

# Air Force IO Basics Course

For your convenience, transcripts of the narration for each lesson on this CD are accessible through the links below.

**Course Introduction**

**DESERT STORM Introduction**

**Deception**

**Defensive Counterinformation (DCI)**

**Electronic Warfare**

**Information Attack**

**Information-in-Warfare**

**Legal/Ethical Issues**

**Operationalizing IO**

**Physical Attack**

**Psychological Operations (PSYOP)**

**Public Affairs (PA)**

**Course Summary**

## Air Force Information Operations Basics Course Introduction

[intro.htm](#)

Welcome to the Air Force Information Operations Basics Course. Our service vision statement identifies six core competencies of the Air Force. Information superiority is the ability to control and exploit information to our nation's advantage and ensures we have decision dominance over our enemies. One of the ways we achieve information superiority is by conducting information operations. The two pillars of information operations are information-in-warfare, whereby we gain and exploit information, and information warfare, which concerns the defense and attack of information and information systems. Information warfare consists of the function of counterinformation, which has two subsets: defensive counterinformation and offensive counterinformation. These major blocks have many supporting elements. If you are feeling overwhelmed at this point, don't be. This course will help you understand these concepts and make sense of them. You'll gain an appreciation of how information operations contribute to aerospace power as well as the impact the media and national and international law has on information operations.

## Desert Storm Introduction Lesson

### [ds1.htm](#)

We'll begin the course, by looking at what some have called the first information war. Coalition successes in Desert Storm happened in large part due to US domination of the information arena. The next few screens will briefly illustrate some of the information operations conducted during Desert Shield and Desert Storm. Can you pick out what they are? Can you identify the doctrinally correct terminology for each? Some of these operations occurred before coalition troops engaged in combat. Some influenced strategic objectives, while others had tactical-level effects. As you'll see, information operations cover the spectrum of conflict and happen at all operational levels. Not all of the elements of information operations will be covered in this brief presentation but, hopefully, you'll come to appreciate that information operations play an important role in modern warfare.

### [ds2.htm](#)

August 2<sup>nd</sup>, 1990. Iraqi forces invade Kuwait. Key members of the Kuwaiti government barely escape as invading forces overwhelm Kuwaiti resistance. The international community condemns the aggression immediately. With Iraqi forces massing on its border, Saudi Arabia requests US forces for its defense. On August 7th, President Bush announces the deployment of the 82<sup>nd</sup> Airborne division and fighter aircraft to defend Saudi Arabia. Bush declares, "A line has been drawn in the sand."

### ds3.htm

Following the invasion, reports of Iraqi atrocities quickly filtered out of Kuwait. Rape, torture, and summary executions are reported, all in violation of the Geneva Conventions for Protection of War Victims. The plunder of Kuwaiti wealth even included reports of babies being removed from their incubators, which were being shipped to Iraq. On August 19<sup>th</sup>, Saddam Hussein announced that up to 10,000 Westerners would be housed at strategic sites as human shields to deter attacks.

### ds4.htm

Diplomatic action quickly formed a coalition committed to not only condemning but acting against the Iraqi aggression. A maritime interception force supported with ships and facilities from 22 nations enforced UN embargo sanctions. By October 1990, Egypt, Syria, France, and Britain had joined with US, Saudi, and Kuwaiti troops on the Saudi-Kuwait border. On November 8<sup>th</sup>, President Bush announced further deployments, including the famous First Infantry Division and the European based Seventh Corp, to provide an offensive option. Over 30 nations joined the coalition, adding forces, basing, and overflight support, as well as money. On January 12<sup>th</sup>, three days before the deadline imposed by UN Resolution 678, the US Congress passed a resolution supporting the use of military force.

storm1.htm

To the Iraqis, it all looked quite normal. The coalition was night flying, like they had for the past several weeks.

January 17th. Twenty minutes before H-hour, Army Apache helicopters, led by Air Force Pave Low 3 helicopters, open a hole in the Iraqi early warning radar line. Ten minutes later, F-117s attack the Intercept Operations Center at Nukhayb. Having blinded and confused the Iraqis, conventional strike packages flow through the hole to hit Scud launchers and airfields while fighter escorts pick off the few Iraqi fighters launched in resistance.

Meanwhile, it's H-hour in Baghdad. Within the next 20 minutes, F-117s and over 50 Tomahawk land attack missiles strike the AT&T building, the air force headquarters, the air defense operations center, the presidential palace, the Tallil Sector Operations Center, the Salman Pak intercept operations center, and Baghdad's electricity distribution grid.

Baghdad defenses frantically searched the skies for the attacking armada. A two-pronged coalition SEAD attack obliged by orbiting massive numbers of decoys and drones over Baghdad while jamming aircraft cloaked the HARM shooters that engaged the radars. The SEAD raid was immediately followed by a second wave of F-117 strikes against the command and control centers. At the same time, B-52s and British Tornados hit forward operating bases along the Kuwaiti frontier. Dawn brought no relief with B-52 air launched cruise missiles pounding Baghdad, A-10s beating up the early warning radar sites, and SEAD packages supporting strikes on airfields and petroleum production. The "mother of all battles" had begun.

storm2.htm

Unable to defend his own skies, Saddam attacked with Scud missiles. Scuds were launched against Israel from sites in western Iraq, and against Saudi Arabia from launch points in southern Iraq. Having no effectiveness as a military weapon, Saddam's goal was entirely psychological. He hoped to provoke an Israeli attack on him, reasoning the Arab coalition partners would not stand against him in de facto partnership with the Jewish state.

To quell the Israeli outcry, the US sent Patriot missile batteries, provided early warning notification of Scud launches, and shifted a large amount of resources to hunting mobile Scud launchers. These resources included scarce F-15E sorties and reconnaissance assets.

The military effectiveness of the Great Scud Hunt is questionable. Even the Gulf War Airpower Survey conducted after Desert Storm, admits there were no confirmed kills of mobile Scud launchers by airpower. The military effectiveness of the Patriots is even arguable given that Scud, as well as Patriot, pieces and parts fell to Earth as indiscriminately aimed as the Scud itself. And yet, these efforts were effective. The Israelis stayed out of the fight and the coalition stayed intact. The presence of Patriots consoled the Israeli and Saudi people. The diversion of resources convinced the Israelis that all possible military measures were being taken, making their involvement unwarranted.

Given that the rate of Scud launches was greatly reduced after the first week, there is some indication the great scud hunt did disrupt the Iraqi operation. In any event, it was people's perceptions that was the real target of both the Scud attacks and the Scud hunt.

storm3.htm

**Pilot:** Hey Joe. What've you got there?

**WSO:** Mom just sent me one of those new GPS receivers.

**Pilot:** Hey, I hear those things are really great.

**WSO:** Yea. The mail room guy said to guard it with my life and not let any tank drivers know I got it. I figure it should help a lot keeping us in our kill box. It's for sure we've got no visuals out there.

**Pilot:** Tell me about it.

**WSO:** Could you go and get the datalink freqs for today. I'm a bit bogged down here since the weather guessers changed our dump targets.

**Pilot:** Sure thing Joe. Think you'll have everything ready to brief in twenty minutes?

**WSO:** I think so.

storm4.htm

**Voice1:** Sarge, do you really think the Iraqis are going to believe the corps is still here?

**Voice2:** Why shouldn't they? They keep tabs on us largely by monitoring our radio transmissions. Our job here is to play these tapes of normal radio traffic so they don't even suspect we moved. Rumor has it, the Air force conveniently missed the listening posts that monitor us when they were bombing everybody else.

**Voice1:** Yea, but what if someone comes looking. I know they left a lot of stuff set up when the corps left but let's face it Sarge, a corps is huge.

**Voice2:** Who's gonna come looking? Their air force hasn't launched a sortie in 2 weeks, except to run to Iran. The counter-recon guys are operating like a corps was here just to make sure nobody gets a peek. And if they do get close, well...think about it from an Iraqi's point of view. How close are YOU going to get? The loudspeakers are playing camp noises and guys are driving stuff around all the time to keep the dust kicked up. Wouldn't seeing the dust clouds on the horizon and hearing the noises be enough for you?

**Voice1:** Well, maybe.

**Voice2:** And if they were REEEAL dedicated and pressed in, what are they are gonna see? Just what they wanted to see, that's what. There's a lot of REAL stuff setting around—all of the non-mission capable gear got left behind. And the fancy decoys they set up are powered so they look good even in night vision goggles. Enough vehicles are moving around all of the time that it would take a real smart patrol a long time to figure that something's not right. I think if I was Abdul, I'd take my peek and run back to my commander and say "Yes sir, I saw 'em with my own eyes."

[storm5.htm](#)

**Voice1:** Gunny, do you think we'll have to hit the beach for real?

**Voice2:** That's what we've been training to do.

**Voice1:** Yea, I know, and it seems the whole world knows it too. Mom sent me a Newsweek article with our whole plan in it, and she says the newspapers have been covering all of our exercises.

**Voice2:** Oh, you can bet the Iraqis know we're out here. You can hear the battleships blasting the coast. We've already raided a few of the islands and oil

platforms. The minesweepers and seal teams have been clearing approach lanes. And here, let me show you this. These are being put into bottles and floated up onto the beaches. And that's just how it's gonna be - we're gonna hit 'em like a tidal wave.

**Voice1:** I sure hope so Gunny.

#### storm6.htm

Messages in bottles weren't the only means used to demoralize Iraqi troops. Beginning in early February, over 29 million leaflets were dropped in the Kuwaiti theater of operations. While many leaflets encouraged desertion and promised humane treatment for surrendering, others targeted specific units warning of impending bombing. The bombings almost always happened as promised and follow-up leaflets warned that further attacks could occur at any time.

The B-52, known to be especially terrifying from operations during Vietnam, was used throughout the theater. The BLU-82 Daisy Cutter, a fuel-air mixture bomb, was used against front-line troops to clear mine fields in preparation for the ground offensive but was also expected to have a significant negative effect on the morale of the entrenched Iraqi soldier. Desertions became epidemic to the point that Baghdad sent assassination battalions into Kuwait to inspire loyalty amongst the troops.

storm7.htm

In the early morning darkness, the First cavalry division and First Marine Expeditionary Force breached the defenses of fortress Kuwait while far to the west, units of the eighteenth airborne corps drove north into Iraq itself. First Cavalry's action was along the Wadi Al-Batin, a dry riverbed forming the western border between Kuwait and Iraq. The Iraqis had heavily fortified the area, expecting the main attack along this historic invasion route. But First Cavalry's actions were only a feint, intending to keep Iraqi defenders frozen in place. Meanwhile, the First MEF was joined by attacks from allied forces on both its left and right several hours later. But the main threat, as yet unrecognized by the Iraqis, was happening in the West. The 18th Airborne Corps was driving north to secure what would become the western and northern flank of the 7th Corp. Both the 18th airborne and 7th corps had been aligned to attack up the Wadi, but under the cover of the air campaign had repositioned far to the west to skirt the main defenses on the Kuwaiti border. This set them up to execute a classic envelopment that would be known as the "Left Hook."

Successes for the first day were so phenomenal that General Schwarzkopf called an audible and ordered 7th corps to begin its drive late that first afternoon instead of waiting until the next morning. This map shows the progress of the ground forces at the end of the first day.

storm8.htm

The predawn hours of the second day of the ground war saw major feints by amphibious forces along the Kuwaiti coast. This kept the Iraqis deployed along the coast from participating in any counterattacks against inland forces. Indeed, the Iraqis attempted to mount a major counterattack against units of the 1st MEF but airpower ripped the Iraqi columns and enabled maneuver advantages by the Marine forces. The Iraqi counterattack soon fizzled. Meanwhile in the west, the 18th airborne corps secured Hiway 8, which represented either a major avenue for reinforcements or an escape route to and from the Baghdad area. With this threat eliminated, the 7th Corps charged north. With the collapse of his counterattack, Saddam Hussein ordered a general withdrawal from Kuwait. Without control of the skies, this proved difficult. The hiway from Kuwait City to Basra came to be known as the "Hiway of Death."

storm9.htm

After two days of battle, the ground forces were in a position to deliver the knock-out punch. In Kuwait, the Marines seized the escape routes from Al Jahra and Kuwait City while Arab-led coalition forces liberated the city itself. In the west, the 7th corps completed its turn to the east. In concert with the 18th airborne corps, they thrust themselves into the flank of the elite Republican Guard.

Many Iraqi units were caught trying to assume new blocking positions to cover the retreat from Kuwait. The speed of the coalition advance was so rapid they were attacked before they were prepared to offer an effective defense. While pockets of stiff resistance were encountered, the lack of a coordinated defense led to the piecemeal destruction of 4 of the 5 Republican Guard divisions. Airpower had dropped most of the bridges crossing the Tigris and Euphrates, greatly impeding the Iraqi retreat. Were it not for exceptionally bad weather, the Hiway of Death might have extended to the Basra city limits.

With the Iraqis expelled from Kuwait and in full retreat, and with the press beginning to characterize the military operation as a massacre, President Bush called for a cease-fire. Capping an extensive air campaign, the ground forces brought the Mother of all Battles to an end in 100 hours.

[cnstrct.htm](#)

History is replete with examples showing a high correlation between information superiority and victory. The Gulf War was no exception.

Information is the lifeblood of the decision cycle. The OODA loop was conceived as a model of that cycle. It consists of 4 phases, Observe, Orient, Decide, and Act. The observation phase collects raw data from sensors about an event. The orientation phase develops a context for the observations and extracts meaning from them. Given this interpretation of reality, decisions are made as to what if anything should be done regarding the event. The action phase executes those decisions.

Looking at the Information Operations construct, the pillar of Information-in-warfare or IIW, largely concerns itself with the observation and orientation phases but also acts as a force multiplier during the action phase through support for the warfighter. IIW's goal is to present a high fidelity representation of reality to the decision-maker thereby increasing the effectiveness of decisions.

Technology has a major impact on IIW. With the doubling of computing power every 12-18 months since the late 1960s, the demand for information has skyrocketed. This demand breeds a dependency that creates a vulnerability. Defensive counter-information mitigates the vulnerability by maintaining the integrity of our decision cycle. It prevents or removes the introduction of false information into the cycle and protects the infrastructure that binds the process together.

Offensive counterinformation recognizes that the enemy also has a decision cycle and attempts to adversely affect it. By introducing false inputs or attacking his information infrastructure we hope to decrease the effectiveness of his decisions and/or increase his time to act.

While the components of information operations have been recognized and practiced by militaries across the centuries, the recent advances in information technology have put information operations on a footing equal to the occupation of territory or even control of the skies.

