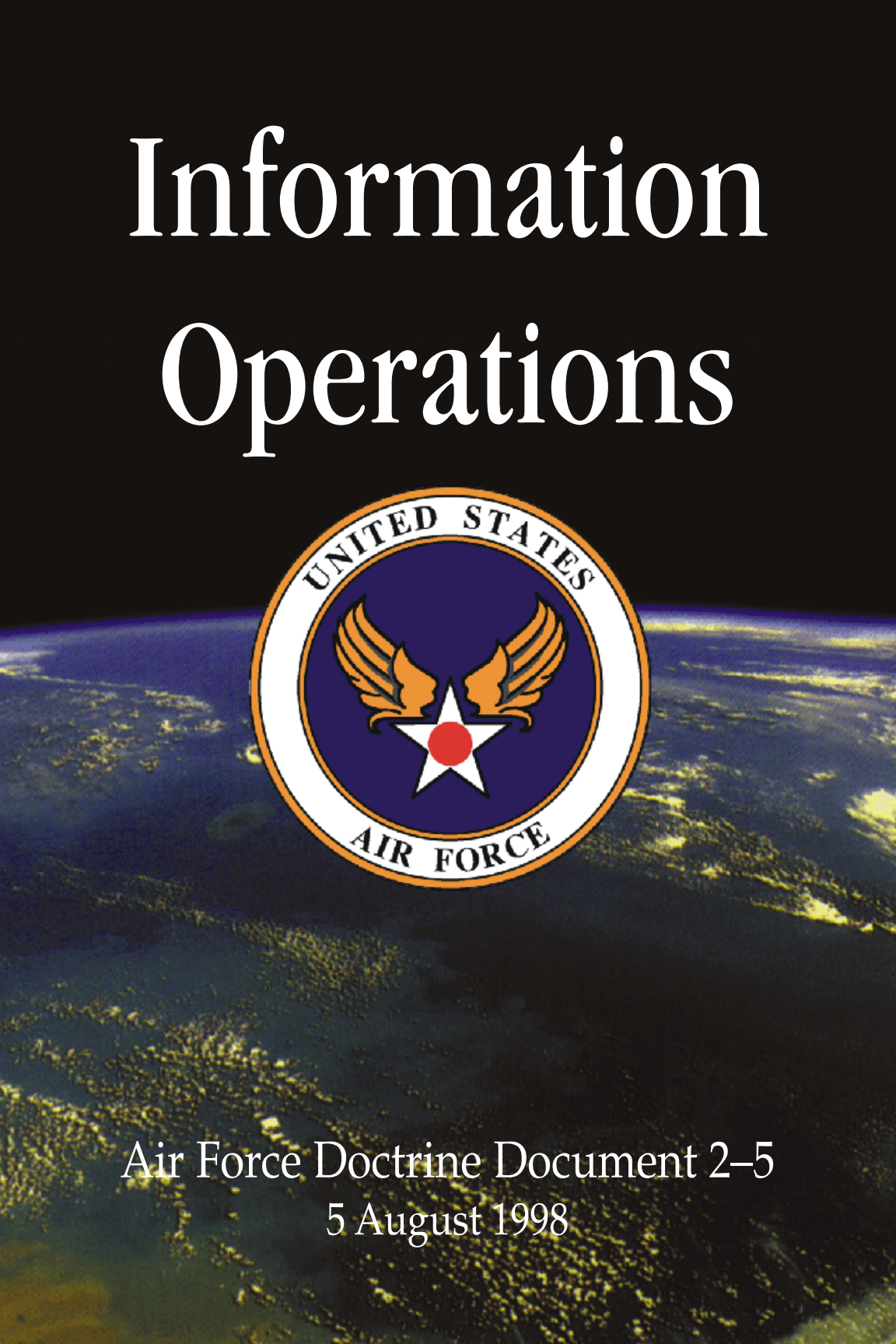
Information Operations



Air Force Doctrine Document 2–5

5 August 1998

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE DOCTRINE DOCUMENT 2–5
5 AUGUST 1998

OPR: HQ AFDC/DR (Maj Stephen L. Meyer, USAF)
Certified by: HQ AFDC/CC (Maj Gen Ronald E. Keys, USAF)
Pages: 53
Distribution: F
Approved by: MICHAEL E. RYAN, General, USAF
Chief of Staff

FOREWORD

Information has long been an integral component of human competition—those with a superior ability to gather, understand, control, and use information have had a substantial advantage on the battlefield. History is replete with examples of how information has influenced political and military struggles—from the earliest battles of recorded history to current military operations in Bosnia. The Air Force's vision in *Global Engagement: A Vision for the 21st Century Air Force* recognized this by identifying information superiority as one of six Air Force core competencies. Today, more than ever, gaining and maintaining information superiority is a critical task for commanders and an important step in executing the remaining Air Force core competencies. The execution of information operations in air, space, and, increasingly, in "cyberspace" constitutes the means by which the Air Force does its part to provide information superiority to the nation, joint force commander, and Service component and coalition forces.

The Air Force believes information operations include actions taken to gain, exploit, defend, or attack information and information systems. **Information operations apply across the range of military operations, from peace to all-out conflict. The Air Force believes that to fully understand and achieve *information superiority*, our understanding of information operations must explicitly include two conceptually distinct but extremely interrelated pillars: information-in-warfare—the "gain" and "exploit" aspects or other information-based processes—and information warfare—the "attack" and "defend" aspects.**

This document focuses primarily on information warfare, particularly the aerospace power function of counterinformation through which the Air Force implements information warfare responsibilities inherent in the Department of Defense definition of information operations.

The emerging Air Force definition of **information warfare is information operations conducted to defend one's own information and information systems or attacking and affecting an adversary's information and information systems. The defensive aspect**, *defensive counterinformation, much like strategic air defense,* **is always operative.** *Conversely,* **the offensive aspect**, *offensive counterinformation,* **is primarily conducted during times of crisis or conflict.** Information war-

Information Superiority — an Air Force Vision of the 21st Century

fare involves such diverse activities as psychological operations, military deception, electronic warfare, both physical and information ("cyber") attack, and a variety of defensive activities and programs. It is important to stress that *information warfare* is a construct that operates across the spectrum, from peace to war, to allow the effective execution of Air Force responsibilities.

Air Force doctrine recognizes a fully integrated spectrum of military operations. Air and space operations can support and leverage information operations, just as the reverse is true. Information warfare takes advantage of the increasing criticality and vulnerability of information and information systems. It is not platform dependent nor is it confined to a particular degree of hostilities across the range of military operations. The fundamentals of information warfare—affecting an adversary's information and information-based systems and defending one's own—have not changed through time. What has changed is the means and route of attack. Additionally, today's information environment presents inherent capabilities and liabilities previously unknown to friendly forces. These capabilities must be exploited, and the liabilities must be effectively managed. **The two pillars of information operations, information-in-warfare and information warfare, though separate and distinct, must be closely integrated with each other and with all aerospace power functions.**

Information has emerged as both a critical capability and a vulnerability across the spectrum of military operations. We must be prepared to attain information superiority across that same spectrum. The United States is not alone in recognizing this need—potential adversaries worldwide are rapidly improving or pursuing their own information warfare capabilities. As the Air Force evolves into the air and space force of the 21st century, it must establish a foundation for developing capabilities critical to meeting the emerging challenges of the information age.

MICHAEL E. RYAN
General, USAF
Chief of Staff

5 August 1998

TABLE OF CONTENTS

Page

INTRODUCTION vii

CHAPTER ONE—The Nature of Information Operations 1
- General 1
- Trends 4
- Threat 5
- Main Considerations 7

CHAPTER TWO—Counterinformation 9
- Offensive Counterinformation Operations 10
  - Psychological Operations 11
  - Electronic Warfare 12
  - Military Deception 13
  - Physical Attack 14
  - Information Attack 15
- Defensive Counterinformation Operations 15
  - OPSEC and Information Assurance 16
  - Counterdeception 17
  - Counterintelligence 18
  - Counterpsychological Operations 18
  - Electronic Protection 19

CHAPTER THREE—Functions Supporting Information Operations 21
- Intelligence 21
- Surveillance and Reconnaissance 22
- Precision Navigation and Positioning 23
- Weather Services 24
- Other Support and Reachback 25

CHAPTER FOUR—Information Operations in Theater Operations 27
- Information Superiority 27
- Effects-Based Approach 27
  - Strategic Effects 28
  - Operational Effects 28
  - Tactical Effects 29
- Counterinformation Planning 30
  - Offense-Defense Integration 33
  - IW Targeting 33

Organizations 34
Information Warfare Organizations 34
Computer Emergency Response Teams 35

CHAPTER FIVE—Summary 37

SUGGESTED READINGS 38

GLOSSARY 39

INTRODUCTION

PURPOSE

This Air Force Doctrine Document (AFDD) explains the Air Force perspective on information superiority, and the relationship between information operations and its two pillars, information warfare and information-in-warfare. This AFDD focuses its discussion primarily on information warfare. The "gain" and "exploit" aspects of information operations are explained in Air Force Doctrine Documents 2–5.1, *Electronic Warfare Operations*, and 2–5.2, *Intelligence, Surveillance, and Reconnaissance*.

