Space: The Next Cyber Frontier?

Wendy Lemke
Space Systems Academic Group
Naval Postgraduate School
Monterey, CA
wenona.lemke@navy.mil

Andrew Metzcus
Space Systems Academic Group
Naval Postgraduate School
Monterey, CA
ajmetzcu@nps.edu

Brad Kinkead
Space Systems Academic Group
Naval Postgraduate School
Monterey, CA
bradley.kinkead@ccsg3.navy.mil

Dave Schroeder
Space Systems Academic Group
Naval Postgraduate School
Monterey, CA
david.a.schroeder@navy.mil

***Abstract*—The United States is increasingly dependent on space systems for all manner of services in the civilian and military sectors. Recent events have demonstrated that degradation, denial, or disruption of space systems is possible via cyberattack, reducing the level of resources required for a potential attack by a state or non-state actor. Navigation and communications capabilities are prime targets for such attacks. Awareness of possible attack scenarios is critical to prevention and mitigation, and certain alternatives are available to replace or augment space systems in the event of a successful attack. (4395 words)**

Keywords—space; satelite; cyber; cybersecurity; survivability; GPS; SATCOM; communications; navigation

I. INTRODUCTION

Possibilities for exploiting, disabling, denying, or destroying space assets via cyber capabilities — as opposed to conventional kinetic or directed energy weapons — are growing. Recent space cyber events, mounting dependence on commercial space systems, and the increasing intersection between space and cyber mean that we need to identify, understand, and mitigate threats US space systems face in the cyber realm.

The United States is increasingly dependent on computers, networks, and information systems to conduct daily life. Similarly, the dependence of the United States military on information systems for command, control, communications, computers, combat systems, intelligence, surveillance, and reconnaissance (C5ISR) continues to grow. Many of these capabilities are delivered primarily or exclusively via space systems.

China, Russia, and the US are all known to have developed various kinetic and other capabilities to destroy, degrade, or deny use of space systems. However, the interconnectedness presented by the nexus of cyber and space systems means that attacks initiated in the cyber realm against space systems are now possible. Such attacks do not require expensive capabilities, and may even be initiated by non-state actors.

The increasing dependence of the US military and intelligence community on information systems — including those delivered via space assets — alongside stagnant budgets, has pushed acquisition programs to supplement government capabilities with commercial systems. These systems are often not as secure as military systems, introduce elements beyond our control, and present another attack vector for an adversary.

We must take steps to characterize, define, and understand the cyber threat against space systems. Cyber is a force multiplier, which allows devastating attacks against information systems to be mounted with comparatively little expense effort. As Stuxnet has shown us, cyber attacks can cause physical destruction. Our dependence on space systems demands a comprehensive understanding of, and defense against, the cyber threat.

II. BRIEF INTRODUCTION TO SPACE CYBERATTACK SCENARIOS

A. Cyberattack Against Ground and/or Space Segment

According to a report from the US-China Economic and Security Review Commissio — a key unclassified source of information about China's military capabilities — two US government satellites were victims of cyberattacks in 2007 and 2008. The satellites were Landsat 7 and Terra (EOS AM-1), both of which are used for earth observation. The report noted a concern that the hack may have been carried out by Chinese government hackers, probing how vulnerable satellite control systems are to such attacks. The hacks were carried out via a ground station in Norway whose systems are on the open internet. (Arthur, 2011) The report does not get into further detail, but is part of a pattern of cyber attacks thought to have originated with the Chinese government. In both cases, the attackers executed all steps to control the satellites, but did not exercise that control. "An intruder who managed to hack into a geosynchronous communications satellite might be able to turn off that satellite's communications to an entire region or order the satellite to fire its thrusters, bumping it out of its internationally assigned orbit." (Werner, 2012)

The report notes that China is "focusing their efforts on information systems technology used in military command, control, communications, and computers, as well as in intelligence, surveillance and reconnaissance applications." Chinese military writings indicate that their goal is "'destroying, damaging, and interfering' with reconnaissance and communications satellites in order to 'blind and deafen the enemy.'" (Walcott, 2012)

