The US Army War College Quarterly: Parameters

Volume 28
Number 3 *Parameters Autumn 1998*

Article 12

8-13-1998

Star Wars in Real Life: Political Limitations on Space Warfare

Frederick W. Kagan

Star Wars in Real Life: Political Limitations on Space Warfare

FREDERICK W. KAGAN

From *Parameters*, Autumn 1998, pp. 112-20.

Just because you have a capability does not mean that you can use it. For more than 50 years the United States has had nuclear weapons, and used them only twice. For almost a century America has had the capability to use chemical and biological weapons, and never has. During the Korean War we had the capability of attacking targets in China, and did not. During the Vietnam War we could have occupied Laos, Cambodia, or North Vietnam, but refrained. In each of these cases political considerations overrode militarily desirable actions, generally because potential international political costs were believed to be greater than any military advantage we might gain.

It is likely that similar constraints will hinder our use of the newest weapon in our arsenal. That weapon is actually a collection of skills and technologies described generally as information operations, the purpose of which is to maintain superiority in electronic communications, intelligence, and targeting over our adversaries. It is time, however, to examine the likely present and future costs and consequences of conducting information operations, for it seems certain that political considerations may again constrain militarily desirable actions. And if that is true, then our vaunted information "supremacy" may turn out to be much less than we anticipate.

The Assumptions

This article examines conventional assumptions about the ability of the United States to establish and maintain "total information dominance" in any future conflict. That condition, when applied to a war game, can free participants from the ambiguities of many geostrategic issues, allowing them to develop the much more familiar, and correspondingly less stressful, operational level of war. The enabling assumption in this instance seems to be that US information operations will have so disrupted an opponent's intelligence-gathering and communications capabilities in space and near-space that US and allied forces will be able to conduct Cold War style operations free of the inconveniences of those technologies.

It has become almost a mantra, among the true believers, that our space capabilities will allow us to see everything and target everything while keeping the enemy completely in the dark. Advocates of the theoretical "system of systems" that is to deliver this capacity pay little heed to the cost and difficulty of developing and maintaining it. Nor are they eager to consider likely countermeasures, secure in their belief that we will be able to blind or disable at will the systems an adversary would need to conduct them. The unspoken policy assumption is that given the capability to deprive our adversary of space or near-space assets, we will certainly do so. That assumption, unfortunately, is likely to prove faulty, as became painfully clear during the April 1998 Army After Next Wargame.

There is a real difference between having the means to carry out offensive operations against an adversary's assets in space or near-space and the political will to do so. We need to begin with definitions, however, for in this business one learns quickly that there are sure to be several for whatever concept is being discussed.[1]

The term "information operations" has specific meanings related to attacking an opponent's information systems and defending friendly information systems. Offensive information operations might blind or destroy satellites and unoccupied aerial vehicles to disrupt reconnaissance systems and communications nets. They might attack satellite downlink centers and other critical communications nodes to achieve similar purposes. More esoteric information operations include using viruses to destroy or degrade computer networks or to generate false intelligence reports in support of deception operations. Defensive information operations include measures to safeguard our own satellite

reconnaissance and communications systems, as well as our own communications networks, from the same kinds of attacks.

Apart from virus attacks on computer networks, information operations will be conducted with weapons that are physical and relatively conventional. Some form of missile will be used to destroy unoccupied aerial vehicles, satellites, and satellite downlinks or communications nodes. Lasers or other directed-energy weapons might be used to destroy or to "dazzle"--disable temporarily--satellite reconnaissance systems. Still others may be directed at the humans in the system.[2] The novelty of this form of warfare is that it directly targets the means used to acquire and distribute intelligence, as well as the physical components of command and control nets. The 1998 Army After Next Wargame did not challenge the belief that yet-to-be-defined information operations systems and procedures will ensure operational and strategic superiority in a future conflict.

