READING 23

Information Warfare

"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 of the Air Force
5 August 1998

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 is 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 changes 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, including both IIW and IW, 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 superiority with the other facets of aerospace power must become a major focus of the Air Force's operational art.

Current 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 nongovernmental 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 Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrin*e, 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 speed 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.

Current Threats

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.

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. IW threats fall into four categories*: compromise, deception/corruption, denial/loss, and physical destruction.* Each poses an inherent risk to both stand-alone 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 reach-back 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 command.
- 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.

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.

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 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. 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 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.

Protecting friendly systems while countering adversary systems gain control of the electromagnetic spectrum. **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 objective*s*. When EW actions are integrated with military operations, rather than just added on, synergy is achieved, attrition is minimized, and effectiveness is enhanced.

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 accordingl*y*. *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 activitie*s. 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 (C2). Two tactical-level examples are using precision-guided munitions against a C2 communications relay station, and inserting a special operations team to cut and/or exploit communication lines.

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

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. Accordingly, 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.

<u>OPSEC is a process</u>. 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.

<u>Information assurance</u> 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. 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 counterpsychological 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.

Conclusion

Information superiority is central to the way wars are fought, and is critical to Air Force and joint operations in the 21st century. As Air Force officers with a vision of global vigilance and experience, you will be uniquely qualified and positioned to play a leading role in developing and applying important new capabilities in the area of information warfare.

Bibliography:
Air Force Doctrine Document (AFDD) 2-5, *Information Operations,* 5 August 1998.