from Case Institute of Technology (1968) and an M.S. in Computer, Information, and Control Engineering from the University of Michigan (1971).

Index

- AAM. *See* Air to air missile
- Abduction, 65–66, 84–85, 87
- Abduction-induction, 85–86, 89, 97–103
- ABIS. *See* Advanced battlespace information system
- ABL program. *See* Airborne laser program
- Absorption and retaliation, 32
- Abstract conflict, 18
- Abstracting in automated intelligence, 122
- Access control, 230, 316–322
- Accountability in security, 312–313
- Accuracy of information, 72
- Acquirement of data, 73–74
- Action categories, 73–74
- Action information, 54
- Active attack, 252
- ADEW. *See* Anti-directed energy weapon
- Advanced battlespace information system, 126–133, 345, 348, 359
- AFCERT. *See* Air Force Computer Emergency Response Team
- Affecting information, 252, 255, 265, 340
- Agents in network attack, 281
- Airborne laser program, 291–92
- Air Force 2025, 359
- Air Force Computer Emergency Response Team, 333
- Air platform for intelligence, 120
- Air tasking order, 132
- Air to air missile, 289
- Alarm reporting, 329
- Alignment transformations, 94
- All-optical network, 379
- All-spectral sensing, 369
- Ambiguity deception, 211
- Analysis of intelligence, 115
- Analytic a priori knowledge, 56
- Anti-directed energy weapon, 378
- Application of intelligence, 116
- Application of knowledge, 73–74
- Application process, 51
- Arguments, deductive and inductive, 57–59
- Artificial intelligence, 66
- Association process, 94–95
- Assurance. *See* Information assurance
- Asymmetric key, 326
- Asymmetric threat, 304
- ATO. *See* Air tasking order
- ATR. *See* Automatic target recognition
- Attack and defend operations taxonomy, 26–27
- Attack operations, 165–68
- Attack plan, 164
- Attack response and restoration, 157, 159–62, 182
- Attack threat, 344–45
- Attrition warfare, 4, 6, 7, 12
- Auditing in security, 329

- Authentication of information, 301–2,
316–19, 321
- Automated intelligence processing, 122–24
- Automated network attack, 375
- Automatic target recognition, 103
- Autonomous distributed sensor
network, 370
- Autonomous information search agent, 371
- Autonomous malicious logic, 375
- Availability of information, 22, 36,
301, 307–9
- Back door, 284, 326
- Backward-chaining reasoning, 88
- Bacteria, 283
- Bad code, 282
- Banking and finance
sector, 177, 179, 185, 287
- Barrier-penetrating sensor, 370
- Basic intelligence report, 116
- Battle damage assessment, 144,
164–65, 230, 242
- Battlespace, 27–30, 38
awareness capability, 128, 130
information architecture, 124–33
knowledge dissemination, 113–14
preparation, 111–12, 114
surveillance/analysis, 112, 114
visualization, 112–14, 125
- BDA. *See* Battle damage assessment
- Behavior blocking by scanning, 338
- Behavior information, 54
- Biological immune response model, 334–35
- Bitway, 183–84
- Blurred boundaries, 30
- Bombs, 284
- Bulk encrypting steganography, 378
- Business, 52–53
information exploitation, 54–56
information use, 52–53
knowledge management, 67, 69, 71
- C2W. *See* Command and control warfare
- C4I. *See* Command, control,
communications, computation,
and intelligence
- Camouflage, concealment, and
deception, 270
- Capacity to act, 4–5
- Capturing information, 252, 255, 340–44
- CBW. *See* Chemical and biological weapon
- CC. *See* Common criteria
- CC&D. *See* Camouflage, concealment,
and deception
- CCITT. *See* International Telegraph and
Telephone Consultative
Committee
- CCM. *See* Counter-countermeasures
- Centers of excellence, 38
- Centers of gravity, 4, 8
- CERT. *See* Computer emergency
response team
- CGI. *See* Common Gateway Interface
- Chemical and biological
weapon, 219, 287–88
- Chemical oxygen iodine laser, 291, 375
- CIAC. *See* Computer incident advisory
capability
- Ciphertext, 322–23, 342
- Civil affairs, 162–63
- Civil law enforcement, 288–89
- Classic logic, 70–71
- Closed intelligence source, 116–18
- Clustering of systems, 335
- CM. *See* Countermeasures