The Flawed Vision

This discussion considers two possible strategic cases. In one, America joins a coalition against a second-tier power whose own space capabilities are limited and who relies extensively on leasing the commercial and military space assets of other nations for information systems, communications, and targeting data. In the other, America is in a coalition against a first-tier power which relies extensively on its own space systems. Which power is likely to be more vulnerable to our information operations?

The second-tier power clearly will not have the ability to challenge us in space. Blinding or destroying its satellite systems will be relatively easy, and its ability to damage our satellite constellation will probably be limited. It is this scenario which makes the "information RMA" so appealing, as it conjures images of American precision-guided munitions ravaging the enemy's infrastructure while any precision-guided munitions the enemy might have lie unused for lack of sensors to guide them. But what of the intelligence provided to this adversary by neutral states or commercial interests? This question, if raised, is usually brushed aside by noting that we can blind neutral satellites too or pressure neutrals not to provide such information to the enemy. The problem, however, should not be taken so lightly.

We will, almost certainly, be technically able to blind neutral space systems as they pass over a theater of operations, but we will probably be unable to do so politically. Worse still, apart from the difficulty of verifying whether neutrals are providing such information, we will probably have virtually no leverage with which to pressure them to stop selling intelligence to our adversaries even as we are fighting them. To understand the problem, we should cast the question of information operations in the paradigm of trade and commerce in time of war. From that standpoint it becomes clear that we will be unable politically to shut off the flow of information to the enemy.

Consider the following scenario. A revived Iraq establishes commercial contracts with Russia, China, and several major international corporations to lease access to their satellites and to purchase raw satellite imagery from them. Communications will be both via satellite downlink directly into Iraq and via fiber-optic ground lines through other states. Russia and China might not agree to provide real-time, live-feed imagery--the sort which would be most useful for targeting--but could provide satellite still imagery with minimal time delay, say under an hour. Such imagery would not constitute targeting data for precision-guided munitions, since an armored unit on the move can traverse 60 kilometers in an hour. It would, however, provide valuable tactical intelligence and early warning, would locate stationary units, and could enable the enemy to focus targeting systems that support precision-guided munitions.

Now suppose that the United States once again finds itself at war with Iraq. We could blind or destroy many if not all of the Iraqi-owned space assets, thereby eliminating their ability to obtain real-time targeting data. Then we discover that the enemy somehow knows the location of our major forces that do not keep moving and hits them with precision-guided and conventional munitions. Worse still, we find that the enemy has identified some of our principal forward support bases and attacked them. In other words, we find that any fixed target or any system that doesn't keep moving comes under attack. We know that the enemy is getting data from Russia, China, and commercial third parties. The President asks what America can do about it; the answer is, probably nothing.

A bold Secretary of State asks the Russians and the Chinese to stop providing the enemy with intelligence. Both deny that they are providing any intelligence with military significance and defend their rights of trade as neutral states to

provide non-military intelligence. The Secretary of State retorts that since the enemy no longer has any functioning space assets, his continued ability to identify and hit US targets must mean that he is getting the intelligence from somewhere, and again insists that Russia and China desist from providing such intelligence, arguing that it almost makes them co-belligerents.

Both nations continue to deny providing targeting data, each arguing that it must be the other which is the culprit. Then a bright Russian ambassador recalls his American history. He reminds the Secretary of State that the right of neutrals to continue to trade peacefully with belligerents is a well-established principle of international law. He points out, furthermore, that violation of that principle twice brought America into wars in which it had hitherto remained neutral. During the wars with Napoleon, the British had attempted to expand their embargo on trade with France to include American neutral shipping. America had gone to war with Britain to defend her right to continue to trade. During World War I the Germans had declared an embargo on Britain which they attempted to enforce with submarine warfare. When they extended submarine warfare to include attacks on American shipping, America entered that war as well.

In each case the argument was made by the embargoing power that the Americans were supplying instruments of war to belligerents, but in each case methods of detecting such trade were inadequate. In the end, both the British and the Germans were forced to assume that any American vessel bound for France or for England was carrying contraband and subject to search-and-seizure or destruction. America went to war to defend her rights of free trade.

