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
Policy (government policymakers, Department of Defense)	Define the objects of security (interests), the security objectives for those interests, and their intent and willingness to apply resources to protect those interests.	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
Strategy (military joint staff, services)	Develop a plan to apply political, economic, psychological, and military force as necessary during peace and war to afford the maximum support to policies.	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

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.	DoD Directive 5200.1, DoD Information Security Program DoD Directive 5205.2, DoD Operations Security Program TRADOC Pam 525-69. Concept for Information Operations. 1 August 1995 TRADOC Pam 525-70. Battlefield Visualization Concept. 1 October 1995 JCS Pub 3-58, Joint Doctrine for Operational Deception JCS Pub 2-01, Joint Tactics, Techniques, and Procedures for Intelligence Support to Joint Operations JCS Pub 3-53. Doctrine for Joint Psychological Operations. 30 July 1993 JCS Pub 3-56. Command and Control Doctrine for Joint Operations. 3 May 1995
Tactics (war fighter)	Equip, train for, and deploy the technical means and tactical doctrine for application of those means to conduct information operations.	U.S. Army FM 100-6, Information Operations 27 August 1996 U.S. Army FM 33-1. Psychological Operations. 18 February 1993 Other field manuals, training manuals, and detailed tactical documents for intelligence, electronic warfare, network attack and exploit operations, special operations, and other operations.

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:

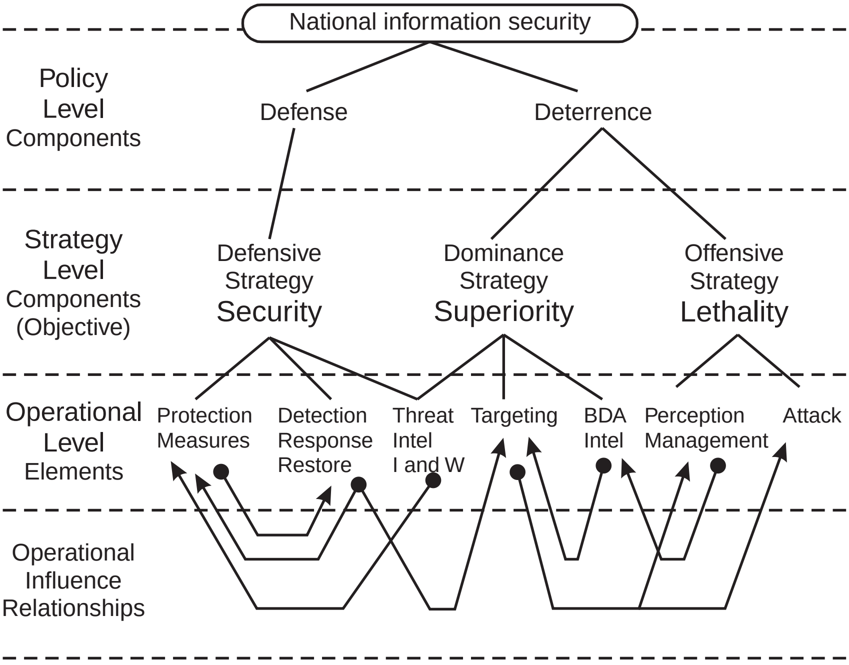

National information security
Policy Level Components
Defense
Deterrence
Strategy Level Components (Objective)
Defensive Strategy Security
Dominance Strategy Superiority
Offensive Strategy Lethality
Operational Level Elements
Protection Measures
Detection Response Restore
Threat Intel I and W
Targeting
BDA Intel
Perception Management
Attack
Operational Influence Relationships

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.