One expert put forth a scenario in which a redundant or less important satellite is hijacked and crashed into a vital one, meaning that the "target" satellite need not be the one breached via a cyber attack. The military has planned for the possibility of operating without services like GPS, but its loss would still have a major impact. (Taylor, 2012) Redundant, retired, parked, or decommissioned satellites could be commandeered via cyber means to destroy other satellites. This is a particularly novel theory on the cyber vulnerabilities of space systems: even if a military satellite itself cannot be attacked, it might still be vulnerable to a kinetic collision from another satellite, initiated via cyber means. (Little, 2012)

A report on a separate breach at NASA's Jet Propulsion Laboratory (JPL) from Chinese-based IP addresses found that "the intruders had compromised the accounts of the most privileged JPL users, giving the intruders access to most of JPL's networks." This is critical because of the source, and because of the scope of JPL's operations, which includes the operation of satellite and spacecraft systems. (Martin, 2012)

Bloomberg News obtained an early draft of the upcoming 2012 annual report of the US-China Economic and Security Review Commission. The report says that China is "'the most threatening actor in cyberspace' as its intelligence agencies and hackers use increasingly sophisticated techniques to gain access to U.S. military computers and defense contractors." A US official called China's efforts to blind or disrupt US intelligence and communications satellites "relentless." The report also detailed China's continued expansion of cyber capabilities, which could be used against military targets and critical infrastructure. Most cyber attacks relied on straightforward techniques, such as "zero-day" exploits. Chinese intrusions appear intended to collect intelligence or technology rather than launch attacks. (Capaccio, 2012)

III. Commercial Space Systems Dependency

A. Commercial Space Systems Dependency

Incredible amounts of information are available at our fingertips from almost anywhere in the world at nearly all times of the day. This nearly guaranteed access to information has changed the course of ordinary business, the availability of an education, and the way people interact. Snail mail, or writing a letter as it were, has been replaced by texting, tweeting, and posting on social networks. People everywhere have become so "interconnected" that it is integrated into their daily lives. However, this "interconnectedness" is not without risk. With the growth of our dependency to space-based communications, so has the threat of cyberattack on its infrastructure.

1) Reliance on Satellite Communications is High and Increasing

Space systems are an integral part of national security and use and access of commercial satellite systems has increased significantly over the last thirty years. Defense spending in support of the space industry has been exceeded by commercial industry in the last decade and, in turn, has provided U.S. military forces with improved capabilities in communications, remote sensing, navigation, and imagery. SATCOM services alone have increased nearly 50 percent in the last decade and global revenues have totaled $160 billion (2009). (Coleman, 2010) This increase in commercially available services, combined with a declining defense budget, has led the U.S. military to rely heavily on commercial services possibly more than on traditionally dedicated space capabilities. This obvious reliance raises a concern about space systems' vulnerability to cyberattacks. (Cooney, 2002)

2) Increasing Vulneratbilities to Cyberattacks

The commercial space industry is expanding into new services that provide advanced communications capabilities. However, the market considers countermeasures costly and unnecessary against threats they deem not likely. Increased IP voice, data and imagery capabilities and mobile broadband or communications-on-the-move capabilities has created an insatiable appetite for satellite capabilities. (Coleman, 2010) This dependence by both the public and the military reveals a vulnerability that an enemy even with little knowledge and expertise and small resources could exploit. The exploitation of space dependency can greatly benefit an unsophisticated foe by dramatically degrading countries with robust space capabilities efficiency economically. Since it appears our socio-economic well-being has become tied to space, what role should the U.S. Government and military play in assuring access for itself and civilians? (Caton, 1995-1996) "The U.S. is facing a dramatically increasing threat from cyberattacks and a future attack on the country's critical infrastructure could have an effect similar to the September 11 terrorist attacks of 2001." (Williams, 2012)

B. Cyberattack Vulnerabilities of SATCOM Services

In the last few years there have been various cyberattacks on satellites. Each attack seems to escalate in threat to the next. "Our nation's defense and critical infrastructure have become more reliant on satellite systems. That increased use and dependence comes with a downside. Because satellite systems are integrated into our national security systems and emergency response systems and are critical components to a modern military, they have become an attractive target of cyberattacks. As the reliance grows, so does the threats of cyberattacks from criminals, terrorists and nations." (Coleman, 2010) The most common forms of cyberattacks are Denial of Service, use of Malicious software (Malware), Accidental interference, and Deliberate interference (Jamming).

