Chapter Six

U.S. MILITARY OPPORTUNITIES: INFORMATION-WARFARE CONCEPTS OF OPERATION

Brian Nichiporuk

INTRODUCTION

Information warfare is often seen as a new threat, a tool for adversaries to use against the U.S. homeland or U.S. forces. Numerous stories about break-ins at Pentagon computers, disabled satellites, and downed phone networks have focused the attention of the public and the national security community on the need for information-warfare defense. The possibility that these new information-warfare tools could threaten America's ability to project power or to realize its national interests is real and deserves analytical attention and public awareness. However, information warfare creates more than just vulnerability—it may also mean many new opportunities for the U.S. military. New information-warfare tools and techniques hold the potential for the United States to achieve its national security objectives using cheaper, more-efficient, and less-lethal methods.

Although these potential opportunities are a frequent topic of research and discussion within the defense analysis community, they have not received much attention beyond very specialized pockets of that community. This topic garners little outside attention, largely because the literature on information-warfare opportunities falls into one of two distinct categories: (1) broad policy and strategic-implications work and (2) highly technical feasibility studies. Research in the former is often too general to be of specific use to military planners. Research in the latter is often highly classified and compartmentalized. This chapter seeks to bridge the gap between the two by providing an operational-level view of how a set of offensive information-warfare concepts of operation (CONOPs) could expand the U.S. Air Force's capabilities to fight future wars (in the

2010–2015 time frame). It seeks to answer the question: How might the Air Force expand its doctrinal thinking about the systematic use of offensive information warfare to improve performance?[1]

What Do We Mean by "Information Warfare"?

One of the major features of information-warfare research is the potpourri of different definitions for the term *information warfare*. Without engaging in that debate, this chapter will simply define information warfare as the process of protecting one's own sources of battlefield information and, at the same time, seeking to deny, degrade, corrupt, or destroy the enemy's sources of battlefield information. This is taken to include six preexisting subareas that have only recently been grouped together under the heading of information warfare: operational security, electronic warfare (EW), psychological operations (PSYOPs), deception, physical attack on information processes, and information attack on information processes.[2] Since operational security is all about defensive information warfare, it is not as important to us here as the other five subareas. Therefore, offensive information warfare consists of the aggregation of EW, PSYOPs, deception, physical attack, and information attack.

EW encompasses the traditional concepts of jamming and spoofing radars and radio communication links. The Air Force's now-retired EF-111 aircraft and the Navy's EA-6B aircraft are good examples of traditional EW platforms. PSYOPs are all about using information dissemination to weaken the enemy's morale and, ultimately, to break his will to resist. Classical PSYOP techniques include the air dropping of propaganda leaflets and using airborne loudspeakers that broadcast demands for surrender to enemy troops. Deception involves the employment of physical or electronic means to camouflage one's own force posture in theater. Deploying dummy aircraft on the tarmac of a major air base or broadcasting radio situation

[1] Note that this chapter previously appeared in an earlier volume in the Strategic Appraisal series. It has been updated and is reprinted here because of its relevance to the present topic. The author would like to thank RAND colleagues Alan Vick, Martin Libicki, Jeremy Shapiro, and Zalmay Khalilzad for their insightful comments on earlier drafts of this chapter.

[2] This grouping is derived from Fig. 8 in Hutcherson (1994), p. 22, as well as Joint Staff (1996), Ch. 2.

reports in the clear from “phantom” or nonexistent units are two instances of deception that have been used in the past.[3] Physical attack is simply the act of physically damaging or destroying an adversary’s means of collecting, processing, and organizing information. This includes means as diverse as using aircraft to deliver dumb iron bombs to destroy a corps-level command bunker and using a high-powered ground-based laser to cripple an enemy communications satellite permanently. Finally, information attack involves the use of computer technology to electronically shut down, degrade, corrupt, or destroy an enemy’s information systems in theater. Viruses, logic bombs, and sniffers are but three of the “information munitions” that experts in this area commonly discuss.

Many authors tend to equate offensive information warfare with information attack. However, for a true appreciation of the breadth of offensive information warfare, it is really necessary to consider all five elements. Indeed, as we shall see later, a rich mix of all five gives the best chance for success in the information campaign.

The Importance of Offensive Information Warfare

Offensive information warfare is not a “new” way of attacking one’s adversary. To be sure, some of the current tools and technologies in this area are novel, but the goals of offensive information warfare today bear striking resemblance to those of the “military deception” campaigns of wars past. In short, while the means for offensive information warfare have changed, the ends have remained similar to those of yesterday.

Broadly speaking, the goals of an offensive information-warfare campaign are to deny, corrupt, degrade, or destroy the enemy’s sources of information on the battlefield. Doing so successfully, while maintaining the operational security of your own information sources, is the key to achieving “information superiority”—that is, the ability to see the battlefield while your opponent cannot.[4] In

[3] Deception may appear to be a purely defensive tool at first glance; however, deception operations have been used throughout history as integral parts of information campaigns that were heavily offensive. Therefore, in this analysis, deception will be considered to be part of offensive information warfare.

[4] For an overview of how important information superiority in general will be to the United States in future conflicts, see Joint Chiefs of Staff (1996).

today’s era of smart weapons and compressed decision cycles, there can be little doubt that the acquisition of information superiority in conventional warfare goes a long way toward achieving final victory.

History provides multiple examples of previous uses of “old-fashioned” offensive information warfare.[5] In the Revolutionary War, American agents supposedly inserted forged documents into British diplomatic pouches as a way of convincing the British that George Washington’s army was far larger than it actually was. During World War I, the U.S. Army in France executed an important deception operation called the “Belfort Ruse” before a major attack on St. Mihiel. The Western Allies in World War II accomplished what was perhaps one of the largest “information warfare” successes in history when they fabricated the Calais invasion force in 1944, fooling some German leaders (including Hitler) into believing that the invasion of Northwest Europe would come at Calais, which is well to the north of the actual Allied landing sites in Normandy.[6] All of these historical examples involved the types of tactics that an early 21st century defense analyst would place in the category of offensive information warfare.

Despite the fact that information-warfare campaigns have occurred before, it is now possible to say with confidence that information-warfare campaigns are a relatively more important part of conventional wars than they have been in the past. The increased importance of information-warfare campaigns to the United States in general and the Air Force in particular is due to a combination of technological, doctrinal, and force-structure factors. First, the growth in information technologies is making offensive information warfare a more potent instrument against enemy militaries. As such, offensive information warfare offers new possibilities and options to the regional commanders in chief (CINCs) when they prepare their war plans. As part of a recognition of these new options, U.S. military doctrine is moving away from the platform-centric warfare of the Cold War toward a new concept of network-centric warfare (Cebrowski and Garstka, 1998). In network-centric warfare, information superiority is an essential ingredient of success. Finally,

[5] The historical examples provided here are drawn from Hutcherson (1994), pp. 23–24.

[6] For a succinct account of the Allied deception campaign before D-Day in 1944, see Ambrose (1994), pp. 80–83.

America's shrinking conventional force structure demands innovative solutions to emerging problems. As the number of U.S. wings, divisions, and combatant ships declines, U.S. commanders will increasingly rely upon advanced information technology and computer-savvy soldiers to gain the upper hand against adversaries in conventional warfare.

In recognition of this fact, this chapter will develop and elaborate four CONOPs that rely on offensive information warfare. Each CONOP is designed to counter some of the new (and not so new) asymmetric strategies that U.S. opponents are likely to use in future regional conflicts. The first section therefore discusses how the use of such strategies by regional adversaries could make the tasks of the Air Force more difficult. A rich literature on asymmetric strategies already exists, so the discussion here will be heavily derivative. Nonetheless, to set the stage for the proposed CONOPs, this section will lay out the types of asymmetric strategies posing the greatest threat to the United States. The second section presents and evaluates four offensive information-warfare CONOPs that appear to be promising countermeasures to this menu of asymmetric options. The chapter concludes with a third section that evaluates the utility of each of the CONOPs presented.