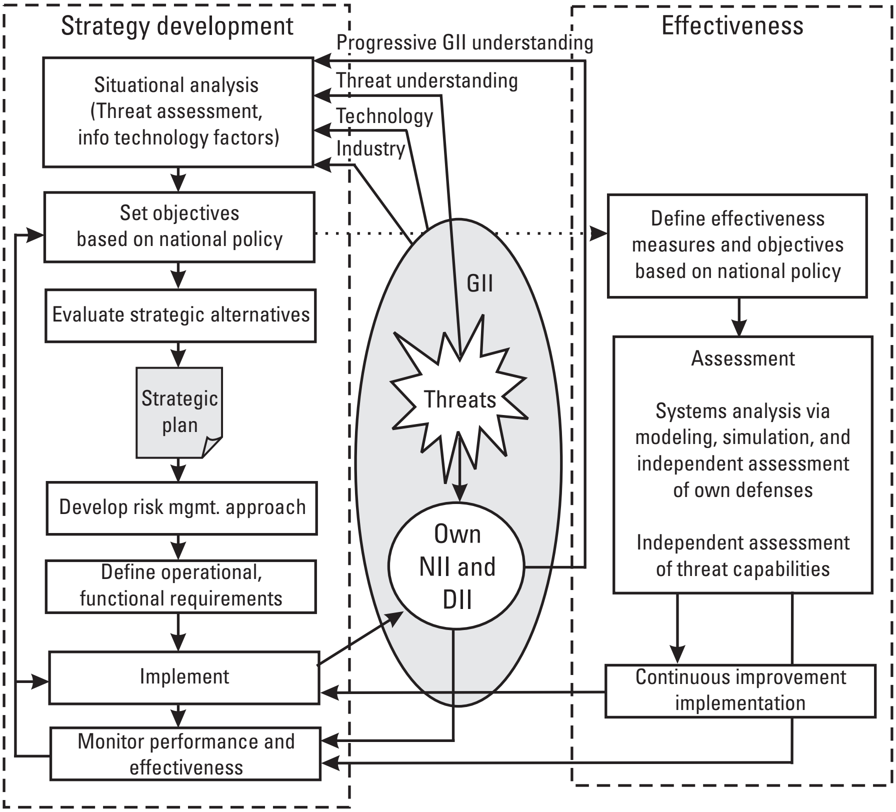

Strategy development
Situational analysis (Threat assessment, info technology factors)
Set objectives based on national policy
Evaluate strategic alternatives
Strategic plan
Develop risk mgmt. approach
Define operational, functional requirements
Implement
Monitor performance and effectiveness
Progressive GII understanding
Threat understanding
Technology
Industry
GII
Threats
Own NII and DII
Effectiveness
Define effectiveness measures and objectives based on national policy
Assessment
Systems analysis via modeling, simulation, and independent assessment of own defenses
Independent assessment of threat capabilities
Continuous improvement implementation

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

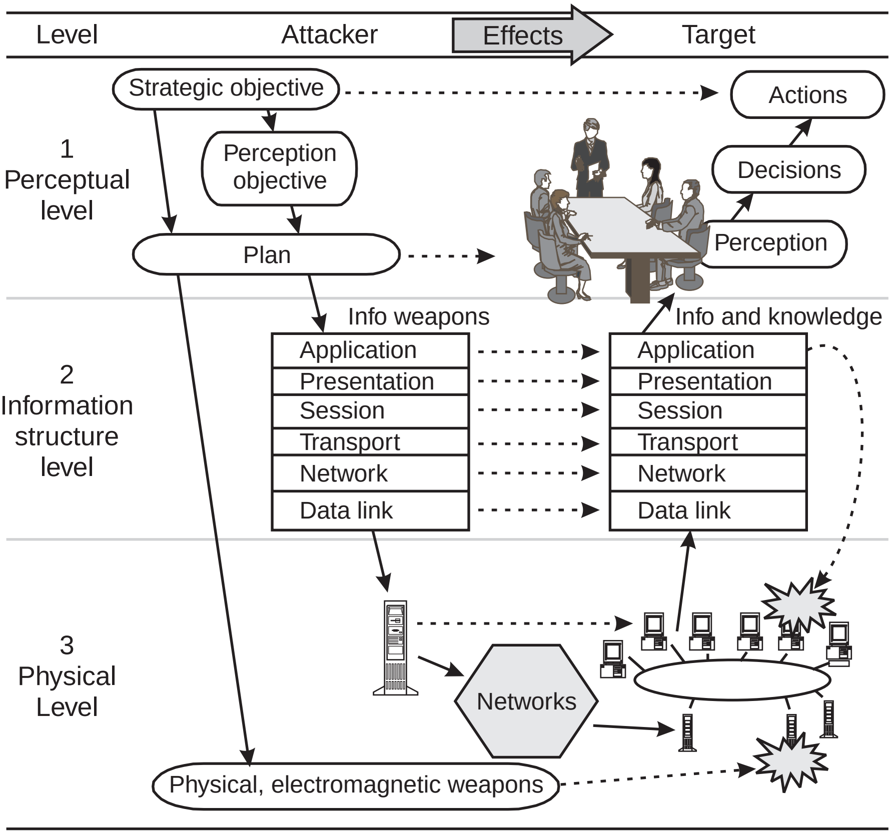


Figure 5.3 Operational model of information operations.