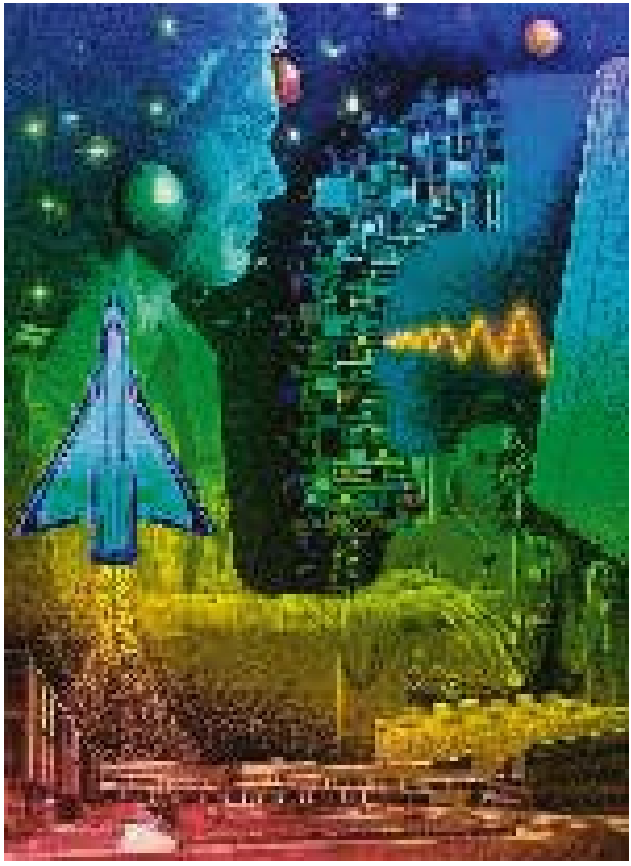
APPLICATION

This AFDD applies to all active duty, Air Force Reserve, Air National Guard, and civilian Air Force personnel. The doctrine in this document is authoritative but not directive; therefore, commanders need to consider not only the contents of this AFDD, but also the particular situation they face.

SCOPE

The Air Force will carry out appropriate information operations actions and functions to properly support national and military objectives. The term "information operations" applies across the range of military operations from peace to war. Even when the United States is at peace, the Air Force is vulnerable to information operations or attack and is aggressively enacting defensive counterinformation programs and capabilities that will deter and respond appropriately to threats. At the far end of the range of military operations, warfighters conduct offensive counterinformation operations while simultaneously protecting friendly information and information systems.

The term "information warfare" generally includes and subsumes previous Air Force definitions for command and control warfare. The primary difference is it is now conceivable to identify, attack, and defeat more than just command and control systems and this must be considered in both offensive and defensive planning.



The execution of information operations in air, space, and cyberspace cross the spectrum of conflict.

CHAPTER ONE

THE NATURE OF INFORMATION OPERATIONS

> ***Dominating the information spectrum is as critical to conflict now as occupying the land or controlling the air has been in the past.***
>
> **General Ronald R. Fogleman**
> ***Cornerstones of Information Warfare***

GENERAL

Just as air and space superiority give the commander the freedom to attack and the freedom from attack, so too is information superiority an enabling function. The ability to support the commander with a fused, all-source, and near real-time presentation of the battlespace, while at the same time complicating the same for an adversary, is the essence of information operations. The ability to improve the commander's capability to observe, orient, decide, and act (OODA Loop) faster and more correctly than an adversary is only part of the equation. Through information operations new target sets emerge, new weapons are available, and the opportunity to directly influence adversary decision making through delays, disruption, or disinformation is a reality. But in the final analysis, *information operations exist to support commanders in determining the situation, assessing threats and risks, and making timely and correct decisions.*

The Air Force believes that dominating the information spectrum is as critical to conflict now as controlling air and space or occupying land was in the past and is seen as an indispensable and synergistic component of aerospace power. The time between the collection of information and its availability to users at all levels has shrunk to heretofore unimaginably short spans. While possessing, exploiting, and manipulating information has always been an essential part of warfare, it may become central to the outcome of conflicts in the future. While traditional principles of warfare still apply, they are increasingly coupled with the realization that the possession and manipulation of information itself

can be a key element of the war-winning equation. More than at any other time in history, *information has evolved from being only an adjunct supporting primary weapon systems to, in many cases, being itself a weapon or target.* Since there are few distinct boundaries in the information environment, *the military limitations of time, terrain, and distance, already reduced in this century by the advent of aerospace power, now are bounded in many cases only by the speed of light.*

Information superiority—the degree of dominance that allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition—is an Air Force core competency upon which all the other core competencies rely. In no other area is the pace and extent of technological change as great as in the area of information and information systems. While information superiority is not solely the Air Force's domain, the strategic perspective and global experience gained from operating in the aerospace continuum make airmen uniquely prepared to gain and use information superiority through robust information operations (IO) and execute its two major aspects: information-in-warfare (IIW) and information warfare (IW).

IO comprise those actions taken to gain, exploit, defend, or attack information and information systems and include both information-in-warfare and information warfare and are conducted throughout all phases of an operation and across the range of military operations.

IIW involves the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on its integrated intelligence, surveillance, and reconnaissance (ISR) assets; its information collection and dissemination activities; and its global navigation and positioning, weather, and communications capabilities.

IW is information operations conducted to defend the Air Force's own information and information systems or conducted to attack and affect an adversary's information and information systems. This warfare is primarily conducted during times of crisis or conflict. However, the defensive component, much like air defense, is conducted across the spectrum from peace to war.

IW consists of the function of counterinformation (CI) and its two subsets, offensive counterinformation (OCI) and defensive counterinformation (DCI).

The Air Force has developed OCI and DCI tactics, techniques, and procedures to gain advantage over its adversaries. IW offers options to achieve national military objectives more directly. Consequently, IW is not only about technology, but also about integrating information-related means to achieve effects in meeting common objectives. Accordingly, commanders must focus on the strategic, operational, and tactical effects desired in any particular situation and bring to bear the right mix of all capabilities to achieve those effects.

The Air Force has embraced the concepts of information superiority, IO, IIW, and IW to limit its own potential vulnerabilities and to exploit the enemy's vulnerability. Pursuing, achieving, and integrating information

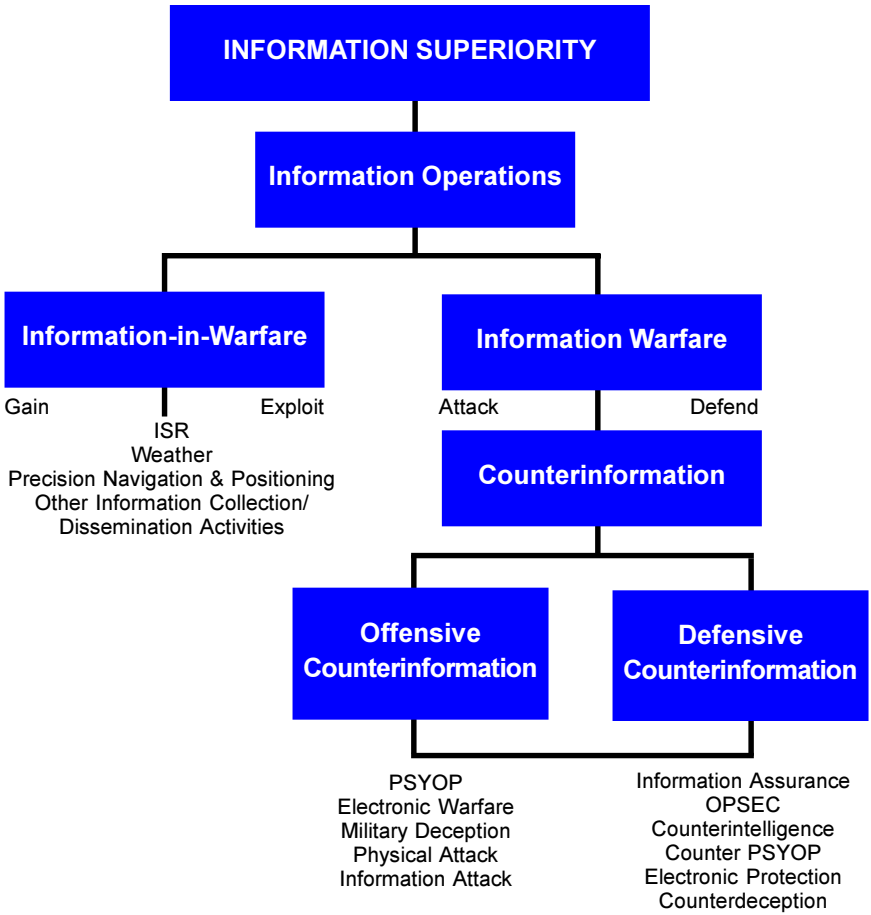


Figure 1.1. Air Force Information Superiority Construct

The national information infrastructure links organizations at the speed of light.