- COA. *See* Course of action
- COE. *See* Common operating environment
- COIL. *See* Chemical oxygen iodine laser
- Collection of intelligence, 113–14, 119–22
- Collection technologies, 365–70
- Command and control
warfare, 10, 17–19, 27–31, 39,
75–77, 79, 83, 108, 153, 188,
193–94
data fusion systems, 269–75
information categories, 130–31
information operations, 200–7
joint service, 35
network vulnerabilities, 268–69
representative scenario, 202–6
taxonomy of elements, 206–7

- Command, control, communications, computation, and intelligence, 126–27, 187, 268–75, 348
- Commercial sector technology, 39
- Common criteria, 304
- Common Gateway Interfaces, 265
- Common operating environment, 38, 190, 192
- Communications integrity, 314
- Communications security, 221, 303, 341, 379
- Completeness check, 101
- Compromise protection services, 314
- Computational sociology, 376
- Computation technology, 10
- Computer emergency response team, 38, 220, 333–34, 339
- Computer incident advisory capability, 330
- Computer infrastructure, 185, 188
- Computer network security, 221, 246, 303
- Computer science, 71
- Confidentiality of information, 22, 302, 307–9
- Conflict type, abstract or physical, 18
- Conformity check, 101
- Connectivity classes, 129
- CONOPS. *See* Operational concept
- Content attack, 254–55
- Content information, 54
- Content scanning, 338–39
- Content security, 321
- Continuous change, 11
- Core technology, 358, 362, 367
- Corporate domain, 19, 20
- Correlation metric, 94
- Corruption of information or services, 23, 230
- Cost/benefit analysis, 75–76
- Counter-countermeasure, 216, 321–22
- Counterintelligence, 220
- Countermeasure, 216–17, 273
- Course of action, 126, 130–31
- Covert channel, 313
- Covert information operations, 10
- Creation of knowledge, 39, 52, 83–89
 - in OODA loop, 89–92
- Cross-entropy, 62, 64
- Cryptographic attack, 278–80
- Cryptographic security, 303, 316
- Cryptography. *See* Encryption
- CSR. *See* Computer system security
- Current intelligence report, 116
- Cyber psychological operations, 376
- Cyber warfare, 16–18, 150, 191–94
- DARPA. *See* Defense Advanced Research Project Agency
- Data
 - definition of, 1
 - as information resource, 50–53
- Data cleansing, 101
- Data encryption standard, 326–27
- Data fusion, 89, 90, 130
 - attack categories, 269–73
 - attack matrix, 273–75
 - deductive, 92–97
 - and data mining, 103–5
- Data mining, 89, 90, 130
 - abductive-inductive, 97–103
 - and data fusion, 103–5
- Data refinement, 94, 97
- Data selection and transformation, 101
- Data warehouse, 99–101
- DBA. *See* Dominant battlespace awareness
- DBK. *See* Dominant battlespace knowledge
- DCI. *See* Director of central intelligence
- Deception, 7, 8, 26, 162–64, 195, 207, 211–13, 215–16
- Deception threat, 275
- Decision function, 91
- Decision theory, 64–65, 70–71
- Deduction, 57–59, 65–66, 84–89
- Deductive data fusion, 92–97
- Deductive decision aid, 370–71
- Deep indexing, 122
- DEFCON. *See* Defense condition
- Defeat of adversary systems, 231
- Defense Advanced Research Projects Agency, 336
- Defense condition, 160

- Defense information infrastructure, 28,
 - 174–75, 186–91, 214, 304
 - information operations, 301–7
 - security analysis, 345–50
- Defense Information Systems
 - Agency, 186, 188
- Defense Messaging Service, 188, 192
- Defense Science and Technology Plans, 360
- Defense Science Board, 350–51
- Defense tools and services, 336–39
- Defensive operations, 152–53
 - attack response, 157–62
 - protection measures, 157
 - technology review, 376–79
 - threat intelligence, 153–57
- Deferred decision, 95
- Demassification, 11
- Denial of services, 23, 195, 215–16,
 - 282–83, 302, 314, 319
- Department of Defense, 171, 304, 359–60
- DES. *See* Data encryption standard
- Destruction, 207
- Detection of attack, 23, 77, 85, 89, 94,
 - 182, 329–33
- Deterrence of warfare, 32–33, 35–37,
 - 144, 183, 333
- DEW. *See* Directed energy weapon
- Diffie-Helman, 327
