INFORMATION WEAPONIZATION OF SPACE

By

James R. Shumate
Lt Col, U.S. Air Force

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature:_____________________

18 May 2001

Not Available -- TDY
Dr William Martel, Faculty Advisor
NWC Space Chair
<table>
<thead>
<tr>
<th>Report Date</th>
<th>Report Type</th>
<th>Dates Covered (from... to)</th>
</tr>
</thead>
<tbody>
<tr>
<td>17052001</td>
<td>N/A</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title and Subtitle</th>
<th>Contract Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Weaponization of Space</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Grant Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shumate, James R.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Performing Organization Name(s) and Address(es)</th>
<th>Program Element Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naval War College 686 Cushing Road Newport, RI 02841-1207</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project Number</th>
<th>Task Number</th>
<th>Work Unit Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sponsoring/Monitoring Agency Name(s) and Address(es)</th>
<th>Performing Organization Report Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sponsor/Monitor's Acronym(s)</th>
<th>Sponsor/Monitor's Report Number(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distribution/Availability Statement</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved for public release, distribution unlimited</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supplementary Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subject Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Report Classification</th>
<th>Classification of this page</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Classification of Abstract</th>
<th>Limitation of Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>UU</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
</tr>
</tbody>
</table>
Information Weaponization of Space

While not a part of the operational factor trinity, information increasingly and profoundly affects the factors of space, time, and force, both individually and in combination. Space has become perhaps the key enabler for operational information for both the United States and its potential enemies. While defense of our capabilities in space is a well-understood and accepted course of action, the offensive use of space is still hotly debated as a part of U.S. space policy. This paper discusses offensive counterspace operations and specifically how information weaponization of space will allow the operational planner to obtain information superiority in the battlespace. Information weaponization can accomplish the task, and consequently it provides a capability to attack and degrade or deny an enemy’s picture of the battlespace.
Abstract

While not a part of the operational factor trinity, information increasingly and profoundly affects the factors of space, time, and force, both individually and in combination. Space has become perhaps the key enabler for operational information for both the United States and its potential enemies. While defense of our capabilities in space is a well-understood and accepted course of action, the offensive use of space is still hotly debated as a part of U.S. space policy. This paper discusses offensive counterspace operations and specifically how information weaponization of space will allow the operational planner to obtain information superiority in the battlespace. Information weaponization can accomplish the task, and consequently it provides a capability to attack and degrade or deny an enemy’s picture of the battlespace.
“Fundamentally, the concept of operational factors rests on the commander’s ability to bring into rough balance the definable factors of space, time, and force versus the assigned operational or strategic objective. The balancing means that shortcomings or deficiencies in a factor of space, time or force is countered by advantages or surplus value of another factor so that the assigned objective can be accomplished. While not a part of operational factor trinity, information increasingly and profoundly affects the factors of space, time, and force, both individually and in combination. Information is in fact an integral part of each of them because the proper evaluation of forces, space, and time is possible only if based on precise information.”

Introduction

Space has become perhaps the key enabler for operational information for both the United States and its potential enemies. While defense of our capabilities in space is a well-understood and accepted course of action, the offensive use of space is still hotly debated as a part of U.S. space policy. Space control, or offensive counterspace operations, is a tool to help shape the battlespace that has been considered and planned for, but has been set aside as a matter of policy. One reason is that it is too difficult to accomplish without serious consequences. This paper discusses offensive counterspace operations and specifically how information weaponization of space will allow the operational planner to obtain information superiority in the battlespace. This will greatly enhance our ability to conduct strategic operations in any theater around the globe.

Of the countless articles written on how to achieve space superiority by using offensive counterspace tools, most rely on destructive methods, notably anti-satellite systems (ASATs), lasers, electromagnetic pulse (EMP) weapons, and other examples of “interesting” approaches. These arguments have been discussed in great detail, and this paper will not address them.
Regardless, as the world becomes more dependent on space assets, i.e., satellites, (commercial and military), information, and networks, these systems will become a critical vulnerability. Since it is relatively impractical to physically attack satellites, we should use methods that are capable, practical, and deniable to some extent. Information weaponization, can accomplish the task, and consequently it provides a capability to attack and degrade or deny an enemy’s picture of the battlespace. Thus, the operational planner gains another tool to help shape and prepare the battlespace.