1) Denial of Service (DoS)

Most cyber organizations define a denial-of-service attack (DoS attack) as an attempt to make a machine or network resource unavailable to its intended users consisting of efforts of one or more people temporarily or indefinitely interrupting or suspending services of a host connected to the Internet. A recent example of DoS attack is the attacks on U.S. banks in the past few months, thought to have originated from Iran.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management. "Attacks on Capital One Financial Corp. and BB&T Corp. occurred on Tuesday and Wednesday. U.S. and banking officials described them as denial of service strikes preventing customers from accessing their information from banking websites." (Mount, 2012) The purpose of these attacks, and others like them, are to saturate the target machine (bank servers in this case) with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable.

2) Malicious Software (Malware)

Malicious software, or malware, is defined as software used or created by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. Malware is designed to infiltrate and damage computers without the users consent. Malware is a general term used to refer to a variety of forms of hostile or intrusive software including viruses, spyware, worms, Trojans, and rootkits to name a few. Malware and an internet connection to satellites through a ground station in Norway allowed hackers to interfere with the operation of two U.S. government satellites in 2007 and 2008. The hackers gained command privileges to the satellite and could have used this to deny or degrade satellite communications in an entire region. (Werner, 2012)

3) Deliberate Interference

Deliberate interference is the intentional jamming or spoofing of a satellite signal. This means saturating the airways with electronic noise at the same bandwidth that the satellite is using to communicate to its ground receiver. An example of deliberate interference, or jamming, against a commercial satellite recently was when Libyan actors jammed Thuraya in 2011. Additionally, Iran has presumably jammed Eutelsat satellite broadcasts extensively and possibly Nilesat and Arabsat as well. The hackers who used malware to gain command privileges to Landsat 7 and Terra deliberately interfered with the satellites' mission by spoofing it. This means they illegally controlled a satellite or made a legitimate controller adjust a satellite that didn't need to be adjusted to the detriment of the satellite and/or its mission.

C. Resilience to Disruption of SATCOM Services

Commercial satellite communications are not naturally resilient to disruption and many were built before the realization that cyberattacks would become so prevalent across all electronic communications platforms. "The infrastructures that gird and support the sinews of information-age society are unacceptably vulnerable to incidental, accidental and intentional disruption from terrorists, criminals, rogue states or peer adversaries. This weakness is so egregious it proffers the alluring, inexpensive and simple alternative of asymmetric strikes that could end run the world's most potent military power." (Campen, 1998) Attacking our space systems could provide an enemy with excellent leverage by degrading our combat efficiency and effectiveness. The Military Integrated Satellite Communications (MISC) study was devised to evaluate the ability of commercial SATCOM systems to satisfy Department of Defense (DOD) requirements. The study was not released publically but the conclusion was that none of the commercial systems are able to support the highly survivable, hardened requirements. "Commercial systems are hardened for life extension in the space environment; however, they do not provide anti-scintillation protection." (Hook, 1999) An enemy has much to gain by exploiting the dependency link between our terrestrial forces and force-enhancing space systems. An assault on U.S. military space systems is a force multiplier for an enemy. An attack on our space assets could impact every element of national power—political, diplomatic, economic, and military. Because "business, government, emergency responders and the military continue to expand their use of space-based assets for communications and real-time remote sensing" steps need to be taken to manage and defend commercial space cyber infrastructure to ensure reliable and available systems. (Coleman, 2010)

1) Vulnerability Mitigation

The potential for a devastating large scale network failure, service interruption, or the total unavailability of service is ever present and continues to increase in volume and complexity from a range of relatively minor acts including cyber vandalism and theft of intellectual property, to more serious crimes such as extortion, industrial espionage, and the stoppage of production and services. In general, the U.S. commercial sector is not well prepared to handle the range of potential threats to its space systems. However, there are cyberwafare/cybersecurity institutions that seek out vulnerabilities and produce protection systems to safeguard the cyber infrastructure and thereby improve the Nation's cybersecurity posture. Some additional courses of action and available technologies that could be used to counter threats to U.S. space capabilities are incorporating hardening, shielding, and redundancy into space systems; developing reliable threat analyses; mobilizing ground control stations; autonomous operations; onboard decoys and systems for attack reporting; and maneuverability. (Giffen, 1982, p. 33-45)