[roadmap.htm](#)

You're now invited to explore information operations or IO in greater depth. Air Force Doctrine Document 2-5 defines information operations as "Those actions taken to gain, exploit, defend or attack information and information systems and include both information-in-warfare and information warfare."

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 assets; its information collection and dissemination activities; and its global navigation and positioning, weather, and communications capabilities. An entire lesson is dedicated to exploring these activities in more detail.

The other pillar of IO is information warfare, or IW, which AFDD 2-5 defines as those information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information and information systems. These actions fall into the realm of counterinformation which 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.

Defensive counterinformation, or DCI, are activities which are conducted to protect and defend friendly information and information systems. A lesson further describes these activities.

On the attack side of IW, offensive counter-information or OCI activities are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems. There's a lesson available for each of the five elements of OCI.

Because ours is a nation of freedom loving people, it's hardly surprising that information operations are well-regulated by law. Our look at IO includes a lesson on the laws and regulations that pertain to the conduct of IO. Another aspect of our national freedom is the military's relationship with the media. We devote a lesson to looking at the role of public affairs and how a balance is maintained in the tension between a free press and a military trying to practice the principle of war called security. Once you've gotten the fundamentals down, you're invited to look at how the military currently organizes itself to conduct IO. The course finale will try to tie everything together and give you a chance to check your mastery of the material. Yes, that's Orwellian doublespeak for "There is a test."

The next page is a copy of this one without all of the narration and we suggest you either bookmark it or add it as a favorite in your browser for easy access to the rest of the course. If you have cookies enabled, your CD will now autostart to that page. We hope you enjoy the rest of the course.

## Deception

[intro.htm](#)

Since ancient times, deception has been an important tool for military success . The focus of deception operations, like other elements of information warfare, is on altering the enemy's behavior. The goal of deception is to mislead an adversary, causing him to act or fail to act in a way that furthers the objectives of the originator. To accomplish this goal, deception requires a thorough understanding of the enemy, his decision-making process, and his preconceptions and biases that planners can exploit.

In the Gulf War, strategists were aware that Saddam's army was accustomed to massive head-on assaults. They encouraged Iraqi expectations by amassing troops along the Kuwaiti-Saudi border where the Iraqis were most concentrated. Once air power had neutralized the Iraqi air force, it was no longer possible for the Iraqis to observe the disposition of U.S. and coalition forces. This allowed the massive troop movements westward, which were further concealed by the decoy bases these forces left behind. Iraqi troops were kept in place along the southern Kuwaiti border by ground attacks and along the eastern shoreline by offshore artillery, feints, and the threat of attack from a large amphibious force. Large-scale amphibious rehearsals, well-publicized by the media, and threatening PSYOP leaflets had convinced the Iraqis to prepare for an amphibious assault. When enemy strategists finally realized the major assault was coming from the west, hundreds of thousands of Iraqi troops were already hopelessly ensnared.

### [obj.htm](#)

The objective of this lesson is for you to comprehend military deception and how it is employed in information warfare. At the end of this lesson you will be able to define deception in the context of information warfare. You will be also able to explain the functions and goals of military deception and explain the categories of deception operations. Finally, you will be able to explain how deception operations have been employed in past military operations.

### [ovrvw.htm](#)

The lesson opens by presenting the definition of deception and follows with an explanation of its functions and goals. The lesson will then present the categories of deception. Finally, the lesson will present some historical examples of deception throughout military history.

### [def.htm](#)

This is the definition of military deception as presented in AFDD 2-5, Information Operations. The focus of deception is on misleading enemy decision makers, causing them to take specific actions or inactions that are advantageous to friendly forces. Deception can distract from, or provide cover for military operations, confusing and dissipating adversary forces. In essence, the primary objective of deception operations is perception management.

## fun.htm

As a perception management tool, military deception attempts to construct an alternate reality upon which the adversary will base his decisions. Deception concentrates on affecting an enemy's decisions and subsequent actions by influencing the observe and orient phases of the OODA Loop. This alternate reality is supported by creating observations of what you want the enemy to see, using camouflage and decoys or, in some cases, real troops and weaponry. With sensory information in place, deception should then focus on an enemy's biases, prejudices, and preconceptions, which are inherent in the orient phase and affect the decision making process. Other IO functions, such as intelligence, can provide key information about the enemy on which to base deception plans.

## plan.htm

Just like PSYOP campaigns, an effective deception plan must be considered early in the planning process and be well coordinated and integrated into the overall campaign plan. Here are some basic maxims planners should consider when developing deception strategies:

First, remember that it is often easier to reinforce a perception than it is to change one. If an adversary is convinced of your intent, it is often better to use that perception to your advantage than to try to convince him to believe something else. Deception strategies that are clear, unambiguous, and contain a grain of truth are easier for the enemy to accept and are easier to protect and maintain.

To avoid overloading the adversary's information systems, deception events should be appropriately sequenced and presented through a variety of media. Remember to coordinate your deception plan with other organizations conducting information operations to ensure that the appropriate information channels are available to present your deception. Planners should develop contingency plans in case problems arise. These plans should address questions, such as "What if the adversary finds out about the deception? And, "Can the overall objective be accomplished without the deception operation?" In addition, planners should strive to protect and maintain the deception plan throughout the course of the operations it supports.

[cat.htm](#)

Joint Pub 3-58 identifies the following four major categories of military deception:

Strategic deception consists of activities planned and executed by and in support of senior military commanders' strategic military objectives, policies, and operations.

At the operational level, military deception consists of activities planned and executed in support of operational-level commanders' objectives. Such operations are planned and conducted in a theater of war to support campaigns and major operations.

Tactical deception consists of operations planned and executed by and in support of tactical commanders' objectives and operations. Tactical military deception is planned and conducted to support battles and engagements.

And finally, Service military deception consists of activities planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems.

[yk.htm](#)

In the Yom Kippur War of October 1973, the Egyptian 3rd army surprised the Israeli Defense Force by attacking across the Suez Canal. Egyptian forces achieved this surprise by conducting strategic, operational, and tactical deception operations.

At the strategic level, the Egyptians conveyed the notion that they would not attack without the support of other Arab nations and that their tactical preparations were merely a precaution against possible Israeli retaliation for Arab terrorist activities.

At the operational level, Egyptian forces repeated exercises portraying an intent to cross the canal until Israelis became complacent and no longer reacted to the threat.

At the tactical level, Egyptian forces camouflaged their equipment from Israeli observers to maintain the impression that this activity was only an exercise.

Though Israeli observers reported the troop buildup and activity, the deception was successful and no action was taken. The Egyptian surprise attack, timed to occur on

Yom Kippur, the Jewish Day of Atonement, overwhelmed the Israelis, though the attackers were eventually driven back by a determined defense and counterattack.

[examp.htm](#)

Here are a few examples of deception throughout military history. Click on a link to view a description.

[sum.htm](#)

In this lesson you were introduced to military deception and its role in information warfare. The lesson opened by presenting the definition of military deception according to AFDD 2-5 and continued by discussing the functions and goals of these operations. The lesson then focused on some of the maxims planners should consider when planning deception operations. Next was a presentation of the categories of deception. Finally, the lesson ended by looking at some historical examples of deception.

Remember, deception operations are designed to influence the perceptions of the enemy and exploit his biases and preconceptions. By infecting the observe and orient phases of the enemy OODA loop, his decision-making process can be manipulated, resulting in actions or inactions that support the objectives of friendly forces. Deception can be employed effectively throughout the range of military operations and should be tightly integrated with other operations. Decision makers at all levels should be prepared to protect against deception operations conducted against the U.S. and its allies.

[quiz1.htm](#)

Here are a few questions to test your knowledge of the previous lesson material.

These questions are for your self-assessment only and are not recorded.

## **Defensive Counterinformation (DCI)**

### [intro.htm](#)

Military reliance on timely and accurate information makes information systems key targets for enemy attack. Therefore, the military must be proactive in its efforts to protect and defend against possible attacks. Defensive counterinformation, or DCI, includes those activities that protect information, information systems, and information operations that support military operations from any potential adversary. DCI when combined with OCI, provides enhanced opportunities for IW to contribute to the achievement of stated military and national objectives.

### [obj.htm](#)

The objective of this lesson is for you to comprehend the defensive counterinformation challenges that the Air Force faces in its efforts to protect its sources of information. The material will enable you to explain why it is important to protect information and information systems. It will further enable you to describe the methods used to protect Air Force information and information systems.

### [ovrvw.htm](#)

The lesson opens by describing OPSEC and information assurance as the primary security measures used to protect and defend Air Force information and information systems. The lesson then presents the remaining DCI functions of electronic protection, counterintelligence, counterPSYOP, and counterdeception.

opsec\_d.htm

AFDD 2-5 defines OPSEC as the process of identifying critical information and subsequently analyzing the friendly actions that accompany military operations. OPSEC activities attempt to identify those actions that can be observed by adversary intelligence systems and to determine indicators that adversary intelligence systems might be able to use to derive critical information. OPSEC activities also select and execute measures that eliminate or reduce the vulnerabilities of friendly actions.

[op\\_terms.htm](#)

OPSEC's most important characteristic is that it is a sequential process. It is not a one-size-fits-all collection of rules and instructions. What applies at a base in the continental United States does not necessarily apply to a base overseas. OPSEC is a methodology that can be applied case-by-case to any operation or activity for the purpose of denying critical information to an adversary. To understand the OPSEC process, you must know three terms which the process refers to: critical information, indicators, and vulnerabilities.

Critical information refers to specific facts about friendly intentions, capabilities, and activities that an adversary can use to negatively affect friendly mission accomplishment. Indicators are those actions and open-sources of information that an adversary can interpret or piece together to derive critical information. Joint Pub 3-54, Appendix C, lists those activities that could possibly serve as indicators. A vulnerability is a condition where friendly actions provide indicators that an adversary can actually use as a basis for timely and effective decision making. Let's take a closer look at the OPSEC process.

[steps.htm](#)

The first step of the 5-step OPSEC process is to identify what is critical information. OPSEC planners address questions the adversary might ask about friendly intentions, capabilities, and activities. Answers to these questions represent the essential elements of friendly information. Critical information is a subset of the essential elements of friendly information. The OPSEC process focuses on protecting vital information—that information that could actually be used to hurt us—rather than attempting to protect all classified or sensitive information. Appendix A of Joint Pub 3-54 lists some examples of what might be critical information.

Step 2, analyze the threat, involves researching and analyzing intelligence information, counterintelligence reports, and open sources of information to identify who the likely adversaries are to the planned operation. Who has the capability and intent to interfere with your operation? How might they do it? What do they already know? And, most importantly, what is their capability to collect critical information they don't already have. This leads us to step 3.

Analyze your vulnerabilities. You'll recall, a vulnerability exists when friendly operations produce indicators that the adversary can actually collect, analyze, and use in a timely fashion to disrupt your operation. So, what indicators does your operation provide? Can the enemy actually collect it? Can he use the information revealed by the indicator quickly enough to interfere with your operation? If so, you've identified a vulnerability.

Risk assessment has two components. First, is to define possible OPSEC measures to mitigate the identified vulnerabilities. Unfortunately, OPSEC measures usually entail some cost in time, resources, personnel or interference with normal operations. The second component of risk management is deciding if that cost is too high. If the cost to mission effectiveness exceeds the harm that an adversary could inflict, then the application of the measure may be inappropriate.

In the final step, you implement the selected OPSEC measures. In the case of planned future operations and activities, the measures are included in specific OPSEC plans. During the execution of OPSEC measures, monitor the reaction of adversaries to the measures to determine their effectiveness and to get feedback to adjust ongoing activities and to plan for future OPSEC activities. That completes the OPSEC process. You may review the notes of any step by placing your cursor over it in the diagram.

op\_oci.htm

Often the best defense is a good offense. OPSEC activities should be integrated with OCI activities. Recall the deception activities that were used to cover the repositioning of the 7th and 18th Airborne Corps during Desert Storm. One of the major indicators of a unit's position is its radio traffic, which provides a bearing to radio direction-finding equipment. The Iraqis were known to collect this indicator. When the Corps were moved, units were left behind to simulate normal radio traffic so this indicator didn't change. Dummy camps were set up and counter-recon patrols intensified to make sure the Iraqis didn't collect any indicators to disabuse them of the notion that they knew where the Corps were. Maintaining these measures was expensive in terms of manpower and equipment, but the payoff was worth it. In similar fashion, physical attack on enemy collectors is OPSEC pure and simple. An F-15's radar cross section is NOT a vulnerability if the enemy has no radars to collect it. The jamming aircraft that escorted the conventional strike packages were using electronic warfare to implement OPSEC. If you ever had the notion that OPSEC was a set of passive measures, strike that from your mind.

[ia.htm](#)

Information assurance is the second security measure used to protect our information and information systems. AFDD 2-5 defines information assurance as those measures taken to protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation. Availability means the information and systems are available when needed. Integrity means the information is free of unauthorized or accidental changes. Authenticity refers to the ability to confirm the source of information. Confidentiality ensures that only those with proper clearance and need-to-know have access to our information and systems. Non-repudiation refers to the methods that prevent the denial of participation of both sender and receiver in an information transaction. Two major efforts to achieve information assurance are communications security or COMSEC, and computer security or COMPUSEC.

### [comsec.htm](#)

COMSEC consists of measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such communications. Communications security includes cryptosecurity, which provides technically sound cryptosystems and procedures for their proper use. Emissions security denies unauthorized persons information of value that might be derived from the intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. Transmission security protects transmissions from interception and exploitation by an adversary. Physical security consists of measures taken to safeguard classified equipment, material, and documents from access or exploitation.

### [compusec.htm](#)

Computer security or COMPUSEC, involves the measures and controls taken to ensure confidentiality, integrity, and availability of information processed and stored by a computer. This includes the policies, procedures, hardware, and software that many of you use every day to protect your computer and its information.

### [ep.htm](#)

As a component of DCI, electronic protection is that division of electronic warfare which involves actions taken to protect personnel, facilities, and equipment from the effects of electronic warfare actions. Electronic protection complements the

electronic attack methods of chaff, flares, and self-protection jamming pods with emission control, electromagnetic hardening, and frequency deconfliction.

