# Satellite Vulnerabilities

EWS Contemporary Issue Paper

Submitted by Captain J. W. Rooker

to

Major R. F. Revoir

18 February 2008

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **18 FEB 2008** | | **00-00-2008 to 00-00-2008** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Satellite Vulnerabilities** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Marine Corps,Command and Staff College, Marine Corps Combat Development,Marine Corps University, 2076 South Street,Quantico,VA,22134-5068** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **Same as Report (SAR)** | **17** | |

From the Gulf War to Operation Iraqi Freedom, use of satellite communications increased more than 300%, and the data rate to support such operations went up by 500%[1]. More and more, the United States Marine Corps is becoming dependent on satellite communications. Perhaps the U.S. Military has become too dependent on satellite communications, which are subject to weather, and increasingly vulnerable to attack, and this is dangerous for the nation and its security. The Military's reliance on satellites for communications and navigational solutions is a vulnerability that puts us at risk.

## Vulnerabilities

Satellites are vulnerable to varieties of attack or degradation, and abilities to protect or compensate are limited. Some satellite links deteriorate when subjected to weather. Nearly all satellites are assailable by technological capabilities ranging from direct ascent weaponry to jamming, spoofing, and hacking.

## Weather

Weather effects on satellite communications can be divided roughly into two categories: terrestrial, and extra-terrestrial. Terrestrial effects are those comprised of planetary weather systems, like rain, that affect satellite communications. Extra-terrestrial weather effects, often called ‘space weather’, are rather more complicated, and range from solar flares to cosmic radiation. Scintillation can also degrade satellite signals. Scintillation is caused by irregularities in the Earth’s ionosphere. This phenomenon can cause severe signal fading to any signal transiting the ionosphere, and can affect, and does, Very High Frequency ranges through L- and C-bands[2]. In any of these cases, the end result is degradation or loss of the signal.

## Technology

Physical attack capabilities are wide ranging. The most accessible targets are right here on Earth. Ground control stations, industrial sites, and critical individuals are all possible objectives for an anti-satellite strike. Attacks could range from simple explosives, to assaults on facilities, to the targeting of critical personnel[3].

Another category of anti-satellite weaponry is known as ‘direct ascent’ weapons. These are rockets fired either from the

planet’s surface, or wing-launched from a high-altitude aircraft, and use kinetic energy to disable or destroy an intended target. For example, rockets carrying a payload of metallic pellets, ball-bearings, or the like, which, having been spread by an appropriate explosive charge, could strike targeted satellites with relative velocities measured in values up to hundreds of miles per second, or more[4], disabling or destroying them. Such rockets are already in use by a number of other nations, including Japan, India, and Brazil[5].

From direct ascent weapons, we move to long duration orbital interceptors. These are anti-satellite weapons that have been launched into parking orbits, and which remain dormant there for months or years in preparation for future use. Russia, at least, is known to possess co-orbital anti-satellite weaponry[6].

Another class of anti-satellite weapons technologies is directed energy weapons. This includes anti-satellite lasers, radio frequency, and particle beam weapons. Lasers damage their targets by heat energy, while the effects of radio frequency weapons, which use bursts of high-powered radio frequency energy to disable electronic components, are more subtle. China is known to possess anti-satellite laser weapons, and to be

developing other directed energy anti-satellite weapons platforms[7].

In addition to physical attacks, satellite communications are also vulnerable to several types of electronic attack. These electronic attack forms generally take the forms of jamming, or spoofing. Jamming is the intentional transmission of radio frequency signals used to disrupt other radio frequency signals. Spoofing is sending fake signals to a system receiver in order to induce it to accept, as valid, someone or something that is not.

Jamming can take a variety of forms. The uplink may be jammed, or the downlink, or the signal may be overpowered. These are related, but different, capabilities. Jamming the uplink requires a directed antenna, knowledge of the frequency to be affected, and enough power to override its source. An example of uplink jamming occurred in the summer of 2003 when a signal emanating from Cuba jammed a U.S. satellite transmission to Iran on a commercial communications satellite[8]. Jamming the downlink is the same. The United States Military already has a demonstrated vulnerability to this per its reliance on the Global Positioning System (GPS). During tank trials in Greece, the British Challenger and United States Abrams suffered from GPS navigational problems. An investigation later revealed that

those signals were being jammed by a French security agency[9]. The possible consequences to our forces during combat operations due to similar actions by a hostile nation or other aggressor are staggering, and we need to prevent it from happing in combat.