EMERGING ASYMMETRIC STRATEGIES

The lopsided American victory in Desert Storm and the successful NATO eviction of Serb forces from Kosovo in 1999 both featured clear displays of the vast margin of superiority the U.S. Air Force holds over any conceivable adversary. Most analysts agree therefore that, in future wars, hostile regional powers will use asymmetric options to counter the U.S. advantage in airpower. To organize our thinking about the contributions that offensive information warfare–oriented CONOPs could make toward defeating these asymmetric strategies, we need to begin by listing and categorizing the different strategies. As was noted earlier, a rich literature on asymmetric strategies has developed over the past few years.[7] The work on

[7] Two examples of this literature are unpublished manuscripts by Marcy Agmon et al. and by Kenneth Watman, both of RAND.

asymmetric strategies has revealed three types of enemy options the United States needs to be concerned about:

- increasing capabilities in selected niche areas
- enemy strategies that target key U.S. vulnerabilities
- creation of political constraints that hinder U.S. force deployments.

Increasing Niche Capabilities

Regional powers could achieve significant niche capabilities in a number of areas. However, the two that present the greatest cause for alarm are surely the acquisition of weapons of mass destruction (WMD) and improvements in command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR) networks.

Enhanced WMD Inventories and Delivery Systems. Several regional powers have stockpiles of biological and chemical weapons, along with the means to deliver them. Making this already difficult problem even more complicated, some regional powers (e.g., Iran, North Korea) may soon come into possession of what can be termed a mature small nuclear arsenal. This would be an arsenal of at least five or six secure and deliverable nuclear weapons supported by a reliable command and control and early-warning network.

The possession of a mature arsenal of nuclear, chemical, or biological weapons by a hostile regional power could restrict airpower's freedom of action.[8] It would be relatively easy for the leadership of that regional power to interpret many types of air strikes that U.S. Air Force planners would regard as strictly "conventional"—such as attacks on air defenses, command and control systems, or mobile missile launchers—as attempts to destroy, or at least degrade, its modest nuclear deterrent.

It is difficult to predict the reactions of small leadership groups in closed states, such as Iran, Iraq, and North Korea, to U.S. air opera-

[8] This concern may become one of more than academic significance to U.S. military planners if President George W. Bush decides to expand the war on terrorism to include military strikes against the "New Axis" nations—Iran, Iraq, and North Korea.

tions that threaten their deterrent. Clearly, if the enemy leadership comes to perceive a U.S. conventional air campaign as part of a thinly veiled counterforce plan, the risk that the adversary will escalate to nuclear use increases.[9] The adversary's homeland might evolve into a kind of sanctuary in which large masses of U.S. combat aircraft and cruise missiles could not operate freely because of concerns about escalation to WMD.[10] We will see later on that offensive information-warfare tools, working in concert with small packets of strike aircraft, could be a mechanism for both regaining some operational freedom and reducing the risks of escalation in a sanctuary-type environment. Offensive information-warfare tools can achieve this purpose because they can temporarily degrade or disrupt elements of an adversary's early-warning and air-defense systems without permanently destroying them. This reduces the chances that a U.S. air-defense suppression campaign will be interpreted as veiled counterforce.

The emergence of a homeland sanctuary in wartime would have concrete implications for Air Force planners and operators. Specifically, the enemy's leadership, national command and control, and internal security networks would all become harder to target. Supply and communications for enemy ground forces could not be disrupted on a regular basis, and a large chunk of the enemy's industrial warmaking capacity (including electric power generation and telecommunications capacity) would be essentially off limits to the orthodox offensive use of airpower.

U.S. leaders could choose not to let the enemy establish a homeland airspace sanctuary. If the U.S. leadership is not highly risk-averse, it could deal with WMD in other ways besides offensive information warfare. The United States could, for example, threaten massive nuclear retaliation for any adversary use of WMD and then proceed to carry out an air campaign against the enemy homeland under the assumption that the threat of escalation dominance by the superior U.S. nuclear arsenal cancels out the enemy's nuclear capability. Another option would be to mount a conventional counterforce campaign aimed at destroying the enemy's WMD capabilities and

[9] For a discussion of related issues, see Wilkening and Watman (1995).

[10] This sanctuary concept was first proposed by RAND colleague Alan Vick in internal discussions in late 1996.

delivery systems (ballistic missiles, cruise missiles, and fighter-bombers) before they could be employed. Yet a third alternative would be to hurriedly develop and deploy effective theater missile defense systems that would have the effect of reducing an adversary's expectations of the damage he could inflict should he attempt to use WMD against U.S. allies or forces in the field.[11] A future U.S. president could well select any of these approaches. However, in the event that the national leadership is highly risk-averse in a future major theater war (MTW), it behooves the Air Force to plan to deal with scenarios in which much of an enemy's homeland is off limits to sustained aerial attack.

Improved C^{4}ISR Capabilities. The information revolution that is now sweeping the world will create more opportunities for regional powers to access advanced space-based communications and reconnaissance systems. Much of this increased opportunity will result from having relatively easy access to multinational commercial assets; some will come from being granted access to dedicated military satellites owned by major powers that could become hostile to U.S. interests (e.g., China, Russia, India); and yet a smaller amount will be due to the development and exploitation of indigenous capabilities.

The proliferation of space-based military and commercial capabilities for both imagery and communications will offer tremendous opportunities for regional powers to increase their capabilities, bringing them closer to those of the United States. The greatest concern in terms of space-based imagery is the proliferation of foreign systems with resolutions equal to or below 5 m. This threshold is critical because 5 m is the level at which one can discern large, soft military targets—such as ports, air bases, and defense ministry buildings—in a theater with enough accuracy to target them specifically using cruise or ballistic missiles, especially if these weapons are Global Positioning System (GPS)–guided.[12] By 2002, France, Israel, India, and Russia will have deployed commercial or military systems

[11] For a review of the recent course of the U.S. missile defense program, see Graham (2001).

[12] See Air Force Space Command (1996), p. 24. Recent RAND analysis has made some quantitative assessments concerning the impact of GPS guidance upon the cruise and ballistic missile accuracies likely to be achieved by the militaries of hostile regional powers. See Pace et al. (1995), especially pp. 45–91.

capable of 5-m accuracy (Air Force Space Command, 1996, p. 24; Stoney, 1997). However, the available evidence suggests that no midsized regional power will be able to build its own spaceborne imagery satellites by 2010.

Growth in communication satellites will be more explosive than for imagery systems. There are plans for a whole host of new commercial space communication systems in both low earth (LEO) and geosynchronous orbits (Keffer, 1996). Some of the planned geosynchronous systems will exploit the Ka-band and will use cross-links between satellites to minimize the need for ground stations. Experts predict that, by the end of this decade, there will be two or three new global Ka-band geosynchronous systems and at least one or two "Big LEO" global constellations. Some of these systems will bring massive capacity increases into the world market. As an example, the Hughes Spaceways Ka-band geosynchronous system is projected to have a capacity of 88 Gb/s. This can be compared to the current total Department of Defense requirement for satellite-communication capacity, which is a mere 12 Gb/s (U.S. Space Command, 1997, p. 4-14). At least five such Ka-band systems have been planned for the near future.

Important advances are also occurring in transoceanic fiber-optic technology. Satellite communications may be the optimal solution for mobile military users, but fiber-optic connectivity is probably the most efficient communication option for fixed military users in rear areas. Research into such areas as wave division multiplexing promises to produce per-fiber capacities of up to 160 Gb/s.[13] The number of transoceanic fiber-optic lines is increasing as well, with many large new projects, such as the FLAG line from England to Japan, now entering service.

The upshot of this proliferation of highly capable commercial imagery and satellite and terrestrial communications is that it will be easier in the future for hostile regional powers to have access to the type of C^4ISR architectures that only the most advanced militaries could access a few years ago. This applies for both voice and data transmissions. The sheer number of available redundant commercial

[13] For an overview of technological developments in the field of undersea fiber-optic lines, see Submarine Systems International (1997).

routes and links will make it almost impossible for the United States to deny service to the adversary on a large scale for a long period of time—because too many communication “choke points” would need to be destroyed, disrupted, or corrupted. However, large-scale service denial for short periods during a theater campaign may still be possible, and such denials would indeed have military significance.

Increased access to overhead imagery will allow regional powers to monitor U.S. and allied force deployments both into and within a theater with greater fidelity than was possible before. The greatest military impact of this new capability is the availability of accurate and timely targeting data to aid in the planning of rapid ballistic- and cruise-missile strikes against air bases, port facilities, and logistics stockpiles being used by U.S. forces in the region.[14] Increased access to highly capable communication systems will lend regional powers the potential for much more timely control of their forces in theater. Decision cycles for these militaries could decrease dramatically. Furthermore, the ability to access large, new international communication networks could facilitate a regional power’s offensive information warfare against the Department of Defense’s worldwide command and control systems.