[ep\\_ex.htm](#)

Emission control consists of using electromagnetic, acoustic, and other emitters to optimize command and control capabilities while minimizing detection by enemy sensors. This can involve low-tech methods like signal mirrors or high-tech spread spectrum radios that are jam resistant and have a low probability of detection. Soviet interceptor tactics called for ground controlled intercepts and attacks with IR missiles so the interceptor made no transmissions with its radio or radar, to give away its position. Electromagnetic hardening consists of actions taken to protect personnel, facilities, and/or equipment against the undesirable effects of electromagnetic energy. Here, an airborne command post is tested against electromagnetic pulse effects produced by nuclear explosions. Of course people can use some hardening too. These goggles filtered the flash of a nuclear blast to prevent blindness. Similar ideas are now being developed to protect people and satellite sensors from the effects of lasers. And finally, you don't want to jam yourself. Frequency deconfliction is a systems management procedure that coordinates the use of the electromagnetic spectrum for operations, communications, and intelligence functions. The joint restricted frequency list divvies up the spectrum so everyone can coexist.

## [ci.htm](#)

Counterintelligence protects information systems and resources from illegal clandestine acts by foreign intelligence services, terrorist groups, and other elements. Counterintelligence threat estimates and vulnerability assessments are major inputs to other DCI initiatives like the threat assessment portion of the OPSEC process. It is vitally important to know how the enemy is getting their information about us. During the late 1960s and continuing into the 1980s, the Soviets seemed to have an unusual foreknowledge of US naval exercises. In 1985 the Walker espionage ring was exposed, and we discovered that the Soviets had been given naval cipher materials.

## [cpsyop.htm](#)

The military engages in defensive actions called counterPSYOP to ensure that friendly forces and populations are not influenced by enemy PSYOP efforts. One method of countering hostile PSYOP is to utilize the services of the Public Affairs office, which can provide timely and accurate information to establish credibility and defend against enemy PSYOP. Combat Camera allows the military to record what is really happening on the battlefield. Additionally, military information dissemination programs can be used to communicate accurate information to friendly troops. While these measures may minimize the intended effects of the adversary's messages, offensive activities, such as the disruption of enemy broadcast capabilities, can be effective in destroying the enemy's capability to conduct hostile operations.

## cd1.htm

Friendly forces must also be aware of enemy efforts to deceive and mislead us in order to advance their objectives. Counterdeception techniques are meant to address this concern. According to AFDD 2-5, counterdeception consists of the effort to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Therefore, counterdeception can ensure friendly decision makers are aware of adversary deception activities, and enable them to take appropriate action. Integrated intelligence, surveillance, and reconnaissance activities play a key role in counterdeception by providing awareness of an adversary's posture or intent and by identifying an adversary's attempts to deceive friendly forces.

## cd2.htm

There are a few basic principles of counterdeception. The first is that deception does not necessarily rely on advanced technology. Therefore, any nation or group, regardless of sophistication, can conduct deception operations. Also, it is difficult for us to be aware of our own preconceptions. Many nations and groups understand U.S. preconceptions and biases and may be skilled at exploiting them to accomplish their deception operations. In addition, while DoD policy prevents the US military from misleading the American public, Congress, or the media, other nations do not have this restriction. This gives them a flexibility that we do not have, enabling them to better conceal their deception operations.

### [sum.htm](#)

During this lesson you were introduced to defensive counterinformation, or DCI, activities and their role in protecting Air Force information, information systems, and information operations. The lesson presented the two security measures of OPSEC with its 5-step process and information assurance which has COMSEC and COMPUSEC as two of its major programs. Electronic protection was presented as our defense against electronic warfare waged by the enemy or ourselves. Counterintelligence is our counter to the enemy's spies, while counterPSYOP protects us from his disinformation efforts and counterdeception prevents his attempts to mislead us. Recognizing the primacy of the offensive, many DCI functions benefit from a healthy dose of OCI in their implementation. This active manifestation of DCI may occasionally blur the line between OCI and DCI. Just remember, all of the DCI functions have as their purpose to protect and defend our information and information systems.

### [quiz1.htm](#)

Now take time to test your knowledge of the previous lesson material. This is for your self-assessment only and will not be recorded.

## Electronic Warfare

[intro.htm](#)

The words of Admiral Mahan reflect the changes in warfare that have resulted from the technological revolution. Today's wars are no longer battles of mere mechanized machinery and combat arms, rather they consist of a complex array of electronic equipment. Many of today's battles depend upon electronic warfare, or EW, as an essential element of success. EW is a specialized tool that enhances many aerospace functions at multiple levels of conflict. Proper employment of EW enhances the ability of US operational commanders to achieve superiority over the adversary.

On the first night of Desert Storm, EW attacks contributed to the destruction of Iraq's air defenses, resulting in complete dominance of the Iraqi air space by coalition forces. Initial attacks by Apache helicopters, F-117's, and other coalition aircraft left Iraqi radar operators blinded and confused by destroying their central control towers. Coalition Suppression of Enemy Air Defenses, or SEAD, attacks further confused the enemy radar by launching massive numbers of decoys that mimicked the radar return of conventional aircraft. Enticed by the decoys and drones, enemy radar operators turned on their equipment to engage the attackers but were blanketed with interference from coalition radar-jamming aircraft. Radar-killing aircraft, carrying, high-speed, anti-radiation missiles, or HARMS, homed in on the Iraqi radar signal, destroying the radar batteries and leaving Iraq's integrated air defense system shattered.

### [obj.htm](#)

The objective of this lesson is for you to comprehend electronic warfare, or EW, and how it can be integrated into Information Warfare operations. The material presented in this lesson will enable you to define electronic warfare. It will enable you to explain the components of EW, as well as explain how those components can be integrated to support the IW portion of a campaign plan.

### [ovrvw.htm](#)

The lesson begins with an explanation of EW fundamentals and their role in information warfare. Next, the lesson will present the three components of EW, electronic attack, electronic protection, and electronic support. The lesson will end with an explanation of how the three components of EW were effectively integrated in the suppression of enemy air defenses, or SEAD operations in the Bekaa' Valley.

### [def.htm](#)

AFDD 2-5.1, Electronic Warfare, defines EW as “any military action involving the use of electromagnetic and directed energy to manipulate the electromagnetic spectrum or to attack an adversary. This publication provides specific guidance for planning and conducting electronic warfare operations in support of national and joint force commander campaign objectives. To fully understand the role of EW in military operations, one must understand the fundamental elements of EW.

## fun.htm

Modern military forces rely heavily on a variety of complex electronic offensive and defensive capabilities. Electromagnetic, or EM, energy is the means by which modern information systems process and store information. Therefore, control of the EM spectrum has a major impact on the success of military operations.

Electromagnetic energy exists in various forms, which are differentiated by the wavelength of their radiation. Some communications systems used wavelengths measured in miles, while X-rays have wavelengths that are fractions of a micron long. In between these extremes are radio, television, radar, and visible spectrum wavelengths. The entire range of wavelengths, from 0 to infinity is called the electromagnetic spectrum.

The term directed energy is an umbrella term, which covers technologies that produce a beam of concentrated electromagnetic energy or atomic or subatomic particles. Military use of directed energy involve the use of various weapons, devices, and countermeasures to either cause direct damage or destruction to enemy equipment, facilities, and personnel.

## com\_1.htm

The three major components of EW are electronic attack, electronic warfare support, and electronic protection. EW spans the IO spectrum. Electronic Attack is categorized as an OCI activity; electronic protection is considered a DCI activity and will be covered in more detail in a later lesson, and electronic warfare support can be

considered an Information-In-War activity since it gains and exploits information from the electromagnetic environment.

Electronic attack, or EA, involves the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment or destructive attack, with the intent of degrading, neutralizing, or destroying enemy combat capability.

EA is divided into two major areas: destructive and non-destructive EA. Destructive EA is comprised of Anti-radiation missiles (ARM) and Directed energy weapons to locate and destroy radiation sources, such as enemy radar.

[com\\_2.htm](#)

Nondestructive EA is employed with the intent of degrading or neutralizing the enemy's combat capability and consists of electronic warfare actions such as jamming and deception.

According to AFDD 2-5.1, electromagnetic jamming consists of actions taken to prevent or reduce an enemy's use of the EM spectrum. Jamming results in distorting the enemy's radar picture; thus distorting the view of the battle space.

Electromagnetic deception involves using the EM spectrum to convey misleading information to an enemy. Deception transmitters can place false targets on the enemy radar's scope, or cause the enemy radar to assess incorrect target speed,

range, or azimuth. Decoys equipped with transmitters that emit radar returns are often employed to mimic real aircraft.

#### [com\\_3.htm](#)

Electronic warfare support or ES is the division of electronic warfare which involves actions taken to search for, identify, intercept, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, ES provides information required for immediate decisions involving electronic warfare operations.

Electronic warfare support data can be used to produce signal intelligence, provide targeting for electronic or destructive attack, and to produce measurement and signature intelligence.

#### [com\\_4.htm](#)

Electronic protection is that division of EW, which involves actions taken to protect personnel, facilities, and equipment from the effects of electronic warfare actions.

Electronic protection consists of three elements presented on the screen. Roll your cursor over the elements for a brief description.

#### [beka1.htm](#)

Now that you are familiar with the fundamentals and components of EW, let's take a look at an example of how the components were integrated into a successful SEAD, or Suppression of Enemy Air Defense, campaign in the Beka'a Valley during the early 1980's.

The Syrians, in support of their operations in Lebanon, constructed numerous surface-to-air missile, or SAM, sites, configured to impede Israeli air operations against Southern Lebanon. Despite repeated diplomatic gestures from the Israelis, which stated that they considered this an infringement of their sovereignty, the Syrians persisted in expanding their IADS structure.

The Israeli's responded with a carefully coordinated attack, employing electronic warfare systems to neutralize the Syrian IADS and protect their own assets. The Israeli Air Force began by conducting electronic support operations using E-2C aircraft, capable of tracking aircraft and surface-to-air missiles. Next, the Israeli's used nondestructive electronic attack, blanketing the SAMs with clouds of tiny metal, reflective bits called chaff, to blind the radar. With the Syrian radar blinded, the attackers launched jet-powered decoys to draw enemy fire. The Syrian SAMs wasted their ordnance on the decoys and ignited smoke screens, which failed to conceal the missile batteries and actually helped the Israelis locate them. The E2C-s switched to an EA jamming mode to provide cover for ARM shooters, which attached the SAMs with destructive electronic attack.

[beka2.htm](#)

In the initial conflict, the Israelis destroyed 17 SAM batteries and 29 Syrian aircraft. Due to the effective integration of EW components, the Israelis accomplished the goal of SEAD, which is to provide a situation in which tactical forces can perform their missions effectively without interference from electronically directed enemy air defenses. As a result, no Israeli aircraft were lost in the attack.

The integration of EW components had a devastating impact on the OODA loop of the Israeli adversary. EA jamming and deception affected the observation phase, causing the Syrians to collect distorted and inaccurate radar information. Based on this false information, the Syrians were oriented to believe they were under attack and decided to launch a counter attack. They took action by launching SAMs and aircraft in retaliation. The actions taken by the Syrians caused them to waste munitions on false targets and expose themselves to ARM shooters, thus supporting the objectives of the Israelis.

[asset.htm](#)

Here are some of the assets the Services use to conduct electronic warfare. Place your cursor over an image to view the description.

[sum.htm](#)

This lesson has introduced you to the concept of electronic warfare. It began by defining EW and followed with a description of the fundamentals of EW and how the electronic spectrum can be controlled and exploited. Next the lesson presented the three components of EW; electronic attack, electronic warfare support, and

electronic protection. The lesson defined each of those components and described how each is employed in EW. Finally, you were shown an example of how EW components can be integrated to enhance military operations.

The conduct of electronic warfare is vital to mission success. Today's weapon and support systems rely on radio, radar, infrared, electro optical, ultraviolet, and laser technologies to function in peace and war. Unhampered use of the electromagnetic spectrum is vital to assure the success of any modern military operation.

[quiz1.htm](#)

Here are a few questions to test your knowledge of the previous lesson material.

These questions are for your self-assessment only and are not recorded.

## Information Attack

[intro.htm](#)

While other activities, like deception, provide an indirect approach to information warfare, information attack offers a direct approach. Deception depends upon the adversary to observe a false reality, process the data into information, and act upon the information in the desired manner. Information attack acts directly on the information, altering it without relying on the adversary's perception or interpretation ability.

In DESERT STORM, the massive troop movements westward were concealed by deception operations, in the form of the decoy bases left behind. Iraqi observers observed the decoy bases and processed their sensory data into information. This information, based on a false reality, was sent to the leadership and resulted in the desired effect—no action was taken. But what if the movement of forces had been concealed in another, more direct manner? Hypothetically, information attack could have been employed to insert or manipulate false intelligence reports into the enemy databases. This lesson introduces you to information attack and its role in information warfare.

[obj.htm](#)

The objective of this lesson is for you to comprehend information attack and its role in information warfare. This lesson will enable you to define information attack, as well as describe its advantages and effects. You will be able to describe the threat posed by information attack and the types of weapons that are associated with it.

### [ovrvw.htm](#)

The lesson begins with a definition of information attack and follows with a discussion of its advantages. The lesson then describes the affects of Information Attack, followed by a discussion of the sources of threat associated with it. The lesson continues with brief descriptions of some of the terms associated with info attack and closes by presenting the Rome Labs computer intrusion case.

### [def.htm](#)

AFDD 2-5 defines information attack as those activities taken to manipulate or destroy an adversary's information or information systems without necessarily changing the physical entity within which it resides. There are several advantages to these types of operations.

Information attack offers the ability to incapacitate an adversary while reducing exposure of friendly forces, minimizing collateral damage, and preventing excessive adversary and friendly loss of life. By using information attack capabilities, conventional sorties can be saved for other targets.

### [effx.htm](#)

When information systems are compromised, an adversary's decision-making process can be affected—perhaps without their knowledge. A successful information attack could destroy an adversary's confidence in their information systems, causing them to rely on less-technical and, in most cases, less secure means to disseminate

critical information. This security vulnerability could allow an adversary's information to be exploited by friendly forces.

[sot.htm](#)

The threat currently facing the US is no longer defined by geographical boundaries as it was during the Cold War or limited to specific times of crisis or conflict.

Information attacks can come from any place at any time.

In general, there are two sources of threat: external and internal. External sources, such as hackers and terrorists, are generally recognized and planned for; however, internal sources of threat are particularly dangerous. They can have a serious and severe impact on operations because of the inherent trust the military has in the individuals who it employs and the information they generate.

Thousands of web servers, including commercial and government sites, are defaced every year and many more attempts are made to breach the security of information systems. While many of those attacks are harmless hackers who do little damage, any of those attempts could be information attackers who penetrate a system for the purpose of manipulating or destroying information. Unlike hackers, who usually leave a calling card or blatant evidence of their conquest, information attackers might never be detected or make their presence known. To find out more about how we defend our information and information systems, refer to the Defensive Counterinformation lesson.