**Defense Strategy**

In the “Defense Strategy” section, the 1996 Quadrennial Defense Review (QDR) identifies several vital U.S. national interests, including “ensuring freedom of the seas and security of international sea lines of communication, airways, and space.” To protect these interests, this report notes that the ability to deter aggression and coercion rests, among several factors, on having “conventional warfighting capabilities that are credible across the full spectrum of military operations.” These capabilities need to be “strategically stationed” or “rapidly deployable,” so that the United States has the capability of reacting quickly to any contingency. This report states that responses could include “limited strikes,” which would need to be conducted “in any environment, including one in which an adversary uses asymmetric means, including nuclear, biological, and chemical (NBC) weapons.”

This report also identifies three requirements associated with the strategy of fighting and winning two major regional contingencies. The first is to be “able to rapidly defeat initial enemy advances short of their objectives in two theaters in close succession, one followed almost
immediately by another."\textsuperscript{6} The other two requirements call for forces able to operate against asymmetric threats, such as NBC weapons, and the ability to “transition to fighting major theater wars from a posture of global engagement.”\textsuperscript{7} The QDR plans to achieve the required military capabilities, in part, with the new technologies emerging from the revolution in military affairs (RMA) by harnessing “new technologies to give U.S. forces greater military capabilities through advanced concepts, doctrine, and organizations so that they can dominate any future battlefield.”\textsuperscript{8} Finally, near the end of the “Defense Strategy” section, the QDR identifies critical enablers for the strategy.\textsuperscript{9} Space is one of those critical enablers, and information weaponization may emerge as a key element of the RMA.

\section*{Information Protection}

Since information has become a key element of government, business, and defense activities, DOD must provide leadership on the current U.S. and international use of space. The extensive use of space for all manner of national activities – civil, commercial, military, and intelligence – has greatly enhanced the effectiveness of U.S. efforts. However, this use of space has created a new vital interest, and presented a huge challenge to the military to protect the key elements of the national infrastructure that are beyond the physical borders of U.S. territory. At the same time, increasing the use of space by other nations has also enhanced the effectiveness of these nations, while creating new vulnerabilities as well.

With the increasing number of countries (and even non-state actors) that have access to space – not to mention other technologies that allow power to be projected into space – the likelihood of earth-bound conflicts spreading into space is growing. However, given the present situation and current trends, our country gains the most from space and thereby has the most
vulnerability to losing space capabilities. This fact, more than any other, will persuade potential U.S. adversaries to develop capabilities to combat America’s asymmetric space advantage. The prospect of these potential adversaries – Iraq, Iran, Libya, etc – agreeing to arms control treaties, much less complying with them, is not encouraging. Once this reality is acknowledged and appropriate conclusions drawn about the U.S. situation, decision-makers will be more inclined to pursue countervailing capabilities both to defend U.S. space assets as well as to project power against the space – and terrestrial – assets of potential adversaries. Space is one of those critical enablers.

**Space Control**

Space control capabilities (also known as counterspace or control of space capabilities) protect the use of space and deny its use to an adversary. Space control is necessary to preserve the force multiplying effect that space assets generate for terrestrial military forces through intelligence/surveillance/reconnaissance (ISR), weather, missile launch warning, and precision navigation data, as well as communication capabilities. At the same time, space control prevents an adversary from using this same militarily useful space for their own, third party, and U.S./allied space systems. To be useful, space control does not have to be achieved throughout all of outer space (i.e., it can be a local condition over a theater or smaller area). It also does not necessarily mean that an adversary has been totally denied the use of any space assets, although this is the highest possible goal, just as air supremacy is the highest possible goal of counterair operations. Space control is composed of four areas of space surveillance,
Of the four areas, negation and prevention have the most applicability to our offensive counterspace task.