D. Infrastructure Management

Human activities are supported by infrastructures such as water supply networks (for consumption and agriculture), energy production networks, road transport, etc. The monitoring and the control of these infrastructures often rely heavily on telecommunication networks. Other economic activities, such as banking, also rely on telecommunication networks, as may some health related and manufacturing activities. This strong dependence with satellite communication services makes it important for the community at large to understand the nature and the potentials of cyberattacks, their effects, the protection measures that should be in place and those that are actually in place, the cost of implementing these measures and the cost of not implementing them. United States Strategic Command (USSTRATCOM) is charged with managing the DOD cyberspace infrastructure and they have further tasked it to United States Cyber Command (USCYBERCOM). The Department of Homeland Security (DHS) "is responsible for overseeing the protection of the.gov domain and for providing assistance and expertise to private sector owners and operators" and play a key role in securing the federal government's civilian cyber networks. (DHS, 2012) Both essentially manage the infrastructure through:

- partnerships with owners and operators of critical infrastructure such as financial systems, chemical plants, and water and electric utilities
- the release of actionable cyber alerts
- investigations and arrests of cyber criminals, and
- education about how the public can stay safe online. (DHS, 2012)

USSTRATCOM, USCYBERCOM and DHS work with the public, private, and non-profit sectors, and every level of government to address the increasing threats and risks of cyberattack on satellite systems.

1) Survivability

"An effective survivability strategy must begin with the decision of which space-based capabilities must survive to support strategic and tactical forces throughout the spectrum of conflict." [10] (Giffen, 1982, p. 52) In the case of commercial satellite survivability, this decision must also take into consideration economic impacts. Generally, hardening, mobility, maneuverability, autonomy, and variable orbit selection techniques will increase space systems survivability. Obviously all of these are not going to be used by the space industry as it would detrimentally increase costs and slow down the design, production, and deployment of satellites.

2) Redundancy

Redundancy requires that spare or reserve satellites be maintained on-orbit and/or replacement satellites that can be launched into orbit on short notice. In either case, an advanced commitment of resources (money) is needed as well as a capability to rapidly launch, which the U.S. does not maintain. The premise behind this concept is that if one satellite fails or is defeated by cyberattack then the other satellites will be available to execute all or some percentage of the essential functions of the mission. Similar to survivability issue, redundancy is very expensive and does not guarantee success. (Giffen, 1982, p. 52)

E. Enhancing Cybersecurity

Continuing information technology advances and the growing dependence on new forms of information services necessitates the application of strong cybersecurity practices to all critical satellite systems, especially in response to the broader threats these systems face. Addressing adequate cybersecurity practices and responses for these environments is taking on greater importance to include the development of a cybersecurity workforce, coordination and prioritization of federal research and development, and promotion of cybersecurity education and awareness for the general public. This requires highly trained people to develop, deploy, and incorporate new cybersecurity protocols and practices and cooperation across DOD and the space industry.

IV. Vulnerabilities in the NAVSTAR Global Positioning System

A GPS outage will affect both civilian and military operations. The US power grid uses GPS timing to accomplish hands-off switching of power to different regions. Civilian aircraft and ships have become heavily dependent on GPS position. The military uses GPS to track satellites, ships, and ground units. GPS dependent targeting is also used in munitions such as the JDAM (Joint Direct Attack Munition) for high accuracy employment. (Boeing, 2012)

Interference with the GPS signal, whether hostile or not, will be a serious problem if not prevented. The civil and military sectors have been increasingly reliant on GPS for position, time, and even safety. One critical civilian component that utilizes GPS indirectly is the power grid. The power grid utilizes GPS for timing and accuracy of the grid's phasor measurement units (PMU). These units provide real time voltage, current, and phase of different power grid locations and in some locations allows for hands-off transfer of power. The use of spoofing has proved that the accuracy of the PMU can be off by as much as 70 degrees phase angle which greatly violates IEEE standards. (Shepard et al, 2012) This type of error would resemble that of an actual fault. The result of this perceived fault would most likely cause the initiation of automatic protective actions that could result in blackouts. If not designed correctly, this means could be used to cut power to strategic locations, whether civilian or military, to cause disruption or chaos.