## terms.htm

Here are some of the terms associated with information attack. Place your cursor over a term for a description.

## rome.htm

One of the most well known and most documented attacks on U.S. information systems is the Rome Labs intrusion case. In March of 1994, a sniffer—a tool used by attackers to covertly collect network login information—was found installed on one of the Rome Labs systems at Griffis Air Force Base, New York. An investigation, by experts from the Air Force Information Warfare Center, revealed that two individuals had gained access to Rome Labs systems, downloaded sensitive research and development data, and installed sniffers on several systems. The attackers used these systems to attack other systems around the world.

Investigators chose to secure most of the systems but left others vulnerable, in order to provide a means to trace the attackers as they continued their activities.

Surveillance showed that the attackers used the Rome Labs systems to attack systems of the Army Corps of Engineers and revealed that the attackers used the nicknames Datastream and Kuji. An informant was able to make contact with Datastream and obtain contact information.

As the investigation continued, the attackers used the Rome Labs computers to gain access to the Korean Atomic Research institute. Tensions mounted as investigators feared the attacks were directed at North Korea and that U.S. military systems would be implicated. The attacks came at a time when the U.S. was undergoing tenuous

negotiations with North Korea on their nuclear program. It was later discovered that the information the hackers obtained was from South Korea.

The investigators believed they were tracking international spies, due to the nature of the attacks and the information they stole. The attackers turned out to be sixteen and twenty-two year olds from the U.K. who hacked government and military sites as a hobby.

#### [sum.htm](#)

Information attack is a powerful and dangerous tool in the arsenal of information warfare. Its power lies in its ability to affect information directly, without depending on the adversary's decision-making process. Information attack is a danger to the U.S. because of the interconnectivity of today's information systems and our reliance on them. By affecting information directly without causing physical harm to information systems, an information attack may go undetected until the damage to information has already been done.

#### [quiz1.htm](#)

Here are a few questions to test your knowledge of the previous lesson material.

These questions are for your self-assessment only and are not recorded.

## Information-in-Warfare

[intro.htm](#)

How do commanders and planners get the meaningful information they need to make decisions and plan operations? To answer this question, let's look back at DESERT STORM.

When Iraq invaded Kuwait on August 2, 1990, satellite systems were first on the scene—high in orbit over the region—providing multi-spectral imagery and environmental data. Once DESERT STORM began, space assets aided navigation in the featureless terrain of the Iraqi desert; enabled real-time, secure, voice communications; provided Scud missile launch detection; and many other functions.

The first air assets deployed to the theater included U.S. Airborne Warning and Control System aircraft, or AWACS, which monitored the skies over Iraq and provided information on the readiness and capabilities of the Iraqi air force. Over 100 additional surveillance and reconnaissance aircraft were deployed to the theater to collect information.

Aerospace assets, such as these, enable the functions of: intelligence, surveillance, and reconnaissance; precision navigation and positioning; weather services; and communications capabilities. These functions provide critical support to air, space, and information operations, by giving commanders the ability to observe the overall battlespace. The information they collect can be processed by intelligence analysts to give military leaders the intelligence support they need to make informed decisions. Together, these functions make up one of two pillars of information operations—Information-in-Warfare.

[obj.htm](#)

The objective of this lesson is for you to comprehend the Information-in-Warfare functions that support Information Operations. The material will enable you to define Information-in-Warfare and to describe how the supporting functions contribute to information operations. Also, it will enable you to understand how the supporting functions are integrated into the conduct of information operations.

def.htm

According to AFDD 2-5, information-in-warfare "...involves the AF's extensive capabilities to provide *global awareness* throughout the range of military operations."

Together, the functions of IIW provide commanders with the ability to observe the overall battlespace, analyze events, and maintain awareness. This lesson introduces you to the specific capabilities and functions of the information-in-warfare components.

This lesson explains how the IIW functions of intelligence, surveillance, and reconnaissance; precision navigation and positioning; weather services; space operations; and other support and reachback activities contribute to information operations.

intel.htm

A wealth of data regarding enemy positions and movement is of little use to commanders without a thorough understanding of the enemy and an interpretation of the information. Intelligence activities provide commanders with situational awareness by the collection, processing, integration, analysis, evaluation, interpretation, and dissemination of available information. In addition, intelligence activities seek to provide a thorough understanding of an adversary, including their strengths and weaknesses.

In support of information operations, intelligence requires the collection and analysis of information regarding an adversary's telecommunications and computer infrastructure. In addition, intelligence analysts strive to accurately estimate an adversary's probable courses of action, including their capability to conduct information operations.

sur\_re.htm

As an integral part of the process of intelligence preparation, surveillance and reconnaissance provide commanders with real-time or near-real-time information, such as locations, dispositions, capabilities, and indicators of intentions. Such activities also provide indications, warning, and situational awareness of threats to the United States and its allies. Furthermore, surveillance and reconnaissance can be used to detect and locate electronic emissions that can be taken advantage of by other information operation elements, such as electronic warfare, information attack, and physical attack operations.

Though surveillance and reconnaissance are often conducted by the same collection platform or team, they are distinct functions. Surveillance refers to the continuous collection of information from the air, space, and earth's surface; while reconnaissance refers to activities conducted to gain information on localized and specific targets within a constrained time frame.

[isr.htm](#)

The Joint Surveillance Target Attack Radar System, or JSTARS, provided useful surveillance and reconnaissance information during the Gulf War. In the closing days of January 1991, JSTARS detected significant enemy troop movement toward the Saudi border while orbiting over southeastern Kuwait. This aircraft, equipped with an advanced radar system, is capable of monitoring enemy vehicular traffic and troop dispositions even at night.

When Iraqi troops crossed the border into Saudi Arabia on January 29th, 1991, JSTARS proved to be a valuable asset for ground and air commanders. JSTARS provided a real-time, theater-wide picture of Iraqi movements as they headed toward the coastal Saudi town. Armed with this information, commanders were able to formulate strategies and allocate resources to appropriate locations. With the help of JSTARS, coalition ground and air forces were able to push the Iraqis back across the border and locate and destroy follow-on forces.

[assets.htm](#)

For additional information on how ISR functions support basic aerospace doctrine, please refer to AFDD 2-5.2.

Here are some of the Air Force assets used to conduct intelligence, surveillance, and reconnaissance missions. Place your cursor over an image to view the description. It is important to remember that these functions are carried out by personnel and assets from every branch of service, in addition to those shown here.

[pnp.htm](#)

Precision navigation and positioning, or PNP, provide air, space, and information operations the capability to attack targets in sensitive areas with greater accuracy.

Global Positioning System, or GPS, satellites allow users to determine position within tens of feet for navigation and precision bombing. The ability to accurately locate targets and deliver firepower greatly reduces the number of aircraft and sorties required to neutralize or destroy a target.

In Desert Storm, MH-53 Pave Low helicopters, equipped with GPS, lead Apache helicopters through the desert to enemy early-warning, radar sites. Apaches destroyed these targets, opening a hole in the Iraqi air defense system.

Like other elements of information operations, PNP is more effective when integrated with other components. For example, GPS can be used in conjunction with intelligence collection to ensure better target identification. The accidental bombing of the Chinese embassy in Belgrade during Operation ALLIED FORCE demonstrated that there is more involved in precision engagement than just putting bombs on target.

[weath.htm](#)

Weather services provide the real-time environmental information needed by military planners at all levels of warfare. Weather is a critical factor in the decision-making process for employing and moving forces, selecting weapons and targets, and choosing appropriate delivery tactics.

Weather presented a particular challenge to planners of air operations over Serbia, during operation ALLIED FORCE. The first 21 days of the air campaign only produced 7 days of favorable weather. NATO's attack sorties were reduced by 30 to 50 percent on bad weather days, even with the use of precision-guided munitions. GPS-guided weapons, like Joint Direct Attack Munition, or JDAM, were able to counter the adverse weather conditions using satellite guidance.

### [space.htm](#)

As seen earlier, air, space, and information operations are inherently intertwined and interdependent. Space systems support a wide range of aerospace operations, but are particularly important to the establishment of information superiority.

The Air Force recognizes four basic space missions: Space control ensures freedom of action and, when directed, denies an adversary freedom of action. Space force support operations include spacelift and command and control of satellites. Space force application would provide firepower from space-based systems. Space force enhancement operations are space operations that provide products and services to multiply joint force effectiveness. This group of operations has the greatest impact on Information-in-Warfare by providing navigation, communications, reconnaissance, surveillance, ballistic missile warning, and environmental sensing functions.

### [satel.htm](#)

As you've seen, space systems enable IIW elements through satellite support. ISR functions are supported by satellite imaging capabilities; weather services rely on the Defense Meteorological Satellite Program, or DMSP; and precision navigation and positioning is provided by the Global Positioning System, or GPS.

Presented here are some of the other space-based assets of particular importance to IIW. Place your cursor over an image to view the description.

[other.htm](#)

Today, the mobility and sustainment of forces, as well as offensive and defensive counterinformation operations, are becoming highly dependent on other agencies that collect and disseminate information. Some of those agencies are presented on the screen. These agencies provide support and reachback capabilities that can enhance the effectiveness of Information-in-Warfare. To view a description of the mission statement of a given agency, place your cursor on the appropriate icon. To view the home page of a given agency, click the link.

[sum.htm](#)

This lesson introduced you to the Information-in-Warfare pillar of information operations. The lesson discussed how intelligence, surveillance, and reconnaissance; precision navigation and positioning; weather services; space operations; and communications capabilities support information operations. It also described some of the aerospace assets employed to carry out these functions. Finally, the lesson briefly introduced some of the additional support and reachback agencies involved in IIW.

IIW functions provide commanders with a clear and accurate battlespace picture. This is accomplished through the careful integration of these elements, producing intelligence that can be used to assess situations and take appropriate action.

[quiz1.htm](#)

Here are a few questions to test your knowledge of the previous lesson material.

These questions are for your self-assessment only and are not recorded.

## Legal/Ethical Issues

[intro.htm](#)

A hacker infiltrated U.S. Department of Defense computers. Known only as Cobra Dawn, the codename assigned by investigators, neither the identity nor the origin of the hacker was ever established. The exploitation apparently began with the guess of a simple password on a relatively unimportant computer. This allowed Cobra Dawn to install a sniffer, a program that covertly collects passwords from those who log on to the system. After obtaining a sizable number of passwords, Cobra Dawn used those to hack other systems because many people use the same passwords on all systems they use. It took a while but finally one of the accounts that cracked had system administrator privileges. Jackpot! Cobra Dawn was then able to do most anything on the network, including editing of audit files meant to catch intruders. Before long, access to unclassified as well as certain classified DoD communications networks was gained. Then the damage began. Some important information was deleted, access to other information was denied to its rightful users, and perhaps most devastating of all, some information was replaced with false data. Suddenly, the U.N. forces in Bosnia began to see the effects of the hacker's work. The troops received beans instead of bullets. The personnel records of all deployed U.S. forces suddenly disappeared. Instead of receiving expected e-mail traffic, in-theater leaders received strings of computer-generated obscenities and irrelevant messages from the World Book Encyclopedia. Suddenly the in-theater commanders couldn't trust any of their electronic data; even data that "sounded right" still had to be checked and double-checked for accuracy. Confusion reigned in the field. Distrusting their information as well as the information passed by allied ground

forces, the air elements were grounded pending resolution of the data security issues. In the aftermath of this damage caused by a single hacker, the questions came. What can the United States legally do to respond to this hacker's intrusion? How should a computer network intrusion be viewed by the affected "victim" state? Is some level of intrusion acceptable? When does a computer intruder "go too far?" When does an information attack become an act of war? What are the main legal issues a military commander must consider in his reaction to a similar situation? While this particular scenario was fictitious, the questions are very real. This lesson will help you answer these intricate questions.

#### [obj.htm](#)

The objective of this lesson is for you to comprehend the legal issues that affect information operations. The material presented in this lesson will enable you to discuss the legal and ethical issues affecting information warfare. It will enable you to comprehend the limitations imposed by domestic and international law on information attack and information assurance.

#### [ovrvw.htm](#)

The lesson focuses on two distinct areas of information operations. The first area deals primarily with how international law affects information attack. The second area focuses on how domestic law affects information assurance, specifically computer monitoring.

[evolve.htm](#)

Specific laws always lag behind technology. However, certain principles always apply, especially in the law of war. Military members are familiar with the advent of submarine warfare and aerial warfare and the fact that initially, there were few specific rules to apply to those arenas. Over time however, rules did emerge to govern these new technologies in their use against other states. This, too, is how the law must evolve with information technology.

Chief Justice Oliver Wendell Holmes once wrote, "The life of the law has not been logic; it has been experience." It seldom happens that a legislature foresees a problem before it arises and puts into place a legislative solution before it is needed. More typically, legislators react to a problem that has already manifested itself. The international legal system operates in the same manner. The international community ordinarily does not negotiate treaties to deal with problems until their consequences have begun to be felt. That's not all bad, since the solution can be tailored to the actual problems that have occurred, rather than to a range of hypothetical possibilities. One consequence, however, is that the resulting law, whether domestic or international, may be sharply influenced by the nature of the events that prompted the legal developments. The law is also strongly influenced by the accompanying policy and political considerations.

The unclear nature of the law in this area has caused a great deal of confusion for operators. Operators simply want a pragmatic answer to the question, "what can we legally *do*?" Looking at the past, the rules for aerial bombardment were derived from

analogy with naval bombardment. So too, we can expect the law as it applies to Information Operations to evolve from the general legal principles which apply to traditional warfare.

#### limits.htm

International law consists of binding legal obligations among sovereign states. Two of the basic principles of the international legal system are that sovereign states are legally equal and independent actors in the world community, and that they generally assume legal obligations only by affirmatively agreeing to do so. The most effective instruments in creating international law are international agreements, such as the United Nations Charter. It is also generally accepted that there is a body of customary international law, which consists of practices that have been so widely followed by the community of nations that they are considered to be legally binding.

International law provides the principles that will keep an offensive information operations campaign from violating basic human rights and the legitimate rights of nations.

The application of international law to many information operations is reasonably well settled, including physical attacks on information systems by traditional military means, psychological operations, military deception, and “electronic warfare” operations. Similarly, electromagnetic pulse weapons and directed-energy weapons such as lasers, micro-wave devices, and high energy radio frequency guns will probably operate in a manner similar enough to that of traditional weapons that one could apply existing legal principles to them without much difficulty. Information

attack however presents some new challenges. The legal regulation of information warfare is still in its infancy. As a general principle, unless the law prohibits us from taking a particular action, we are free to do so--legally. Political restraints are another matter. This principle means that in the area of information warfare we have many options open to us.