**Negation**

Negation involves active operations to deny an adversary the use of space. USSPACECOM identifies three key tasks in this area: “Target Identification – complicated by a dynamic, networked environment; Weaponeering – must be precise to achieve desired effects; and Operations Cycle – includes mission planning, execution, and combat assessment.” Negation operations can be described in terms of the five “D’s”: destroy, degrade, disrupt, deny, and deceive. The first two “D’s” – destroy and degrade – involve physical damage of the satellite, which usually results in a permanent effect on the mission; “destroy” completely negates the satellite’s mission while “degrade” only partially negates the mission. The second two “D’s” – disrupt and deny – are temporary conditions which do not result in any permanent damage to the satellite’s mission and likely not to the physical satellite; “deny” is the total temporary negation of the satellite’s mission while “disrupt” is the partial temporary negation of the mission. The fifth “D” – deception – refers to actions that create false information within the satellite’s data (i.e., a form of information operations). The various “D’s” can be accomplished a number of ways, including application of energy by physical contact (kinetic energy attacks with missiles or particle beams) or by some type of electromagnetic radiation (including visible/infrared lasers, high power microwaves, or other radio frequency energy). The weapons that deliver this energy can be earth-based or space-based. Information weaponization addresses the last four "Ds" and consequently gives us a capability that should be considered.
Negation attacks can be made against any element of the satellite system, including the space segment, the link segment, or the ground segment (where the ground segment could actually be located in the air, on or under the sea, or underground as well as on the ground). Attacks against the ground segment could be made by weapons in space, but also by earth-based weapons. Consequently, not all negation activities involve space weapons, since neither the weapon nor the target of the weapon are in space.

One important preference would be for weapons that have temporary or reversible effects. This would help make them more acceptable internationally and provide more flexibility against third party satellites being used by an adversary. Another would be for weapons that are highly selective or surgical -- can deny specific services on a satellite – to make these effects more acceptable and flexible. However, kinetic energy weapons that attack targets in space would be restricted by the policy guidelines on debris and protection of U.S./allied/friendly satellites, which would affect peacetime testing and wartime operations.

**Prevention**

Prevention involves activities to deny adversaries the use of information or services from U.S. or other nation's space assets. USSPACECOM identifies three key tasks: “Detect Use – both unauthorized use and exploitation of U.S. and third party systems; Assess Mission Impact – to drive course of action development; Timely and Flexible Reaction – using all actions short of military response.” These activities have largely diplomatic implications for other nation’s satellites. For U.S. satellites, various prevention techniques are possible, including use of selective availability settings for navigation satellite data or turning off satellite broadcasts in the desired region of denial. Since USSPACECOM has defined this part of space control as using
only non-military actions, there are no parts of protection applicable to weaponization.

However, information weaponization may serve this purpose well in lieu of "normal"
weaponization.

Non-destructive Approaches to Offensive Counterspace

Space-based anti-satellite weapons could deny an enemy the ability to use its space-
based systems. These concepts are expensive and pose many technical challenges.

Alternatives to space-based weapons have the potential to be equally effective, more flexible,
more technologically feasible, and less expensive.

Diplomacy

The least expensive approach to denying an enemy access to space is most practical
against nations that rely on leasing third-party assets. This condition could be prevalent as
commercial enterprise devoted to providing communications become even more common.
Consequently it may be possible to convince the corporations or nations providing the service to
cut off access during a conflict. In fact doing much more may be politically impractical, since
direct attacks would be difficult to justify even if it could be proven that a corporation was
providing an adversary with satellite support.

Unfortunately diplomatic pressure may not be effective since corporations will lose
customers if they cannot be relied upon in emergencies. This approach also requires the United
States to have considerable international support, which would raise concerns if the United
States acted unilaterally.¹³
The potential problems with a diplomatic approach were highlighted during the Persian Gulf War. The Iraqi government had been buying satellite imagery from the French company SPOT Image prior to the war, but international condemnation of Iraqi actions prompted the company to cut off access. SPOT Image also refused to provide imagery to television and other media organizations, which prevented Iraq from gathering information from these sources. A potential shortcoming of this approach is illustrated by the fact that SPOT Image retained the option of selling imagery to the media if another source started doing so. In fact, the Earth Observation Satellite Company (EOSAT) started selling directly to Iraq despite the US embargo. Fortunately the images available from EOSAT were of lower resolution than those produced by SPOT (30 meter versus 10 meter resolution), which permitted SPOT Image to hold to its initial decision.12

Nondestructive Jamming

A more practical approach to denying an enemy use of his space-based assets may be to jam the communication links between satellites and ground stations. Since this approach would not damage satellites, commercial enterprises that may own them would be less of a concern, thus it might also make it more viable. However jamming communications between satellites and ground stations may prove difficult because the large antennas used by ground stations are highly directional, which would require considerable amounts of power. An additional problem would be positioning the jamming platform within the line of sight of the target ground station. Such an approach would depend on having total air supremacy, which may not always prevail. Some satellite-dependent communications systems, on the other hand,
are easier to jam. These systems rely on lower power, non-directional antennas on the ground, and sensitive receivers on the satellite.