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: • 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: • 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: • 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.

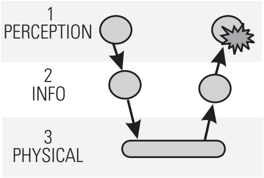
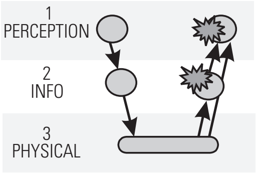
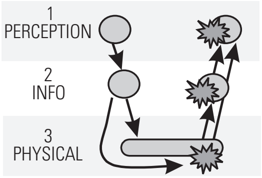
The attack threads through the IW model for three categories of information warfare are illustrated in Table 5.3. Exploitation of the physical and information layers purely for purposes of perception management, or psychological warfare (PSYWAR), is illustrated at the top of the figure. Command and control 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
NETWAR • Pure PSYWAR • Political Warfare	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.	
NETWAR • PSYWAR • Economic Warfare • Denial of Service	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.	
Command and Control Warfare (C2W)	All three layers of the infrastructure are exploited, attacked, and used to convey the perception themes. Targets are military and national leaders (decision makers).	

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:

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

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

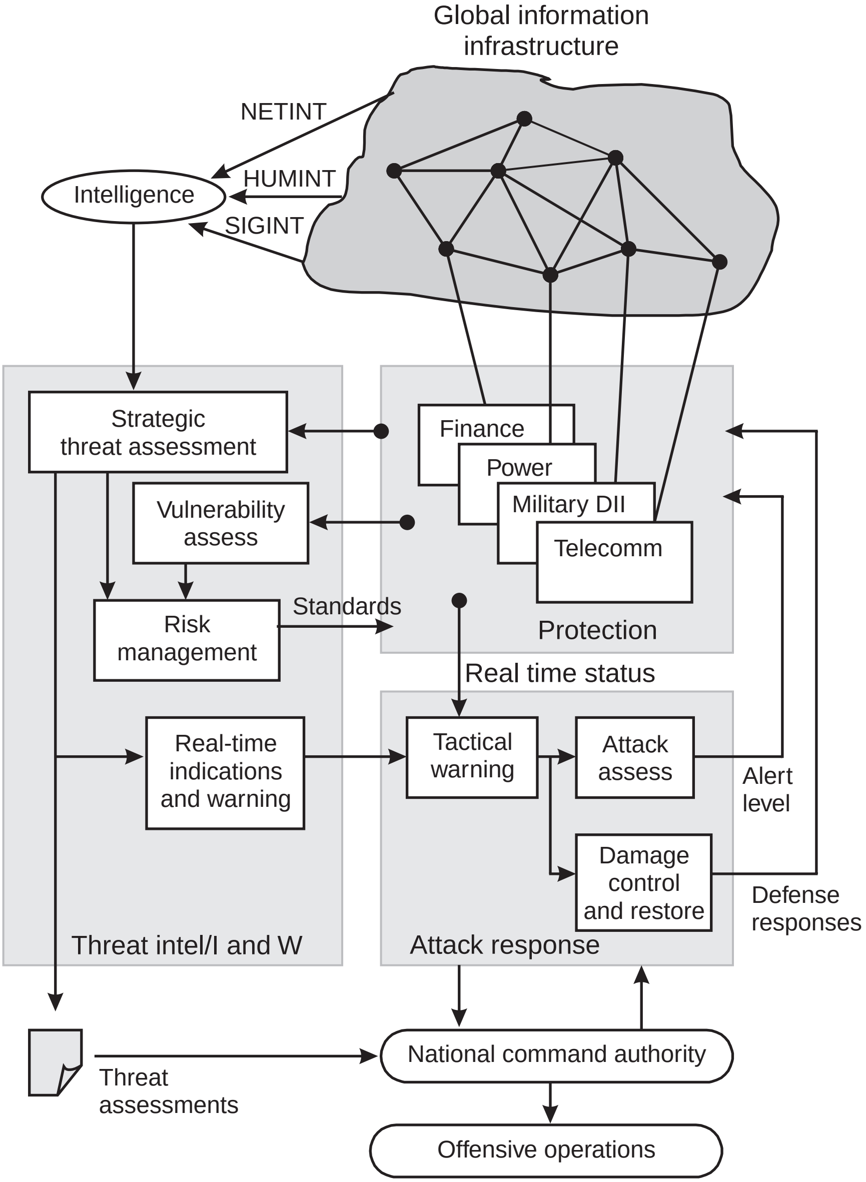


Figure 5.4 Defensive operational elements provide proactive and reactive protection of the information infrastructure.