- Digital data link, 130
- Digital organism, 371, 376, 378–79
- Digital signature, 328
- DII. *See* Defense information infrastructure
- Direct attack, 24–27, 168, 254–56
- Directed energy weapon, 218, 288–92,
 - 340, 345, 375–76
- Directive 3600, 38
- Direct multidimensional presentation, 373
- Director of central intelligence, 295
- DISA. *See* Defense Information Systems Agency
- Discovery of knowledge. *See* Knowledge discovery
- Discretionary protection, 310–11
- Discrimination, as information measure, 62
- Disguise of sources of attack, 231
- Disruption of services, 23, 195, 215–16,
 - 275, 282
- Dissemination technologies, 366, 372–73
- Distributed operating systems, 371
- Distribution of knowledge, 73–74
- DMS. *See* Defense Messaging Service
- DNA molecular computing, 372
- DNS. *See* Domain naming service
- Documentation in security, 313–16
- DoD. *See* Department of Defense
- Domain knowledge, 89
- Domain naming service, 262
- Domains of conflict, 18–20
- Dominant battlespace
 - awareness, 107–8, 110–11, 126
- Dominant battlespace
 - knowledge, 108, 110–11, 126
- Dominant maneuver, 31, 108
- Drill down function, 103
- Dynamic malicious logic, 375
- Dynamic state of inferred knowledge, 89
- Dynamic target, 95
- EA. *See* Electronic attack
- Economic availability of information, 357
- Economic warfare, 16–18, 193
- EES. *See* Escrowed Encryption Standard
- Effective force management, 128, 131–32
- Effectiveness metrics, 293
- Effectiveness of information. *See* Utility of information
- Effectiveness of military forces, 110–13
- Electrical power attack, 287
- Electromagnetic compatibility, 289, 344
- Electromagnetic hardening, 39, 340, 346
- Electromagnetic interference, 344
- Electromagnetic pulse weapon, 39, 290–91,
 - 344–46, 375–76
- Electromagnetic security, 341–44
- Electronic attack, 7, 214–16, 242, 288–92
- Electronic communications, 2–3, 8, 172
- Electronic operations, 213–17
- Electronic order of battle, 54
- Electronic protection, 214–15
- Electronic security, 303
- Electronic support, 214–15, 242
- Electronic warfare, 18, 26, 30, 200, 207,
 - 212–15
- Element performance, 75–76

- El Gamal, 327
- Emanations security, 246, 303, 341–44
- EMC. *See* Electromagnetic compatibility
- Emerging technology, 359, 361, 364, 368, 378
- EMI. *See* Electromagnetic interference
- EMP. *See* Electromagnetic pulse weapon
- EMSEC. *See* Emanations security
- Enabling technology, 358, 361, 363, 367, 377–78
- Encryption, 316, 321–23
 - alternatives, 323–27
 - digital signatures, 328
 - end-to-end, 341
 - key management, 328–29
- Energetic particle weapon, 292
- Energy sector, 177, 179, 184
- Entrapment, 333
- Entropy, 60–64
- EOB. *See* Electronic order of battle
- EP. *See* Electronic protection
- Epistemology, 69–70
- ES. *See* Electronic support
- Escrowed Encryption Standard, 329
- Ethics and legality, 253
- European Information Technology Security Evaluation Criteria, 304
- Event detection performance, 77
- EW. *See* Electronic warfare
- Exploitation of information, 23–26, 54–55, 80, 83, 85, 89, 124, 152, 195, 215–16, 261, 264
- Exploitation threat, 275
- External attack, 254–55, 321–22, 329–30, 333, 346
- External threat, 153–55, 304–6, 331
- False alarm, 330
- File Transfer Protocol, 265, 267
- Filtering by firewall, 319–21
- Financial parameters, 68
- Firewall, 318–322, 329, 333
- Focused logistics, 31
- Form information, 54
- Forward-chaining reasoning, 88
- FTP. *See* File Transfer Protocol
- Full-dimension protection, 31
- Full-spectrum dominance, 107
- Fuzzy logic, 58
- GCCS. *See* Global Command and Control System
- Genealogy check, 101
- GEO. *See* Geostationary orbit
- Geostationary orbit, 176
- GII. *See* Global information infrastructure
- Global cellular communications, 372
- Global Command and Control System, 38, 188–89, 191
- Global information infrastructure, 29, 173–77, 201, 214, 315, 358
- Global positioning system, 72, 215
- Global warfare strategy, 32–33
- GPS. *See* Global positioning system