Denial of GPS can occur in various ways. One of the simplest methods of disruption of the GPS system is human error. This was evident in January 2010 when 10,000 military receivers lost navigation capability for several days due to improper software being uploaded at the GPS ground control station. (Elliot, 2011) Physical and non-physical attacks against satellites or the ground stations that control them could also

permanently disrupt the GPS system. Security upgrades to the GPS system do provide some protection against cyberattack. One of the major causes of concern in the vulnerability of GPS is at the receiver. (GlobalSecurity 2012) The received power is very low and makes it vulnerable to jamming and unintentional interference. GPS is also vulnerable to spoofing which is the broadcast of signals with deliberately misleading information. Having these vulnerabilities realized will help prevent these circumstances from occurring or better prepare users for an outage should one occur. There are other countries heavily invested into space denial, which could render the GPS system inoperable. China is known be working heavily in the cyberspace field, and have successfully destroyed one of their spacecraft at an altitude of over 500 miles with a missile. (Gertz, 2010) However, physical attack of the GPS system is unlikely due to its much higher altitude, but not impossible. The GPS system is in orbit at approximately 12,600 miles. (GlobalSecurity 2012) A cyberattack may be a more effective attack vector.

V. Military Alternatives

There are a number of alternatives in development or are ready to be deployed that can replace, or mitigate the partial or complete loss of space systems. They range from non-technical solutions all the way to the launch and replacement of a compromised or lost space system.

One way for tactical war-fighters to be able to fight through or adapt to a satellite communications degraded or denied environment is not a technical solution. Training and conditioning users of space and satellite systems for the degradation or denial of those systems and the use of alternate, redundant systems is critical. The Navy has been conducting this kind of training for years. In February of 2012, the US Navy conducted exercise Bold Alligator off the United States Eastern seaboard involving "participants included two submarines, 25 ships, 120 aircraft, 20,000 Sailors and Marines, along with forces and assets from eight other countries." (Beardsley, 2012)

This was the Joint Task Force Exercise and Composite Unit Exercise certification events for the USS ENTERPRISE (CVN 65) Carrier Strike Group and the USS IWO JIMA and 24th MEU. During the exercise, the war-fighters were presented with a number of situations and scenarios that denied or degraded satellite voice or data communications paths. The objective was to force the war-fighter to adapt to the situation and develop alternative paths in an attempt to maintain command and control. Specifically, "if super high frequency (SHF) IP platforms were denied, there was an extremely high frequency (EHF) platform available. If an UHF command net was lost, EHF or Iridium satellite phones could be used for secure point-to-point communications." (Beardsley, 2012)

The point of these exercises serve to flex the composite warfare commander leadership into developing practices and procedures that will allow the organization to continue to fight while independent of restricted or denied communications, especially via satellite. The loss of satellite communications can limit the battlefield commander today from maintaining continuous command and control (C2) of all assets assigned, which are typically dispersed over a wide geographical area. This loss of C2 results in a loss of situational awareness (i.e. more "fog of war") for the commander and their assigned assets. Resultant effective combat power is lost naturally. If the subordinate commanders have a clear understanding of the commander's intent, with stated goals and objectives, and desired mission end-state, and then are granted trust in carrying out their assigned tasks before entering a satellite communications denied environment; the partial or complete loss of extended, over-the-horizon communications can be mitigated. On a technical note, even in reduced geographical battle space situations, technology exists to ensure there are survivable communications in environments where there is considerable electromagnetic interference. The "use of systems like Have Quick, can provide [line-of-sight] anti-jam, secure communications for […] forces" (FAS, 1999)

With the loss of satellites, the sphere of influence can become narrower, almost to a crippling degree. In Afghanistan for example, troops are often put into deep valleys where communications back to headquarters are impossible due simply to the terrain; they simply cannot see back to the satellite to establish UHF satellite communications with headquarters. To address this issue, the Department of Defense has contracted for the development of the "Battlefield Airborne Communications Node (BACN)". This system "provides a high-speed, Internet protocol (IP)-based airborne network infrastructure that extends communications ranges, bridges between radio frequencies, and 'translates' among incompatible communications systems." (Defense Industry Daily, 2012) Currently, the system is being fitted into block-20 Global Hawk unmanned aerial vehicles (UAV) by Northrop Grumman through a $47.2 million contract that will "provide long endurance and high-persistence gateway capabilities." (Rosenberg, 2012, p. 48) Placing these Global Hawk "BACN equipped" assets over the valley with troops in sight of it can have their communications relayed to headquarters and provide real-time tactical updates to the commander.

