Global: Satellites, security and the social graph

In our age of telecommunications convergence, and the infusion of social media throughout all communications, it is unremarkable that satellite communications would face the same risks of cyber attack as are facing the telecommunications industry generally. With our increased reliance on space technology, these risks present real issues and vulnerabilities.

The nature of satellite communications, however, presents some significant structural differences and susceptibilities for cyber terrorism, hacking and risk avoidance.

Satellite cyber-attack terminology

"Soft" kills: informational, reversible or temporary disabling without destruction.

"Hard" kills are permanently disabling or destructive. While hard kills can include missile attacks, air raids or sabotage, they also include various directed energy attacks, including microwave, particle beam, electromagnetic pulse weapons and laser weapons, but can also include self-destruction commands or actions intended to cause loss of satellite control.

Jamming includes use of electronic interference or signals that overpower communications channels. Jamming is deliberate interference with satellite signals.

Deception reflects the forgery or interception of transmissions to or from the attacking space system.

Advanced Persistent Threat (APT) is typically used to refer to a cyber threat by a group, including a foreign government, with both the capability and the intent to effectively and persistently target a specific entity for attack.

Some general facts [1]

1. The U.S. Navy faces 110,00 cyber attacks every hour, or more than 30 every second.
2. One-third of attacks globally are said to originate from China.
3. Nearby in Tokyo, in an effort to develop its defenses against cyber attacks, Japan concluded its first government-approved hacking contest in February 2013.

Satellites as a target

There are approximately one thousand military and civilian satellites orbiting earth today, all of which are potential targets for cyber attack. These satellite systems are subject to cyber attack through "soft" kills to the satellite, but can also take the form of "hard" kills to the satellite system. Soft kills seem likely to be the most common approach since they may keep hidden the source of the activity, but they can equally paralyze or destroy a satellite.

> "Soft kills seem to be the most common approach"

Satellite systems are susceptible to cyberattack through both their ground-based and space-based components, through manipulation of their electronic links, in any number of ways and system components:

- Taking control of (or nullifying the ability to control) a satellite
- Deliberately interfering with satellite transmissions, by jamming, denying, degrading, or forging (counterfeiting) signals, either from the ground or from other satellites
- Key targets of communications link attacks are satellite uplink (transmitting information from ground station to satellite) and downlink (transmitting information from satellite to ground systems) facilities
- Accessing (and potentially leaking) satellite-produced or stored information

[1] http://www.voanews.com/content/japan-first-government-sponsored-hacking-contest/1597014.html
http://www.v3.co.uk/v3-uk/news/2238996/akamai-study-finds-a-third-of-all-cyber-attacks-originate-from-china
http://thenextweb.com/us/2012/12/05/us-navy-sees-110000-cyber-attacks-every-hour-or-more-than-30-every-single-second/

- Implanting computer virus and logic bombs into satellite information systems
- Compromised chipsets, ground systems, internet links and other system components or interfaces can be the vehicles for satellite cyberattack
- Compromising other satellite or terrestrial based networks used by the satellite, or with which the satellite can in turn interfere
- Using the above techniques to lay the http://www.voanews.com/content/japan-first-government-sponsored-hacking-contest/1597014.html

Military, civilian and commercial satellites serve a broad range of services including voice, data and internet communications, broadcast services, mapping, space exploration, global positioning, meteorology, surveillance, navigation, and emergency services. In some cases, the satellite produced or stored information can be highly sensitive, putting national security at risk.

> "Taking control of the satellite can disable the nation's security and defense"

In the most extreme of cases, taking control of the satellite can disable the nation's security and defense in the case of attack. In the past, there have been reports of satellite jamming tests and laser blinding of U.S. reconnaissance and French satellites, as well as a variety of other antisatellite capability demonstrations believed to be by the Chinese government.[2] In January 2012, a virus infecting Japan Aerospace Exploration Agency computers caused information to be sent to the International Space Station.[3]

In the case of commercial satellites, the cyber-risk can be analogous to taking down a significant part of the telecommunications grid in a terrorist attack, or to political censorship by shutting down social media in-country.[4] Further, as commercial satellites become more connected with the internet, the cybersecurity risks increase and there is a greater diversity of concerns.