Enemy Strategies That Target Key U.S. Vulnerabilities

Another asymmetric option available to regional adversaries of the United States is the use of strategies that threaten key U.S. vulnerabilities and centers of gravity. Such strategies and tactics would be most effective in conjunction with the improved capabilities discussed above, but they could also pose a threat if used on their own. Three strategy types merit consideration: short-warning attacks, antiaccess operations, and deep-strike operations. Each will be covered briefly below.

Short-Warning Attacks. The first strategy that could be used would be a so-called standing-start attack, in which the U.S. intelligence community has little warning of an impending attack. Such an attack would take place before any major U.S. deployment to the region had begun.

[14] See Stillion and Orletsky (1999), Chapters Two and Three.

A short-warning attack would force the Air Force either to fight with major early disadvantages or to take time to build up its strength in the theater, thus letting the regional adversary make some initial territorial gains. This would be a difficult decision to make. If the President and the Secretary of Defense elected to commit combat aircraft immediately to battle against a standing-start attack, the Air Force might have to operate initially without its normal complement of critical enabling assets, such as tankers, the Airborne Warning and Control System, the Joint Surveillance and Target Attack Radar System, jamming aircraft, and dedicated air-defense suppression aircraft. In such a situation, the Air Force also could find itself at a heavy numerical disadvantage in early air-to-air engagements.

The upshot is that the Air Force could suffer significant losses in the early phase of a standing-start attack, especially if the opponent possessed advanced surface-to-air missile systems.[15] Risks would also be involved if the President and the Secretary of Defense chose to delay their response until U.S. forces were fully deployed. Serious political implications could result from the territorial losses that a local U.S. ally would almost certainly suffer in a delayed-response scenario. While most conceivable short-warning attack scenarios would not result in an ultimate U.S. defeat, they would almost certainly all extract a greater price in terms of blood and treasure.

Antiaccess Operations. Perhaps the cardinal mistake the Iraqis made during Desert Shield and Desert Storm was the six months of unhindered deployment and buildup time they gave to coalition forces before the January 1991 commencement of hostilities. During the height of a deployment of U.S. forces into a theater during an MTW contingency, future regional adversaries will have greater opportunities to avoid the error the Iraqis made and to mount strike operations designed to hinder U.S. access to critical points in the battlespace. This would likely be done through the use of missiles, unmanned aerial vehicles (UAVs), mines, and aircraft to damage and/or shut

[15] Of special concern here are the advanced "double digit" Russian-made surface-to-air missiles, like the SA-10. Russia is marketing these systems to several countries that could become military adversaries of the United States. China, for example, already deploys a version of the SA-10.

down both aerial and sea ports of debarkation in the region so as to cut down the throughput capacity of such facilities.[16]

Although the Air Force is attempting to diminish the threat of antiaccess operations by shaping itself into an expeditionary force with enhanced force-protection capabilities, the realm of offensive information warfare should also offer possibilities for mitigating the antiaccess threat.

Deep-Strike Operations. The final threat in the area of strategies and tactics has to do with deep-strike operations that a regional adversary could mount during the counteroffensive stage of an MTW, the phase during which U.S. forces would be fully assembled in theater and attempting to roll back any initial gains that the adversary had made. During this phase of an MTW, the logistical demands of major ground and air offensive operations will compel the United States to amass large stockpiles of fuel, ammunition, and spare parts throughout the rear areas of the theater. Major scripted offensive operations would also force U.S. air bases in the region to operate at a high tempo, possibly with little room for slack. These realities would create tempting targets for an adversary's remaining cruise and theater ballistic missiles. While the aforementioned antiaccess operations would concentrate on disrupting and delaying a U.S. deployment into theater, the goal of deep-strike operations would be to slow down and prolong a U.S. counteroffensive so as to keep U.S. forces off balance and to inflict greater casualties, possibly breaking down the U.S. national will to continue the campaign. Likely targets for adversary cruise and ballistic missiles in the deep-strike campaign would include ammunition and fuel storage sites throughout the theater, air bases, the theater air operations center, early-warning radars, anti–tactical ballistic missile batteries, ports, troop concentrations, and headquarters.

Political Constraints on U.S. Force Deployments

Not all of the troubling asymmetric options available to a regional adversary involve military means. Indeed, some of the most potent options may be political and diplomatic. There are a variety of diplomatic tactics available to a smart regional adversary for the

[16] Stillion and Orletsky (1999), Chapters Two and Three.

purpose of complicating U.S. military deployments. The goal of such tactics would be to intimidate potential or existing U.S. allies to back out of political coalitions or at least to deny the use of their air bases to U.S. forces. The blunt approach for an adversary would be to attempt direct coercion against a U.S. ally by threatening that ally's cities with WMD attacks from theater-range delivery vehicles. More-nuanced political strategies could include furnishing support to opposition groups in allied countries and encouraging them to foment civil unrest during a crisis. An alternative approach for regional adversaries would be to emphasize carrots over sticks by promising substantial political and/or economic rewards to their neighbors for keeping U.S. airpower off their soil.

Denial of U.S. access to theater bases would most likely force the Air Force to adopt a standoff approach to combat—that is, conducting air operations from bases outside the immediate theater. The Joint Forces Air Component Commander (JFACC) would face a number of penalties as a result of the need to pursue a standoff CONOP, including lower sortie rates for strike and counterair operations, greater demands on the tanker fleet, reduced chances of rescuing downed aircrews, increased pressure on heavy bombers and cruise missiles to hit deep fixed targets because of a lack of alternative delivery vehicles, a substantial degradation in the capability to hold critical mobile targets at risk, increased difficulty in supporting U.S. and allied ground forces, increased aircrew fatigue, and greater maintenance turnaround times. Indeed, early reports indicate that the fall 2001 air campaign against the Taliban and Al Qaeda in Afghanistan faced exactly these kinds of problems while it was being run largely from distant bases.

A recent RAND study examined the operational effects of using a standoff strategy in response to an adversary's employment of chemical or biological weapons against close-in air bases. The study found that a 600-mile standoff range in Southwest Asia reduces the Air Force's sortie rate by approximately 25 percent; in Northeast Asia, a 500-mile standoff range reduces the sortie rate by roughly 30 percent.[17] Such reductions could result in a substantially longer and bloodier conflict than would otherwise be necessary.

[17] Chow et al. (1998), pp. 66–78.

DEVELOPING OPERATIONAL CONCEPTS FOR FUTURE OFFENSIVE INFORMATION WARFARE

Now that we have identified the major asymmetric options available to regional adversaries, we can begin to think about the role of offensive information warfare in improving U.S. chances of dealing successfully with such challenges. Figure 6.1 maps each of the asymmetric options outlined above to a CONOP using offensive information warfare that provides a possible way to negate the enemy's strategy. The following subsections will discuss each of the potential offensive information-warfare CONOPs in detail. Here, we will only provide a preview.

Short-warning attacks can perhaps best be dealt with through effective regional deterrence strategies. The "information-based deterrence" CONOP attempts to expand upon previous notions of deterrence by using an array of information technologies to affect an opponent's perception of the overall political and military situation in his region during peacetime or during a crisis.

WMD possession and base denial are grouped together because both strategies have to do with an adversary striving to decrease the Air Force's freedom and capability to operate over his homeland on a sustained basis. We attempt to address these through a CONOP enti-

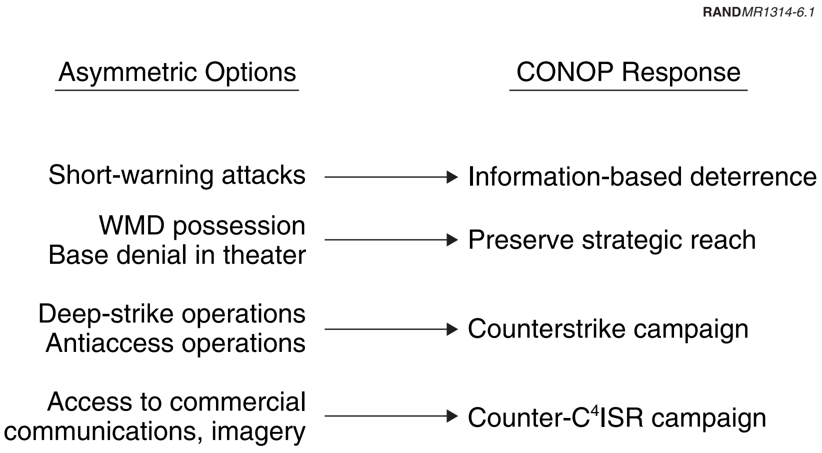

Figure 6.1—Adversary Asymmetric Options and Potential U.S. CONOPs

tled “preserve strategic reach,” which seeks to use offensive information warfare to suppress enemy air defenses to facilitate conventional strategic air attacks upon selected targets in the enemy homeland.