An important objective in most conflicts is to disrupt the enemy’s command and control system. In conventional wars against small, less sophisticated enemies (for instance Iraq), it has usually been easy to do this, but new developments in communications may make this more difficult in the future. Cellular telephone systems with global coverage use large constellations of satellites in low orbit to carry phone calls around the world. A relatively small nation, such as Iraq or Yugoslavia, could easily purchase sufficient capacity on these systems to provide military communications throughout its country. While such a service would be expensive, it would cost much less than building an entire satellite communication system. The problems it creates for any country attempting to disrupt this type of communication system may make it a particularly attractive option.

When attempting to disrupt an enemy’s command and control network it could be problematic for the United States to destroy the third-party commercial satellites that comprise it. Destroying all of the satellites would not only be very expensive in terms of weapons required, but also the corporations that own those satellites and other nations would probably condemn such actions. While the United States could ignore international opinion if the reason is important, a less controversial solution would be preferable. Ideally it would be possible to persuade the corporation running the system to deactivate service to an opponent, but this may not always be the case. The best method for interrupting these communications may be conventional jamming of the handheld phones used by field commanders. While this is not an
elegant solution, it is feasible since any large-scale interference with a satellite-based telephone system would have global implications.

If an adversary owns and maintains its space-based assets, then the United States would have freer reign in disrupting them. One method would be to prevent the satellites from receiving commands from the ground. While jamming the large, highly directional antennas of the ground stations might be difficult, satellite antennas, conversely are vulnerable. The results of jamming these signals would vary from slow degradation of the orbit, to disrupting SATCOM networks, to preventing reconnaissance satellites from being tasked. This later effect may be useful, but its effectiveness would be difficult to verify, since it might not be obvious that a reconnaissance satellite is no longer performing its mission.

Another type of jamming possible against reconnaissance satellites that take visual or infrared (IR) picture is to use portable devices that track a satellite while it is overhead and train a laser on it. Experiments have shown that even low-power lasers can temporarily blind optical sensors. Even relatively low-power lasers have demonstrated the capability to damage the optical sensors of satellites. An engineering experiment was conducted at White Sands, New Mexico that directed a 30-watt laser at an orbiting test satellite. Even this low-powered laser caused enough damage to create “a lot of panic,” at the Pentagon.

Command Override

Rather than jamming, another approach may be to take command of a problem satellite via brute force (very high wattage) override. It may be possible to break the codes used to command the maneuvers of a satellite and send spurious instructions. If transmitters were placed so that they could greatly overpower legitimate commands, or send commands when the
legitimate transmitters are out of range, a satellite could be prevented from performing its mission. In contrast to jamming a satellite, the reactions of the satellite would make it possible to verify the attack had been successful. It is unlikely that a brute force command override would go undetected by an enemy; therefore the "plausible deniability" aspect would be lost.

**Space Tug**

Another alternative would be to develop a satellite capable of physically moving an uncooperative satellite. This “space tug” has been proposed for regaining control of malfunctioning satellites that are trapped in useless orbits or do not respond to maneuver commands. The same device could be used to disrupt control of a third party or enemy satellite by maneuvering it so that it could not take pictures of the designated area. If the satellite’s owners were unable to monitor other spacecraft in orbit, then this assault could possibly be made surreptitiously. The challenges of launching a "space tug" and surreptitiously maneuvering into position make this option difficult to accomplish. An enemy would doubtlessly regard this, at the least, an act of piracy, and at the most an act of war.

**Nondestructive Offensive Counterspace Summary**

Alternatives to physically destroying an enemy’s space-based assets offer the least controversial approaches to denying an enemy’s access to space. From diplomatic efforts with third party providers, to jamming command and control links, nondestructive methods could be both effective and inexpensive. These approaches would be most effective against a less capable foe, while a peer competitor probably could counter them. Considering the potential implications of an enemy’s unhindered access to space, it is also prudent to consider more
definitive measures for space control. Information weaponization can be that more definitive measure.