superiority with the other facets of aerospace power must become a major focus of the Air Force's operational art. Figure 1.1 below presents the Air Force understanding of information superiority and how the related pieces of IO normally fit together to provide an integrated capability.

TRENDS

Today, information systems are part of larger information infrastructures. These infrastructures link individual information systems through numerous and redundant direct and indirect paths, including space-based systems. There is a growing information infrastructure that transcends industry, the media, and the military and includes both government and nongovernment entities. It is characterized by a merging of civilian and military information networks and technologies. Collecting, processing, and disseminating information by individuals and organizations comprise an important human dynamic, which is an integral part of the information infrastructure. Just as importantly, our weapon systems, capabilities, and operations are now inextricably linked to larger information infrastructures. Air Force operations have always depended on what today is called the defense information infrastructure (DII), the collection of shared or interconnected information systems that serves the Department of Defense's local, national, and worldwide information needs. Due to an increasing dependence upon commercial systems, the DII is part of and must rely on the national information infrastructure (NII), the still-larger collection of US government and commercial systems and

networks. The NII is intermeshed with and dependent upon the global information infrastructure (GII), which consists of massive networks of systems worldwide. In reality, a news broadcast, a diplomatic communiqué, and a military message ordering the execution of an operation *all* depend on the GII. **The Air Force's increased ability to access, process, and store information, coupled with its ever-increasing dependence on information systems and information infrastructures has driven the Air Force to reexamine and redefine how it integrates information-related activities into its functions. Thus, as argued in AFDD 1, *Air Force Basic Doctrine*, dominating the information spectrum is as critical to conflict now as controlling air and space, or occupying land was in the past, and is viewed as an indispensable and synergistic component of aerospace power.**

The explosion in information technologies (computers, processors, and decision tools) has already changed both the Air Force's military systems and concepts of operations in fundamental ways. It is difficult to name a single major Air Force weapon or system that does not rely on sophisticated electronics and extremely precise information—and that dependence will only increase. In a world where computer processing chips double their speeds every 18 months and are readily available, the Air Force must be able to adapt both its technologies and its operational concepts even faster than it does today. Truly, flexibility is even more the key to aerospace power in the information age.

An outgrowth of this increasing reliance on information-dependent weapon systems and capabilities is that ISR has become fundamental to successful military operations of any kind. ISR assets seek to obtain a superior understanding of an adversary's information and other strengths and weaknesses to provide information vulnerability analysis. In some cases, it is difficult to distinguish between what is an ISR capability versus an IW capability; in fact, sometimes a platform or system can be both. Thus, ISR is also a critical part of the DII and must be protected, while it provides key information enabling protective, retaliative, and offensive IW activities.

THREAT

The threats currently facing the United States are no longer defined solely by geographic or political boundaries as during the cold war. As technology advances, society's ability to transfer information and an adversary's opportunity to affect that information increases and, in some

cases, may eclipse the security designed into the information systems. Just as the United States plans to employ IO against its adversaries, so too can it expect adversaries to reciprocate. Numerous countries have discovered the benefits of IO. They employ psychological operations (PSYOP), electronic warfare (EW), and military deception and now are collecting available intelligence via the Internet and creating malicious code and hacking cells. Terrorists, criminals, and hackers are becoming more of a threat as they discover the benefits of using the electronic environment to accomplish their goals. Since US socioeconomic and military infrastructures are highly dependent on the free flow of information, a knowledgeable adversary has the ability to infiltrate and attack information systems. This "Achilles' heel" of the United States can be the great equalizer for a militarily inferior adversary. IO must minimize an adversary's ability to impact US military information while allowing the United States to prosecute IO.

Each of the threats listed in figure 1.2 below pose an inherent risk to weapon and support systems that rely on information system support. The overall capabilities are expressed whether the threats are structured or unstructured. The structured threat is organized, is financially backed, has clear objectives, and has the means for infiltrating and obtaining information. Unstructured threats are those with a limited support structure and limited motives. Structured and unstructured threats may be conducted by "insiders": some recruited by the adversary, some pursuing their own objectives. *The potential of internal threats continues to be one of the largest areas of concern.*

Information Warfare Threats

Compromise	Deception/ Corruption	Denial/ Loss	Destruction
Malicious Code System Intrusion Psychological Ops Intel Collection Technology Transfer Software Bugs	Malicious Code System Intrusion Military Deception Spoofing Imitation	Malicious Code System Intrusion Lasers Physical Attack Nuclear & Non-nuclear EMP Virus Insertion System Overload Radio Freqency Jamming	Malicious Code Bombs Directed Energy Weapons Lasers Physical Attack Nuclear & Non-nuclear EMP Chemical/ Biological Warfare

Figure 1.2. Information Warfare Threats

IW threats fall into four categories: compromise, deception/corruption, denial/loss, and physical destruction. Each poses an inherent risk to both standalone and networked weapon and support systems that rely on information systems. These threats can be employed by both organized entities, such as nation-states, and unstructured threats, such as rogue computer hackers.

MAIN CONSIDERATIONS

For the foreseeable future, commanders and leaders will focus on the following as main considerations for the Air Force's efforts in IO:

- The two pillars of IO, IIW and IW, while separate and distinct, are intrinsically and inextricably linked and must be integrated in their application to achieve information superiority.
- Even more so than other air and space operations, counterinformation operations must be performed simultaneously and in parallel. Specific IW actions can alternate between OCI and DCI in a continuing cycle, literally at the speed of light.
- The Air Force performs theater-level strategic, operational, and tactical information warfare, employing a combination of deployable and reachback capabilities, in concert with Aerospace Expeditionary Task Force themes.
- The Air Force, when tasked, will vigorously support national, strategic-level IW, though mostly planned outside the military Services.
- DCI is the Air Force's overall top priority within the information warfare arena. Commanders are accountable for DCI posture and execution within their commands.
- Air Force IW efforts will focus on implementing IW capabilities through warfighting component commands in support of joint warfighting commands.
- IW activities and operations must be integrated within the normal campaign planning and execution process. There may be campaign plans composed primarily of IW actions; however, there should never be separate IW campaigns.

Counterintelligence operations can include actions to neutralize terrorist threats.

CHAPTER TWO

COUNTERINFORMATION

Information warfare is a broadly defined concept encompassing and integrating many types of activities and capabilities extending throughout the spectrum of conflict. IW capabilities can accomplish control and force application objectives and support enhancement objectives. As defined, IW involves extensive planning, includes many classic security functions, may accomplish independent offensive strikes, and yet also requires integration into full-dimensional protection. IW can be conducted in support of nearly all warfighting objectives and functions (such as interdiction and counterair, or to enhance and enable ISR efforts), in support of other Service component and theater objectives, or in support of national tasking.

Counterinformation (CI) is an aerospace function that establishes information superiority by neutralizing or influencing adversary information activities to varying degrees, depending on the situation. The focus of CI is on countering an adversary's ability to attain an information advantage. It does this through information denial, degradation, disruption, destruction, deception, and exploitation. All of these measures can confuse, delay, or inhibit adversary offensive actions and reduce reaction time for critical defensive measures.

CI is conducted throughout the spectrum of conflict, as appropriate and necessary, in keeping with US policy and legal requirements. Thus, CI operations can include support of military operations other than war and peacetime defense of Air Force or friendly operational or support networks. Combined with counterair and counterspace, CI creates an environment where friendly forces conduct operations with the requisite freedom of action while denying, neutralizing, or influencing adversary information activities as required. Figure 2.1 (page 10) lists the general activities of CI.