Next, there is the risk that the enemy may mount antiaccess and deep-strike operations. Both these asymmetric options involve the use of relatively new technologies (e.g., GPS-based targeting) to strike at U.S. and allied rear areas. The “counterstrike campaign” CONOP is a possible remedy. Counterstrike also uses a variety of offensive information-warfare tools, this time to disrupt an enemy’s strike-planning and execution functions.

Finally, the increasing ability of regional powers to exploit space-borne communications and imagery assets is mapped against a CONOP called the “counter-C^4ISR campaign.” Counter-C^4ISR uses a variety of offensive information-warfare tools to disrupt an enemy’s ability to collect and process information gained from overhead assets.

Information-Based Deterrence

The overarching goal of the information-based deterrence CONOP is successfully manipulating the attitude of a potential adversary during peacetime or a crisis to prevent him from ever attacking an ally. Such efforts have been made in the past, but technological growth is creating opportunities to increase the power of information campaigns aimed at either long- or short-term deterrence.

Information-based deterrence strives to sow doubt in the mind of a potential adversary about the likely outcome of his aggression. This can be done in three ways: turning international opinion against the aggressor, altering his perception of the military correlation of forces in theater, and fostering instability in his country. Information-based deterrence does not require a pure strategy; it can include a combination of two or three options, depending on the circumstances. Although these three mechanisms could also be used during wartime itself as a means of coercing an enemy, history demonstrates that wartime coercion is much more difficult than is deterrence. Therefore, the U.S. military would have a better chance of success with these mechanisms using them within the context of a deterrence effort.

Three cautions are important when discussing perception-shaping strategies against other states. First, in recent times, technology has often outpaced international norms and standards. We still do not have a clear sense of which types of perception-shaping activities will be construed as legitimate peacetime behavior and which as casus belli by international organizations and institutions. Therefore, to reduce the risk of inadvertent escalation, it will be necessary to rethink our doctrine for perception shaping periodically in accordance with developing international norms and standards.

Second, perception-shaping activities carry a constant threat of "blowback": Operations designed to manage the opponent's perceptions may end up distorting our own perceptions to an equal or even greater extent. For example, while it may be advantageous to convince the enemy that U.S. forces are more capable than they actually are, it would be less helpful to convince oneself of that fiction. Yet, because of the need for consistency and secrecy to accomplish perception-shaping objectives, these two effects are, in practice, not completely separable.

Third, deterrence of any sort relies on convincing the adversary not to act. While our actions can affect the adversary's calculus, we must always be prepared for deterrence to fail. For our purposes, this reality means that information-based deterrence is not the complete solution for short-warning attacks. Other means must be developed to cope with the possible failure of information-based deterrence.

Turning International Opinion Against the Aggressor. A major U.S. strength lies in its ability to create wide coalitions against potential enemies that can isolate opponents from external support, both material and moral. Such coalitions reinforce U.S. combat power, reduce enemy access to critical supplies, and provide a greater legitimacy for U.S. action—a legitimacy that solidifies domestic U.S. support for deterrence actions and war, if that becomes necessary. Repeatedly, U.S. leaders have stressed that U.S. forces will only engage in a multilateral context. An increased likelihood of such a coalition will therefore have a deterrent effect on potential foes.

Creating and maintaining such coalitions require that international opinion views U.S. foes as aggressors with little regard for international law or human rights. Optimally, such a coalition would be sustained by a continuous and long-standing information campaign.

However, new conflicts and enemies can arise, and U.S. leaders must be prepared to cut such coalitions nearly from whole cloth. Particularly in the case of a short- or no-warning attack (such as occurred on September 11, 2001, in New York and Washington, D.C.), prospective foes will take great care to hide their intentions until shortly before hostilities break out. Preventing and responding to short-warning attack or responding to a no-warning attack therefore may necessitate a rapid-reaction information campaign that is prepared to foster the appropriate climate of international opinion.

In the short period before the outbreak of hostilities, a rapid-reaction information campaign has two basic parts. First, television and radio broadcasts of accurate information from U.S. sources should show enemy intent and preparations for attack. Second, the information campaign should include television and radio broadcasts that demonstrate both U.S. friendly intent and allied military prowess. These broadcasts should go to enemies and prospective allies, as well as to domestic audiences.

Both before and after hostilities break out, short-warning attacks often provide ready material for images that will outrage and inflame international opinion against the aggressor. Such attacks will typically require such preparations as the loading and unloading of trains, massing of supplies and forces, and shock attacks by rapidly moving forces. Capturing these preparations and attacks on video or satellite imagery will demonstrate the enemy's aggressive intent, give the lie to any pretext they might have established for invasion, and serve to catalyze international opinion and support for a broad coalition to oppose aggression. There is some historical precedent for the use of simple images as a tool for marshaling international opinion against an aggressor. During the Cuban Missile Crisis, for example, aerial reconnaissance photos of Soviet missile sites in Cuba helped strengthen the U.S. position at the United Nations.

Increasingly, the independent media can be counted on to capture and broadcast this information. However, some countries still maintain fairly effective control over even foreign media outlets operating in their territory. To avoid leaving such things to the intrepid action of individual reporters, information deterrence could be aided by a rapid-reaction information force that can quickly establish video surveillance of potentially hostile territory. UAVs equipped with video equipment and command planes capable of gathering, editing, and instantaneously disseminating that coverage are the essential features of such a force. If the risks of such aircraft being shot down or identified over enemy territory are too great, one could even use satellite imagery to provide evidence of mass graves, burned-out villages, etc. At the same time, U.S. leaders would need to work hard to counter enemy propaganda campaigns by tirelessly presenting the major elements of the true situation on a wide spectrum of information outlets (Internet, television, radio, etc.). Video coverage of the battle area will help expose any enemy attempt to portray U.S. actions in a deceptive light. Great effort needs to be expended to provide counterevidence for the inevitable enemy propaganda campaign. Good video images can make ruses—such as the Iraqi attempt to portray a U.S. attack on a military target as an attack on a facility that served solely as a baby-milk factory—nearly impossible.

It is critical that such a campaign maintain a consistency of message and purpose throughout its broadcasts. This kind of campaign should make no effort whatsoever to deceive or manipulate the international media, concentrating instead on the simple goal of using modern technology to highlight the hard physical evidence of a rogue state's or nonstate actor's aggressive intentions. Deceptive techniques are unnecessary and counterproductive in this context. In an age of numerous media outlets and largely unconstrained information flows, it makes little sense to risk American credibility as an honest international citizen by manufacturing video images.

Altering the Enemy's Perception of the Correlation of Forces. When leaders of the various ex-Yugoslavian factions met at Dayton, Ohio, to divide zones of control in Bosnia, the U.S. military provided satellite imagery to assist in the demarcation of borders. To the shock of the participants, the imagery demonstrated a knowledge of terrain and force dispositions far in excess of what the participants had previously believed possible. Indeed, the imagery showed a three-dimensional picture of the contested areas that demonstrated a more detailed knowledge of the participants' own forces than the parties themselves possessed. All sides now understood that the U.S. military could see virtually anything on the battlefield; the implicit threat was that it could destroy anything it could see.[18]

[18] For accounts of this episode, see Watters (1996); Libicki (1997), Ch. 3; and Nye and Owens (1996), p. 32.