The World War I parallel is particularly disturbing. Germany was well aware in 1917 that a resumption of unrestricted submarine warfare would bring America into the war. The German high command, however, calculated that the damage to Britain would bring her to her knees long before America could intervene significantly in Europe. In other words, the Germans believed that the military advantage gained in the short term by unrestricted submarine warfare would be so decisive that the long-term political and military consequences were irrelevant. That they were not irrelevant was due to the fact that America responded asymmetrically to the German decision. The United States began to build merchant ships at a rate the Germans had not foreseen, and we developed the convoy system to protect against German submarine attacks. Not only was England not brought to her knees, but trade across the Atlantic actually began to increase, and America was given the time to bring its enormous military potential to bear, mobilizing much more quickly than the Germans had expected.

The situation with regard to information is no less complex and no more suited to attempts to impose "information embargoes" unilaterally on our enemies. Those supplying such information will, in the first instance, deny it. Depending on the method of transmission of such information, we may or may not be able to prove to our own satisfaction that they are doing so, but it is highly unlikely that we will be able to prove to the satisfaction of the international community that they are. Even if we can show, moreover, that satellite imagery of a theater of war is being provided, we must still be able to argue convincingly that such imagery is an instrument of war. We will probably lose that argument. The neutrals, if caught, will argue that they are providing satellite imagery of various regions of the world to provide defensive early warning, and that, since they are not even providing real-time targeting imagery, there can be no question of their right to continue to supply such data. The bottom line is that we will almost certainly fail to convince neutrals to stop providing imagery voluntarily if their interests do not run with ours.

An aggressive President, concerned about justifying losses in war, might then inform the Russians and the Chinese that he will selectively blind their satellite systems with space- and ground-based laser-dazzlers as they pass within observation range of the theater of war. It is easily within our capabilities to do this, and there is little the other nations can do to prevent it. Unfortunately, both the Russians and the Chinese respond that such actions are acts of war and will lead to retaliation and escalation. This argument confuses many people at first, for it is argued that dazzling a satellite temporarily does it no permanent harm and cannot, therefore, be seen as an act of war. The argument points to the fact that we need a new definition of "hostile act" in the information age; it seems clear that dazzling a satellite will have to fall within any such definition.

In the first place, a hostile act does not necessarily have to cause any physical damage. A warplane overflying a border without permission is committing an act of aggression even if it takes no other action. Under certain circumstances even simply illuminating an aircraft with a targeting radar may be considered a hostile act.[3] The selective blinding of

neutral satellites over theaters of war, however, does indeed do them harm. In a coalition war against a revived Iraq, which will certainly possess the capability to use weapons of mass destruction of some form, the Russians have a vital national security interest in observing what transpires in that theater so close to their own territory. If we deny them the ability to detect the launch and follow the flight pattern of Iraqi theater ballistic missiles, for instance, we thereby degrade or destroy their ability to take appropriate countermeasures should those missiles, intentionally or unintentionally, strike targets in or near Russian territory. At the very least we will be inviting the states whose intelligence assets we blind to take measures to prepare for hostilities, the expansion of which they will be unable to foresee. Since intelligence is power and knowledge is safety, blinding intelligence assets inherently causes damage and constitutes a hostile act.

The problem of dealing with commercial non-governmental organizations gravely complicates this issue. With corporations the matter revolves less around the definition of a hostile act and more around the possible measures of retaliation those corporations could take. Suppose that the Iraqis establish contracts to purchase satellite imagery from, say, a major Canadian communications company. Suppose that when called upon to stop providing such imagery, that company refuses, citing its legal rights to continue to execute its contracts in the absence of international information embargoes. Suppose that the United States takes measures to blind the satellites of that company as they pass over Iraq. Suppose that the company retaliates by shutting down its communications systems in protest.[4] The disruption caused by these actions would reverberate throughout America's own military capabilities. Moreover, it would cause such an outcry in the American business community that the political leadership would almost certainly be forced to abandon the measures. The power of information means that those who obtain and disseminate it are themselves very powerful. Should they resist efforts to restrict the flow of information, it will be very difficult, in the real world, to coerce them to do so.