Satellites and the "Mainframe" paradigm. As in the case of terrestrial, computer based cyber attacks, in the original computer network paradigm there was a walled off, limited-access computer mainframe model that provided significant protection against security breach. While some satellites are similar to the mainframe model in various respects, the vulnerability of satellites to attack has increased exponentially as technological interference, control and hacking attacks have also exponentially increased in recent years.

Some interference, as has been seen by global satellite operators and their customers, is a result of targeted governmental political actions to block dissenting political perspectives. Recent examples of this include Iran's satellite jamming of news broadcasts of the BBC, Voice of America and Radio Free Europe not only into Iran, but also into countries ranging from Morocco to Eastern Europe to Indonesia[5] as well as incidents originating from Cuba, Libya, Indonesia, Syria, Bahrain, China, Kyrgyzstan and Uzbekistan.

> "Satellite jamming is a growing scourge and a threat to the vital flow of free information"
>
> *Peter Horrocks, Director BBC Global News*

Historically, satellite operators have been reluctant to publicize cases of intentional interference, but the rapid increase in incidents has caused the industry to issue public statements to bring attention to the problem. Satellite fleet owner Eutelsat has reported that jamming incidents doubled between 2010 to 2011, increased again threefold between 2011 and 2012, and reported 340 incidents in the first ten months of 2012.[6] Middle-east operator Arabsat similarly recorded a three-fold increase in jamming attacks during the 2011 to 2012 period.

Threat to control of satellites. At another level, access to satellite control has been hacked. According to the November 2011 Report to Congress by the US-China Economic and Security Review Commission (November 2011 Report) at least two U.S. government imaging satellites, Terra EOS and Landsat 7 have "each experienced at least two separate instances of interference consistent with cyberactivities against their command and control systems."[7] In the case of the Terra satellite, the hackers "achieved all steps required" to assume control of the satellite, although actual commands were not issued. The November 2011 Report observed:

> If executed successfully, such interference has the potential to pose numerous threats, particularly if achieved against satellites with more sensitive functions. For example, access to a satellite's controls could allow an attacker to damage or destroy the satellite. The attacker could also deny or degrade as well as forge or otherwise manipulate the satellite's transmission. A high level of access could reveal the satellite's capabilities or information, such as imagery, gained through its sensors. Opportunities may also exist to reconnoiter or compromise other terrestrial or space-based networks used by the satellite.[8]

The November 2011 Report found that the techniques deployed in these activities were consistent with authoritative Chinese military writings: "according to *Military Astronautics*, attacks on space systems 'generate tremors in the structure of space power of the enemy, cause it to suffer from chain effects, and finally lose, or partly lose, its combat effectiveness'" and that "[o]ne tactic is 'implanting computer virus and logic bombs into the enemy's space information network so as to paralyze the enemy's space information system.'"[9]

In the case where U.S. or other countries' satellites have been accessed, it is unknown whether and what cyber activities are implanted in these satellites as a pre-staging for an Advanced Persistent Threat.

> "State-sponsored hackers are patient and calculating. They have the time, money and resources to burrow in and wait. You may discover one breach only to find that the real damage has been done at a much higher level[10]"
>
> *Robert Mueller, FBI Director*

[2] 2011 Report to Congress of the U.S.-China Economic and Security Review Commission, One Hundred Twelfth Congress, First Session, November 2011 (U.S. Government Printing Office, Washington: 2011) (November 2011 Report), pages 213-14, footnotes 306-307.