While such knowledge was useful in negotiating the peace, it might be even more useful in deterring a future MTW. The U.S. military, particularly the Air Force, excels at simulation, which it uses to train its troops in conditions as realistic as possible. These simulations can similarly be used to demonstrate U.S. combat power, without actually employing it. Indeed, in the summer of 1998, NATO carried out simulated air raids over Kosovo as a deterrent to further Serb repression in that province. Realistic simulations have a tremendous capacity to impress an enemy's population, frighten his soldiers, and radically alter the enemy's assessment of U.S. military power. Such simulations would include images of U.S. military equipment operating, simulated attacks on significant military targets, and broadcasts of past U.S. combat successes. While these simulations and replays will certainly give insight on actual U.S. combat capabilities, they need not always reflect actual U.S. capabilities or intentions. As noted, if a simulation is realistic enough, it will create such a strong image in the mind of the adversary that it will irrevocably alter his perception of the correlation of forces, regardless of actual U.S. capabilities.

Fostering Instability. Every society contains divisions simmering below an often calm exterior. Nondemocratic societies, especially, contain latent tensions that, if exploited, can severely limit a country's ability to engage in offensive military action. Offensive information warfare offers many new covert means to exploit the tensions because it increases the opportunity to communicate directly with constituent parts of the adversary's society. As the information revolution increases the number and types of communication channels within any society, the opportunities to introduce false data into communication links between constituent parts of the society also increase.

It should be noted that fostering instability is the riskiest of the three methods of information deterrence. It should only be used against nations that pose a particularly grave military threat. It is also the most difficult method to implement as it requires a detailed understanding of the target society and the cultural context in which such action will be received. Inappropriate or clumsy efforts to foster instability may well create unity in an otherwise divisive polity by providing evidence of an external threat to the nation. The United States should not attempt this type of tactic unless it possesses an experienced cadre of intelligence analysts who have proven themselves to have an extremely high degree of cultural understanding and sophistication with respect to the target state.

Nonetheless, by exploiting cleavages among the government, the population, and the military (the so-called Clausewitzian trinity), it could sometimes be possible to convince the adversary leadership that its hold on power is fragile and that it thus cannot afford any type of military contest, let alone one with the United States. There are many ways such an approach could be pursued. False messages inserted into national communication networks could be used to create mistrust between the civilian and military leaderships by spreading rumors of military coup plots or planned purges against the officer corps. Support to nongovernmental organizations operating on the Internet could be used to spread popular disenchantment with government policies and to foster public protests against the regime. The United States could also use media organizations in the target country and its neighbors as a lever to influence public opinion in the adversary state and turn that opinion against its own government's policies. Finally, the low-technology approach should not be forgotten: Leaflets dropped from U.S. aircraft were extremely effective during the Gulf War in convincing Iraqi troops to surrender (Hosmer, 1996).

Some nations will be far less vulnerable to such measures than others by virtue of their closed political systems. However, as time goes on and as international connectivity increases, there will be fewer and fewer nondemocratic nations that can be sanguine about their ability to insulate themselves against the effects of a well-coordinated information strategy exploiting the mass media, the Internet, and proprietary communication networks.

Preserving Strategic Reach

The prospect of facing regional adversaries with mature nuclear arsenals raises questions about how much freedom the Air Force will have to conduct parallel warfare against the enemy homeland without substantially increasing the risk of escalation. The prospect of having local allies deny the U.S. Air Force the use of bases in the theater means that it may be prohibitively expensive and dangerous to employ air assets over the enemy's territory for the reasons outlined above.

The "preserving strategic reach" CONOP is intended as a response to these emerging challenges. The chief mechanism of preserving strategic reach is the periodic use of offensive information-warfare means to degrade the enemy's integrated air-defense system (IADS).[19] The significant degradation of the enemy IADS would allow the U.S. Air Force to operate over enemy territory in reasonable safety and, given well-chosen targets, with much less fear of nuclear escalation. As with information-based deterrence, however, preserving strategic reach may not be the final solution to these problems. Using offensive information warfare will not eliminate the possibility of escalation and will not completely make up for the loss of theater bases. Nonetheless, it represents an important part of the response to these relatively new challenges.

More-conventional operations to suppress enemy air defenses that use physical attacks, such as those mounted by F-16s equipped with High-Speed Anti-Radiation Missiles, contain a risk of escalation when used against an adversary with WMD. The adversary leadership may not be able to distinguish such an operation from an attempt to destroy nuclear warning and command and control systems in preparation for a counterforce attack designed to eliminate the adversary's nuclear deterrent. Such operations also require putting friendly forces at risk and are particularly difficult and dangerous to launch from a standoff posture. Offensive information-warfare operations contain a much smaller risk of escalation because they need not involve physical attacks on command and control systems and because they can be done covertly. They do not put friendly forces at risk and are not affected by the loss of theater bases, because they can be launched just as easily from outside the theater.

Any IADS contains information systems and information-based processes that are essential for its operations and that are lucrative targets for offensive information warfare. Schematically, an IADS consists of one or a few air-defense headquarters connected by communication links to sensors, such as early-warning radars, EW sensors, or aircraft like those for the Airborne Warning and Control System. Each headquarters also communicates with and controls a

[19] An IADS includes surface-to-air missiles, antiaircraft artillery, air-superiority fighters, and the communication and sensor infrastructure that connects them.

variety of antiaircraft weapons, such as fire-control radars, missile launchers, and air-superiority fighters.

Without physical destruction, offensive information warfare can attack an IADS at three points. First, offensive information warfare can attack the system's sensors, either degrading their ability to gather information or feeding them false data. Second, offensive information warfare can degrade or plant false information in the communication links between headquarters and the sensors or shooters. Third, offensive information warfare can degrade or deceive the information processes that compile the sensor information, interpret it for human decisionmakers, and assign particular weapons to targets.

The centralized nature of this system implies that the air headquarters is a critical choke point, the disabling of which will render the entire system useless without the need to disable every sensor and weapon. This point should not be taken too far, however. An IADS can be configured to work in several modes from centralized to fully autonomous. The characteristics of these systems in each different mode should be well understood because information munitions that prove effective against an IADS operating in centralized mode may be ineffective against the same set of surface-to-air missile batteries and sensors operating in autonomous mode. Indeed, in autonomous mode, the local air-defense headquarters may not even be that significant to the overall function of the system.

The decision about which part of the system to attack therefore depends on the reason for using offensive information warfare to bring down the IADS. If escalation to WMD is a concern, the emphasis should be on allowing the enemy to believe that the IADS is still functioning even as one has severely degraded its effectiveness. While attacks on sensors and communications can be useful under such circumstances, attacks on the information processes themselves are probably most useful under such circumstances because errors in such processes are difficult to trace, badly understood, and widely expected in the normal course of operation. Such processes can be degraded by means of various information munitions (viruses, worms, logic bombs, etc.) prepositioned or inserted into the enemy air-defense computers. This degradation could cause the IADS to fail to assign targets, assign targets to inappropriate weapons, lose orders to weapons, misinterpret sensor data, or mistarget surface-to-air missile batteries. If cleverly applied, these weapons can go undetected, and any errors in IADS information processes will be attributed to operational errors. The key difficulty in such an attack is timing. The information munitions must “go off” only just before the air strike, or the degradation in the IADS is likely to be detected and corrected. Timing such information munitions is a tricky problem. Viruses and worms travel at an unpredictable rate, and logic bombs are difficult to trigger remotely. One must also keep in mind that some threat air-defense systems will contain bounds-checking features that ensure the system does not malfunction in certain drastic ways (such as assigning targets to inappropriate weapons); these bounds-checking features could present clues that an information attack was in progress to an alert and well-trained air-defense commander.

If the offensive information-warfare attack is meant to allow the United States to operate from a standoff posture, the information attack need not be so unobtrusive in its methods. In this case, the most lucrative targets are the extremities of the system: the sensors and the antiaircraft weapons. Offensive information warfare would attempt to disable the sensors or weapons temporarily in particular nodes of the IADS in closely timed coordination with strike missions routed to pass through the resulting geographic gaps. Such temporary effects could be achieved by overloading sensors with false data, jamming communications via EW, inserting false data into communication streams, or conducting perception-shaping campaigns via broadcast or leaflets that threatened operators who turned on their radars or acquired allied targets.

Two caveats are in order. First, as we have already seen, timing is crucial for realizing the full potential of the preserving strategic reach CONOP. Precise timing of effects will be difficult to achieve and will require Air Force planners with considerable skill. Second, there is the issue of reliable damage assessment for offensive information-warfare attacks against IADS. How do you know if your attack has done its job and if it is safe for manned aircraft to fly through the area? This information-warfare battle damage assessment (BDA) problem could become larger the more frequently this particular CONOP is used. A cunning enemy, once he sees a pattern developing, may set traps by intentionally shutting down the radars in an air-defense sector during an offensive information-warfare attack and then luring American aircraft into an ambush. Once again, the only solution here is to support research into technologies that might make information-warfare BDA a more accurate science.