- Ground platform for intelligence, 120
- Gulf War, 7–8, 201–2, 218, 292
- Hacker warfare, 18
- HAE UAV. *See* High-altitude endurance unmanned air vehicle
- Hard decision, 94
- Hard kill, 275
- HEL weapon. *See* High-energy laser weapon
- HEMP. *See* High-altitude electromagnetic pulse weapon
- HIC. *See* High-intensity conflict
- High-altitude electromagnetic pulse weapon, 290–91, 344–45
- High-altitude endurance unmanned air vehicle, 366, 369
- High-bandwidth broadcast, 372–73
- High-dimensional visualization, 373
- High-energy laser weapon, 291–92, 375
- High-intensity conflict, 19
- High-power microwave weapon, 290, 375–76
- High-value target, 241–42
- Hot backup computer, 335
- HPM weapon. *See* High-power microwave weapon
- HTTP. *See* Hypertext transfer protocol
- Human capital, 66
- Human choice domain, 6

- Human factors, 4–6, 9
- Human intelligence, 117–18, 122, 281, 333
- Human services sector, 178, 180
- HUMINT. *See* Human intelligence
- HVT. *See* High-value target
- Hypermedia object information base, 372
- Hyperspectral imaging, 369
- Hypertext transfer protocol, 265, 267
- I&W. *See* Indication and warning
- IBW. *See* Information-based warfare
- IC21—The Intelligence Community in the 21st Century, 360
- IDEA. *See* International data encryption algorithm
- Identification friend or foe, 316
- Identification of object, 95
- Ideological conflict, 19
- IETF. *See* Internet Engineering Task Force
- IFF. *See* Identification friend or foe
- II. *See* Information infrastructure
- IIDR. *See* Information indexing, discovery, and retrieval
- Imagery intelligence, 117–18, 122
- IMINT. *See* Imagery intelligence
- Incident detection and response, 329–33
- Indexing in automated intelligence, 122–24
- Indication and
 - warning, 29, 32, 153–57, 331
- Indirect attack, 24–27, 165, 254–55
- Induction, 57–58, 66, 84–85, 87
- Inductive decision aid, 370–71
- Inference method, 99
- Inferred knowledge, 89
- Info bomb, 282
- Information
 - characteristics of, 49–50
 - definition of, 1–2
 - meaning of, 50–56
 - role in warfare, 2–3
- Information access, 358
- Information age shift, 10–13
- Information and communications sector, 177–79
- Information assurance, 180, 182–83
 - component properties, 301–2
 - elements of, 307–9
 - threat categories, 304–7
 - trusted computing base, 313
- Information attack, 19, 21
 - air force definition, 27
 - elements of, 254–56
 - targets, 8–9, 276–81
 - warfare model, 4–10
 - weapons, 281–86
- Information-based warfare, 10, 20, 69, 75, 362–64, 367–68
- Information business, 55–56
- Information consistency, 229
- Information defend, 21
- Information differential, 30
- Information domain, 5
- Information dominance
 - technology, 19, 365–66
 - collection, 366–70
 - dissemination/presentation, 372–73
 - processing, 370–72
- Information grid, 128–29, 186
- Information hierarchy, 50–51
- Information increase, 61, 63
- Information indexing, discovery, and retrieval, 122–24, 371
- Information infrastructure, 27, 241–42
 - categories, 173–75
 - definition of, 173
 - in IO support system, 241–42
 - war forms, 191–94
- Information leverage, 54
- Information operations, 171–73
 - air force definition, 26
 - command and control warfare, 200–7
 - definition of, 148, 171
 - infrastructure targets, 173–91
 - major functions, 21
 - network warfare, 194–200
 - operational model, 148–52
- Information Operations Support System
 - background, 232
 - cell system, 233–37
 - command relationships, 243–45
 - mission, 233–36
 - operations, 237–43
 - policy, 247–49
 - purpose, 232

- security, 246
- technical architecture, 236–37
- threats, 232–33
- training, 247
- Information operations tasking order, 237
- Information product, 54–55
- Information productivity, 68
- Information security, 155, 157–58, 174, 182, 207–8, 220–21, 246, 349
 - functions of, 302–3
 - trusted computing, 310–16
- Information superiority, 107–24
- Information theory, 58–64, 70–71
- Information warfare, 10
 - and nuclear warfare, 31–32
 - components and goals, 21