All of which is to say that it may be extremely difficult to cut off completely the flow of information to a second-tier enemy even though we can easily destroy his own space assets quickly. There is no doubt that an attack on an adversary's space systems will seriously degrade his intelligence and his command and control capabilities, but it will not eliminate them. American logistics bases and other fixed assets within range of the enemy's strike systems will continue to be at risk. Even American ground forces that do not remain more or less continually in motion may be at risk from enemy systems using satellite still imagery an hour or more old to target them. Information operations in the real world are likely to be much less decisive than the most radical supporters of a revolution in military affairs would have us believe, even against second-tier enemies.

With first-tier opponents the situation becomes more complicated. A revived Russia, a modernized China, a rearmed Germany or Japan will be able to put into space and deploy on the ground anti-satellite systems, laser-dazzlers, and other information operations systems with which to attack our own space systems. We will almost certainly continue to have measurable superiority in this area, at least for the foreseeable future, but we should expect first-tier adversaries to be capable of significantly disrupting our space systems. The President who contemplates acts of aggression against first-tier nations will have to weigh carefully the costs and benefits of initiating hostile space operations.

Although it would certainly improve our security if we destroyed the ability of peer adversaries to use real-time imagery for their precision weapon systems, we will have to weigh that gain against the cost of the degradation (by enemy counter-measures) of our own capabilities in that area and in others. It may be that space-war will be the most attractive option, but we will have to be prepared to fight with less-than-perfect intelligence and communications as enemy systems attack our own systems. If both we and our adversaries choose to refrain from such a confrontation, then we may retain near-perfect intelligence and communications at the cost of allowing our enemy to do approximately the same. In either case, it is extremely unlikely that a war against a first-tier enemy would see American information supremacy matched against enemy information impotence.

A New Model

This discussion is not intended to show that information operations in the future will be impossible or irrelevant. It seems evident, however, that we should not take for granted the simple and idealized vision of American military supremacy attained through information operations against powerless enemies. The problems are more complex, and we have not even asked many of the key questions.

One major problem will be fitting information operations into the joint environment. This is not a question of which services will provide the platforms, but of how those operations will be incorporated into joint planning and the conduct of operations. If we abandon the assumption that information operations will from the outset of hostilities and throughout the duration of the fight both blind the enemy and provide perfect intelligence to our shooters, then it becomes clear that such operations will have to be phased and timed carefully to support, protect, and enable operations on the ground, on the sea, and in the air. The task of an information operations commander will be to attain temporary information dominance over the battlefield to coincide with a key phase of conventional operations, just as the task of an air commander is to achieve temporary air superiority, or the task of a naval commander is to achieve temporary control of the sea. The trick will be coordinating that temporary dominance with the conduct of the conventional fight.

At what command level will information operations blend into the joint environment? On the one hand, tactical commanders will certainly want to call for support from information assets just as they now call for artillery, air, or naval support in critical situations. On the other hand, such calls will have to be fitted into an overall information operations plan which supports the campaign objectives. But the nature of those operations means that political and international considerations come to the fore much more rapidly than they do with conventional munitions, and senior commanders as well as political leaders are likely to demand a correspondingly greater ability to control and guide the conduct of information operations during a conflict. Such demands are likely to centralize control of those operations at higher levels, inevitably reducing the ability of information operations to respond to tactical requests. But centralization may prove costly; it could create crucial delays in responding to requests from tactical commanders and provide attractive targets in the centralized US command and communications nodes to an adversary's own information operations systems.

The traditional conventional solution for fire support assets of separating theater assets from those controlled at corps or division level will probably not work for information operations. If, as seems likely, the components of the system of systems are closely coupled, it could prove very difficult to place segments of those systems in reserve for direct support to tactical commanders. The whole system of systems may have to respond to every request for support, whether issued by theater commanders or by tactical unit commanders. It will have to evaluate those requests, prioritize them, and act on those priorities faster than enemy systems can respond. The system of systems will require a new model of command and control, and a new model of jointness, if it is to operate in a world in which the adversary's capabilities have been only partially degraded and our own are functioning imperfectly.