Satellite links may also be over-powered. Some readers may be old enough to remember the ‘Captain Midnight’ incident of this type. In April of 1986, a Florida man used the teleport equipment where he worked to over-power HBO’s signal to a commercial satellite, interrupt the movie in progress, and broadcast his own message. While many people found this amusing, it should be understood that the satellites upon which so much of the military’s communications depend are potentially vulnerable to similar attacks, which is not very funny at all.

Satellite communications systems are also vulnerable to hacking, just like other computer operated and controlled equipment. A successful hack of satellite control systems could allow for options ranging from control to destruction of the satellite in question. In his paper, Kevin Poulsen notes that “Critical commercial satellite systems relied upon by federal agencies, civilians and the Pentagon are potentially vulnerable to a variety of sophisticated hack attacks that could cause service disruptions, or even send a satellite spinning out of control, according to a new report by the General Accounting Office, the investigative arm of Congress”[10]. He goes on to say

that “some satellite companies don't encrypt the tracking and control uplinks through which the satellites are controlled from the ground, making them vulnerable to spoofing, with potentially dire results”[11].

## United States Warfighting Reliance on Satellites

The United States has become reliant on its satellite communications for the prosecution of armed conflict, most especially in the form of GPS capable or dependent weapon systems. In its conduct of the current war on terror in Iraq, the United States has made habitual use of precision guided munitions, like the Joint Direct Attack Munition (JDAM). The United States recently used a new, GPS guided artillery round called the Excalibur in combat for the first time in Iraq, with successful results[12]. During the battle for Fallujah, GPS guided munitions allowed for close air support to be brought in as close as one hundred meters from friendly forces, when the traditional distance for such support was one thousand meters[13]. Robert S. Dickman, retired Air Force General and Air Force deputy undersecretary for military space said, “We can’t fight without space”.[14] If an enemy learns to spoof false GPS data into our GPS reliant weapons, they could be turned against us, or our allies.

## Satellites and Intelligence, Surveillance, and Reconnaissance

We have become dependent also on our satellite surveillance assets in order to fight more effectively. Satellites, and satellite communications, “played a major role in providing coalition forces with round-the-clock, uninterrupted ISR”, with “space intelligence, surveillance, and reconnaissance (ISR) systems…fundamental to air power—especially to the execution of rapid-response air strikes.[15] Surveillance satellites provided unprecedented coverage of the battlefield and continue to do so, giving us a tremendous informational and intelligence advantage. But if we lose those satellites, or the links to them, we also lose the advantages of them, and have nothing with which to span the breach. Imagine how much less effective would be the war on terror without these capabilities.

The unmanned aerial vehicles (UAVs) that we employ, and on which we rely so heavily, have become dependent on satellite communications, particularly GPS. The impressive Global Hawk UAV that has provided so much useful, real-time surveillance data for the warfighters and decision makers depends on Ku-band satellite communications, as well as GPS, in order to function[16]. The Hellfire capable Predator UAV is similarly reliant[17]. The Marine Corps’ own Scan Eagle has comparable requirements[18]. If an

enemy can disable or destroy the satellites on which these systems depend, or hack, jam, or spoof them, he will have effectively gouged out our eyes.

## Satellites, Communications, and C2

We now depend on satellites and their communications systems to provide us with command and control of our forces. “Communications satellites were the key to distributing information among weapon systems, sensors, command posts, and forces in the field…the central function of space systems is to provide satellite linkages for theater and battle-zone communications, thereby surmounting line-of-sight limitations and extending the range of voice and data transmissions that are crucial to ISR and to timely command and control”[19]. Again, this clearly implies that if we lose those systems or links, we also lose, or at best severely degrade, a critical warfighting function, and we do not have the same capability resident in a non-satellite platform, and we should, or we should develop something comparable.

## Consider the Consequences

The possible consequences of not just losing our satellite

communications capabilities, but of having them subverted, are both wide ranging, and potentially staggering, both socially, and politically. As described above, our GPS equipped tanks have proven vulnerable to foreign interference. What might happen if our precision guided munitions were jammed?

Imagine a scenario where the GPS guided Excalibur artillery round, having been jammed, struck wide of its intended target. What would happen if it landed in a crowded street? What if a jammed JDAM fell on an open-air market, and killed several hundred civilians? We all remember just how ferociously world opinion turned against Serbia and the Serbs after a mortar attack on a market in Sarajevo. That sort of public opinion fire-storm, spurred on by the media, could be devastating to the war effort, and the enemy's information operations campaign would surely exploit it to our disadvantage. We cannot afford that.