 - DoD definition, 19–21
 - Libiki's seven categories, 18
 - Steele's classifications, 18–19
 - technology categories, 362–64
- INFOSEC. *See* Information security
- Infrastructure, 12, 21
- Infrastructure layer, 149–52
- Instantiation, 87
- Institutional domain. *See* Corporate domain
- Intangible values, 11, 68
- Integrated simulation server, 236, 238
- Integration of information
 - technology, 103–5
- Integrity of information, 22, 301, 307–9, 314, 339
- Intelligence, surveillance, and reconnaissance, 10, 38–39, 83, 113–24, 129, 201
 - automated processing, 122–24
 - sources, 116–20
 - technical collection, 119, 121–22
- Intelligence-based warfare, 18
- Intelligence operations, 28–29, 219–20
 - definition of, 2
 - estimates, 116
 - in IO support system, 243, 245
 - offensive, 164–65, 276–81
- Intelligence preparation of battlespace, 111–12, 254
- Interactive networking, 373
- Interception tools in network attack, 281
- Interconnect protocol, 267
- Internal threat, 153, 155–56, 304–306, 321, 330–31, 346
- International data encryption algorithm, 327
- International Standards Organization, 304
- International Telecommunications Union, 304
- International Telegraph and Telephone Consultative Committee, 304
- Internet, 177–78, 194, 212–13, 256, 262, 265–67, 358
- Internet access mapping, 262
- Internet Engineering Task Force, 304
- Internet protocol, 315–16
- Intrusion detection, 230
- IO. *See* Information operations
- IOSS. *See* Information Operations Support System
- IP. *See* Interconnect protocol
- IPB. *See* Intelligence preparation of battlespace
- ISO. *See* International Standards Organization
- ISR. *See* Intelligence, surveillance, and reconnaissance
- ITO. *See* Information operations tasking order
- ITSEC. *See* European Information Technology Security Evaluation Criteria
- ITU. *See* International Telecommunications Union
- IW-A. *See* Information attack
- IW-D. *See* Information defend
- JDL. *See* Joint Directors of Laboratories
- Jihad, 19
- Joint Directors of Laboratories, 92–94
- Joint operations, 35, 38
- Joint technical architecture, 304
- Joint Vision 2010, 31, 108–9, 126, 202, 359
- Joint Warfighter Science and Technology Plan, 229–31
- JTA. *See* Joint technical architecture
- Kant, Immanuel, 56
- Kerberos authentication, 316, 318

- Kerchoff's principle, 278
- Key management, 278, 322, 328–29
- Kinetic energy weapon, 218, 282, 286–87
- Knowledge and warfare, 2, 21, 50–53, 56
- Knowledge capital, 68
- Knowledge-creation processes, 83–89
- Knowledge discovery, 52, 86, 89, 102
See also Data mining
- Knowledge management, 66–70
- Known pattern template, 330
- Language translation, 373
- Layering concept, 314–16
- Learning organization, 11
- Learning phase, 86
- Legality of attack, 253
- Legal protection, 182–83
- LEO. *See* Low earth orbit
- LIC. *See* Low-intensity conflict
- Likelihood of message occurrence, 58–60
- Linked multimedia visualization, 125
- Logic, 57–58, 70, 84–85
- Logic contagion, 282
- Logistic process, 109
- Low earth orbit, 176
- Low-intensity conflict, 19, 287
- Making Intelligence Smarter: The Future of U.S. Intelligence*, 360
- Malicious logic, 282–86, 375
- Management, in information age, 12
- Mandatory protection, 310–11
- Maneuver warfare, 12
- MASINT. *See* Measurements and signals intelligence
- Mass disruption, 139
- Mass protection, 139
- MCTL. *See* Military Critical Technologies List
- Meaning refinement, 92–93, 95, 97
- Measurements and signatures intelligence, 117–18
- Measures of effectiveness, 75, 293–95, 348
- Measures of information, 60–64
- Measures of performance, 293–94, 348
- Media, 185, 194–95, 201, 209
- Mediated heterogeneous database, 371
- Medium-bandwidth global communication, 372
- Medium earth orbit, 176
- Medium-intensity conflict, 19
- MEII. *See* Minimum essential information infrastructure
- Memorandum of Policy on Information Warfare, 38, 75
- MEMS. *See* Microelectromechanical system
- MEO. *See* Medium earth orbit