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	Friendly forces 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 preconceived 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).

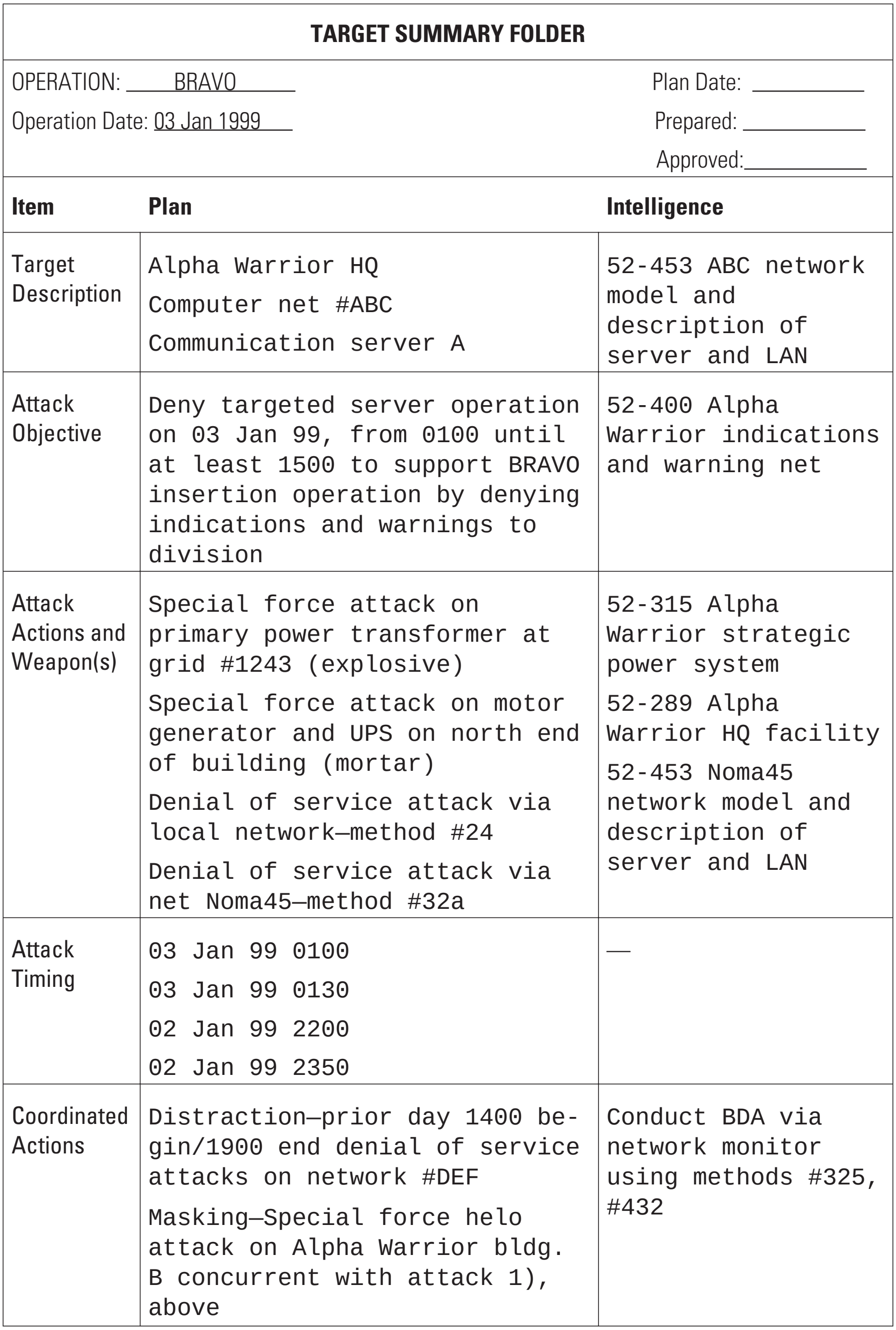
The wireless network line will be monitored throughout the attack to perform real-time battle damage assessments in support of the BRAVO insertion operation. These assessments monitor the effectiveness of the denial of I&W (of the insertion) to division HQ.

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: BRAVO Plan Date: ____________

Operation Date: 03 Jan 1999 Prepared: ____________

Approved: ____________

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.