From jamming such a signal, it's a short theoretical step to hacking and spoofing; if it can be jammed, sooner or later it will also be vulnerable to someone else's control. As stated, nations like Russia and China are working diligently to subvert our satellite C2 capabilities. If our GPS system were hacked, an enemy could feed false data to any and all of our dependent weapons systems, and potentially cause them to strike wherever they pleased. They could direct them against our forces, and

that would be bad enough. What if they were intentionally directed against our allies? That might fracture the coalition. If they were directed against a mosque, or a schoolyard, the fallout would make Hadditha pale in comparison. The damage to our national prestige and credibility might be irreparable.

Satellites, and satellite based services, continue to be of great utility to the armed services. They are tools of which we should take advantage, but not at the cost of putting ourselves, and our nation, in jeopardy by relying on them so totally. While capable, they are corruptible, and while valuable, they are more and more vulnerable. No nation can afford to have all its eggs in one basket; alternatives need to be considered, developed, and implemented.

Notes

[1] O'Hanlon, Michael. "The State of Space: From Strategic Reconnaissance to Tactical Warfighting to Possible Weaponization." *Global* Security. 21 June 2006. < http://www.globalsecurity .org/space/library/congress

/2006_h/060621-ohanlon.pdf> (17 December 2007)

[2] Kennewell, John, and McDonald, Andrew, *Satellite Communications and Space Weather*, <http://www.ips.gov.au/Educational/1/3/2> , (2 December 2007)

[3] Dinerman, Taylor, "Hybrid wars and satellite vulnerabilities" thespacereview. 13 March, 2006. <http://www.thespacereview.com/article/574/1>

[4] Adams, Thomas K., Lieutenant Colonel, United Sates Army, Retired, "10 GPS Vulnerabilities". <http://www.c4i.org/gps-adams.html>

[5] Thomson, Allen, "Satellite Vulnerability: a post-Cold War issue?", fas.org. February 1995. <http://www.fas.org/spp/eprint/at_sp.htm>

[6] Grego, Laura. "A History of Anti-Satellite Weapons Programs". ucsusa.org. 30 May, 2006. <http://www.ucsusa.org/global_security/space_weapons/a-history-of-asat-programs.html>

[7] Dougherty, John E. "China advancing laser weapons program." WorldNetDaily. 22 November, 1999. <http://www.wnd.com/news/article.asp?ARTICLE_ID=15233>

[8] Broadcasting Board of Governors, *BBG Condemns Cuba's Jamming of Satellite TV Broadcasts to Iran*, 15 July 2003, <http://www.fas.org/irp/2003/07/ bbg071503.html> (9 Dec 2007)

[9] Adams, Thomas K., Lieutenant Colonel, United States Army, Retired, *10 GPS Vulnerabilities*, <http://www.c4i.org/gps-adams.html>, (2 Dec 2007)

[10] Poulsen, Kevin, *Satellite systems hackable – study*, 9 October 2002,<http://www.theregister.co.uk/2002/10/09/satellite_systems_hackable_study/> (2 December 2007)

[11] Poulsen, Kevin, *Satellite systems hackable – study*, 9 October 2002,<http://www.theregister.co.uk/2002/10/09/satellite_systems_hackable_study/> (2 December 2007)

[12] Multi-National Corps—Iraq, Public Affairs Office, Camp Victory, *Precision guided munitions kills top al Qaeda leader*, 17 July 2007, <http://www.mnf- iraq.com/index.php?option=com_content&task=view&id=12899&Itemid=128target=_blank> (3 February 2007)

[13] Stout, Jay, Lieutenant Colonel, United States Marine Corps, retired, *Close Air Support Using Armed UAVs?*, July 2005, < http://www.military.com/NewContent/0,13190,NI_0705_Air-P1,00.html> (3 February 2008)

[14] Canan, James W., *Iraq and the Space Factor*, <http://www.aiaa.org/aerospace/Article.cfm?issuetocid=393&ArchiveIssueID=41> (3 February 2008)

[15] Canan, James W., *Iraq and the Space Factor*, <http://www.aiaa.org/aerospace/Article.cfm?issuetocid=393&ArchiveIssueID=41> (3 February 2008)