- Message size and utility, 72–73
- MIC. *See* Medium-intensity conflict
- Microcellular wireless communications, 372
- Microchemical organism, 376
- Microelectromechanical system, 370
- Micro unmanned air vehicle, 370
- Microwave programming, 290
- Military Critical Technologies List, 360
- Military-operational intelligence, 113, 115
- Military operations taxonomy, 24–27
- Military science, 33–35, 38, 52
- Military-tactical intelligence, 113, 115
- MILSATCOM, 188
- Minimal protection, 310
- Minimum essential information infrastructure, 160
- Misdirection deception, 211, 213
- Mission server, 236, 238
- MLS. *See* Multiple levels of security
- Mobile agent, 281
- Modeling function in on-line analytic processing, 103
- MOE. *See* Measures of effectiveness
- MOP. *See* Measures of performance; Memorandum of Policy on Information Warfare
- Morphological modification, 212
- Multicast broadcast, 373
- Multidimensional analysis, 103
- Multimedia database, 371
- Multiple levels of security, 246
- Mutual information, 61
- NA. *See* Network attack
- NACSI. *See* National COMSEC Instructions

- NACSIM. *See* National COMSEC Information Memoranda
- National Computer Security Association, 220
- National Computer Security Center, 302, 310
- National COMSEC/EMSEC documents, 341–42
- National COMSEC Information Memoranda, 341
- National COMSEC Instructions, 341
- National information infrastructure, 19–20, 28–30, 140–44, 174–75, 177–86, 214, 304
- National Institute of Standards and Technology, 304
- National Security Agency, 314, 341
- Navigation warfare, 215–17
- NCSA. *See* National Computer Security Association
- NCSC. *See* National Computer Security Center
- NDEW. *See* Nuclear directed energy weapon
- NEMP. *See* Nuclear electromagnetic pulse weapon
- Neocortical warfare, 21
- NETINT. *See* Network intelligence
- Network Information Center, 262
- Network integrated intrusion detection, 378
- Network intelligence, 117–18, 195, 276–81
- Network management and control, 217, 230
- Network mapping, 262–63
- Network security model, 314–15
- Network support, 242–43
- Network warfare, 16–17, 28, 30, 153, 191–94, 242
information operations, 194–200
Internet attacks, 265–67
processes, 259–65
representative scenario, 195–99
targeting, 276–81
taxonomy of elements, 200
vulnerabilities, 256, 258–60
weapons, 281–86
- New knowledge, 57–58
- New World Vistas, 359
- NIC. *See* Network Information Center
- NII. *See* National information infrastructure
- NIPRNET, 188
- NIST. *See* National Institute of Standards and Technology
- Nonrepudiation, 302
- Non-state sponsored threat, 154
- NS. *See* Network support
- NSM. *See* Network security model
- Nuclear directed energy weapon, 290
- Nuclear electromagnetic pulse weapon, 290
- Nuclear warfare, 31–32, 139, 219
- Object refinement, 92, 94–95, 97, 271
- Observation process, 6–8, 50–51, 91, 112, 127
- Observe, orient, decide, act loop, 27–28, 34, 89–92, 127, 129–30, 132–33, 241, 254, 268, 292–93
- Offensive information, 251–53
- Offensive operations, 160
analysis, 164–65
attack, 165–68
perceptions management, 162–64
targeting/damage assessment, 164–65
- Offensive technology review, 373–76
- Office of Management and Budget, 29
- Office of Secretary of Defense Studies, 360
- OLAP. *See* On-line analytic processing
- OMB. *See* Office of Management and Budget
- One-directional model of warfare, 4–10
- On-line analytic processing, 103
- OODA loop. *See* Observe, orient, decide, act loop
- OOTW. *See* Operations other than war
- Open communication, 36
- Open intelligence source, 116–18
- Open network, 36
- Open security standards, 304–10
- Open source intelligence, 117–18, 122, 333
- Open space and skies, 36
- Open system computing, 371

- Open System Interconnection, 150, 183–84
- Open treaties, 36
- Operational concept, 38, 229–31
See also Information Operations
 Support System
- Operational model of warfare, 148–52, 167
- Operational orders, 236, 241
- Operational security, 155, 157–58, 173, 182, 207–8, 200, 222, 246, 306, 349