Preserving strategic reach should only be used if the following three conditions are met. First, U.S. policymakers need to have made a clear decision that other approaches to reducing the significance of the adversary's WMD have less potential. These other approaches include deterrence through the threat of massive retaliation; deterrence through the threat of escalation dominance; and a conventional counterforce campaign aimed at destroying WMD ordnance, delivery vehicles, and storage sites through the use of precision-guided munitions and the use of effective theater missile defenses to reduce adversary expectations about the ultimate results of any WMD attacks with theater ballistic missiles. In many cases, the other approaches could be more appropriate to the situation at hand than the cautious strategy embodied in preserving strategic reach.

Second, it will be critical for other components of the unified geographic command to be fully aware of the JFACC's concept of offensive information warfare and also to be prepared to coordinate actions if necessary. The importance of sharing information across organizational boundaries must not be underestimated when planning for offensive information warfare.

Last, national-level authorities must be made aware of the risks of enemy retaliation against the U.S. National Information Infrastructure in response to U.S. offensive information-warfare attacks against enemy IADS. These authorities should take appropriate precautionary measures. Addressing these vulnerabilities would give the United States more freedom of action to use offensive information warfare in MTWs.

Counterstrike

The purpose of the counterstrike CONOP is to keep the enemy from mounting antiaccess operations against U.S. power-projection capabilities and deep-strike operations designed to target U.S. logistics bases critical for sustaining U.S. air operations. Offensive information-warfare operations provide a new capability in this regard because they offer an opportunity to attack the enemy's rear areas and affect his capacity for antiaccess and deep-strike operations even before U.S. forces have deployed in strength to the theater. Through remote attacks on the enemy's planning and assessment processes, offensive information warfare denies him the use of a homeland sanctuary from the very beginning of the deployment.

It should also be noted, however, that offensive information warfare in this context is intended to be used in conjunction with conventional attacks on enemy strike assets. Offensive information warfare will enhance the effectiveness of conventional counterstrike operations, especially early in the battle, before all forces have deployed, but it will not replace the traditional missions.

At the most basic level, offensive information warfare is useful for this purpose because strike operations are highly information intensive. Successful strike operations require detailed planning, careful coordination, and reliable data on target locations. When viewed as an information process, strike operations can be seen as iterative, with three stages: planning, execution, and BDA. Offensive information warfare will aim to disrupt or defeat all three stages of that process. For this purpose, the United States would deploy an information-warfare squadron to the theater to support the JFACC. This squadron would also have access to numerous information-warfare centers based in the continental United States that can provide analysis and expertise, such as the Army's Land Information Warfare Activity or the Air Force Information Warfare Center.

Strike Planning. Strike planning is the process of allocating and coordinating scarce attack assets (cruise missiles, ballistic missiles, strike aircraft) to inflict the greatest possible damage on the target's operational capacity. To be employed efficiently, such a planning process will need to have access to mountains of data on U.S. capabilities, force-deployment plans, orders of battle, air defenses, and target locations. Planners will also need more prosaic data, such as terrain and navigation information and weather reports.

Offensive information-warfare operations can deny or corrupt all these data sources by attacking information systems. The adversary will use a variety of information systems to collect, process, and disseminate the data. Most of the imagery, weather, and navigation data necessary to pinpoint fixed U.S. targets will be collected from commercial satellites, as well as from such open sources as commercial maps and media outlets. Terrestrial and satellite communications will be used to disseminate raw data to planners, strike plans to the assigned units, and mission plans to the individual shooters. Finally, the creation of any complex strike plan will involve software to evaluate the mountain of data involved, produce mission plans, and transfer data to weapon systems.

There are many methods for denying and corrupting the data. Some are quite conventional, such as limiting access to critical facilities, camouflaging ship and aircraft movements, or periodically moving high-value assets and air defenses. Other methods are more novel and potentially more effective. Physical destruction or electronic jamming of critical junctures in the strike-planning process—satellites, satellite downlink stations, and mission-planning centers—will be particularly effective. Information munitions could also be implanted in the enemy's strike-planning system to render it inoperable at critical moments.

We should keep in mind that planners are adaptive and will find workarounds to the problems of missing data, downed systems, and destroyed communication links. A more subtle method, then, might be to corrupt the mission-planning process, thus causing the enemy to squander scarce strike resources. This can be done primarily by introducing false data on U.S. and allied force disposition, terrain, and even weather data into the enemy's striking-planning process. There are many potential points of access, the most promising being via falsified, corrupted, or hijacked satellite downlinks. Since the enemy may collect some targeting data on large, fixed targets long before a strike, another option is to implant errors in the enemy's mission-planning hardware or software to cause subtle errors in the strike-planning process.

Strike Execution. Strike execution is the process of carrying out the strike plan. For information systems, strike execution depends primarily on a dense system of communication links and navigational aids. This includes communication links—from command and control units to aircraft and missile launchers—used to make changes in the mission plan or report intelligence gained from the mission, communications between aircraft used to synchronize the attack, and navigational data acquired from satellite systems, such as GPS or GLONASS.[20]

Once again, each of these links is potentially vulnerable to destruction or disruption. Most vulnerable are the navigational systems. Without this type of navigational data, enemy cruise missiles and even strike aircraft will be far less accurate. U.S. forces can easily turn off or jam GPS and can jam GLONASS in local areas. Of course, this may also adversely affect the U.S. capacity to operate. Even if access to GPS were limited to U.S. and allied forces, the enemy might well be able to jam U.S. access to GPS in retaliation. Any degradation of satellite navigation systems must always be assessed in a relative perspective. Given that there is a good possibility that the loss of GPS would affect U.S. forces more than it would enemy forces, a more effective measure might be to introduce errors into the GPS or GLONASS signal at critical periods during strike execution. Alternatively, the United States could use information munitions to attack the information processes that load targeting and navigational data into enemy cruise missiles and strike aircraft. Both attacks could introduce navigational errors that should cause strike aircraft to attack erroneous targets or cause cruise missiles to collide with terrain features.

Similarly, the United States could hope to introduce false data into communication links between strike assets and command and control centers or between the strike aircraft themselves. Such false data could generate false targets or give false target updates to strike assets already in the air. Unfortunately, the growing use and sophistication of encryption techniques makes such insertion increasingly difficult, so jamming these links may soon become the only option. Nonetheless, aircraft or cruise missiles that are unable to receive information from their command and control centers will be unable to adjust their mission plans to reflect real-time changes in target disposition and will be unable to function as forward sensors.

New offensive information warfare or related methods may also soon be available for destroying the platforms themselves. One can well imagine having the technology available to generate bogus electronic signals that would prevent arming or prematurely activate warheads

[20] GPS is a U.S. satellite navigation system. GLONASS is a similar Russian system.

on inbound cruise missiles and fighter aircraft. Another interesting possibility is the use of high-altitude electromagnetic pulse weapons based on airborne platforms to disable navigation, flight control, target acquisition, and fire-control systems on inbound aircraft and cruise missiles, rendering them all but useless as offensive weapons or causing them to crash.

Battle Damage Assessment. BDA, the least examined part of the strike process, is critical for a successful overall strike plan. Given the scarcity and price of sophisticated strike assets, it is vital to know which defensive systems have been disabled and which targets have been destroyed in order to allocate strike assets efficiently and safely. BDA has several information sources, including the strike asset itself; open-source media outlets; human intelligence agents; and remote-sensing platforms, such as satellites, UAVs, and surveillance aircraft.

Once again, all of these data sources can potentially be degraded or destroyed by offensive information-warfare operations. Although jamming and physical destruction of communications and satellite downlinks will be very useful measures in this regard, BDA also presents ample opportunity for deception. False damage signatures may fool strike aircraft into thinking they have hit their target. Careful camouflage can fool satellite imagery into believing that targets have been destroyed or, conversely, remain unharmed.