Information Weaponization

While each of the above mentioned space control counter measures has advantages and disadvantages, the disadvantages are substantial enough to force us to consider other methods. Information weaponization has the potential to provide an offensive counter measure that is acceptable to political and operational planners. Direct attacks on an enemy’s satellites in peacetime as part of a pre-emptive operation could alert an opponent that an attack is eminent, and could trigger a counter attack on U.S. satellite systems. Since the United States is more dependent on its satellite systems, this may prove prohibitive to operational planners. If an enemy was probed or “attacked” by an undetectable cyber weapon, there would probably be a lower likelihood of a counter attack or an alerting of their forces. However, information warfare weapons could be restricted by policy guidelines that define satellites as sovereign territory and interpret any interference with their operations as an infringement on those rights. This is due to the importance of determining potential information warfare attack paths and its likely effects prior to a wartime attack. A policy consideration would have to be made to accommodate this need.

There have been countless probes and “cyber attacks” on government and non-government computer systems in recent years. The Pentagon has been under attack by an unknown assailant for several years by a program dubbed “Moonlight Maze.” It seems reasonable that the United States military might develop similar capabilities that permit similar
probes or attacks. It follows that this capability could be a tool the operational planner could use when planning course of action.

There are two aspects of every satellite, the command and control and mission elements. The command and control portion is, in general, the attitude control, orbital position, power management, and overall disposition of the satellite. The mission portion is the communications, intelligence, navigation, or early warning missions (among others) that the satellite was designed to do. Both “ends” of the satellite are electronically vulnerable with different results from attack.

The mission end of a satellite can theoretically be spoofed, jammed, or fed incorrect information, which could induce a "psychological operations" effect. The enemy thinks that it has a clear picture of the battlespace, when in fact it has been given a picture that has been manipulated. Obviously, if the enemy is relying on information that has been altered, it will deploy forces and plan actions that could be advantageous to the United States. This could allow us to mass or maneuver without detection, and provide a measure of security for U.S. forces.

Conversely, instead of attacking the mission end of the enemy’s satellite, we could attack the command and control end. This effect could be best described as causing a loss of the basic health of the satellite. A command that turns on thrusters could cause a satellite to tumble. Turning off the satellite’s battery recharging capability could cause it to “black out.” We could also turn off a receiver that was used to input commands causing it to drift into an unusable orbit or into a different altitude. The effect of these efforts would be a useless rather
than a spoofed satellite. The enemy would have a reduced picture of the battlespace. Again a semi-blinded enemy would permit operational planners greater latitude of options of action.

Information warfare operators are likely to be on the ground and use transmitters in space to relay instructions to targets. This situation reinforces the point that there are no space-based versions of information warfare (disregarding the case of an astronaut in the shuttle, the international space station, or some future space plane acting as the information warfare operator, since this is unlikely in the foreseeable future). However, one could envision an information warfare attack that uses a space-based transmitter as a relay in an analogous fashion to a ground-based laser using an orbiting mirror to direct the laser beam to a remote target. In both the IW and laser cases, the space-based element that directs the attack against the remote target becomes a space weapon.

**Conclusion**

As space becomes even more important in providing information to operational commanders, we must find better ways to exploit it. Information and its influence on the operational factors of time, space, and forces will become even more critical in the future. Information warfare as a part of offensive counterspace operations will allow us to affect the enemy’s ability to receive information. Whether the information is corrupted, manipulated, reduced, or eliminated does not matter because the advantage will be a matter of degree. The effects that information has on the operational factors will determine the overall advantage we gain from an information weaponization of space.
Notes

1 Milan N. Vego, *Operational Warfare*, (Naval War College Publication 1004, 2000), 95
3 Ibid., 5.
4 Ibid., 5.
5 Ibid., 7.
6 Ibid., 9.
7 Ibid., 9.
8 Ibid., 11.
9 Ibid., The United States must retain superiority in space. Global intelligence collection, navigation support, meteorological forecasting, and communications rely on space-based assets. To maintain our current advantage in space even as more users develop capabilities and access, we must focus sufficient intelligence efforts on monitoring foreign use of space-based assets as well as develop the capabilities required to protect our systems and prevent hostile use of space by an adversary.
11 Ibid., CoS-53
12 USSPACECOM, *USSPACECOM Long Range Plan (Draft)*, 12 Dec 97, CoS-43
17 Ibid, the create “a lot of panic…” is based on personal experience, I was in the Pentagon when the results of the laser test were briefed and many senior leaders were concerned with how the public and the rest of the world would perceive our efforts
18 National Science and Technology Council, *Fact Sheet*, 2.
Referenced Bibliography


Selected Bibliography