The tricky part then is to know what current law prohibits, and that is why the JAG is your friend!! Your judge advocate will help you navigate these uncertain waters. The Law of Armed Conflict sets limitations on military actions after we've entered hostilities and the United Nations' Charter sets some parameters for the use of force prior to entering hostilities.

[loac.htm](#)

Once we have entered hostilities, the Law of Armed Conflict, better known as LOAC, provides the most basic principles with which to analyze a proposed information attack. Following is a review of the major principles of LOAC and how they may apply to possible information operations scenarios.

Military necessity dictates that targets have military value. Obviously, military infrastructure is a legitimate target. Often, the civilian infrastructure supports a country's military effort. The destruction of the civilian infrastructure may provide an attacker a military advantage. Military necessity would then allow such an attack.

The principle of proportionality requires the military value gained from an attack exceed the expected collateral damage. As an example, the destruction of a nation's transportation system might easily pass the test of military necessity. If a side effect were the mass starvation of the populace, the attack may fail the test of proportionality. Therefore target analysis must consider not only a target's military value but also the expected direct and indirect collateral damage that a target's destruction would cause.

Distinction requires combatants be distinguished from noncombatants: With very limited exceptions, only members of a nation's regular armed forces are entitled to use force against the enemy. They must distinguish themselves from noncombatants, and they must not use noncombatants or civilian property to shield themselves from attack. This rule grew up when combatants could see each other and make a judgment of whether or not to open fire based in part on whether or not the individual in the sights wore an enemy uniform. When the unit of combat came to be a vessel, tank, truck, or aircraft, it became more important that such vehicles be properly marked than that their occupants wear a distinctive uniform. Persons who commit combatant attacks without authorization are subject to criminal prosecution.

The principle of humanity prohibits the use of indiscriminate weapons or attacks that cause injury not justified by military necessity. The dum-dum bullet and laser weapons specifically designed to cause permanent blindness to unenhanced vision are both outlawed because they cause injuries that exceed what is required by military necessity.

The final principle to consider is that of chivalry. War must be conducted in accordance with well-recognized formalities and courtesies. This principle recognizes certain visual and electronic symbols which identify persons and property that are protected from attack. Among these are prisoners of war and prisoner of war camps, the wounded and sick, and medical personnel, vehicles, aircraft, and vessels. Any misuse of these protected symbols to immunize a lawful military target from attack constitutes the war crime of perfidy. Suppression of such acts is necessary to preserve the effectiveness of such symbols, since known misuse may lead the combatants to disregard them. For similar reasons, it is unlawful to feign surrender, illness, or death to gain an advantage in combat, as well as to broadcast a false report of a cease-fire or armistice.

You may review the notes for any of the LOAC principles by placing your cursor over it. Now we will examine how LOAC would apply to information attack.

[loac\\_ex.htm](#)

Many of the scenarios envisioned for information attack involve the disruption of public utilities or a nation's economic infrastructure – such as its banks and stock exchanges. Would such attacks be legal? It depends... Purely civilian infrastructures must not be attacked unless the attacking force can demonstrate that a definite military advantage is expected from the attack. Stock exchanges, banking systems, universities, and similar civilian infrastructures may not be attacked simply because a belligerent has the ability to do so. In a long and protracted conflict,

damaging the enemy's economy and research and development capabilities may well inhibit its war effort, providing a lawful basis on which to target such capabilities.

During Desert Storm, one of the earliest targets of the coalition bombing campaign was the electrical power system in Baghdad. Considering the important military uses being made of electricity from that system, it was clearly a lawful military target. The Iraqi government then made a public pronouncement that the coalition's attack on the city's electrical power system constituted an act of attempted genocide. The logic of this position was that the city's sewage system depended on electrical pumping stations, so when the electricity went out the sewage system backed up and created a threat of epidemic disease. No one took this claim very seriously, but this incident highlights the fact that when an attack is made on an infrastructure that is being used for both military and civilian purposes the commander will not be in a proper position to weigh the proportionality of the expected military advantage against the foreseeable collateral damage unless the commander has made a reasonable effort to discover whether the system is being used for civilian purposes that are essential to public health and safety. This principle operates in exactly the same way whether the attack is carried out using traditional weapons or in the form of a computer network attack.

Another scenario involves the use of computer viruses or other malicious logic to cripple an enemy's information systems. If such code spreads outside of the targeted systems, especially into systems of neutral or friendly nations, we might very well be charged with using an indiscriminant weapon. Violation of the principle of humanity could occur if the consequences of such an attack caused the release of

dangerous forces like the opening of a dam's floodgates or a Chernobyl-like meltdown of a nuclear reactor.

Taking over an enemy's computer network to misroute supplies and reinforcements would probably be a legitimate act. Using the same network to declare a false end to the war would probably be perfidy.

With very limited exceptions, only members of a nation's regular armed forces are entitled to use force against the enemy. If a computer network attack is launched from a location far from its target, it may be of no practical significance whether the "combatant" is wearing a uniform. Nevertheless, the law of war requires that lawful combatants be trained in the law of war, that they serve under effective discipline, and that they be under the command of officers responsible for their conduct. This principle argues for retaining the requirement that information operations during international armed conflicts be conducted only by members of the armed forces.

Another interesting issue is whether an information attack should be launched from a .mil address or whether it would be permissible to launch it from a .com address, to obscure the origins of the attack.

Although there are novel features of information operations that will require expansion and interpretation of the established principles of LOAC, the outcome of this process appears to be reasonably predictable. Thus, if an information attack obtains a military advantage without disproportionate collateral effects in a humane and chivalrous manner it probably is a legitimate act under LOAC.

Other.htm (Change bullets to – Foreign Domestic Law and – US Domestic Law)

If a CINC or a joint task force commander decides to order execution of a certain information operations activity by forces under his or her command who are deployed in a foreign country, the commander may have to consider whether or not such activity is prohibited under local law. The answer may be important at two different levels of analysis. First, the individuals who issue or execute such an order might be subject to prosecution in a host nation criminal court; and second, the commander might feel obligated on a policy basis to refrain from issuing such an order.

A Commander also must consider whether U.S. domestic law may subject a military member to criminal prosecution for conducting information attack. Representatives of the Department of Justice have made it clear on numerous occasions that domestic statutes, such as those prohibiting unauthorized access and unauthorized interception of electronic communications apply fully to the actions of government agents, whether they are engaged in law enforcement, intelligence, national security, or other activities. The Office of Legal Counsel of the Department of Justice, however, has concluded in a written opinion that these statutes would not apply to the actions of U.S. military members acting on behalf of the President pursuant to the President's foreign affairs and Commander-in-Chief authority.

neutral.htm

Another important element of international law that impacts information attack during hostilities is the Law of Neutrality. Nations not engaged in a conflict may declare themselves to be neutral. A neutral nation is entitled to immunity from attack by the belligerents, so long as the neutral nation satisfies its obligation not to assist either side. If a neutral nation is unable or unwilling to halt the use of its territory by one of the belligerents in a manner that gives it a military advantage, the other belligerent may have a right to attack its enemy in the neutral's territory.

How, then, does this general concept apply in an information era where communication channels criss-cross a nation's territory and may be used by belligerents on either or both sides?

Under the general principle, if a neutral nation permits its information systems to be used by the military forces of one of the belligerents, the other belligerent generally has a right to demand that it stop doing so. If the neutral refuses, or if for some reason it is unable to prevent such use by a belligerent, the other belligerent may have a limited right of self-defense to prevent such use by its enemy. It is quite foreseeable, for example, that a belligerent might demand that a neutral nation not provide satellite imagery of the belligerent's forces to its enemy, or that the neutral cease providing real-time weather information or precision navigation services.

There appears, however, to be a limited exception to this principle for communications relay systems. The 1907 *Hague Convention* provides that "A

neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraph apparatus belonging to it or to Companies or private individuals,” so long as such facilities are provided impartially to both belligerents. The plain language of this agreement would appear to apply to communication satellites as well as to ground-based facilities.

There is nothing in this agreement, however, that would suggest that it applies to systems that generate information, rather than merely relay communications. These would include the satellite imagery, weather, and navigation systems mentioned above, as well as other kinds of intelligence-producing systems such as signals intelligence. For example, if a belligerent nation demanded that the U.S. government deny GPS navigation services to its enemy, and if the U.S. were unable or unwilling to comply, the belligerent might have the right to take necessary and proportional acts in self-defense, such as jamming the GPS signal in the combat area.

[sd.htm](#)

As discussed above, the law of war authorizes a nation engaged in an international armed conflict to employ armed force to attack lawful military targets belonging to the enemy. The focus of this section, however, is on the application of international law principles in circumstances where we have not entered a state of armed conflict, which means peacetime, including the conduct of military operations other than war. For this analysis, we look primarily to the United Nations' Charter.

The members of the United Nations have agreed in Article 2 (4) of the UN Charter to “refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”

The Charter provides two exceptions to this prohibition. First is Article 51 which provides for the Inherent Right of Self-Defense in Response to an “Armed Attack,” and Article 42 for United Nations Security Council resolutions, which authorize the use of force in response to a threat to the peace or an act of Aggression.

The basic question, which must be answered, is when the use of information attack becomes an “armed attack” authorizing the use of force in self-defense. In other words when is self-defense authorized in response to hostile information attack?

There’s no way to be certain how these principles of international law will be applied by the international community to computer network attacks. As with other developments in international law, much will depend on how the nations and international institutions react to the particular circumstances in which these issues are raised for the first time.

If we focused on the means used, we might conclude that electronic signals, imperceptible to human senses, don’t closely resemble bombs, bullets, or troops. On the other hand, it seems likely that the international community will be more interested in the consequences of a computer network attack than in its mechanism. It might be hard to sell the notion that an unauthorized intrusion into an unclassified

information system, without more, constitutes an armed attack. On the other hand, if a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian death and property damage, it may well be that no one would challenge the victim nation if it concluded that it was the victim of an armed attack, or an act equivalent to an armed attack.

There has been some support for the proposition that a nation has an inherent right to use force in self-defense against acts that do not constitute a classic armed attack. This view is supported by the inclusion of General Assembly's definition of aggression of acts that do not entail armed attacks by a nation's armed forces, such as the unlawful extension of the presence of visiting forces, or allowing a nation's territory to be used by another state "for perpetrating an act of aggression against a third State."

It's far from clear the extent to which the world community will regard computer network attacks as "armed attacks" or "uses of force," or how the doctrines of self-defense and countermeasures will be applied to computer network attacks. The outcome will probably depend more on the consequences of such attacks than on their mechanisms. The most likely result is an acceptance that a nation subjected to a state-sponsored computer network attack can lawfully respond in kind, and in some circumstances it may be justified in using traditional military means in self-defense. Unless the nations decide to negotiate a treaty addressing computer network attacks, which seems unlikely anytime in the near future, international law in

this area will develop through the actions of nations and through the positions the nations adopt publicly as events unfold. U.S. officials must be aware of the implications of their own actions and statements in this formative period.

Infoass.htm

As stated above, the discussion up to this point has assumed we know who an intruder is, and that we are confident in characterizing his intent. In practice, this is seldom the case, at least in the early stages of responding to computer intrusions. The above legal analysis may change if the identity and location of an intruder is uncertain, or if his intent is unclear. Immediately following an information attack, it's often difficult to determine when the response should shift from the customary law enforcement and counter-intelligence modes to a national defense mode. The current presumptive response to a report of an intrusion into a government computer system is a law enforcement investigation. The basis for this is that in most cases the identity, location, intentions, and motivation of the intruder are unknown in the early stages of the investigation. Accordingly, at the outset of a response to a computer intrusion, the only body of investigative authority that clearly applies is that for investigating crimes.

It's time now to look at the other IA, information assurance. Domestic law is what largely applies here and it can be very complicated. Contrasting sharply with the wide open spaces afforded information attack, the law regulating our information assurance activities is more like a minefield - not too bad if you know where you're

going, but one misstep can really ruin your day. Think of the JAG as your map through the minefield. Trust your map. The JAG is your friend.

#### [monitor.htm](#)

As Air Force dependence on computers and electronic communications grow, there is a corresponding need to guard the communications systems against attack or misuse, making asset protection a crucial part of the Air Force mission. The DoD's first line of defense for protecting our information systems is monitoring. Monitoring is performed for various reasons by various actors. System protection is done by network professionals, operational security is done by Telecommunications Monitoring and Assessment Program people such as those at Air Intelligence Agency, and monitoring to gain legal evidence in response to computer intrusions is performed by law enforcement investigators. The rules can be very complicated and vary based upon the agency involved and the reason for the monitoring. Although the information assurance function is a combination of all these types of monitoring, the Air Force's first line of defense against system malfunction and, more importantly, unlawful intrusions into our communications networks is the system administrator conducting systems protection monitoring. It is sometimes difficult to separate the different monitoring functions in the Air Force, so if you become confused, remember, the JAG is your friend.

#### [mon\\_law.htm](#)

There are two primary legal constraints to government monitoring: the 4<sup>th</sup> Amendment and the Electronic Communications Privacy Act. The Fourth

Amendment to the Constitution guarantees persons will be protected against unreasonable searches and seizures. An individual's Fourth Amendment rights are violated only if governmental officials "infringe on an expectation of privacy that society is prepared to consider reasonable." This requires a balancing of interests; the reasonableness of the invasion of an employee's Fourth Amendment interest is balanced against the importance of the government interests justifying the intrusion. This balancing is not significantly different from that done when searching a government office or dorm room. The privacy rights of military members are often subjugated to an overriding need to recognize the demands of discipline and duty.

The Electronic Communications Privacy Act, or ECPA, was designed to confer an expectation of privacy to electronic and wire communications, which may exceed those protected under the 4<sup>th</sup> Amendment, and it generally prohibits the interception or accession of electronic communications. The ECPA applies to intercepting live communications or accessing temporarily stored communications. The ECPA has three exceptions pertinent to our analysis; the systems provider exception, the consent exception and the court order exception. Place your cursor on each exception to learn more about them.

[mon\\_sum.htm](#)

Monitoring is a powerful weapon in the information assurance arsenal. Monitoring will often identify who conducted the attack and where the attack originated. This information is needed in the normal course of mounting an effective defense. There are many legal restraints on how monitoring must be performed to protect the

delicate balance act between individual rights of privacy and public safety. There are many things a monitoring agency CAN do but there are only certain things they may legally do!