- Operations other than war, 235
- OPORDS. *See* Operational orders
- OPSEC. *See* Operational security
- Optical storage, 371
- Organization process, 11–12, 50–51, 73–74
- Organization threat intelligence, 219
- Orientation process, 5–6, 7, 8, 91, 127
- OSD. *See* Office of Secretary of Defense Studies
- OSI. *See* Open System Interconnection
- OSINT. *See* Open source intelligence
- PA. *See* Physical attack
- Passive attack, 252
- Passive conductive measure, 292
- Password authentication, 316–18
- Pattern description, 89, 97–100
- PCCIP. *See* Presidential Commission on Critical Infrastructure Protection
- Peace, 35–37
- Penetration of system, 220, 231, 254–55, 262–64
- Penetration testing, 350
- Perception operations, 5, 7–9, 21, 27, 167, 194, 241
 compared to knowledge, 52
 and layer concept, 148–52, 239–40
 management in offense, 162–64
 security, 307–9
- Performance metrics, 293
- Personal domain, 19–20
- Personnel security, 307–9, 339–40
- PGM. *See* Precision guided munitions
- PGP. *See* Pretty good privacy
- Philosophy, 52–53, 56–58, 70–71
- Physical destruction, 6, 18, 26, 200, 207–8, 215, 216–19, 231, 242, 275, 282, 286–92
- Physical distribution sector, 178, 180
- Physical domain/level, 5, 7–8, 27, 30, 150–52, 241–43
 security, 246, 307–8, 339–46
- Plaintext, 322–23, 342
- Pointcast, 373
- Policy, 139–140
 definition of, 140
 security, 140–44
- Political warfare, 16–17, 193
- Precision engagement, 10, 31, 108, 110, 368
- Precision geospatial information system, 371
- Precision guided munitions, 287, 289, 376
- Preemptive indication, 230
- Preparing for the 21st Century*, 360
- Presidential Commission on Critical Infrastructure Protection, 177, 186
- Pretty good privacy, 327
- Private key, 325–26
- Private sector defense, 29–30, 183
- Processing technology, 115, 365, 370–72
- Process loop acceleration, 12
- Process refinement, 93, 95–96
- Production mechanism, 13
- Production of information, 11, 115–16
- Protection of forces, 109
- Protection of information, 19, 73–74, 144, 157–58, 180–86, 301
- PSTN. *See* Public switched telephone network
- Psychological operations, 7–8, 17–18, 26, 30, 151–53, 162, 195, 200, 207–11, 235, 239, 241, 376
- PTN. *See* Public telecommunications network
- Public affairs, 162–63
- Public health system model, 336
- Public key, 325–28
- Public switched telephone network, 179
- Public telecommunications network, 177
- PYSOPS. *See* Psychological operations

- Quantum computing, 372, 376
Quantum cryptography, 379
- Radioelectronic combat, 202
Radio frequency energy
 weapon, 214, 288–91
Radiological weapon, 219
RC2/RC4/RC5, 327
Reach through function, 103
Reaction to threat, 230
REC. *See* Radioelectronic combat
Refinement feedback, 103
Relationships between entities and events, 86
Relationships between forces, 75
Report, observation, 50, 115–16
Response degrees, 23
Response function, 29, 329–33
Restoration of information, 302, 338
RF. *See* Radio frequency
Risk management, 64, 156–57, 339, 348–50
Risk of threat equation, 155
RMA. *See* Revolution in military affairs
ROE. *See* Rules of engagement
Root access, 264
RSA cryptosystem, 327
Rule-based system, 88
Rules of engagement, 243
- SAM. *See* Surface to air missile
Satellite communications, 176, 188, 368
Scale of operations, 11
Scanners, 281, 286, 336–339
Sea platform for intelligence, 120
Secret algorithm, 324–27
Secure wide area network, 315–16
Security, 26, 29–30, 39
 access control, 316–22
 defensive operations, 230, 345–50
 in IO support system, 246
 open standards, 304
 policy, 140–44
 services/certification, 339
 strategy, 144–48
 trust policy model, 312
 See also Information security;
 Operational security
SEE. *See* Single event effect
- Semiautomated network attack, 375
Semiotic theory, 65–66, 70–71
SEMP. *See* Switching electromagnetic pulse
Sensitivity label, 312
Sensor attack, 269–71, 321
Sensor detection performance, 77
Sensor network, 368
Service availability, 230
SGEMP. *See* System-generated