A way to retain some intelligence, surveillance and reconnaissance (ISR) capabilities are to use balloons, blimps, and tethered aerostats. Aerostats, for example, can stay aloft for weeks or months providing critical ISR to the war-fighter. The Persistent Ground Surveillance System (PGSS) being deployed by the US military in Afghanistan has reconfigurable payloads that include "radars, full-motion video, electro/optical (E/O) systems and infrared sensors." (Walsh, 2011, p. 45) These systems are ideal for the tactical or operational levels, but will not be able to provide the strategic, theater-wide ISR picture that would have been provided via satellites.

For high data-rate, high-bandwidth communications backhauls, the use of leased trans-oceanic fiber lines and trunks can be used to pass critical information around the world in a matter of seconds. These data links actually have considerably higher data rates than current satellite links. Some of these undersea cables span more than 8,000 miles. "These cables are just three inches thick, carry just a few optic fibers, and have total capacities of between 40Gbps and 10Tbps, and latencies that are close to the speed of light and just a few milliseconds in duration." (Anthony, 2012) The US military currently leases trunk space on some of these cables, and in a satellite

denied environment, they can be exploited to maintain critical data and voice communications.

Precision navigation and timing is critical for ships at sea and is used for many of the weapons systems employed in the US military. Many years ago, before GPS, the United States had a system called Long Range Navigation (LORAN), which used low frequency radio waves emitted from multiple locations that allowed ships to triangulate their location. This system lost favor when the much more accurate GPS became available. LORAN was de-funded by the US government, and in 2010 all signals were terminated. Today, a successor to LORAN is the "eLoran" system, which transmits precisely-timed 100kHz shaped-radio frequency pulses from terrestrially-based master and secondary locations. "Modern eLoran works in much the same way as GPS but it is an independent and complementary system, offering a navigation system with no failure modes in common with GPS or any other satellite based system. (Research and Radionavigation, 2012) While the eLoran system hasn't gained widespread acceptance as of this date, many users of GPS understand its vulnerabilities and want to have a non-satellite back-up alternative.

VI. Conclusion

Space is an increasingly important realm for the U.S. and its allies, and cyber is an increasingly attractive vector via which to target it. Successful attack scenarios have already been theorized and demonstrated. We must devote resources to the understanding of the threat, and the protection of our space assets.

References and Additional Reading

Anthony, Sebastian. (September 21, 2011). The Secret World of Submarine Cables. http://www.extremetech.com/computing/96827-the-secret-world-of-submarine-cables (accessed December 8, 2012).

Arthur, C. (2011, October 27). Chinese hackers suspected of interfering with U.S. satellites. *The Guardian*. http://www.guardian.co.uk/technology/2011/oct/27/chinese-hacking-us-satellites-suspected (accessed November 12, 2012).

Beardsley, Peter J. (2012). NCTAMS LANT Support Joint Training and Operations. *CHIPS: the Department of the Navy's Information Technology Magazine*. http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=3913 (accessed November 20, 2012).

Boeing, "Joint Direct Attack Munition (JDAM) Overview," http://www.boeing.com/defense-space/missiles/jdam/index.htm (accessed December 1, 2012).

Butler, A. (2012, November 7). U.S. Air Force Exploring New Protected Satcom Concepts. *Aviation Week* http://www.aviationweek.com/Article.aspx?id=%2Farticle-xml%2Fasd_11_07_2012_p04-02-514205.xml (accessed November 12, 2012).

Capaccio, T. (2012, November 5). China Most Threatening Cyberspace Force, U.S. Panel Says. *Businessweek*. http://www.businessweek.com/news/2012-11-05/china-most-threatening-cyberspace-force-u-dot-s-panel-says (accessed November 12, 2012).

Capaccio, T. and Bliss, J. (2011, October 27). Chinese Military Suspected in Hacker Attacks on U.S. Satellites. *Businessweek*. http://www.businessweek.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html (accessed November 12, 2012).