[sum.htm](#)

The Information Operations arena is rapidly changing due to its ever-changing technology. The law is trying to catch up to this new era of warfare. The key thing to remember is that generally, in the international arena, if an activity is not prohibited by existing law then it's permitted. In this lesson you've learned how the Laws of Armed Conflict, Laws of Neutrality, and the inherent right of self-defense impact Information Attack. You've also seen the Fourth Amendment and other domestic laws complicate the use of monitoring for information assurance. Perhaps the most important thing to remember is simply this --when in doubt, talk to a lawyer. Remember, they're your friends.

## Operationalizing IO

### [intro.htm](#)

Many different capabilities and activities must be integrated to achieve a coherent IO strategy. Intelligence and communications support are critical to conducting offensive and defensive IO. The thoughtful design and correct operation of information systems are fundamental to the overall conduct of IO. To be successful, IO must be integrated with air, land, sea, and space operations and support national and military objectives.

### [obj.htm](#)

The objective of this lesson is for you to understand the level of effort necessary to accomplish the Air Force IO mission. The material presented in this lesson will enable you to describe the role of different Air Force organizations involved in the IO mission, explain the mission of the Air Force IW Flights in supporting the Commander Air Force Forces, and describe the role of USSPACECOM in computer network operations.

### [ovrvw.htm](#)

The lesson opens by identifying the national level documents and organizations involved in Information Operations. The lesson then presents the joint level documents and organizations and follows with a discussion of the various Air Force agencies involved in Info Ops activities. After presenting the chain of command and reachback resources, the lesson ends by summarizing the challenges faced by warfighters as they conduct IO activities.

### [docs.htm](#)

Guidance for IO at the national level comes from three sources. The Department of Defense Directive S-3600.1, entitled “Information Operations,” and the Chairman of the Joint Chiefs of Staff Instruction 3210.01A, entitled “Joint Information Operations Policy,” outline general and specific information operations policy for Department of Defense components. These documents also delineate specific IO responsibilities. Chairman of the Joint Chiefs of Staff Instruction 6510.01B, entitled “Defensive Information Operations Implementation,” provides specific policy concerning defensive IO.

### [natorg.htm](#)

Presented here are some of the national organizations involved in IO. Place your cursor over an agency’s logo to view their mission statement. Click on the links to view their web sites.

### [jtdoc.htm](#)

Joint Pub 3-13, “Joint Doctrine for Information Operations” contains specific policy and guidance for joint IO. This document represents a significant milestone in defining how joint forces use information operations to support our national military strategy. This document discusses the integration and synchronization of offensive and defensive IO in the planning and execution of combatant commanders’ plans and operations across the spectrum of conflict. The guidance provides joint force commanders and their component commanders with the knowledge needed to plan, train for, and conduct IO.

suppt.htm

The Services provide the joint combatant commands with the forces needed to accomplish their missions. For example, the Air Force provides units from Air Combat Command to US Joint Forces Command. Within the IO mission realm, Air Combat Command has resources from the 8th Air Force and from the Air Intelligence Agency. Eighth Air Force is the lead Numbered Air Force for the conduct of Air Force IO. Other NAFs also have IW resources, as we'll see later. Air Combat Command also supports other joint organizations, two of the more notable ones being the Joint Information Operations Center, called (jii-yoc) and the Joint Task Force for Computer Network Operations. Both of these are organized under the unified command USSPACECOM. Currently, the 8th Air Force Deputy Commander for IO is also the commander of AIA and the commander of JIOC, which makes their integration almost seamless. The next few screens will cover these organizations in more detail.

[itorg.htm](#)

As one of the nation's nine Unified Commands, U.S. Space Command coordinates the use of the Department of Defense's military space forces in providing Space Forces Support, Space Force Enhancement, Space Force Control, Space Force Application, and Computer Network Operations. USSPACECOM runs the Joint Information Operations Center, which is the principal field agency for joint information operations support for the combatant commands. The center provides support to planning, coordination, and execution of DoD information operations worldwide. Additionally, the center assists with the development of IO doctrine, tactics, and procedures. To accomplish the computer network operations mission, USSPACECOM established the Joint Task Force – Computer Network Operations. Its center is located at the headquarters of the Defense Information Systems Agency, and is the focal point for defense of DoD computer systems and networks. It monitors incidents and potential threats to DoD systems and establishes links with other federal agencies through the National Infrastructure Protection Center to share information on activities across the information infrastructure. When attacks are detected, the JTF directs DoD-wide recovery actions to stop or contain damage and restore network functions to DoD operations.

[aforg.htm](http://aforg.htm)

The Air Intelligence Agency, AIA, is the single agency for the performance of Air Force wide intelligence roles and functions. AIA provides full-spectrum information operations products, applications, services and resources to Air Force major commands, Air Force components and national decision-makers. AIA also provides intelligence expertise in the areas of C2 protection, security, acquisition, foreign weapons systems and technology, and treaty monitoring. A major organization within AIA is the Air Force Information Warfare Center, or AFIWC. AFIWC's mission is to develop, maintain and deploy information warfare capabilities in support of operations, campaign planning, acquisition and testing. AFIWC acts as the time sensitive, single focal point for IW intelligence data. It provides technical expertise for computer and communications security and is the Air Force's focal point for tactical deception and operations security training. The AFIWC also organizes, trains, equips and deploys teams to support joint and service exercises and performs vulnerability analysis of electronic systems as part of the Telecommunications Monitoring and Assessment Program. AFIWC has organized itself into many units to perform its mission including the Air Force Information Warfare Battlelab. The purpose of the Air Force battlelabs is to identify off-the-shelf technology that could provide new military capabilities and demonstrate those capabilities for possible adoption by the war-fighting organizations. AFIWC also owns the Air Force's IW schoolhouse. The 39th Information Operations Squadron at Hurlburt conducts the formal training for all of the Air Force's IW warriors.

## [naf.htm](#)

The numbered air force is the senior war-fighting echelon in the Air Force. We mentioned that the 8th AF is the lead NAF for conducting Air Force IO. Its 70th Intelligence Wing collects, analyzes and reports current information needed to support IO. The 67th Information Operations Wing is responsible for executing information operations missions. Of particular note, the 67th IOW operates the Air Force Computer Emergency Response Team or AFCERT. The JTF-CNO, which you'll recall was under USSPACECOM, actually exercises Tactical Control over AFCERT as well as the other services computer emergency response teams. We'll next look at the most fundamental Air Force IW unit, the IW Flight.

## [lw\\_flt.htm](#)

IW flights are deployable units that can provide full OCI and DCI planning capability for a NAF level combat entity. Nine IW flights are currently assigned to the NAF and MAJCOM headquarters shown on the screen. The 26-29 personnel of the IW flight have expertise covering the full gamut of information operations. During peacetime, they would provide support to the deliberate planning process as well as the training function. During contingencies, an IW flight can deploy and operate out of the air operations center in support of the Commander Air Force Forces who would often be dual-hatted as the JFACC. Their expertise would be used to integrate IO operations into the air campaign. IO activities are executed using the various IW assets you've learned about throughout the course.

### [intio.htm](#)

The JFACC and his air campaign exists to support the Joint Force Commander's objectives. The other components also support the JFC who ultimately gets his guidance from the national command authorities. The other components offer many assets and capabilities to the IO campaign plan. Furthermore, as the supported commander, the JFC can count on the support of other CINCs like USSPACECOM with his IO assets as well as all of the national level IO organizations we covered earlier. How do all of these organizations come together to create a harmonious IO campaign plan? The answer is the Joint IO Cell.

### [jtiocell.htm](#)

A fully functional IO cell is paramount to successful IO. The Joint Force Commander is responsible for establishing an IO cell. As you can see, the service and functional component reps are only a small part of this organization. The Air Force rep would probably be a dual-hatted member of the IW Flight working out of the AOC. The JFC's staff, which includes the IO cell, develops and disseminates planning guidance for IO that is passed to the components and supporting organizations and agencies for decentralized planning and execution. The IO cell integrates the broad range of potential IO actions and activities that could contribute to the JFC's desired end state in an area of responsibility or joint operations area. Presented here is a typical Joint IO cell. Refer to Joint Pub 3-13 to view the specific duties and responsibilities for each component.

[sum.htm](#)

Compare this view of the IO planning process to the one at the start of the lesson.

This graphic illustrates how the IO world suffers the effect of stovepiping, duplications of effort, and turf wars. This can only be expected given that the explosion of IO has largely been enabled by relatively recent technology. With no central plan for the technology's development, organizations developed capabilities independently. The IO world probably benefited from this to some extent. A healthy competition for survival insured only the best capabilities prevailed. The joint planning process provides a framework for bringing these diverse capabilities together to provide coordinated information operations that support a JFC's objectives. This process not only insures coordination within the IO community, but also allows for the synergistic integration of information operations with air, land, sea, and space operations.

## Physical Attack

[intro.htm](#)

Information Warfare is not so much about eliminating an enemy, as it is about influencing his perception and modifying his behavior. Destroying an adversary's troops and weaponry puts our lives and resources at risk and may adversely affect the desired end state. Instead, we can employ physical attack, in the form of precision-guided munitions, to reduce the enemy's warfighting capability by targeting vital areas of his information systems.

Think back to DESERT STORM: What were the targets struck within the first few minutes of the war, and why was their destruction important? They weren't tanks or troops—they were information systems. It was vital to the success and safety of follow-on air operations that the Iraqi air defense system be suppressed. Striking the radars blinded the system. Hitting its control systems decapitated it, leaving its arms and legs flailing in uncoordinated spasms. The initial strikes did not eliminate many Iraqi troops or weapons—its effect was largely one of intimidation. Surface-to-Air Missiles fired without radar guidance, and interceptors hid in their shelters.

[obj.htm](#)

The objective of this lesson is for you to comprehend the role of physical attack in information warfare. At the end of the lesson, you will be able to define physical attack within the context of information warfare, and you will be able to discuss how physical attack could be used to disrupt an adversary's flow of information.

### def1.htm

Here is how AFDD 2-5 defines physical attack. A key phrase in this definition is the use of “hard kill” weapons against designated targets. A second key phrase refers to the disruption and destruction of an adversary’s information system. These phrases make an important distinction between all physical attack and physical attack within the context of information warfare.

### def2.htm

When is a physical attack an IW attack? It depends on what is being targeted. The target must be related to an adversary’s information or information systems. By destroying the communications infrastructure, the flow of information is disrupted, thereby reducing the adversary’s ability to communicate between organizations and leadership. Eliminating electricity and power sources could hinder an adversary’s ability to collect information and could also disrupt the distribution of that information. A possible list of targets might include various types of command, control, and communications nodes; intelligence operations; and sources of electricity. It is important to take collateral damage into account when pursuing these types of targets. And, you must also consider the possibility that the operations of other friendly forces might rely on the systems and structures being destroyed.

### examp1.htm

Now take a look at some examples of possible physical attack targets. Can you tell which ones could be targets of an IW physical attack? Click on the best answer at the bottom of your screen.

examp1.htm (communication system)

That is correct. This system allows commanders to communicate with their subordinates. The disruption of this information system would reduce the commander's ability to direct subordinates.

That is incorrect. This system allows commanders to communicate with their subordinates. The disruption of this information system would reduce the commander's ability to direct subordinates.

examp2.htm (power grid)

That is correct. It is an IW physical attack as long as the objective is to reduce the adversary's ability to power their communication systems, thus disrupting the flow of information.

That is incorrect. It is an IW physical attack as long as the objective is to reduce the adversary's ability to power their communication systems, thus disrupting the flow of information.

examp3.htm (suspension bridge)

That is correct. This is actually a trick question. Like the previous example, this depends on why the bridge was targeted. Many bridges carry communication cables beneath them. If the bridge was targeted for its communication cables, then it could be an IW physical attack.

That is incorrect. This is actually a trick question. Like the previous example, this depends on why the bridge was targeted. Many bridges carry communication cables beneath them. If the bridge was targeted for its communication cables, then it could be an IW physical attack.

examp4.htm (enemy troop barracks)

That is incorrect. Probably not if targeted solely to eliminate personnel. However, it could be used to support a PSYOP campaign aimed at reducing enemy morale and encouraging surrender.

That is correct. Probably not if targeted solely to eliminate personnel. However, it could be used to support a PSYOP campaign aimed at reducing enemy morale and encouraging surrender.

[sum.htm](#)

This lesson has shown you how physical attack can be used in Information warfare. The lesson began by reminding you of the impact of physical attack on the success of operation DESERT STORM and continued by explaining the criteria of an IW physical attack.

Now that you've had a chance to look at some examples of IW physical attack, you should be able to use what you have learned to identify numerous other examples from throughout military history. It is important to keep in mind that "information" is not a new commodity, confined to the modern, information age. As early as the 12<sup>th</sup> century the Mongols realized the importance of the flow of information. It was common Mongol military practice to disrupt an enemy's communications before attacking.

Just remember, IW physical attacks employ physical weapons to affect an adversary's flow of information, whether it's voice communications to and from headquarters, early-warning radar signals, or satellite imagery of troop locations.

## Psychological Operations (PSYOP)

[intro.htm](#)

Our ability to deter conflict and aggression is fundamental to the maintenance of our nation's security. Psychological operations support this objective by attempting to reduce the morale and combat efficiency of enemy troops. To accomplish this, Psychological Operations, or PSYOP, convey the perception to the enemy that attack will be both costly, in terms of lives and resources, and unsuccessful. When properly employed, PSYOP results in a behavioral change that fulfills the objective of deterring conflict. PSYOP is not only applicable to enemy troops in the field but to their military commanders, political leaders, and civilian populations.

PSYOP became a part of military strategy long before the "PSYOP" label was applied. Sun Tzu wrote about the "supreme excellence" of subduing the enemy without a fight. And, Genghis Kahn employed PSYOP by spreading rumors about the strength and fierceness of his army.

In recent times, the expansion of mass communications capabilities has enhanced PSYOP by providing faster, wider, and more media-rich channels to convey messages to the target audience. Worldwide news broadcasts can affect international opinion in a few seconds, resulting in attitudes and emotions that can influence the decision-making process of a nation's leadership.

Low-tech methods, such as printed leaflets, are still effective and were employed as recently as DESERT STORM and ALLIED FORCE to encourage enemy defection

and surrender. Remember the marine tidal wave leaflet that was floated onto the Kuwaiti shore during the Gulf War? That PSYOP leaflet served as a terrifying image to reduce enemy morale but also supported the credibility of the deception plan. The leaflet's imagery of an amphibious assault, combined with real images of exercises broadcast on CNN, was enough to convince the Iraqis that the main thrust of the coalition counterattack would come from the sea.