Perhaps the most promising method of complicating the enemy's BDA process is by tainting open sources. In the future, much BDA may be done through the media or through human agents reporting openly available information from within the target zone via e-mail, cell phones, etc. The problem of open-source BDA of strike operations will no doubt persist and, indeed, may increase as more of the population gains access to cell phones and Internet e-mail. Offensive information-warfare operations can turn this intelligence drain into an asset by planting false information on battle damage into open sources. False damage reports and even false video images of bomb damage (or, conversely, of false images of still-operating facilities) can greatly complicate enemy planning. In contrast to information deterrence, if this activity damages the credibility of the media and human agents as sources of BDA, so much the better. It is again important to be aware of the risk of blowback: Special BDA spoofing efforts against the enemy may well fool some planners and operators on the U.S. side who are not familiar with these programs.

The Utility of Counterstrike. The importance of counterstrike will vary with the current phase of conflict. Pentagon planners have divided MTWs into three phases: halt, stabilize (or "buildup and pound"), and rollback. The counterstrike CONOP would be the most useful during the halt phase of a stressful MTW, in which the enemy has physical forward momentum on the ground and a numerical advantage in the air. Normal U.S. air and missile defenses may not be fully deployed, creating opportunities for the opposing side to mount deep-strike and antiaccess attacks against American and allied rear areas.

The usefulness of counterstrike drops steeply as one enters the buildup-and-pound and counterattack phases of an MTW. During the last two phases, the Air Force will presumably have established a comfortable level of air superiority; anti–tactical ballistic missile systems, such as Theater High-Altitude Area Defense and Patriot, will be fully deployed throughout the battlespace; and dispersal and decoy arrangements will be in place at the Air Force's main operating bases. In such an environment, counterstrike would probably be unnecessary, and it would be far better to devote offensive information-warfare resources to other purposes.

Counter-C^{4}ISR

The "counter-C^{4}ISR campaign" CONOP involves using a mix of offensive information-warfare tools and techniques to attack adversary sensors and communication assets across the board at critical "transition points" during a campaign. The goal of the counter-C^{4}ISR campaign is to reduce the enemy's battlespace awareness at key junctures by degrading his ability to collect and process information from space, airborne, and ground-based C^{4}ISR assets.

Earlier in this chapter, it was noted that the size and capacity of global commercial satellite and terrestrial communication networks is increasing at a rapid rate. By the 2010–2015 time frame, there will be so many redundant communication paths and links in existence that it will be impractical to achieve large, sustained reductions in the enemy's C^{4}ISR capacity across the board from the tactical level up through national-level command and control. In fact, available evidence suggests that the United States was not even able to achieve this goal completely against Iraq during Operation Desert Storm.

However, this reality does not render counter-C^{4}ISR futile. Instead, it suggests that U.S. operations should focus on degrading key choke points of the enemy's C^{4}ISR system at critical moments in the campaign, rather than on an attempt to destroy all enemy communications.

Increased access to commercial space-based imagery, communication, and navigation systems will greatly enhance the enemy's C^{4}ISR capacity but may also make the systems more vulnerable to offensive information warfare. Use of space-based systems will introduce choke points into the enemy's C^{4}ISR system. Satellites themselves become critical nodes that, if disabled, would drastically reduce enemy C^{4}ISR capacity. Commercial communication satellites require downlink stations and locally dense communication networks that are also vulnerable to physical and information attack. Imaging satellites also require downlink stations and an imagery analysis center to read, interpret, and disseminate the information gleaned from satellites. Reception of GPS navigation, while more dispersed, will often require differential GPS transmitters to achieve needed accuracy. A well-timed attack that disables or degrades these systems may well leave the enemy worse off, especially for short but critical periods of time, than if he had never grown accustomed to their significant advantages over terrestrial communications, surveillance, and navigation.

Counter-C^{4}ISR involves many of the same means and mechanisms as the two previous CONOPs, "preserving strategic reach" and "counterstrike." There is a fundamental difference in their goals, however. Counter-C^{4}ISR is designed to have a decisive effect on the outcome of a campaign, while the other CONOPs would have more-limited objectives. Counter-C^{4}ISR is a potential war winner; preserving strategic reach and counterstrike are not. This distinction means that, even more than the other CONOPs presented, counter-C^{4}ISR requires tight integration with the regional CINC's overall campaign plan. Indeed, counter-C^{4}ISR will depend for its success on careful synchronization with more-conventional attack assets. This implies placing responsibility for the C^{4}ISR campaign firmly in the hands of the JFACC, rather than creating a special information-warfare component commander, so that the principle of centralized control with decentralized execution can be maintained. Creating a special information-warfare component command may sound appealing at first blush, but would probably be unwise, because it would only add another layer of command and control that could slow down U.S. and allied decision cycles. Enemy forces will use C^4ISR systems to anticipate U.S. force movements and order force movements in response. They will use satellite reconnaissance to show large force movements or attack preparations, such as the movement of large amounts of supplies and weapon platforms. They will use commercial communication satellites, as well as dedicated terrestrial communications, to receive human intelligence on such movements and to order counterpreparations and strike missions against massing U.S. forces and supplies. They will use satellite navigation to provide targeting information to cruise missiles and strike aircraft on the position of key U.S. forces and supplies. Finally, they will use advanced software and computer systems to program targeting information into cruise missiles. Again, the intent of counter-C^4ISR is to deny the enemy these sources of information and information processes, not always or everywhere, but just at the critical moments and places where they are most needed.

This implies that the leading edge of the rollback phase offensive will be a coordinated offensive information-warfare attack on these information systems, including physical attacks. The exact nature of that attack would depend on the CINC's overall campaign plan. As an example, however, it will be helpful to consider how the CINC might have attempted to achieve a surprise flanking attack, such as U.S. forces accomplished during Desert Storm, despite the presence of a sophisticated enemy C^4ISR system.

The first, and probably most difficult, task would be to allow the large force movement necessary to accomplish such a flanking maneuver to go undetected. This would require first jamming or disabling any commercial imagery satellites capable of providing images of the staging area. As these systems will be assets of neutral nations, this may require a certain delicacy of approach. One possibility is nonlethal attacks from ground-based antisatellite (ASAT) lasers that could only temporarily blind a satellite. A less-controversial method would be precision weapon attacks on the enemy's imagery analysis centers or the satellite's communication links with enemy command centers.

Unless such movements take place in trackless deserts, they are also likely to be detected by enemy agents on the ground. This unpleasant reality implies that the movement must be accompanied by efforts to cut off the enemy's external communications. The means to accomplish this task include local jamming of commercial communication satellites from mobile transponders, precision-guided weapon attacks on satellite communication downlink stations, and information munitions implanted in key communication switches that control communications with the downlink station. Once again, the enemy is likely to be able to reconstitute these systems in the space of days or even hours, so timing is critical.

Although counter-C^{4}ISR may not be able to prevent, for a sufficient period, enemy detection of a movement of the same scope as the famous Desert Storm "left hook," it can also help in stymieing enemy responses. First, attacks on communication links will make it difficult for enemy commanders to receive satellite imagery and targeting data or to give and receive orders to respond to U.S. movements. Second, as with the counterstrike CONOP, the United States can hope to deny, degrade, or corrupt enemy access to satellite navigational aids and information processes that control enemy targeting systems. U.S. forces on the move, once detected, will present tempting targets for enemy cruise missiles. If their navigational and targeting systems can be degraded at the critical moment, however, they will present little danger to U.S. forces.

Over the long term, counter-C^{4}ISR would benefit operationally from the deployment of space weaponry. Such systems as space-based co-orbital jammers, lasers, and obscurants would increase the chances of success for this CONOP. However, the price in terms of arms-race risks and military opportunity costs could be steep, and it is not clear that the price would be worth paying.

There are tangible arms-race risks to consider when thinking about the deployment of space-based ASAT weaponry. Other nations with significant scientific, industrial, and technical wherewithal could respond by deploying their own such systems to threaten U.S. satellites. The result of this could be a net negative for the United States, since the U.S. military's main advantage in future wars will come from its superior ability to collect, process, and act upon large amounts of data in very compressed time cycles. Conflicts in space resulting in the destruction or degradation of U.S. communication or imagery satellites would hurt American military capability more than they would a regional adversary's, even if the United States inflicted more damage on enemy space capabilities than it suffered itself. Furthermore, the deployment of space-based ASAT systems could invite adversaries to use asymmetric options to negate U.S. space capabilities-options that could include terrorist acts against U.S. commercial and military satellite ground stations worldwide. Another possibility would be retaliatory jamming against U.S.-owned satellites, including the GPS navigation satellites.