The realization that we will not be able to cut off the flow of information to the enemy brings with it the conclusion that we will have to develop technologies to attack other segments of the adversary's sensor-shooter systems. The easiest way is to blind those systems in space, but we must allow for that to be closed to us for political reasons. Therefore, we need to refocus our efforts to attack the enemy shooter systems and the links between the sensors and those systems.

But the abysmal record of attempts to locate and destroy SCUD missile launchers, even in the absence of Iraqi information operations, does not bode well for current capabilities to attack shooters on the ground. We will need better ways to solve this problem. Theater ballistic missile defense and defense against intercontinental ballistic missiles must be pursued aggressively; it is also essential to be able to defend against cruise missile attacks--a much more difficult proposition. In the future, though, we may face directed-energy systems which will be difficult or impossible to oppose once they have been fired. The only solution may be finding ways to prevent the transmission of targeting data from enemy sensors to those systems or to corrupt the data transmitted.

That solution will probably continue to be elusive. We will not know where all of the adversary's strike systems are, nor will we know all of the sources of its targeting data. Satellite communications systems may be easily jammed or destroyed, but the political difficulties, costs, and consequences of such offensive actions in space may make them impossible to carry out for non-technical reasons. Even shutting down satellite systems will not suffice in an age of fiber-optic cable. The odds are that in any conflict some adversary sensors will continue to direct some of its shooters throughout hostilities and we will be unable to prevent that outcome for a variety of technical and political reasons. Information operations, like the rest of war, will continue to be a duel--nonlinear, and subject to friction and to chaotic effects.

There can be no doubt that information operations will be important in future conflicts, and there is little doubt that America's armed forces will have to reorganize themselves and rethink their doctrines to adapt. It is easy to slip into visions of the future that are simplistic, however, and assume away the enduring complexities of war. "Thought experiments" such as the Army After Next wargames help to bring out those complexities, in the process identifying issues that must be addressed by all the services. We should set out to cast off the pleasing, simple, but erroneous visions which attract many to the information revolution in military affairs. That is but the first task in moving toward a more mature concept of the role of information operations in future war and deciding how we need to change to adapt.

NOTES

1. The basic Army doctrinal definitions of "information operations" and "information warfare" may be found in TRADOC Pamphlet 525-69, "Concept for Information Operations," 1 August 1995. Information operations: "Continuous military operations within the military information environment that enable, enhance, and protect the commander's decision cycle and mission execution to achieve an information advantage across the full range of military operations. Information operations include interacting with the global information environment and, as required, exploiting or degrading an adversary's information and decision systems." Information warfare: "Actions taken to preserve the integrity of one's own information system from exploitation, corruption, or destruction while at the same time exploiting, corrupting, or destroying an adversary's information system and in the process achieving an information advantage in the application of force." I have listed here more explicitly what these definitions might mean in the real world, reflecting, in part, what I observed at the Army After Next wargame.

2. For an assessment of potential personnel vulnerabilities in these operations, see Timothy L. Thomas, "The Mind Has No Firewall," *Parameters*, 28 (Spring 1998), 84-92.

3. This point was most forcefully illustrated recently when an American F-16 fighter flying cover for allied aircraft operating in Iraq's southern "no-fly" zone fired an anti-radiation missile at an Iraqi ground radar installation which illuminated the allied aircraft with targeting radar.

4. I am indebted to Colonel Jacques Hamel of the Canadian Army for this insight.

Dr. Frederick W. Kagan is assistant professor of military history at the US Military Academy, West Point, N.Y. He received a Ph.D. from Yale University in Russian and Soviet military history. He participated in the 1998 Army After Next spring wargame in April as a role-player--he was Russia.

Reviewed 13 August 1998. Please send comments or corrections to carl_Parameters@conus.army.mil