#### [obj.htm](#)

The objective of this lesson is for you to comprehend psychological operations and how they may be employed to influence an adversary's behavior. At the end of the lesson you will be able to define PSYOP as well as explain its different categories and types. You will be able to identify the tools used to conduct PSYOP, and you will be able to explain the principles and objectives of PSYOP. Finally, you'll be able to explain how PSYOP has been used in past military operations.

#### [ovrvw.htm](#)

The lesson begins with a definition of PSYOP and follows with a discussion of the publications which guide PSYOP activities. The next topic addresses the categories and general types of PSYOP and follows with a look at the tools used to conduct these operations. The lesson continues with a discussion of the key agencies, followed by a presentation of the principles and objectives of PSYOP planning. An explanation is given of how PSYOP fits into the operational environment. And, finally, the lesson ends with a look at PSYOP examples from past military operations.

[defined.htm](#)

This is the definition of PSYOP from AFDD 2-5.3. PSYOP disseminates truthful information to foreign audiences in support of US policy and national objectives. PSYOP span the entire spectrum of military operations—from peace all the way through war. Because they can provide a critical, force-multiplying capability useful at all levels of operations, PSYOP are a vital element in securing national objectives.

[basis.htm](#)

The development of the 1985 PSYOP Master Plan ensured PSYOP would be injected into military operations at all levels. Due to changes in legislation, the creation of the United States Special Operations Command, and changes in foreign policy, the Master Plan was rewritten in 1990. Since then, numerous documents have been released which provide direction to the Services in terms of developing, training, equipping, and employing PSYOP as a mission essential task.

Joint Pub 3-53, *Doctrine for Joint Psychological Operations*, provides guidance to joint force commanders and provides doctrine for joint operations and training.

AFDD 2-5.3, entitled *Psychological Operations*, provides doctrine for Air Force PSYOP. This document promulgates the Air Force perspective on psychological operations.

AFI 10-702 explains how to plan and execute PSYOP, and it delineates MAJCOM and Field Operating Agency responsibilities. Since Air Force PSYOP should never be conducted independently, Air Force doctrine is closely aligned with joint doctrine and shares many of its principles.

#### category.htm

According to AFDD 2-5.3, PSYOP can be divided into four categories: strategic, operational, tactical, and consolidation. Just as it is important to understand the differences between the PSYOP categories, it is also important to understand that the categories may overlap. Actions in each category may start, stop, and restart at any time during a campaign. These categories are intended to convey capabilities rather than outline employment guidelines. The determination of the appropriate category, type, and method of PSYOP is the responsibility of the PSYOP planner.

#### stpsy.htm

Strategic PSYOP are conducted on a global or regional basis in support of US goals and objectives. Strategic PSYOP are conducted predominantly outside of the military arena but can utilize DOD assets and may be supported by military PSYOP and other air operations. Strategic PSYOP may take many forms, such as diplomatic positions, announcements, communiqués, or deployments. An increase in US military presence can provide a powerful psychological message to adversaries. For example, the large-scale deployment of U.S. forces to the Persian Gulf as part of Operation Desert Shield sent a powerful message of U.S. resolve to the Iraqi leadership.

#### oppsy.htm

Operational PSYOP are conducted in a defined geographic area to promote the effectiveness of a theater commander's objectives, campaigns, and strategies. These operations are designed to strengthen US, allied, or coalition capabilities to conduct military operations in the theater by encouraging enemy forces to defect,

desert, flee, surrender, or take other actions, which support US objectives.

Persistent offensive attacks can have a synergistic effect with PSYOP, accelerating the degradation of enemy morale and encouraging desertion. Operational PSYOP efforts may also enhance force protection by influencing the local populace to report terrorist activities, sabotage, or other threats to US or friendly forces.

#### tacpsy.htm

Tactical PSYOP are normally conducted in conjunction with other tactical operations against opposing forces or audiences. At this level, PSYOP are normally targeted for individual engagements and are limited to short-term objectives. Planners tailor persuasive communications, in a variety of media formats, for the foreign target audience. For instance, during Operation JUST CAUSE, Air Force aircraft supported tactical ground forces by broadcasting radio and television messages that urged the Panamanian populace to remain in their homes and out of harm's way. In similar situations, Air Force assets can be employed to broadcast radio, TV, and loudspeaker messages which may influence a wider audience.

### conpsy.htm

Consolidation PSYOP are conducted in foreign areas where enemy forces or a potentially hostile populace pose threats to US and friendly forces. Consolidation PSYOP help influence the foreign populace to support US local objectives, and allow supported commanders to exercise operational freedom. PSYOP may be particularly effective during foreign internal defense operations. For example, if US forces are helping a foreign government to remove land mines, PSYOP could publicize the effort to gain support from the local populace, thereby creating a safer working environment for US personnel.

### types.htm

While PSYOP can be described in terms of category, they can also be described by their type. Cohesive PSYOP refers to actions geared toward uniting a group of people. Cohesive PSYOP activities consist of actions such as promoting a local government in a favorable light and providing public information as to where food and water supplies are located. Cohesive PSYOP can be used to improve civil and military relations and to disseminate information to the public to counter messages of hostile propaganda. Cohesive PSYOP can also be used to unite an audience against a common enemy.

Divisive PSYOP is used to the opposite effect. The goal of divisive PSYOP is to cause the enemy to lose its will to fight. This is accomplished by exploiting a population's weaknesses and encouraging dissension among the populace. Divisive PSYOP also consists of efforts directed at weakening enemy opposition by exploiting enemy intolerance and prejudice, and by encouraging defection and

apathy among enemy troops. Due to its exploitative nature, divisive PSYOP may cause more harm than good and should be used with caution.

#### [tools.htm](#)

Here are some of the tools that are used to conduct PSYOP. Keep in mind that the tools are often used in tandem to support a common objective. Roll your mouse cursor over the pictures for a brief description.

#### [key.htm](#)

Several DoD agencies are responsible for conducting PSYOP. The United States Special Operations Command, USSOCOM, is the executive agent and force provider for all CONUS-based PSYOP units. The Army coordinates most of the PSYOP activities for the US military through Headquarters U.S. Army Special Operations Command. Their PSYOP missions are conducted by the 2nd, 4th, and 7th Psychological Operations Groups with the 4th POG taking on most of the responsibilities. The 4<sup>th</sup> POG plans and conducts PSYOP activities worldwide in operations that span from peacetime through war.

#### [keyaf.htm](#)

The Air Force has several agencies, which participate in PSYOP activities. The Air Intelligence Agency is the functional manager for Air Force level PSYOP and is rapidly becoming the focal point for PSYOP activities. In addition, the 193rd Special Operations Wing flies the Commando Solo aircraft. Although each of the services bring or support various PSYOP capabilities, close coordination with USSOCOM is essential for effective PSYOP operations.

[fun.htm](#)

When effectively employed, PSYOP provide a number of benefits. As a force multiplier, PSYOP are low-cost, high-impact tools, which allow the JFC to communicate with and influence an adversary or selected foreign audience; as such, it provides leverage for our commanders. In the end, it may preclude the need to deploy additional forces, and it may reduce the period of an operation. As a non-kinetic weapon in the IO arsenal, PSYOP can also enhance the use of political, military, and economic instruments of national power. Though relatively cheap compared to the use of bombs and missiles, PSYOP can have a significant impact on an enemy's actions.

[psyob.htm](#)

PSYOP objectives can be general or specific. The general objectives are to reduce the efficiency of an enemy's fighting forces, advance US or multinational efforts by influencing the attitudes and behaviors of selected audiences, and obtain cooperation from multinational partners and neutral nations. Concerning specific objectives, PSYOP are used in support of other information operation elements. In addition, the specific objectives will depend on whether the activities are conducted in military operations other than war or in war itself. To view a list of specific objectives, click on one of the underlined links.

[psypr.htm](#)

An effective PSYOP campaign does not happen by accident. It takes time, coordination, and integration with campaign planners to get the biggest bang for the buck. There are a few principles that planners should follow to ensure the

effectiveness of a PSYOP campaign. First, the objectives should be clear and should correspond to the supported commander's vision of how the campaign should proceed. The objectives should also be consistent with concurrent diplomatic, economic, political, and informational efforts, and they should include a thorough analysis of friendly and adversary PSYOP capabilities, strengths, and weaknesses. In addition, planners must ensure that media messages are appropriate for and can be understood by the target audience. Finally, planners must evaluate PSYOP results to ensure that the activities accomplish the intended outcome.

#### openv.htm

As planners prepare PSYOP activities, they must consider the operational environment as it ultimately affects the outcome of PSYOP activities. In today's environment, US Forces conduct their jobs along side individuals from different services, agencies, countries, and cultures. Our forces must also be prepared to support all possible military options—whether it's sending a security force or providing humanitarian assistance—and they must continually adapt in an environment of ever-changing technology and increased information access.

Planners must also consider the operational environment of tomorrow. Instantly available information is creating a global community that is in touch with events as they happen from nearly anywhere in the world.

As technology continues to advance, the U.S. military's reliance on computers and technology to conduct PSYOP will increase. As a result, U.S. adversaries will take advantage of this reliance to advance their own agendas, and may even employ the

same technology against the U.S. We must be increasingly aware of our potential weaknesses and be prepared to change our tactics in order to protect U.S. interests.

[examp.htm](#)

Here are some examples of PSYOP print media employed throughout military history. Click on a link to view the example.

[just.htm](#)

As mentioned earlier, multiple PSYOP activities are often employed in tandem.

In December of 1989, troops were deployed to Panama to counter concerns for the safety of U.S. personnel, threats to U.S. interests, and instability within the Panamanian government and military.

At the strategic level, loudspeaker, radio, and TV assets helped minimize civilian interference and resistance to U.S. efforts. Use of these tools also helped foster support for both U.S. military operations and Panamanian government efforts to restore law and order.

At the tactical level, loudspeaker announcements and Commando Solo broadcasts tried to convince the enemy to surrender and helped to warn innocent civilians of harm. To circumvent hostile propaganda, the United States commandeered the national TV channel and established a 10,000-watt radio station. Also, posters and newspapers served to increase public awareness and neutralize hostile propaganda. Virtually all operations were successful as indicated by enemy surrenders, public

response, civilian compliance, absence of hostile propaganda, and the restoration of commercial information services.

#### future.htm

Future technological advances may affect how psychological operations are conducted in the years ahead. Sophisticated communication systems, already in place around the world, are capable of undermining U.S. information dominance and impeding operations.

Satellite systems are providing global coverage for communications, such as broadcast TV, and internet, in places where a wired infrastructure does not exist. The possibility of anytime, anywhere, high-speed data transmission and reception is nearly reality.

Unmanned Aerial Vehicles, in conjunction with these satellites, are capable of broadcasting real-time video from the battlefield—and possibly into your living room. Video insertion, morphing, and voice digitization technology could provide the ability to alter a person's appearance, their voice, and their message.

Digital archiving provides the capability to store and search vast amounts of video, sound, and print media.

Laser imaging and holographic projection may provide new dissemination methods. Instead of dropping leaflets or using loudspeakers, messages may be projected into the night sky where they could be read by entire cities.

In sum, PSYOP planners must be prepared to meet the challenges created by the technological advancements of the next century.

[sum.htm](#)

This lesson has introduced you to the concept of Psychological Operations. The lesson provided a definition of PSYOP along with the various publications, which provide doctrine for PSYOP. In addition to covering the categories, types, tools, key agencies, and the principles and objectives of PSYOP, the lesson discussed the current and future PSYOP operational environment. The lesson culminated by presenting some examples of PSYOP materials employed in the past and by discussing how advances in technology may affect future PSYOP operations.

[quiz1.htm](#)

Here are a few questions to test your knowledge of the previous lesson material. These questions are for your self-assessment only and are not recorded.

## Public Affairs Operations

[intro.htm](#)

No narration

[objsob.htm](#)

The objective of this lesson is for you to comprehend how Air Force public affairs operations are used in information operations. This lesson will enable you to understand how the media affects information warfare. You'll be able to explain how public affairs operations are used in informational flexible deterrent options and explain how themes, messages, and images are used to counter adversary propaganda.

[overview.htm](#)

To really understand public affairs operations' role in information operations, you need to understand the global information environment and see how today's media environment is different from what we faced in past conflicts. We'll then examine the concept of information as an instrument of national power and that it provides the theater commander informational flexible deterrent options. As an example, we'll look at a case study where PA operations aided a virtual force projection to achieve a national objective. We'll discuss how PA operations fit in with the IO planning cell considerations and, as a specific example, how PA operations can counter enemy PSYOP.

### glinfenv.htm

The first point to understand about today's global information environment is that the media is everywhere, even behind enemy lines as we saw in Desert Storm.

Furthermore, they can be in your living room almost instantaneously with raw, unedited scenes of the carnage of war. The second point to understand is that media attention on an issue can bring enormous pressure on political leaders. The Scuds falling in Riyadh and Tel Aviv had effects completely out of proportion to their military impact. The fallout of these points is that you should want to be the media's first and best source of information. The role of Public Affairs is to make sure your message is the one being received in living rooms across the world. The bottom line is that the media will find someone to talk to and if it's not you, it could be your enemy.

### media.htm

What are some of the consequences of the media being everywhere? First it makes it a lot harder to hide military actions. The proliferation of commercial imaging satellites would make the left hook used in Desert Storm a lot harder to pull off today and the Allied invasion of Normandy in WWII would be impossible. Secondly you can't lie. If you do, someone will find out the truth and then no one will ever believe you again. In the long run, the strategic value of public confidence in the integrity of your operation is far greater than the value of any fleeting military advantage that might come from lying. Not only that, it's also prohibited to engage in propaganda or

even censor or withhold information unnecessarily. The media has also caused a convergence of the tactical with the strategic. National and international media attention on an issue – particularly on events that provide powerful, graphical visual images -- can focus the attention of the nation, the world, and most importantly – national leaders onto an issue, thereby forcing US policy makers to take quick action in response. This is sometimes called the “CNN effect.” The “highway of death,” from Desert Storm, was the result of a tactical engagement of retreating Iraqi forces. Some of the images of this gave the impression that US technology was being used to slaughter hopeless Arabs just trying to get away. This perception put enormous pressure on US leaders to quickly end the hostilities. These are somewhat negative effects of the global information environment. However, on the positive side, the global information environment also provides a means for communicating our messages quickly and affordably to a global audience, providing an opportunity to achieve national security objectives through the strategic use of public information. Unfortunately this is a two-edged sword, for the enemy will have similar access and similar opportunities. Furthermore, as most US adversaries are autocratic regimes not concerned with the long-term value of their integrity and credibility, they will be all too quick to employ propaganda and unethical public information tactics against us in an effort to gain military or diplomatic advantage. Thus, the global information environment presents a vital battlespace for today’s modern warrior.