CI, like counterair and counterspace, consists of both offensive and defensive aspects.

- **Offensive counterinformation (OCI)** includes **actions** taken to **control** the information environment. OCI operations are designed to *limit, degrade, disrupt, or destroy* adversary information capabilities and are

Counterinformation	
Offensive Counterinformation	**Defensive Counterinformation**
Psychological Operations Electronic Warfare Electronic Attack Electronic Protection Electronic Warfare Support Military Deception Physical Attack Information Attack	Information Assurance Operational Security Counterdeception Counterintelligence Counterpsychological Operations Electronic Protection

Figure 2.1. Prominent Counterinformation Activities

dependent on having an understanding of an adversary's information capabilities.

- **Defensive counterinformation (DCI)** includes those **actions** that **protect** information, information systems, and information operations from any potential adversary. DCI includes such programs as *operations security (OPSEC), information assurance, and counterintelligence.*

- OCI and DCI are analogous to the traditional Air Force constructs of offensive counterair (OCA) and defensive counterair (DCA). While the analogy is not perfect, there are strong parallels and airmen can apply many of the hard-won precepts of OCA-DCA to OCI-DCI. As with OCA and DCA, commanders must focus on the required effects rather than on dogmatic themes to distinguish OCI from DCI operations. The dividing line between the two can be exceedingly thin and the transition nearly instantaneous.

OFFENSIVE COUNTERINFORMATION OPERATIONS

OCI operations rely on having an understanding of an adversary's information capabilities, dependencies, and vulnerabilities. OCI activities that can affect an adversary's capabilities and exploit vulnerabilities include: PSYOP, EW, military deception, information attack, and physical attack.

Psychological Operations

COMMANDO SOLO aircraft perform psychological operations.

PSYOP are designed to convey selected information and indicators to foreign leaders and audiences to influence their emotions, motives, objective reasoning, and ultimately their behavior to favor friendly objectives. *PSYOP have strategic, operational, and tactical applications.* Modern PSYOP are enhanced by the Air Force's ability to communicate, with precision and discrimination, massive amounts of information to target audiences with the intent of influencing their perceptions and decision-making processes. Examples of this information include promises, threats of force or retaliation, conditions of surrender, safe passage for deserters, or support to resistance groups. During operations in Haiti, Air Force COMMANDO SOLO aircraft broadcast two radio messages each day informing the population that the "Son of Democracy," President Jean-Bertrand Aristide, would soon return. During Operation JUST CAUSE, ground units employed loudspeakers to drive Panamanian dictator Manuel Noriega, a fugitive from justice, out of his hiding location and to induce the surrender of thousands of Panamanian Defense Force personnel. In similar situations, Air Force assets can be employed to broadcast radio and loudspeaker messages that may influence a wide audience.

At the strategic level, PSYOP may take the form of political or diplomatic positions, announcements, or communiqués. At the operational

> ***The real target in war is the mind of the enemy commander, not the bodies of 17 of his troops.***
>
> **Captain Sir Basil Liddell Hart**
> ***Thoughts on War*, 1944**

and tactical levels, PSYOP planning may include the distribution of leaflets, the use of loudspeakers, and other means of transmitting information that encourage adversary forces to defect, desert, flee, or surrender and to promote fear or dissension in adversary ranks. Persistent PSYOP attacks can have a synergistic effect, accelerating the degradation of morale and further encouraging desertion.

Electronic Warfare

EW is any military action involving the use of electromagnetic and directed energy to manipulate the electromagnetic spectrum or to attack an adversary. This is not limited to radio frequencies but includes optical and infrared regions as well. EW assists air and space forces to gain access and operate without prohibitive interference from adversary systems. During Operation Desert Storm, effective force packaging, which included self-protection, standoff, and escort jamming and antiradiation attacks, contributed to the Air Force's extremely low loss rate.

The three major subdivisions of EW are electronic attack, electronic protection, and electronic warfare support. All three contribute to air and space operations, including the integrated IO effort. Control of the electromagnetic spectrum is gained by protecting friendly systems and countering adversary systems. **Electronic attack** limits the adversary commander's use of the electronic spectrum; **electronic protection** (the defensive aspect of EW) enhances the use of the electronic spectrum for friendly forces; and **electronic warfare support** enables the commander's accurate estimate of the situation in the operational area. Electronic attack and electronic warfare support must be carefully integrated with electronic protection to be effective. The responsible commander, normally the joint force air component commander (JFACC), must also ensure maximum coordination and deconfliction between EW, ISR, and communication activities.

EW is a force multiplier. Control of the electromagnetic spectrum can have a major impact on success across the range of military operations. Proper employment of EW enhances the ability of US operational commanders to achieve objectives. When EW actions are integrated with military operations, rather than just added on, synergy is achieved, attrition is minimized, and effectiveness is enhanced.

> ***All warfare is based on deception.***
>
> **Sun Tzu**
> ***The Art of War*, c. 500 BC**

Military Deception

Military deception misleads adversaries, causing them to act in accordance with the originator's objectives. *Deception operations span all levels of war and simultaneously include both offensive and defensive components.* Deception can distract from, or provide cover for, military operations, confusing and dissipating adversary forces. Counterdeception (discussed later in the DCI section) ensures friendly decision makers are aware of an adversary's deception activities so they may act accordingly. *Deception requires a deep appreciation of an adversary's cultural, political, and doctrinal perceptions and decision-making process, which planners can then exploit.*

A classic example of military deception is World War II's Operation FORTITUDE NORTH, when the Allies heavily bombed the Pas de Calais rather than Normandy, feeding the German bias for believing the former would be the invasion site. A modern deception opportunity could, for example, be presented by an adversary's dependence on non-refuelable fighter aircraft. If the Air Force can induce opposing commanders to launch their fighters too early to effectively threaten Air Force offensive strike forces, it is as though the adversary's sorties were never launched.

Deception operations depend on accurate and reliable intelligence, surveillance, and reconnaissance operations as well as close cooperation with counterintelligence activities. *The key is anticipating adversary motives and actions.* When formulating the deception concept, particular attention must be placed on defining how US commanders would like the adversary to act at critical points. Those desired actions then become the goal of deception operations.

Deception operations must be planned from the top down, and subordinate deception plans must support higher-level plans. Plans may include the employment of lower-level units, although subordinate commanders may not know of the overall deception effort. Commanders at all levels can

plan deception operations but must coordinate their plans with their senior commander to ensure overall unity of effort. OPSEC may dictate only a select group of senior commanders and staff officers know which actions are purely deceptive in nature. However, limiting the details of deception operations can cause confusion and must be closely monitored by commanders and their staffs.

Deception operations are a powerful tool in military operations. Forces and resources must be committed to the deception effort to make it believable, and are worth the short-term costs.

Physical Attack

As an element of an integrated counterinformation effort, physical attack refers to the use of "hard kill" weapons against designated targets. The objective is to affect information or information systems by using a physical weapon. *Physical attack disrupts, damages, or destroys an adversary's information system through destructive power.*

Coupling precision-guided munitions and advanced delivery platforms, employing cruise missiles or gunships, or infiltrating a small strike team to neutralize a communications node are key examples that require precision to accurately attack an adversary's information system, including command and control (C^2). Two tactical-level examples are using precision-guided munitions against a C^2 communications relay station and inserting a special operations team to cut and/or exploit communication lines.

Future attacks may come from unexpected directions.