Campen, COL A. D. (1998, July). National Vulnerability Intensifies as Infrastructure Reliance Grows. *Signal*, 20. http://www.highbeam.com/doc/1P3-32205077.html (accessed November 19, 2012).

Caton, J. L. (Winter 1995-1996). Joint Warfare and Military Dependence on Space. *Joint Forces Quarterly*, 48-53. http://www.dtic.mil/dtic/tr/fulltext/u2/a525617.pdf (accessed November 19, 2012).

Coleman, K. (2010, March 1). Cyber War = Space War. DefenseTech. http://defensetech.org/2010/03/01/cyber-war-space-war/ (accessed November 12, 2012).

Coleman, K. (2010, September 22). Satellites could come under cyber siege. *Defense Systems*. http://defensesystems.com/articles/2010/09/02/digital-conflict-cyber-threat-to-satellites.aspx (accessed November 12, 2012).

Cooney, W (2002, May). "Protecting Commercial Space Systems: A Critical National Security Issue." Research Report, Naval War College. http://www.dtic.mil/dtic/tr/fulltext/u2/a405817.pdf (accessed December 9, 2012).

Cynamon, MAJ C. H. (1999, April). "Protecting Commercial Space Systems: A Critical National Security Issue." Research report, Air Command and Staff College. http://www.dtic.mil/dtic/tr/fulltext/u2/a405817.pdf (accessed November 19, 2012).

Defense Industry Daily. (2012, November 4). Bringing Home the BACN to Front-Line Forces. http://www.defenseindustrydaily.com/Bringing-Home-the-BACN-to-Front-Line-Forces-05618/ (accessed November 23, 2012).

Department of Homeland Security. (2012). Cybersecurity Overview. http://www.dhs.gov/cybersecurity-overview (accessed December 9, 2012).

DeWeese, S. (2009). Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. *The U.S.-China Economic and Security Review Commission*, McLean: Northrop Grumman Corporation. http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf (accessed November 17, 2012).

Elliott, D. (2011, June 2). "GPS Outage is an Alert about U.S. Military Reliance on Devices, Expert Says," *Dallas News*. http://www.dallasnews.com/news/20100602-GPS-outage-is-an-alert-about-9700.ece (accessed December 1, 2012).

Estes, GEN H. M. III. "Department of Defense Advanced Military Satellite Communications Capstone Requirements Document." HQ U.S. Space Command, Peterson AFB, CO.

Federation of American Scientists, (1999). AN/ARC-164 HAVE QUICK II. http://www.fas.org/man/dod-101/sys/ac/equip/an-arc-164.htm (accessed December 8, 2012).

Gertz, B. (2010, December 15). Inside the Ring: China's A2/AD Threat. *The Washington Times*. http://www.washingtontimes.com/news/2010/dec/15/inside-the-ring-251245374/?page=1 (accessed December 1, 2012).

Gertz, B. (2012, April 27). Beijing's Battle Plan: Chinese military writings reveal cyber, space war plans. *Washington Free Beacon*. http://freebeacon.com/beijings-battle-plan/ (accessed November 12, 2012).

Giffen, R. (1982). "U.S. Space System Survivability – Strategic Alternatives for the 1990s." Research Report, *National Defense University*. http://www.fas.org/spp/military/program/asat/giffen.pdf (accessed December 9, 2012).

GlobalSecurity.org "Navstar Global Positioning System," http://www.globalsecurity.org/space/systems/gps.htm, (accessed December 1, 2012).

Hersh, S. M. (2010, November 1). The Online Threat. *The New Yorker*. http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh (accessed November 12, 2012).

Hsiao, L. C. R. and Stokes, M. (2012). "Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests." *Project 2049 Institute*. http://project2049.net/documents/countering_chinese_cyber_operations_stokes_hsiao.pdf (accessed November 19, 2012).

Hook, COL J. A. Jr. (1999, April). "Military Dependence on Commercial Satellite Communications Systems -- Strength or Vulnerability?" Research Report, Air War College.

Humphries, M. (2011, November 19). Chinese hackers took control of NASA satellite for 11 minutes. Geek.com. http://www.geek.com/articles/geek-pick/chinese-hackers-took-control-of-nasa-satellite-for-11-minutes-20111119/ (accessed November 12, 2012).