[pubinfbs.htm](#)

The objective in the public information battlespace is the most critical of centers of gravity: national will. The importance of national will has been recognized throughout

history. Sun Tzu called it moral influence, von Clausewitz saw it as the result of the proper balancing of the paradoxical trinity, and Douhet, an early airpower theorist, thought it so fragile that it could be destroyed by bombing the populace. The goal then is to protect and bolster our own national will and that of our allies while diminishing that of our enemies. Two ways PA operations can bolster our national will is to gain and maintain public support for our operations and by maintaining the morale of our troops. The enemy's will can be targeted by influencing their government's decision-makers and occasionally by direct appeal to the enemy populace. The instrument or weapon for these operations is a rapid flow of accurate, honest information. During Desert Shield, President Bush taped a message that was played uncensored to the Iraqi people. In it he explained that America had no quarrel with the Iraqi people, but only with its leadership.

[iop.htm](#)

The global information environment combined with information's impact on the national will has caused us to recognize that information is an instrument of national power. When combined with the economic, diplomatic, and military instruments of national power, an irresistible synergy can evolve. This synergy is recognized in the adaptive planning process as outlined in the Joint Strategic Capabilities Plan or JSCP. The JSCP directs combatant commanders to develop flexible deterrent options or FDOs to employ in those cases of peacetime instability. Informational FDOs are executed by PA operations, and—when combined with the other instruments of national power—can help to defuse situations without the use of force.

## lfdo.htm

How can the information instrument of power be used in FDOs? First of all, an open dialog with the media allows our leadership to gain and maintain public support for issues of national concern. By explaining national and coalition policies, aims, and goals, the public becomes informed before media speculation or enemy disinformation can erode public support. The adversary also becomes well informed of what's expected of them. This can be quite beneficial in those instances where formal diplomatic channels may be constrained. By keeping the issue in the news, pressure can be placed on an adversary denying them a possible *fait accompli* or victory through indifference. While our message is being presented to the world, we can expect the adversary to use the media to spread disinformation and propaganda to undermine our positions. By quickly providing complete and credible information, PA ops can contain, minimize, or counter such tactics by the adversary. We'll next look at how informational FDOs were used in an actual operation.

## haiti.htm

In 1994, the United Nations authorized the use of force to remove the military dictatorship that had seized power in Haiti. It called upon the US to help restore the legitimately elected government of President Aristide who was in exile. Public affairs operations were directed to educate the American public about the conditions in Haiti to generate public support. Public addresses by the President and interviews with military leaders demonstrated US resolve and capability. President Clinton dispatched a last ditch diplomatic effort led by former President Carter as one final attempt to bring a peaceful end to the standoff. As it appeared even this high-level

initiative would fail, President Clinton ordered a military invasion to restore democracy. However, national leaders made the decision to authorize the media to cover the pre-departure, boarding and take-off operations for the invasion. These were broadcast around the world in real-time. Watching these events unfold on television from Port-au-Prince and finally recognizing that months of diplomatic threats would now, in fact, be backed up with overpowering military force, the dictator acquiesced to the terms of the diplomatic team. Word of this concession was relayed back to Washington and from there to the already airborne military aircraft. Thanks to the success of this “virtual force projection,” their arrival and operations were virtually unopposed. Through a synergistic application of the diplomatic, military and information instruments of national power, bloodshed was avoided. More importantly, President Aristide was returned to power peacefully and American national security objectives were achieved.

#### [coordpa.htm](#)

The Haitian case study highlights the value of well-planned, well-coordinated PA ops. While much of the planning for public affairs operations has to be done after a crisis develops and circumstances begin to unfold, some planning work is done in advance. In deliberate planning, operations plans contain an Annex F which includes a strategic analysis of the theater’s information environment and anticipates the enemy propensity to use propaganda. It also provides a plan for the deployment of PA personnel and equipment and an organizational structure for their employment. Having these plans “on the shelf” and exercising them frequently ensures that “the PA weapon” can be rapidly and decisively employed even in times

of crisis. Most international crises in the post-Cold War world develop quickly and relatively unpredictably. The US government and its military responds to crises with contingency planning. Whenever tensions arise abroad, an Interagency Core Group, or ICG, comes together to develop and coordinate a broad national level information strategy. The goal is to ensure all agencies of the federal government speak with one voice to present a consistent message during the crisis. The ICG is chaired by the Under Secretary of State for Public Diplomacy and Public Affairs who leads the coordination between senior PA leaders representing key departments and agencies from across the US government.

At the task force level, public affairs personnel use the national level guidance to shape their planning when working with their commanders to support the CINC's strategic intent. The task force public affairs office, usually called a Joint Information Bureau or Combined Information Bureau, works with the unified command PA office to develop a detailed PA communication plan, or Proposed Public Affairs Guidance. Once this is approved by the task force commander, it is forwarded to the supported CINC's PA office for coordination and then on to the Office of the Assistant Secretary of Defense for Public Affairs. There it is coordinated within the Pentagon and with other appropriate federal agencies before a final version is released by OASD/PA as authoritative PA guidance. Disseminated worldwide to all command levels, this PA Guidance ensures all PA communications support the mission and sustains public trust at home and abroad.

[painio.htm](#)

Military operations in today's global information environment demand that PA operations be coordinated across the government and across the US military. However, they also have to be well coordinated with military plans at the operational and tactical level. A wise CINC will also make sure PA strategies and plans are well coordinated and integrated with the theater's information operations. Public Affairs operations play a key role in information-in-warfare because of its collection and dissemination activities. PA operations, though distinct from information warfare, may support IW activities—especially in the OPSEC and counter-psyop missions and must be well coordinated with any PSYOP and deception plans if they are to be effective. PA ops will also play a key role in maintaining morale and minimizing the damage of any successful enemy attack whether it be of a physical or information nature.

[painiiw.htm](#)

The information collection activities of PA operations allow them to fulfill their role as trusted counsel to the commander. By collecting and analyzing domestic and foreign news content, PA operations can monitor foreign and domestic public opinion and help to predict the likely impact that a commander's decisions and operational actions will have on troop morale and public opinion. Their unique insight into the media process can prepare commanders to deal effectively with the press. Their analysis will also predict issues likely to be used by enemy propagandists, thereby providing lead time for preparing and coordinating PA strategies and tactics. In this way, PA ops dissemination activities play a key role in sustaining public trust and

support for the mission and maintaining the morale of troops in the field and their families at home.

[pa\\_opsec.htm](#)

PA is the only organization authorized by DOD to release information to the public.

There is a delicate balance between maximizing operations security, or OPSEC, and leveraging the value of public information for deterring enemy behavior, sustaining allied support, maintaining political will at home and bolstering combat resolve in the field. Consider the consequences in Haiti if the dictatorship had not folded at the last minute—those paratroopers would have been greeted by a fully alerted resistance.

One method for managing this risk is to develop a critical information list, a detailed breakdown of information that should not be disclosed. All releases to the public must go through a security and policy review process to make sure critical information is not released and that the information proposed for release conforms with PA Guidance. In today's world, militaries of democratic nations do not practice battlefield censorship. Not only would censorship be a violation of the First Amendment but with today's technology and the number of media outlets usually present in a warzone, it would be logistically impossible to execute. The military can't prevent the media from reporting what they know. Thus, the key is for the military to carefully control the release of strategic and operational details. This principle of controlling what is released to the media rather than trying to censor what they print or broadcast is referred to as practicing security at the source. This principle is the cornerstone for how public affairs personnel interact with reporters in the field.

decept.htm

PA operations will not tell lies for the mission. In the long run, it's always counter-productive to do so. Lies destroy the credibility of the US government, our national leaders and all information flowing from the operation. Ultimately, this undermines the military mission and could even lead to its failure. Besides that, federal law prohibits it. Although military personnel can not lie to the media, nothing requires that they share everything they know. It's imperative that PA be informed of deception operations so that the proper issues get on the Critical Information List so deception operations are not compromised. Knowing the truth also prevents them from inadvertently telling lies. This all falls into the realm of deconfliction to prevent compromises, but PA can actually support a deception. You'll remember that the press was allowed to cover the Marine's amphibious assault exercises during Desert Shield. When the ground offensive began and an amphibious assault was not the centerpiece of the strategy, some members of the press complained that they had been duped about the amphibious assault. They have no grounds for this. Those exercises were real - not a lie. As part of a good deception, the Marines were a credible threat that reinforced notions held by Saddam and apparently some of the press that an attack would come from the sea. Indeed, the gunny sergeant didn't know if he would hit the beach with his young Marines. In fact, if the 1st MEF had bogged down in their drive up the middle, the assault might very well have happened.

### pa\_psyop.htm

PSYOP and PA ops are separate and distinct activities but closely related. Both reach foreign audiences with their messages. It's important that their messages and tactics be coordinated and deconflicted. Coordination allows a synergy to develop between the operations, but care must be taken to avoid tainting the PA message. PA strives for an accurate reporting of the facts. With the facts well understood, the objectives of PSYOP behavior modification appeals are achieved more easily. By building upon the truthful themes and messages used by PA ops, PSYOP can be much more effective.

### c\_psyop.htm

While we keep PA ops and PSYOP separate and distinct, our enemies are usually not so discriminating. Indeed the international media is often the favored channel of the enemy PSYOP campaign. It's cheap and readily available. The media pursue objectivity by presenting both sides of an issue. Enemy leaders will often find this an appealing opportunity. During Desert Storm, CNN preceded its reporting from Baghdad with the disclaimer that the report was censored by the Iraqi government. But the reports came through nonetheless. Since enemy propaganda operations are waged in the public information battlespace and they influence international opinion, national will, and the political guidance given to military commanders, it falls upon PA ops to counter them. PA operations do this with a timely flow of consistent messages through a variety of means and media.

[proptech.htm](#)

Because enemy propaganda operations can have such an asymmetrical impact on warfare, it's important to be able to recognize the most common propaganda techniques the enemy may use against us. Place your cursor over a term to see more information about it.

[c\\_prop.htm](#)

The best way to defeat enemy propaganda and lies is to plan for it and counter it with a rapid flow of your own truthful and accurate information. In Public Affairs operations, as with almost every other dimension of modern warfare, commanders are well advised to seize and maintain the initiative. During Allied Force, PA ops were coordinated so that the NATO nations had a press conference or some other major media event ongoing almost 18 hours of every day. This allowed NATO to frame the debate and occupy much of the public information battlespace. This made it harder for Serbia to get the airtime they wanted for their propaganda designed to erode support for NATO. Jamie Shea, the NATO spokesman for Operation Allied Force, outlined several other principles of wartime PA strategy in a speech he delivered following the campaign. Several principles Shea advocated included: Put your message in pictures. Pictures get you on TV and influence emotions. Words alone do not affect emotions or attitudes – no matter how compelling they may be. Expend the resources needed to give the media the pictures they can use. This means public affairs personnel must coordinate with operations and intel personnel ahead of time to get and declassify the powerful imagery needed to tell the operation's story in a compelling manner. Get complete, truthful information about an

event out first - especially on mistakes or blunders. As a general rule, he who speaks first frames the debate. Don't let a mistake become an atrocity by allowing the enemy's propaganda and lies to misrepresent an incident while you hunker down. Delays in responding will only make the damage that much more difficult to overcome. To counter enemy propaganda, your word must carry more weight than the enemy's. Just like one "oh shucks" can wipe out a dozen "atta-boys", your credibility with the news media can take decades to establish but be destroyed overnight. Successfully applying these PA ops tactics requires that PA be a central piece of the leadership team and well coordinated with all other aspects of the operation.

#### sum.htm

Today's global information environment has spawned the public information battlespace. With the ability to target a nation's very will and shatter alliances in an instant, public information has come to be recognized as an instrument of national power. PA operations take an equal footing with the other instruments of national power in providing flexible deterrent options for the CINC. As such, they're an integral piece of effects based operations strategies. As we saw in Haiti, the release of information through public affairs operations can be a valuable weapon for driving a crisis back to peace. In times of tension abroad, a broad strategy for national public affairs operations is hammered out through an interagency process. PA ops personnel at the joint task force level develop PA plans in the form of a Proposed Public Affairs Guidance message and coordinate it for DoD-wide release to ensure public trust and support and troop morale are maintained. The importance of the

public information battlespace and the capabilities that PA ops provide demand that PA operations be included in a commander's overall information operations plan. Coordination is required not only to avoid conflicts, but to maximize the support that PA ops can provide to many other IO capabilities and initiatives. In some cases, like countering enemy propaganda, PA ops may actually be the lead element in an IW activity. The keys to maximizing PA's contribution is proper planning for their use in IO and maintaining their absolute credibility by dealing only in the truth.

## Air Force IO Basics Course Summary

[sum.htm](#)

This course introduced you to the basic concepts of Information Operations. First, we reviewed many of the events of the Gulf War, highlighting some of the Information Operations conducted prior to and during that conflict. Where you able to pick out any Information Operations the first time through?

Next, we looked at the basic concepts of IO, using the Gulf War as a frame of reference to help illustrate the major elements. Hopefully, you were able to view the first Information War in a new light and with a greater appreciation for the contribution Information Operations had to the overwhelmingly successful victory in the gulf. Perhaps you will have a greater understanding of the IO implications of other historical events or of current and future events as they unfold throughout your life.

The ability to control and exploit information has been—and will always be—vital to the success of military operations. The Air Force recognized this importance by identifying Information Superiority as one of its six core competencies. One of the ways we achieve Information Superiority is by conducting Information Operations.

This course introduced you to the two pillars that support Information Operations: Information-in-Warfare and Information Warfare. You learned that the pillar of Information-in-Warfare consists of capabilities that help us gain and exploit information. These capabilities are based on integrated intelligence, surveillance and reconnaissance assets; information collection and dissemination activities; and global navigation and positioning, weather, and communications capabilities.

The pillar of Information Warfare, involves the defense and attack of information and information systems. The Defensive Counterinformation lesson covered activities conducted to protect and defend friendly information and information systems. The various Offensive Counterinformation lessons focused on activities conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems.

Other lessons dealt with the impact of the media on IO, the legal and ethical issues to be considered, and discussed the relationships and functions of the organizations that conduct these operations.

Now that you have a basic knowledge of IO, please take the time to test your knowledge of the course material. When you have completed the test, please fill out the short exit survey to provide us with feedback about the quality of this course.

Thank you for participating in the Air Force IO Basics Course.

## **AFIOBC Course Finale Instructions**

[test.htm](#)

Here are a few questions to test your knowledge of the course material. These questions are for your self-assessment only and are not recorded.