Information Attack

Information attack refers to those activities taken to manipulate or destroy an adversary's information or information system without necessarily changing visibly the physical entity within which it resides. Penetration of an adversary's information system has great value in combat because it offers the ability to incapacitate an adversary while reducing exposure of friendly forces, reducing collateral damage, or preventing excessive adversary losses. By using new information attack capabilities and tools, conventional sorties can be saved for other targets. Manipulation of databases or parameters of reporting systems can cause incorrect information to influence leaders' decision making or destroy the adversary's confidence in its information systems. An effective information attack could force an adversary to use less technical means because of friendly intrusion into the system. An example of information attack might be to interject disinformation into a radar data stream to cause antiaircraft missiles to miss intended targets. *Information attack may be seen as attacking the "observation" and "orientation" component of the OODA Loop because the adversary's ability to rely on "observations" is affected.*

DEFENSIVE COUNTERINFORMATION OPERATIONS

> ***We have evidence that a large number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks on military-related computers.***
>
> **John M. Deutch**
> **Director, Central Intelligence Agency**
> ***The Washington Post*, 26 June 1996**

DCI operations are those actions protecting Air Force information and information systems from the adversary. The Air Force uses DCI to provide the requisite defense critical to the military's ability to conduct operations. Actual incidents—ranging from a teenager's computer attacks against US research and development facilities to an adversary's deliberate jamming of systems critical to displaying the air picture for the joint force air component commander—demonstrate how critical defending information is to military operations. Due to unique US dependencies on and vulnerabilities of information systems, **DCI is the Air Force's overall top priority within the information warfare area.** *Accord-*

ingly, commanders are responsible for DCI posture and execution within their commands. The goal of DCI is to ensure the necessary defense of information and information systems that support military operations. When combined with OCI, the net result will be an enhanced opportunity to use IW to successfully achieve stated military and national objectives. DCI weaves together related disciplines and capabilities toward satisfying a stated objective. Capabilities that can be integrated to conduct DCI include OPSEC, information assurance, counterdeception, counterintelligence, counterpsychological operations, and electronic protection. These various defensive capabilities are mutually supporting (that is, any one can be used as a countermeasure in support of another) and can support offensive activities. Additionally, to capitalize on defensive information effects, the capabilities must be applied in a "layered defense." However, they can also conflict with each other and with offensive activities if they are used without knowledgeable coordination and integration. For example, security measures, such as information assurance, would strive to minimize an information system's security breach as quickly as possible to protect the systems, while counterintelligence may want to allow continued access to identify and exploit the adversary.

OPSEC and Information Assurance

The Air Force uses security measures to protect and defend information and information systems. **Security measures include OPSEC and information assurance. OPSEC** is a process of identifying critical information and subsequently analyzing the friendly actions that accompany military operations and other activities to:

- Identify those actions that can be observed by adversary intelligence systems;
- Determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful; and
- Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

OPSEC is a process. OPSEC is not a collection of specific rules and instructions that can be applied to every operation; it is a methodology that can be applied to any operation or activity for the purpose of denying critical information to the adversary. OPSEC is applied to all military activities at all levels of command. The commander, Air Force forces

(COMAFFOR), should provide OPSEC planning guidance to the staff at the start of the planning process when stating the "commander's intent" and subsequently to the supporting commanders in the chain of command. By maintaining a liaison with the supporting commanders and coordinating OPSEC planning guidance, the COMAFFOR will ensure unity of effort in gaining and maintaining the essential secrecy considered necessary for success.

Information assurance *is those measures to protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and nonrepudiation (ability to confirm source of transmission and data).* This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Information assurance is applied to all military activities at all levels of command. The COMAFFOR should provide information assurance planning guidance to the staff when stating the "commander's intent" and subsequently to the supporting commanders in the chain of command. The information assurance process is applied through technology-based activities.

Information assurance includes the protection of information systems against unauthorized access or information corruption. It encompasses computer security, communications security, and those measures necessary to detect, document, and counter such threats.

- Computer security involves the measures and controls taken to ensure confidentiality, integrity, and availability of information processed and stored by a computer. These include policies, procedures, and the hardware and software tools necessary to protect computer systems and information.
- Communications security includes measures and controls taken to deny unauthorized persons information derived from telecommunications while also ensuring telecommunications authenticity. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information.

Counterdeception

Counterdeception is the effort to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Counterdeception can

ensure friendly decision makers are aware of adversary deception activities to take appropriate action. Integrated ISR activities provide awareness of an adversary's posture or intent and also identify an adversary's attempts to deceive friendly forces. As the Air Force develops more integrated and near-real-time information processes, methods for identifying adversary deception must extend beyond the traditional intelligence process.

Counterintelligence

Counterintelligence protects operations, information, systems, technology, facilities, personnel, and other resources from illegal clandestine acts by foreign intelligence services, terrorists groups, and other elements. Counterintelligence threat estimates and vulnerability assessments identify exploitable friendly information weaknesses and vulnerabilities. The importance of a strong counterintelligence capability is illustrated by the cold war example of the John Walker case. From the late 1960s to the 1980s, the United States suspected the Soviets had foreknowledge of American naval exercises; however, it was not until the Walker espionage ring was exposed that the United States discovered that the Soviets had been given naval cipher materials.

Counterpsychological Operations

> ***No enterprise is more likely to succeed than one concealed from the enemy until it is ripe for execution.***
>
> **Niccolo Machiavelli**
> ***The Art of War***

Numerous organizations and activities (for example, ISR, military units, and commanders) can identify adversary psychological warfare operations attempting to influence friendly populations and military forces. Countering such messages is vital to successful operations. Air Force commanders must consider how Public Affairs, Combat Camera capabilities, and military information dissemination can convey accurate information to the targeted audiences and mitigate the intended effects of an adversary's psychological operations. When required, OCI operations such as information attack, physical attack, or EW can hinder distribution of the adversary's message. COMMANDO SOLO, unmanned aerial vehicles, and

space-based broadcast capabilities can likewise support counter-psychological operations and public affairs activities.

Electronic Protection

As discussed in the OCI section, EW is any military action involving the use of electromagnetic and directed energy to manipulate the electromagnetic spectrum or to attack an adversary. On the defensive side, *electronic protection guarantees the use of the electronic spectrum for friendly forces.* Electronic protection is an important part of the defensive DCI mix and must be fully coordinated and integrated with OCI capabilities, activities, and operations.

CHAPTER THREE

FUNCTIONS SUPPORTING INFORMATION OPERATIONS

Critical functions such as ISR, precision navigation and positioning, and weather enhance the employment of air, space, and information operations. Together, these functions provide commanders the ability to observe the overall battlespace, analyze events, and maintain awareness. Assets such as Airborne Warning and Control System; Joint Surveillance Target Attack Radar System; unmanned aerial vehicles; airborne reconnaissance platforms such as the U–2 and RC–135; weather platforms such as the WC–130; and space systems help shape operations by giving commanders a superior ability to assess situations and take appropriate action.

The space medium and the systems that operate in space are of critical importance to the Air Force and its ability to engage on a global basis. Each Air Force core competency, but particularly information superiority, relies on the attributes of space systems to meet the stringent requirements for navigation, weather, command and control, intelligence, surveillance and reconnaissance, and other essential capabilities. The Air Force is unique in its ability to capitalize on the attributes of space systems by being able to respond with rapid mobility and firepower to the near-real-time information afforded by systems operating in space.

The following IIW functions contribute to increasing overall IO effectiveness:

INTELLIGENCE

Accurate and timely intelligence is an important element in achieving campaign objectives, including IO tasks. In addition to maintaining databases for nodal analysis and assessing foreign capabilities, intelligence provides situation awareness, which is essential for monitoring and assessing global conditions. Intelligence activities seek to obtain a superior understanding of the strengths and weaknesses of an adversary's information systems and infrastructure to provide information vulnerability analysis. Intelligence creates opportunities for systematic exploitation of an adversary's liabilities and helps isolate forces from their leadership. Data fusion, assisted by technological advances in computer capabilities, can

Reconnaissance aircraft such as the U–2 are a mainstay of battlespace awareness.

provide immediate worldwide crisis support. Intelligence collection and analysis must be conducted constantly while keeping the capabilities and requirements of IO in mind, much like how Air Force intelligence activities have traditionally been focused on their applicability to air warfare. Furthermore, intelligence support of IO requires the collection and analysis of information in traditional areas (such as orders of battle and warning) as well as specific details of an adversary's telecommunications and computer infrastructure—not just what systems a country has but details of how they are installed, work, and are used. In addition, intelligence analysts strive to accurately estimate an adversary's probable courses of action, including their capability and intentions to conduct IW. This level of analysis in some cases exceeds current capabilities and will require the development of new collection systems and techniques or perhaps the reprioritization of current collection and analytical assets.

SURVEILLANCE AND RECONNAISSANCE

Intelligence preparation of the battlespace provides warfighters with a mission-focused and tailored understanding of an adversary. As an integral part of that process, surveillance and reconnaissance provide commanders with real-time or near-real-time information on adversary locations, dispositions, capabilities, and indicators of intentions. Surveillance and reconnaissance provide indications and warning and situation awareness of threats to the United States and its allies. Air, space, and ground systems and teams provide intelligence on opposing force orders of battle, disposition, capabilities, and events underway. For example, Air Force Special Tactics Teams, as part of a joint special operations team, can provide crucial intelligence, most notably in the deep battlefield prior to,

New generation reconnaissance assets provide more options for joint force commanders.

during, and after hostilities. These teams also help identify adversary centers of gravity. Space-based surveillance and reconnaissance systems now provide near global coverage. Air Force assets offer commanders a responsive collection capability that supports the decision-making process. Surveillance and reconnaissance, in practice, are often conducted simultaneously by the same collection platform or team. However, the functions are differentiated by the following definitions: **surveillance** *is continuous collection of information from the air, space, and earth's surface;* **reconnaissance** *is conducted to gain information on localized and specific targets within a constrained time frame.* Surveillance and reconnaissance are essential in any military operation, to include IO. For example, surveillance and reconnaissance can be used to detect and locate electronic emissions that can be taken advantage of by information attack and physical attack operations.