[3] http://www.space.com/14231-japan-space-agency-computer-virus.html

[4] One recent example is that of India, where more than 250 websites have been blocked, Google and Facebook ordered to pull content, and legal action threatened against Twitter if it did not delete certain accounts. See http://www.theatlantic.com/international/print/2012/08/when-is-government-web-censorship-justifed-an-indian-horror-story/261396/

[5] / Press Release, Eutelsat, dated October 4, 2012. "Eutelsat condemns jamming of broadcasts from Iran and renews appeals for decisive action to international regulators"

http://www.eutelsat.com/news/compress/en/2012/html/PR%206212%20interference%20iran/PR%206212%20interference%20iran.html

[6] http://www.bbc.co.uk/mediacentre/latestnews/2012/201112wsjammingconferencehtml

[7] November 2011 Report, p. 216.

[8] November 2011 Report, p. 216.

[9] November 2011 Report p. 217, and footnote 321.

[10] CNN Money http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm?iid=EL

Satellites as a Tool of Social Media. Satellites historically were based on non-IP communications technologies, and hence less susceptible to cyber-attack. As satellite missions move toward an end-to-end interoperable IP environment, they become more susceptible to attack at the same time that cyber-sophistication has increased.

As satellite communications mimic terrestrial communications in their function and role, in addition to the "mainframe" risks, satellites and their users face the same, more extensive risks as do terrestrial communications users that do not have the "mainframe" isolation or defenses. Connecting satellites to the internet significantly increases satellites' and their related ground systems' vulnerability to (low-cost) cyber-attack. With the increase in satellites' roles in individual communications and broadcast services, the risks to safeguard of personal data, financial information, and other business data increases.

While satellites are often thought to provide more secure communications than their terrestrial wired and wireless counterparts, as hackers continue to increase their sophistication there is no reason to believe that cybercrimes for satellites will not increase with their terrestrial counterparts.

> "Eutelsat has added an anti-jamming technical solution"

Preparing to Meet the Threat. "The cybersecurity challenge is complex and dynamic, especially because there is a powerful upside to the continued embrace of digitalization and connectivity."[11] The integration of these susceptibilities into space systems further exacerbates the inherent special cyber sensitivities of satellite systems. Security measures that may have been sufficient in the past will not meet the cyber threats of the future. In the past, for unsophisticated or unintentional sources of interference, increasing the power of the satellite uplink could overwhelm the interference source. But as in the case of the terrestrial world, as cyber technologies increase in sophistication, a more sophisticated tool kit is needed to combat the new cyber risks.

New tools that specifically cater to the satellite industry are being made available to satellite operators. Eutelsat, which has been a vocal opponent of intentional interference, has added an anti-jamming technical solution to one of its scheduled Middle Eastern satellites, where it has met with significant intentional signal interference. This protective technology has previously been cost-prohibitive according to Eutelsat. But a new public-private cooperative initiative, the European Space Agency's (ESA) Flight Heritage Program, has facilitated the addition of new satellite de-risking technologies to flight hardware. In addition, the ESA program has considered critical satellite needs to avoid impacts to mission-critical components.[12]

While these new developments may help counteract cybersecurity threats for new satellites, owners of existing satellites should develop plans to assess risks and determine if there are cost-effective solutions available. Our firm and other consultants prepare guides to help operators conduct network assessments to determine the level of risk that exists, assess its existing resources, put plans in place to monitor potential cyber attacks and make decisions regarding the cost-effectiveness of available countermeasures. No guarantees exist that a particular operator's system will not be chosen for a cyber attack. But measures can be taken to reduce the level of risk, and to understand the current situation and provide meaningful analyses to the managers of the company making decisions on where to allocate resources. And it is only a matter of time before customers insist upon defensive programs being in place.

Randy S. Segal
Partner, Northern Virginia
T +1 703 610 6237
randy.segal@hoganlovells.com

Steven M. Kaufman
Partner, Washington
T +1 202 637 5736
steven.kaufman@hoganlovells.com

[11] Harriet Pearson, Cybersecurity: The Corporate Counsel's Agenda, BNA Privacy & Security Law Report, 11 PVLR 1792, 12/17/2012.

[12] Peter B. de Selding, "Eutelsat to Field Test New Anti-jamming Capability," January 28, 2013, SpaceNews p. 4, Volume 24, Issue 4.