KURTIN PLLC
Attorneys at Law

CLIENT ADVISORY: SATELLITE HACKING AND CYBERSECURITY

May 8, 2013

The growing threat of cyber-attacks and network hacking has reached the satellite-space sector, posing a growing challenge to satellite fleet operators and raising questions as to whether commercial satellites will in the future need to be "hardened" to the standard of the most secure military satellites. Although the threat of cyber-attacks emanates from several nations, non-state actors and even individuals, a significant amount of attention has focused on the role of People's Republic of China (China).

The U.S.-China Economic and Security Review Commission (USCC), a U.S. Congressional commission charged with monitoring the trade and economic relationship between the U.S. and China and assessing its security implications, issued an annual report in August 2011 (available at www.uscc.gov) that concluded that computer hackers, possibly affiliated with China's military, had interfered with two U.S. government earth terrain and climate surveillance satellites, Landsat-7 and Terra AM-1, several times in 2007 and 2008. In one 2008 case, according to the USCC report, the hackers achieved command and control of the Terra AM-1 spacecraft, although they did not exercise that control.

According to the USCC report, the hackers used a commercially operated ground station located in Spitsbergen, Norway to gain access to the two satellites, and also took measures to obscure their attacks and cover their tracks. The report did not specify the nature of the hackers' attacks, but underscores the increasing vulnerability of both military and commercial satellites to hacking attacks and intrusions. The two satellites, which are not "hardened" against both attack and signal interception as are the most sensitive of Department of Defense and National Security Agency satellites, are nevertheless sources of strategically valuable reconnaissance data in their own right, and can obviously serve as practice for attacks on more secure satellites. In the case of Landsat-7 and Terra AM-1, the Norwegian earth station uses Internet Protocol (IP) for data transfers, and is more vulnerable at that network node than closed network data file transfer systems would be. The USCC report warned that hacking attacks pose the risk of destabilizing or degrading orbits, damaging or destroying satellites, and blocking, manipulating, forging or otherwise interfering with uplink and downlink transmissions. Although the report did not accuse the Chinese government or military of orchestrating the attacks, it asserts that the attacks are consistent with known and published Chinese doctrines for disabling other countries' space systems.

Plainly, Landsat-7 and Terra AM-1 were unnecessarily vulnerable. However, it is not clear how protected even the most hardened assets are, and the necessary level of cybersecurity is an always moving, always receding, target. Satellite networks are wireless networks, and wireless networks are intrinsically more vulnerable to attack than closed landline networks. Most satellite communications encryption employs so-called public-key cryptography using asymmetric algorithms; meaning that the sender of a transmission uses a public key or a certain byte length, and the transmission can normally be decoded only by a recipient entrusted with a different, private key mathematically linked to the public key. While this encryption method has been highly successful, the use of a public key by the sender of a transmission renders the encryption susceptible to "brute force" attacks by use of extreme computational power that is available to state players if the potential gain in information is justified by a cost-benefit analysis. A lot of satellite software does not come up to this standard. In February 2012, *Network World* and other publications reported that researchers had cracked the GMR-1 and GMR-2 satcom encryption algorithms of the European Telecommunications Standards Institute (ETSI), used to secure civilian satellite telephone communications.

The report of hacking comes as China itself emerges as a major space power. China operates over 70 satellites and has proven heritage access to space through its China Great Wall Industry Corp. "Long March" family of launch vehicles. China has also rapidly developed as the third human-crewed space-faring nation, has recently conducted successful rendezvous and docking procedures in clear preparation for a space station venture and may also be considering human space flight beyond low earth orbit, possibly a mission to the moon.