PRECISION NAVIGATION AND POSITIONING

Precision navigation and positioning (PNP) have enhanced the accuracy of both weapons and delivery platforms to the point that weapons are increasingly more capable of target discrimination. Many factors contribute to a weapon's ability to target with greater accuracy. Modern aircraft sensors, targeting systems, and precision-guided munitions allow accurate location of targets and delivery of firepower. Space support, integrated intelligence, and precision navigation equipment allow accurate delivery of unguided ordnance.

PNP provide air, space, and information operations the capability to attack targets in sensitive areas. The ability to locate and deliver accurate firepower through physical attack, for example, greatly reduces the number of aircraft and sorties required to neutralize or destroy a target. Air, special ground teams,

Global positioning systems have revolutionized warfare.

and space forces armed with PNP equipment are able to attack moving targets in sensitive areas. Users of the global positioning system can process satellite signals and determine position within tens of feet, velocity within a fraction of a mile per hour, and time within a millionth of a second.

At 0400 hours on 16 January 1991, Air Force special operations forces' MH–53 Pave Low helicopters, the only helicopter equipped with GPS at the time, began the Gulf War by leading Apache helicopters to Iraqi EW/ground controlled intercept sites. The Apaches destroyed the sites, thus opening a "hole" in the Iraqi integrated air defense system for conventional air forces to attack Iraqi targets.

WEATHER SERVICES

The weather services provided by the Air Force supply timely and accurate environmental information, including both space and atmospheric weather, to commanders for attaining objectives and developing plans at the strategic, operational, and tactical levels. The weather services gather, analyze, and provide meteorological data and environmental information for mission planning and execution. *Environmental information is integral*

to the decision-making process for employing forces and planning and conducting air, ground, sea, and space launch operations supporting IO. It influences the selection of targets, routes, weapon systems, and delivery tactics.

OTHER SUPPORT AND REACHBACK

The nature and complexity of the GII, NII, and DII have fundamentally altered some aspects of the nature of war. Today, mobility and sustainment of forces, as well as OCI and DCI operations themselves, are becoming highly dependent on reachback capabilities through those infrastructures. Agencies and organizations that provide support to the COMAFFOR include the National Security Agency, Joint Command and Control Warfare Center, Joint Warfare Analysis Center, Defense Information Systems Agency, Air Force Office of Special Investigation, and Air Intelligence Agency. Such reachback capabilities can yield significant advantages and should be pursued as a means of improving combat effectiveness and reducing personnel risks. On the other hand, commanders and leaders also must recognize emerging dependencies on reachback capabilities and actively seek to identify and eliminate any associated vulnerabilities through the DCI focus.

Space support for IO is provided by the Commander in Chief, United States Space Command through the Commander, Air Force Space Command. Available space systems include communications, navigation, and weather satellites. *Operational tasking of Air Force space systems is made through the joint air operations center to the Air Force Space Command's space operations center, with Air Force Space Support Team (AFSST) support if required.* Deployable assets will be included in theater operations plans and included in deployment documents such as the time-phased force and deployment data, when appropriate.

Assigned space staff officers, theater space liaison officers, or AFSST personnel with appropriate systems expertise will advise the COMAFFOR IW team or Information Warfare Squadron (and others as required) on space system capabilities that may assist IO efforts and integrate space capabilities with the joint air operations center. Space operations officers, at the appropriate levels, will act as the liaison between the COMAFFOR or JFACC and Air Force Space Command units that operate, control, and execute space capabilities. These officers work as part of the COMAFFOR IW team/Information Warfare Squadron to help develop space control and IO courses of action and integrate these space capabilities into COMAFFOR or JFACC air and space operations plans.

CHAPTER FOUR

INFORMATION OPERATIONS IN THEATER OPERATIONS

INFORMATION SUPERIORITY

One of the COMAFFOR and JFACC's priorities is to achieve information superiority over an adversary by controlling the information environment to improve friendly operations. This goal does not negate the need to achieve air and space superiority but rather facilitates efforts in those areas and vice versa. The aim of information superiority is to have greater situational awareness and control over the adversary. IO may be the means to reach the commander's objectives directly or it may serve as a force multiplier, enhancing and synergistically complementing other methods of warfighting. Information superiority is attained through efforts directed at integrating various measures to gain, exploit, deny, degrade, disrupt, deceive, or destroy the adversary's information and its functions while protecting friendly information. The effort to achieve **information superiority depends upon three fundamental components: effects-based approach, integrated counterinformation planning, and information warfare organizations.** The rest of this chapter will focus on these three critical components.

Cyber war is warfare of the present.

EFFECTS-BASED APPROACH

Fundamental to the Air Force's success in the next century is its ability to focus on the effects desired to achieve campaign objectives, whether at the strategic, operational, or tactical levels. This holds as true for IO as for any other air and space capability. Generally, the intent behind a particular mission or action de-

termines its level of application rather than specifying the use of particular weapons or platforms. Planners should clearly define the desired effect, then identify the optimum capability for achieving that effect. The following sections provide examples of the types of effects IO can achieve.

Strategic Effects

Some information operations, particularly some OCI operations at the strategic level of war, will be directed by the National Command Authorities and planned in coordination with other agencies or organizations outside the Department of Defense. *Such operations should be coordinated among supporting Air Force units, the combatant commander IO team or cell, and other supporting components, if present, to ensure unity of effort and prevent conflict with possible ongoing operational-level operations.* However, due to the sensitivity of such operations, they may not always be coordinated with other units, but rather deconflicted at the highest level possible to ensure fully integrated, successful operations. *Nevertheless, information operations may also be conducted at the strategic level of war as part of normal theater operations.* Specific effects IO can achieve at this level are:

- Influence both friendly and adversarial behavior conducive toward achieving national objectives through the promotion of durable relationships and partnerships with friendly nations.
- Terminate adversary leadership resistance against US national objectives by affecting willpower, resolve, or confidence. Create a lack of confidence in an adversary's military, diplomatic, or economic ability to achieve its goals or defeat US goals. Incapacitate an adversary's ability to lead due to lack of communication with its forces or understanding of the operating environment.
- Deter aggression, support counterproliferation of weapons of mass destruction, and support counterterrorism.

Operational Effects

IO at the operational level of war can be conducted by a combatant commander within the assigned area of responsibility or joint operation area and by the COMAFFOR. IO at this level can also be conducted across the range of military operations. *IO at this level will involve the use of military assets and capabilities to achieve operational effects*

through the design, organization, integration, and conduct of campaigns and major operations. Specific effects IO can achieve at this level through IW are:

- Negate an adversary's ability to strike. Incapacitate its information-intensive systems. Create confusion about the operational environment.
- Slow or cease an adversary's operational tempo. Cause hesitation, confusion, and misdirection.
- Negate an adversary's command, control, communications, computers, and intelligence capability while easing the task of the war-to-peace transition. Using nonlethal IW techniques instead of physical attack preserves the physical integrity of the target leaving it for use later if needed or prevents great cost later to reconstruct it during the war-to-peace transition.
- Influence adversary and neutral perceptions away from adversary objectives and toward US objectives inducing surrender or desertion.
- Enhance US plans and operations by disrupting adversary plans.
- Disrupt the adversary commander's ability to focus combat power.
- Influence the adversary commander's estimate of the situation. By creating confusion and inaccuracy in the assumptions an adversary makes regarding the situation, the direction and outcome of military operations can be influenced.

Tactical Effects

Air Force or functional component commanders direct the execution of tactical-level IW. *The primary focus of IW at the tactical level of war is to deny, degrade, disrupt, or destroy an adversary's use of information and information systems relating to C2, intelligence, and other critical information-based processes directly related to conducting military operations.* Specific effects are:

- Deny, degrade, disrupt, or destroy adversary capabilities and information on friendly forces.
- Reduce the size or capability of adversary forces.
- Deny adversary knowledge of forces.