Kenyon, H. (2011, November 10). Navy seen fighting in satellite-denied conflicts. *Defense Systems*. http://defensesystems.com/articles/2011/11/10/milcom-navy-information-dominance.aspx (accessed November 12, 2012).

Krekel, B, Adams, P., and Bakos, G. (2012). Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Research Report, Northrop Grumman Corp. http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf (accessed November 12, 2012).

Little, J. (2012, October 3). Satellite Hacking: Where Cyberwar Meets Spacewar. *Blogs of War*. http://blogsofwar.com/2012/10/03/satellite-hacking-where-cyberwar-meets-spacewar/ (accessed November 12, 2012).

Martin, P. K. (2012). "NASA Cybersecurity: An Examination of the Agency's Information Security." Testimony before the Subcommittee on Investigations and Oversight. U.S. House of Representatives. http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf (accessed November 17, 2012).

Mount, M. (2012, October 18). New cyber attack on U.S. banks; Iran suspected. *CNN*. http://security.blogs.cnn.com/2012/10/18/new-cyber-attacks-on-u-s-banks-iran-suspected/ (accessed December 9, 2012).

Murphy, D. (2012, November 6). 'Cyberterror' and Chinese hackers. *Christian Science Monitor*. http://www.csmonitor.com/World/Backchannels/2012/1106/Cyberterror-and-Chinese-hackers (accessed November 12, 2012).

Potter, B. (2008, June). Satellite Interference: Tech to the Rescue. *SATMAGAZINE.com*. http://www.satmagazine.com/cgi-bin/display_article.cgi?number=848918337 (accessed December 9, 2012).

Reinsch, Hon. W. A. (2011). Annual Report to Congress of the U.S.-China Economic and Security Review Commission. Washington DC: U.S. Government Printing Office. http://www.uscc.gov/annual_report/2011/annual_report_full_11.pdf (accessed November 17, 2012).

Research and Radionavigation. (2012). eLoran Background Information. http://www.gla-rrnav.org/radionavigation/eloran/background_information.html (accessed December 9, 2012).

Rosenberg, B. Editor. (2012, January/February). Airborne Node. *Defense Systems*.

Serbu, J. (2012, November 8). On cyber defense, U.S. 'stuck at the starting line'. *Federal News Radio*. http://www.federalnewsradio.com/473/3110944/On-cyber-defense-US-stuck-at-the-starting-line (accessed November 12, 2012).

Shepard, Bhatti, Humphreys. (2012). "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks," The University of Texas at Austin, Aaron Fansler, Northrop Grumman Information Systems.

Staff writers. (2012, October 31). U.S. Naval Office Looks for Methods to Strengthen, Alternatives to GPS. *Inside GNSS.* http://www.insidegnss.com/node/3254 (accessed November 13, 2012).

Taylor, J. (2012, October 23). Space: the new cyber crime frontier. *The Independent*. http://www.independent.co.uk/life-style/gadgets-and-tech/news/space-the-new-cyber-crime-frontier-8194801.html (accessed November 12, 2012).

Walcott, J. (2012, April 18). Chinese Espionage Campaign Targets U.S. Space Technology. *Businessweek*. http://www.businessweek.com/news/2012-04-18/chinese-espionage-campaign-targets-u-dot-s-dot-space-technology (accessed November 12, 2012).

Walsh, David. (2011, September). Unmanned aerostats furnish vital geospatial intelligence. Defense Systems.

Werner, Debra. (2012, January 23). Hacking cases draw attention to SATCOM capabilities. *Defense News*. http://www.defensenews.com/article/20120123/C4ISR02/301230010/Cover-Story-Hacking-Cases-Draw-Attention-Satcom-Vulnerabilities (accessed November 12, 2012).

Williams, M. (2012, October 12). Future cyber attacks could rival 9/11, cripple U.S., Panetta warns. *InfoWorld*. http://www.infoworld.com/d/security/future-cyber-attacks-could-rival-911-cripple-us-panetta-warns-204734 (accessed November 19, 2012).

Zetter, K. (2012, March 1). Report: Hackers Seized Control of Computers in NASA's Jet Propulsion Lab. *WIRED Threat Level.* http://www.wired.com/threatlevel/2012/03/jet-propulsion-lab-hacked/ (accessed November 12, 2012).