 electromagnetic pulse
SHADE. *See* Shared data environment
Shared data environment, 192
SIGINT. *See* Signals intelligence
Signals intelligence, 117–18, 122, 366
Signature scanning, 338
Simulations, 292–95
Single event effect, 219
SIPRNET, 188
Situation refinement, 92, 95, 97, 271
Situation server, 236, 238
SKIP JACK, 327
Societal domain, 19
Soft kill, 275
Space platform for intelligence, 120
Spatial view visualization, 125
State-based detection, 332
State-sponsored threat, 154
Steganography, 324–25, 378
Strategic command, 35
Strategic intelligence, 73, 113–15, 118–19
Structural capital, 66
Sun Tzu, 2–3, 9
Surface to air missile, 289
Surveillance, 220, 359
Survivable system, 221, 303, 334–36
S/WAN. *See* Secure wide area network
Switching electromagnetic pulse, 291
Symmetric key system, 325
Synthetic a posteriori knowledge, 56
Synthetic a priori knowledge, 56
System-generated electromagnetic pulse, 291
- Tactical warning and assessment, 159–62
Tactics of attack, 252
Targets/targeting, 164–65
 behavior, 75
 categories in IO system, 244

- Targets/targeting (continued)
 - nontraditional, 8
 - offensive attack, 276–281
- TCB. *See* Trusted computing base
- TCP. *See* Transmission control protocol
- TCSEC. *See* Trusted computing security
 - evaluation criteria
- Technical attack, 167, 219–20
- Technical intelligence collection, 119–22
- Technical security, 307–9
- Techniques of attack, 252
- Technology
 - development of, 13, 38–40
 - high and low, 18
 - information objectives, 52–53
 - types of, 358–65
- Technology ownership, 357–58
- Telecommunication access mapping, 263
- Telecommunications sector, 185, 287
- TEMPEST, 341–42
- Temporal perspective, 99, 256
- Terrorism, 287
- Themescape visualization, 125
- Third-wave nation, 186, 188
- Threatening behavior template, 330
- Threat intelligence, 153–57
- Threat refinement, 92, 95, 97, 271
- Threats
 - categories, 304–7
 - data fusion attack, 273–75
 - to IO system, 232–33
 - to network, 260
 - warnings, 230
- Time-critical target, 132
- Timeliness of information
 - flow, 7, 10, 72, 119, 256
- Toffler, Alvin, 10–12, 36
- Toffler, Heidi, 10–12, 36
- Toolkits in network attack, 281
- Tracking of object, 95
- Traffic analysis, 330, 332
- TRANSEC. *See* Transmission security
- Transformations of warfare, 10–15, 30–33
- Transmission Control Protocol, 267
- Transmission security, 303, 379
- Trap door, 284, 326
- Trojan horse, 283–84
- Trusted computing and
 - networking, 310–16, 377–78
- Trusted computing base, 312–13
- Trusted security
 - evaluation, 303–4, 310–11, 349
- UAGS. *See* Unattended ground sensor
- UAV. *See* Unmanned air vehicle
- Ultraspectral imaging, 369
- Ultrawideband emission, 289
- Unattended ground sensor, 366
- Uncertainty in inferred knowledge, 89
- Understanding process, 50–51
- Uniformity check, 101
- Uniqueness of message, 58–60
- UNIX attack, 261–62
- Unmanned air vehicle, 366, 369–70
- User access, 264
- USS *Vincennes*, 212
- Utility function, 64–65
- Utility of information, 70–78
- UWB. *See* Ultrawideband emission
- Value function, 64–65
- Value of information, 66, 68–69
 - definition of, 66–69
 - utility measurement, 70–78
- Van Eck emissions, 342, 344
- Verified protection, 310–11
- Vietnam War, 10
- Virtual network, 188
- Virtual private networking, 316, 321
- Virtual reality technology, 373
- Virus, 283–86
- Visualization
 - of battlespace, 112–14, 125
 - in data mining, 102–3
 - technology, 373
- Vulnerability assessment, 230, 345–48
- Warehoused data, 99–101
- Warfare, definition of, 1
- War games, 292–95
- Warm backup computer, 335
- Waves of civilization, 12–14
- Wealth production, 13

- Weaponeering, 164
- Weapons
 - delivery means, 281–82
 - information, 256–57, 281–286
 - physical destruction, 218–19
- Weapons of mass destruction, 17, 108, 139
- Web spoofing, 212–213
- Wheel relationship visualization, 125
- Will to act, 4, 6, 9
- Wisdom, 21, 51, 53
- WMD. *See* Weapons of mass destruction
- Worker specialization, 11
- World War II, 171
- Worm, 283