Information operations are fully integrated in the air operations center.

COUNTERINFORMATION PLANNING

The COMAFFOR maintains awareness of an adversary's information infrastructure, capabilities, and operations through an IW team within the air operations center (AOC). An Air Force IW team, a specialty team within the AOC, will be established during a crisis or conflict (including war) and work as an integral part of the AOC to help integrate Air Force IW activities into a joint air and space operations plan, air tasking order (ATO), and space tasking order. *The COMAFFOR's IW team's efforts are fully integrated with the Strategy, Combat Plans, Air Mobility, and Combat Operations Divisions in the AOC.* The team is composed of expert representatives from various IO organizations brought together to collect and disseminate information, to develop IW courses of action (COAs), and to assign tasks.

A typical IW team is comprised of permanent, principal, and temporary members. (See figure 4.1, page 31.) Permanent members have no other responsibilities in the AOC, are experienced in their position, and usually have specific training. Principal members are experts within their functional area, who are required for the IW team's mission and stay with the team, but have other AOC responsibilities. Temporary members contribute special expertise as the need arises. When the COMAFFOR has an

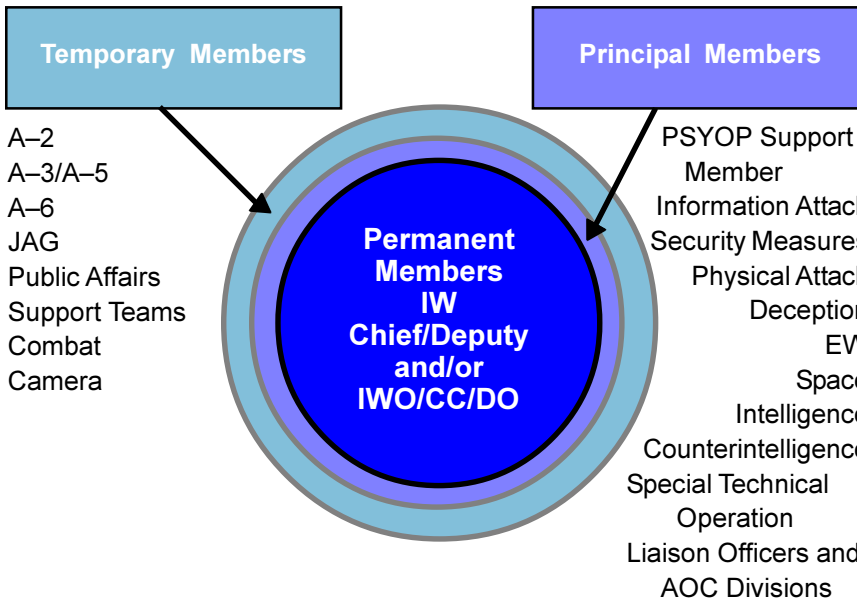


Figure 4.1. Typical Information Warfare Team

assigned, organic information warfare organization (IWO) available, the IWO performs the duties and responsibilities of core and resident IW team members. The core of the COMAFFOR IW team is normally comprised of the numbered air force IW office and special technical operations chief and deputy, or the IWO commander and director of operations when the COMAFFOR has an IWO available.

The IW team develops IW COAs based on COMAFFOR-assigned tasks from joint force commander (JFC) objectives. **The resulting plan should include both defensive and offensive aspects of counterinformation**. A successful counterinformation plan contributes to the security of friendly forces by bringing an adversary to battle on friendly forces' terms, seizing and maintaining the initiative, ensuring agility, contributing to surprise, isolating adversary forces from their leadership, and creating opportunities for a systematic exploitation of adversary vulnerabilities. *The key to successful information warfare is its integration throughout the planning, executing, and terminating phases of all joint and multinational operations.*

This requires coordination among all in-theater operations, including reachback capabilities. Through the JFACC, the COMAFFOR also ensures coordination among OCI and DCI actions both internally and externally

with other joint force IO organizations. COMAFFOR IW capabilities should be considered and integrated into the overall theater campaign, not just as an add-on but as a primary capability the Air Force brings to the conflict.

This normal coordination and integration process within a joint task force is highlighted below:

- The JFC develops theater campaign objectives and will normally designate a "joint force" IO officer to accomplish broad IW oversight functions. The joint force IO officer heads the JFC IO team or cell, when designated.
- The JFC IO team/cell (composed of select representatives from each staff element, Service component, and supporting agencies' augmentees responsible for integrating the capabilities and disciplines of IO) derives campaign IW objectives from JFC guidance. These IO team or cell objectives are broad and should not involve detailed execution. That is left to the components to accomplish. This process adheres to the Air Force tenet of centralized control and decentralized execution.
- Service components address campaign IW objectives and the effects required to achieve them. Primary and supporting components are designated.
- The COMAFFOR IW team/IWO takes Air Force component tasks, as determined by the JFC's objectives and commander's intent, for execution.
- The COMAFFOR IW team holds IW coordination meetings daily, or as required, to develop and coordinate COAs to present to the COMAFFOR for approval. The JFC IO team or cell may serve to deconflict Service component operations courses of action if required.
- If COMAFFOR COAs are approved, the COMAFFOR IW team or IWO integrates them into the ATO or tasking process by coordinating with the Combat Plans and Combat Operations Divisions in the AOC. If a COA is not approved, it is either terminated or shelved for future consideration.
- The COMAFFOR IW team/IWO must ensure rules of engagement and IW operating requirements and authorizations, such as special target lists, are taken into consideration. The team must coordinate IW-specific intelligence requests and requirements and stay in contact with the appropriate assets to resolve problems and coordinate requirements

and taskings. The IW team chief must ensure target deconfliction with the Combat Plans Division. For instance, if a particular node must be preserved for IW purposes, it must be placed on the restricted target list. The IW team or IWO coordinates use of Air Force IW assets with the Combat Plans Division's core teams for inclusion in the ATO.

Offense-Defense Integration

One of the most important lessons of military history is the need for a shrewd balance between offense and defense. **Accordingly, successful military operations must carefully integrate both OCI and DCI elements.** *A balanced approach, combining all the tools, disciplines, and capabilities of information warfare as needed and appropriate, will yield the best long-term effects.* Commanders must ensure their staffs carefully balance their planning processes in both OCI and DCI to avoid either an overemphasis on offensive capabilities or an electronic Maginot Line.

OCI and DCI must be deconflicted and priorities established. For example, information assurance efforts would prefer to sever a security breach into Air Force information systems quickly while counterintelligence may wish to allow continued access to identify and exploit the attacker or to conduct a deception operation. PSYOP may seek to reveal information that OPSEC normally would deny. Operational commanders are responsible for such decisions, under the guidance of higher-level campaign plans and, when appropriate, the National Command Authorities.

IW Targeting

IW planners recommend IW targets to support the theater campaign plan. Targeting begins with the commander's intent, a strategy-to-task methodology, and includes legal and political guidelines. Following these instructions, the targeting process relies on clearly delineated national, theater, and command objectives and the effects required to achieve

> ***One approach to interdiction is wrecking bridge spans using laser-guided bombs. Alternatively, we might be able to alter the adversary's planners' information, falsely categorizing the bridges as destroyed, causing [them] to reroute forces and supplies.***
>
> ***Cornerstones of Information Warfare***

them to devise a maximum payoff for each course of action. JFCs establish broad planning objectives and guidance for attack of an adversary's strategic and operational centers of gravity and defense of friendly strategic and operational centers of gravity as an integral part of joint campaigns and major operations. *The IW team evaluates information target systems, functional relationships, and friendly and adversary critical nodes and recommends appropriate offensive and defensive IW missions for inclusion in the ATO.* In the weapon selection and force application stage of targeting, target vulnerabilities are matched with weapons characteristics to produce IW strike package nominations.

The IW team, in coordination with the Combat Plans Division, integrates IW target nominations into attack plans and tasking orders. Using JFC guidance, apportionment, and the approved target list, the master air attack plan team provides details on the execution of this guidance using available air resources. The ATO-airspace control order production team converts the master air attack plan into the attack tasking in the ATO and the associated special instructions.

ORGANIZATIONS

Information Warfare Organizations

Today, the Air Force has a single Information Warfare Squadron (IWS) primarily focused on DCI operations that include activities to defend friendly information and information systems. In the future, the COMAFFOR's IW capabilities may come either in the form of an IWS or as a yet undetermined ad hoc or formal IWO. Regardless of what formal or informal organization provides the COMAFFOR with IW capabilities, future IWOs will bring similar capabilities to the fight. The following discussion highlights those capabilities.