[16] Air Force Technology, *RQ-4A/B Global Hawk High-Altitude, Long-Endurance, Unmanned Reconnaissance Aircraft, USA*, **<** http://www.airforce-technology.com/projects/global/> (3 February 2008

[17] Air Force Technology, *Predator RQ-1 / MQ-1 / MQ-9 Reaper - Unmanned Aerial Vehicle (UAV), USA*, < http://www.airforce-technology.com/projects/predator/> (3 February 2008)

[18] Katzman, Joe, *Scan Eagle UAVs a Success in Iraq*, <http://www.windsofchange.net/archives/006808.php> (3 February 2008)

[19] Canan, James W., *Iraq and the Space Factor*, <http://www.aiaa.org/aerospace/Article.cfm?issuetocid=393&ArchiveIssueID=41> (3 February 2008)

## Bibliography


Adams, Thomas K. “10 GPS Vulnerabilities”. *C4i.org*. <C4i.org/gps-adams.html> (2 December 2007.)

Akir, Ziad I. “Space Security: Possible Issues and Potential Solutions”. *College of Communication, Ohio University*. <http://satjournal.tcom.ohiou.edu /pdf/issue6/ziad.pdf> (2 December 2007).

Cavossa, David. “Satellites and U.S. National Power”. *Space*. <http://www.space.com/spacenews/archive06 /CavossaOpEd_071706.html> (2 December 2007).

Dinerman, Taylor. “Hybrid wars and satellite vulnerabilities”. *The Space Review*. 13 March 2006. <http://www.thespacereview.com/article/574/1>(2 December 2007).

Dougherty, Jon E. “China advancing laser weapons program Technology equals or surpasses U.S. capability”. *World Net Daily*. 22 November 1999. <http://www.wnd.com/news/ article.asp?ARTICLE_ID=15233> (2 December 2007).

Grego, Laura. “A History of Anti-Satellite Weapons Programs”. *The Union of Concerned Scientists*. <http://www.ucsusa.org/ global_security/space_weapons/a-history-of-asat-programs- .html> (2 December 2007).

Kennewell, Jon, and McDonald, Andrew. “Satellite Communications and Space Weather”. *Identity and Passport Service*. <http://www.ips.gov.au/Educational/1/3/2> (2 December 2007).

O’Hanlon, Michael. “The State of Space: From Strategic Reconnaissance to Tactical Warfighting to Possible Weaponization”. *Global Security*. 21 June 2006. <http://www.globalsecurity.org/space/library/congress/2006_h/060621-ohanlon.pdf> (17 December 2007).

Peters, Ralph. “A Maginot Line in the Sky Beat Our Satellites, Beat America”. *New York Post*. 26 October 2007. <http://www.nypost.com/seven/10262007/postopinion/opedcolumnists/a-maginot-line-in-the-sky.htm?page=0> (2 December 2007).

Poulsen, Kevin. “Satellite systems hackable-study Unencrypted uplinks invite hijinks”. *The Register*. 9 October 2002. <http://www.theregister.co.uk/2002/10/09/satellite_systems_hackable_study/> (2 December 2007).

Thomson, Allen. “Satellite Vulnerability: a post-Cold War Issue?”. *Federation of American Scientists*. 11 February 1995. <http://www.fas.org/spp/eprint/at_sp.htm> (2 December 2007).

Wilson, Tom. “Threats to United States Space Capabilities”. *Global Security*. <http://www.globalsecurity.org/space/library/report/2001/nssmo/article05.html#15> (2 December 2007).

“Hypothetical Attacks”. *Decode Systems*. <http://decodesystems.com/attacks.html.> (2 December 2007).

“Broadcasting Board of Governors Condemns Cuba’s Jamming of Satellite TV Broadcasts to Iran”. *Federation of American Scientists*. 15 July 2003. <http://www.fas.org/irp/news/2003/07/bbg071503.html> (2 December 2007).

Army Field Manuel 24-33, Chapter 3. “Remedial Electronic Counter-Countermeasures Techniques”. *Federation of American Scientists*. <http://ftp.fas.org/irp/doddir/army/fm24-33/fm242_4.htm> (2 December 2007).

“Libya jamming ‘exposed vulnerability’”. *British Broadcasting Corporation news*. <http://news.bbc.co.uk/2/hi/science/nature/4602674.stm> (2 December 2007).

Dougherty, Jon E. “China advancing laser weapons program”. *World Net Daily*. <http://www.wnd.com/news/article.asp?ARTICLE_ID=15233> (2 December 2007).