Reports of hacking attacks against U.S computer networks by state or state-sponsored players have circulated for years, but have been resistant to concrete proof. While the Pentagon and Congress have identified sources of hacking attacks other than China, they are on record as believing that China is the source of much of it, and that the attacks are part of a larger pattern of digital government and industrial espionage against security-related information and intellectual property. The USCC and Pentagon further believe that China has particularly targeted the U.S. defense establishment for intrusion. China has denied the reports and asserted that the allegations are intended by the U.S. Government to vilify China unjustly. The USCC's 2009 annual report acknowledged that there was no proof that hackers were affiliated with the Chinese government, but asserted that much of the hacking activity against government and industrial digital networks bore Chinese "handwriting," among other things, originating from Chinese IP addresses.

The implications of the 2009 and 2011 USCC reports cannot be underestimated. The efforts that both government and commercial operators may have to make, and require satellite manufacturers to participate in, to secure satellites against hacking and their transmissions, including the content borne by those transmissions, against interception, cannot be underestimated, and, as stated, is a moving, always receding, target. Customers will demand the best protection obtainable, and those costs will be, in whole or in part, passed on to customers or imperil margins. To the extent the U.S. Government is relying on commercial satellites for an increasing range of services under the "hosted payload" model, the pressure to protect against hacking will be even greater.

Perhaps as importantly, it is critical to substantiate the allegations being made. Knowing something and proving it are not the same thing, and if the U.S. or other concerned International Telecommunications Union administrations can prove that the source of hacking is China or China-affiliated persons or organizations, it will be better positioned to exert pressure unilaterally, multilaterally and through non-governmental organizations to pressure China to desist. As China develops as a space-faring power itself and a potential target of the same kind of attack, it will of course have reason to think more about the consequences of doing so, just as its increasing production of intellectual property will alter its perception of the acceptability of intellectual property piracy. Until that happens, and perhaps even after it does, satellite hacking remains a credible and serious threat.

However, satellite hacking is only part of the overall cybersecurity issue of intrusion into space sector computer networks for military or industrial espionage purposes. On March 22, 2013, *The New York Times* reported that NASA had shut down a large public database and decided to limit access to agency facilities by foreign citizens to hinder efforts by other countries to obtain sensitive space technology information. NASA administrator Charles Bolden announced the moves following the arrest of a Chinese citizen, Bo Jiang, at Dulles airport after he boarded a Beijing-bound flight. Mr. Jiang had been working as a contractor at NASA's Langley Research Center in Virginia, and was arrested on board his flight in possession of an allegedly undeclared laptop computer, hard drive and SIM card.

The database in question is the NASA Technical Reports Server, a giant repository of public access information compiled in the form of technical and scientific journal articles, videos, presentations and other materials. While several prominent members of the scientific community asserted that the database shutdown was an overreaction to the Jiang arrest, Major General Bolden stated that the Agency review was necessary to review whether materials controlled under U.S. technology export laws and regulations had accidentally been put on the server, allowing their effective "export" without a license in violation of the State Department ITAR or Commerce Department EAR regulatory regimes. At issue, as usual in the U.S., is the balancing of the critical free and fair exchange of information in an open society with the need to prevent intellectual property theft and industrial, military and government espionage that threatens critical national security and other interests.

The fact that NASA operates both Landsat-7 and Terra AM-1 and the Technical Reports Server may highlight an issue of security consciousness endemic to NASA itself. NASA is a civilian agency not part of the intelligence community, and has an express research and dissemination of knowledge and information mission that arguably is unlikely to coincide with a culture of best security practices. Indeed, the mission of an agency like NASA may be intrinsically incompatible with best security practices. However, NASA may be the canary in the coalmine in this situation, for if its land-based and in-orbit security protocols are lacking, it is unlikely that the commercial fleet is more secure. And the commercial fleet transmits untold amounts of sensitive civil information from the worlds of finance, science, navigation, media and other sectors. Moreover, the increasing reliance of the military and other government agencies on "hosted payloads" and other capacity of the commercial fleet means that hacking and other cyber-attacks on in-orbit satellites, ground stations and associated networks have more than civil implications, as serious as those might be.

Owen D. Kurtin