The IWO ensures all the air component's key sensors, weapon systems, and dissemination systems are not degraded by an attack on critical information or information systems. IWO reactions to an attack to tactical systems include counterattack (by physical or technical means), containment, or feeding the attacker false information (for example, deception). Specific duties may include operational tactics, analysis, and maintenance of support DCI data bases, assisting in the recovery of attacked systems, performing in-theater security assessments, evaluating defensive capabilities, and identifying vulnerabilities by providing tactical warning and

attack assessment. An IWO can be the central collection agency for responding to incidents and recommending priorities for recovery. IWO DCI activities will be integrated with base-level Network Control Centers, Major Command Network Operations and Security Centers (NOSC), and the Air Force Information Warfare Center's (AFIWC) Air Force Computer Emergency Response Teams (AFCERTs) to provide a layered defense.

An IWO provides the COMAFFOR with real-time operational network intrusion detection and perimeter defense. This dedicated first-line of defense is employed at the COMAFFOR's direction to defend information networks both in-theater and in-garrison, complementing the general defenses provided by the base-level Network Control Center. Equipped with advanced systems, an IWO deploys automated equipment and augmentation forces in theater, as needed, to perform information operations.

Computer Emergency Response Teams

Each of the Services have formed Computer Emergency Response Teams (CERTs) for rapid response to their deployed Service forces and for use by some combatant commanders for similar response to subordinate joint forces within the combatant command area of responsibility or joint operating area. In addition, the Defense Information Systems Agency can deploy CERTs to areas of responsibility of joint operating areas in response to specific requests for this capability. Services and joint forces submit requests for CERTs through the normal chain of command for administrative and logistic support. Requests for CERTs from DISA should be submitted through the supported combatant commander. The AFCERT was established as the single point of contact in the Air Force for computer security incidents and vulnerabilities. The AFCERT coordinates the AFIWC's technical resources to assess, analyze, and provide countermeasures for computer security incidents and vulnerabilities reported Network Control Centers, IWS, and NOSC. The AFIWC will also assist in identifying foreign IW capabilities and intentions (for example, indications and warning).

Major commands also provide security measures (Network Operations and Security Centers) to protect data fusion, assessment, and decision support. Commanders must play an active role in the support and management of activities within their operational areas. To accomplish this, they also have systems and tools identical to those supporting the AFCERT. The major command's IW support personnel monitor and support the

day-to-day operational issues associated with their subordinate bases and units. Their mission focus is to ensure their command's operational and support systems are fully capable of meeting the objectives set forth in applicable mission statements, operation plans, and other pertinent requirements documents. As appropriate, they support their commanders with appropriate security measures, such as information security, decision analysis, and other technological capabilities.

CHAPTER FIVE

SUMMARY

Information superiority is central to the way wars are fought and is critical to Air Force and joint operations in the 21st century. **The Air Force, with its global perspective and experience, is uniquely qualified and positioned to play a leading role in developing and applying important new capabilities.**

There are two aspects of information operations that help achieve information superiority: IIW, the traditional collection and exploitation, and IW, the "attack and defend" aspects. This document has focused primarily on IW, but *IW must always be applied in operations that are fully coordinated with the IIW pillar and that are integrated into the wider aerospace operations plan.*

There is no question that information operations and the more specific construct of information warfare will evolve in the coming years and decades. Air Force members must apply this doctrine to current and planned systems. As we learn lessons in the real world, operators at every level and from every career field must provide solid inputs and guidance back into the doctrine process. The Air Force needs the help of every member as it grows, adapts, and improves the application of IO and IW to the art of war.

At the very Heart of Warfare lies Doctrine …

SUGGESTED READINGS

Alan D. Campen, *The First Information War: The Story of Computers and Intelligence Systems in the Persian Gulf War* (Air Force Communications Electronics Agency International Press). 1992.

Alan D. Campen, *Cyberwar: Security, Strategy and Conflict in the Information Age* (Air Force Communications Electronics Agency International Press). 1996

Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (Doubleday Press). 1989.

John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (RAND). 1997

Alvin and Heidi Toeffler, *Creating a New Civilization: The Politics of the Third Wave* (Turner Publishing, Inc.). 1995.

GLOSSARY

Abbreviations and Acronyms

AFCERT	Air Force Computer Emergency Response Team
AFDD	Air Force Doctrine Document
AFIWC	Air Force Information Warfare Center
AFSST	Air Force Space Support Team
AOC	air operations center
ATO	air tasking order
C2	command and control
CERT	computer emergency response team
CI	counterinformation
COA	course of action
COMAFFOR	commander, Air Force forces
DCA	defensive counterair
DCI	defensive counterinformation
DII	defense information infrastructure
EW	electronic warfare
GII	global information infrastructure
IIW	information-in-warfare
IO	information operations
ISR	intelligence, surveillance, and reconnaissance
IW	information warfare
IWO	information warfare organization
IWS	information warfare squadron
JFACC	joint force air component commander
JFC	joint force commander
NII	national information infrastructure
NOSC	Network Operations Security Centers
OCA	offensive counterair
OCI	offensive counterinformation
OPSEC	operations security
PNP	precision navigation and positioning
PSYOP	psychological operations
US	United States

Definitions

command and control—The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called **C2**. (Joint Pub 1–02)

counterinformation—Counterinformation seeks to establish a desired degree of control in information functions that permits friendly forces to operate at a given time or place without prohibitive interference by the opposing force. Also called **CI**.

deception—Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (Joint Pub 1–02)

defensive counterinformation—Activities which are conducted to protect and defend friendly information and information systems. Also called **DCI**.

electronic warfare—Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW**. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. **electronic attack**—That division of electronic warfare involving the use of electromagnetic or directed energy to attack personnel, facilities, or equipment with the intent of degrading, neutralizing or destroying enemy combat capability. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism to include: lasers, radio frequency (RF) weapons, and particle beams. b. **electronic protection**—That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called **EP**. c. **electronic warfare support**—That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, inter-

cept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called **ES**. Electronic warfare support data can be used to produce signals intelligence (SIGINT), both communications intelligence (COMINT), and electronics intelligence (ELINT). (Joint Pub 1–02)

information—1. Unprocessed data of every description which may be used in the production of intelligence. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (Joint Pub 1–02)

information assurance—Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DODD S–3600.1)

information attack—An activity taken to manipulate or destroy an adversary's information systems without visibly changing the physical entity within which it resides.

information-in-warfare—Involves the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on integrated intelligence, surveillance and reconnaissance (ISR) assets; its information collection/dissemination activities; and its global navigation and positioning, weather, and communications capabilities. Also called **IIW**

information operations—Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called **IO**. (DODD S–3600.1) The Air Force believes that in practice a more useful working definition is: *[Those actions taken to gain, exploit, defend or attack information and information systems and include both information-in-warfare and information warfare.]* {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

information superiority—The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or deny-

ing an adversary's ability to do the same. Also called **IS**. (DODD S–3600.1) The Air Force prefers to cast 'superiority' as a state of relative advantage, not a capability, and views IS as: *[That degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.]* {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

information systems—The means used to acquire, transform, store, or transmit information. (DODD S–3600.1)

information warfare—Information operations conducted during time of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called **IW**. (DODD S–3600.1) The Air Force believes that, because the defensive component of IW is always engaged, a better definition is: *[Information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information and information systems.]* {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

military deception—Actions executed 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 the friendly mission. (Joint Pub 1–02)

offensive counterinformation—Offensive IW activities which are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems. Also called **OCI**.

OODA Loop—A theory developed by Col. John Boyd (USAF, Ret.) contending that one can depict all rational human behavior, individual and organizational, as a continual cycling through four distinct tasks: observation, orientation, decision, and action.

operations security—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vul-

nerabilities of friendly actions to adversary exploitation. Also called **OPSEC**. (Joint Pub 1–02)

physical attack—The means to disrupt, damage, or destroy information systems through the conversion of stored energy into destructive power.

psychological operations—Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called **PSYOP**. (Joint Pub 1–02)

security measures—The means to protect and defend information and information systems. Security measures include operations security and information assurance.

storage—Maintaining information for later retrieval and access by the user. Access to the stored data may be via remote or local means. This access may be by user retrieval or provided automatically by the storage system. Various media exist to store information including magnetic disk, laser optical disk, magnetic tapes, etc.

transmission—Disseminating information to the user through a variety of media such as fiber-optic, voice, radiowave, cable, or other segments of the electromagnetic spectrum.

You are the United States Air Force

At the Heart of Warfare lies Doctrine