All in all, the operational advantages afforded to the Air Force in terms of being able to better execute the counter-C^4ISR campaign look to be outweighed by the many potential disadvantages created by space-based ASAT deployments. The counter-C^4ISR campaign will still likely be effective with only ground-based ASAT assets and would even have some use if employed without any ASAT weaponry at all. However, it would be wise for the United States to continue a research and development program into space-based ASAT technologies and also to be prepared to deploy an operational system if another nation shows signs of getting ready unilaterally to place an ASAT system in space.

COMPARING THE FOUR CONOPS

Table 6.1 is a crude attempt to summarize the strengths and weaknesses of the four CONOPs that have been presented. Our four offensive information-warfare CONOPs are listed vertically along the column at the far left. Each of the four is then assessed against five metrics: the risk of escalation that the CONOP carries with it, the

Table 6.1

Comparing the Four CONOPs

	Escalation Risk	Long-Term Relevance	Against Medium Powers	Against Large Powers	Military Decisive-ness
Information-based deterrence	Medium	Yes	Yes	Yes	Yes
Preserving strategic reach	Low	Yes	Yes	Yes	No
Counterstrike	Low	Yes	Yes	Maybe	Maybe
Counter-C^4ISR	Medium	Maybe	Yes	Maybe	Maybe

ability of the CONOP to remain relevant as the revolution in information technology continues, the usefulness of the CONOP against medium-sized powers (such as North Korea and Iraq), the usefulness of the CONOP against larger powers (such as Russia), and the potential of the CONOP to be militarily decisive in and of itself.

First, in terms of escalation risk, none of the CONOPs described presents an extreme escalation risk. Information-based deterrence, because it will take place before any hostilities have broken out, may contain some escalation risks, especially if it involves fostering instability in the target state. If the offensive information-warfare campaign is discovered and if that campaign is considered tantamount to an act of aggression, it may provoke an adversary to conventional retaliation. Because international norms on how to treat information attacks are still evolving, it is difficult to say how any adversary might react to this provocation. Indeed, some Russian writings, for example, declare that Russia would interpret an offensive information-warfare campaign against its homeland as being tantamount to physical attack. While this is probably hyperbole, it does point out the need to be especially careful in using offensive information warfare against states that perceive themselves to be in a position of ever-increasing weakness. Preserving strategic reach was specifically designed to minimize escalation risk. Counter-C^{4}ISR, however, presents some risk of nuclear escalation, if the enemy has built a small nuclear arsenal. Because this CONOP involves overt attacks on the enemy's command and control networks and because these networks will likely also be used for control of the nuclear arsenal, there is some risk that the enemy will regard these CONOPs as preparatory to a counterforce first strike and respond by escalation. Preserving strategic reach was specifically intended to solve this problem.

As for long-term relevance, all the CONOPs except counter-C^{4}ISR should remain viable options for the foreseeable future. Counter-C^{4}ISR may become obsolete if international connectivity continues to increase at its current exponential rate. Under such circumstances, the density of the enemy's communication and surveillance networks will limit the number of choke points in the system and, consequently, the possibility of seriously degrading the system even for short periods of time. Counterstrike could lose some of its relevance if the sophistication and proliferation of digital signature technology reach a point where even regional powers could prevent the insertion of false information into the strike-planning and execution processes.

All of the CONOPs will have utility against medium-sized powers. Indeed, they were designed with such powers in mind. Against larger powers, the utility of counterstrike and counter-C^4ISR will greatly diminish. Information deterrence does not depend on the size of the adversary, while preserving strategic reach can still be used to allow U.S. air assets to operate safely over particular areas of a larger adversary. However, the size and density of the communication networks of a large power would make it extremely difficult to create even the short communications blackout required for counter-C^4ISR without taking drastic steps, such as the use of a high-altitude nuclear burst for electromagnetic pulse effects. Counterstrike may not be an efficient use of resources against an adversary who has very large numbers of cruise missiles and fighter aircraft available during the halt phase. Against such an adversary, it may be better to combine passive defenses with offensive counterair operations to deal with the threat of antiaccess and deep-strike attacks.

Finally, we arrive at military decisiveness. Only information-based deterrence has the potential to be militarily decisive, because it can dissuade an adversary from even starting a conflict. Preserving strategic reach is certainly not decisive, because its whole purpose is distraction, not decisiveness. Counter-C^4ISR could be decisive under certain circumstances but not in others. Ultimately, counter-C^4ISR creates the conditions under which other means of warfare press decisive operations against the opponent; counter-C^4ISR is an enabler of decisive operations rather than a component of them. Counterstrike falls into the same category. The only scenario in which counterstrike could become decisive would be against an adversary who staked all his hopes on deep-strike and antiaccess operations against U.S. rear areas during the halt phase and had no backup plan in case the attacks failed. In such a scenario, counterstrike could act to fend off the attacks and thus implicitly compel the adversary to sue for peace. In virtually all other instances, counterstrike does not offer an opportunity for a decisive outcome in and of itself.

REFERENCES

Agmon, Marcy, et al., *Thwarting the Superpower: How the Smart Adversary Might Use Political Weapons to Offset U.S. Military Power*, Santa Monica, Calif.: RAND, unpublished manuscript.

Air Force Space Command, “Space Capabilities Integration,” briefing slides, July 12, 1996.

Ambrose, Stephen E., *D-Day, June 6, 1944: The Climactic Battle of World War II*, New York: Simon & Schuster, 1994.

Cebrowski, Vice Admiral Arthur K., and John J. Garstka, “Network-Centric Warfare: Its Origin and Future,” *Naval Proceedings*, January 1998, pp. 28–35.

Chow, Brian, Gregory S. Jones, Irving Lachow, John Stillion, Dean Wilkening, and Howell Yee, *Air Force Operations in a Chemical and Biological Environment*, Santa Monica, Calif.: RAND, DB-189/1-AF, 1998.

Graham, Bradley, *Hit to Kill: The New Battle over Shielding America from Missile Attack*, New York: PublicAffairs, LLC, 2001.

Hosmer, Stephen T., *Psychological Effects of U.S. Air Operations in Four Wars 1941–1991: Lessons for U.S. Commanders*, Santa Monica, Calif.: RAND, MR-576-AF, 1996.

Hutcherson, Norman B., *Command and Control Warfare: Putting Another Tool in the War-Fighter’s Data Base*, Maxwell Air Force Base, Ala.: Air University Press, September 1994.

Joint Chiefs of Staff, *Joint Vision 2010*, Washington, D.C., July 1996.

Joint Staff, *Joint Doctrine for Command and Control Warfare*, Joint Publication 3-13.1, February 7, 1996.

Keffer, John W., “Trends in Commercial Satellite Communications Systems and Implications for MILSATCOM,” briefing slides, November 20, 1996.

Libicki, Martin, *Defending Cyberspace and Other Metaphors*, Washington, D.C.: National Defense University Books, 1997.

Nye, Joseph, and William Owens, “America’s Information Edge,” *Foreign Affairs,* Vol. 75, No. 2, March/April 1996, pp. 20–36.

Pace, Scott, et al., *The Global Positioning System: Assessing National Policies*, Santa Monica, Calif.: RAND, MR-614-OSTP, 1995.

Stillion, John, and David T. Orletsky, *Airbase Vulnerability to Conventional Cruise-Missile and Ballistic-Missile Attacks: Technology, Scenarios, and U.S. Air Force Responses*, Santa Monica, Calif.: RAND, MR-1028-AF, 1999.

Stoney, William, "Land Imaging Satellites Planned to Be Operating in the Year 2000," data sheet, Mitretek, July 22, 1997.

Submarine Systems International, Inc., "Global Undersea Networks for Government Applications," briefing slides, July 1997.

U.S. Space Command, "Department of Defense Advanced Satellite Communications Capstone Requirements Document," June 23, 1997.

Watman, Kenneth, *Asymmetric Strategies for MRCs*, Santa Monica, Calif.: RAND, unpublished manuscript.

Watters, Ethan, "Virtual War and Peace," *Wired*, 4.03, March 1996, p. 49.

Wilkening, Dean, and Kenneth Watman, *Nuclear Deterrence in a Regional Context*, Santa Monica, Calif.: RAND, MR-500-A/AF, 1995.