Culture Mandala: Bulletin of the Centre for East-West Cultural and Economic Studies, Vol. 10, No. 1, December 2012- May 2013, pp21-50.

SATELLITE HACKING: A Guide for the Perplexed[i]

By Jason Fritz BS (St Cloud), MIR (Bond)

1. Introduction: Three Key Questions

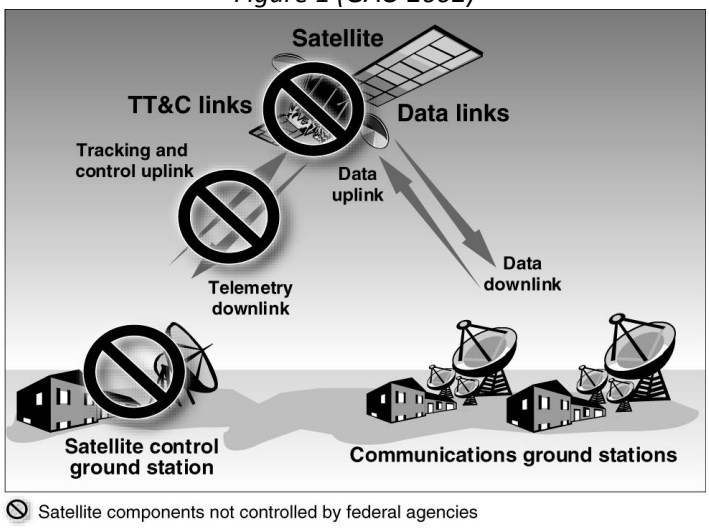
Satellites are vital to sustaining the current balance in the global economy, society, and advanced militaries. As such, states are increasingly recognizing satellites as critical infrastructure. They provide a significant role in climate and natural disaster monitoring, communication, early warning systems, global broadcasting, meteorology, navigation, precision strikes, reconnaissance, remote sensing, surveillance, and the advancement of science and understanding. Satellite services also have a supporting role in "mobile and cellular communication, telemedicine, cargo tracking, point-of-sale transactions, and Internet access" (GOA 2002). The global commercial space industry alone has "estimated annual revenues in excess of $200-billion" (Space Security Index 2012). As of December 2012, there are an estimated 1046 operational satellites belonging to 47 states in addition to various international entities and collaborations (UCS Satellite Database 2012). Beyond states, 1,100 firms in 53 countries use outer space as part of their operations (Robertson 2011).

A significant disruption to satellite services would have damaging effects on society. However, news headlines of satellites being hacked, such as those stemming from the 2011 Report to Congress of the US-China Economic and Security Review Commission, degrade discussion in international relations by oversimplifying the topic. Limiting the information given might be due to security concerns or a lack of attention span on the part of its intended audience; however oversimplification gives the impression that an individual hacker sitting at their computer can access satellites with a few simple keystrokes. Conversely, it might lead others to dismiss the topic as fiction when there is a credible threat that needs to be addressed. This paper will investigate key questions relevant to the topic of satellite hacking: What is the structure of satellite systems? What does it mean to 'hack' a satellite? And why are these systems vulnerable to hacking?

2. The Structure of Satellite Systems

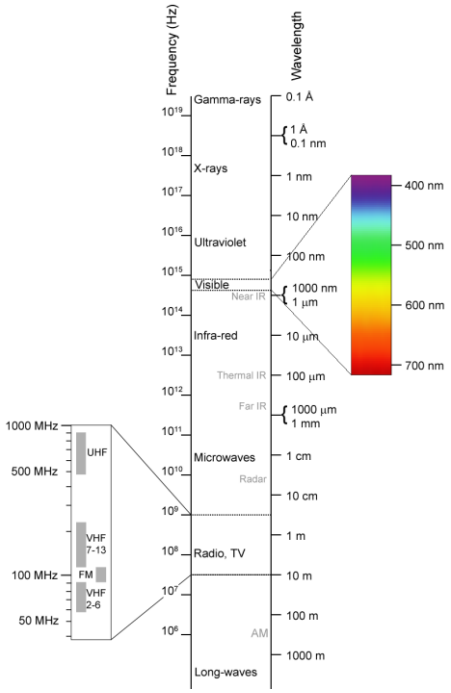
In order to better address satellite hacking, it is first necessary to have an understanding of how satellites work. Most satellite systems conform to a broad template. As shown in figure one, this consists of the satellite itself, a tracking, telemetry, and control (TT&C) ground station, communications ground stations, and uplinks and downlinks between these ground stations and the satellite. The satellite itself is composed of a bus and payload. The payload is usually a collection of electronic devices specific to that satellite's desired function. For example, a surveillance satellite would contain imaging equipment, while the payload for a communications satellite would include transponders for receiving and relaying signals such as telephone or television. The bus is the platform housing the payload; this includes equipment for manoeuvring, power, thermal regulation, and command and control (Wong and Fergusson 2010, pp35-36). TT&C ground stations "perform tracking and control functions to ensure that satellites remain in the proper orbits… and to monitor their performance. Communications ground stations process imagery, voice, or other data and provide, in many cases, a link to ground-based terrestrial network interconnections" (GAO 2002). These ground-based terrestrial network interconnections communicate to and from the communications ground station but not directly to the satellite.

Figure 1 (GAO 2002)



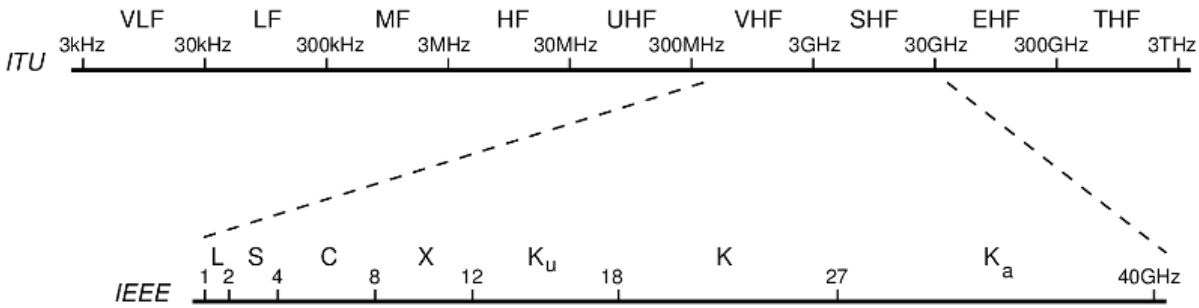
In addition to communication ground stations, there are a wide range of commercial user terminals which can receive data downlinks, and in some cases transmit data uplinks. Examples of downlink only user terminals include GPS navigation devices commonly found in automobiles and satellite TV dishes (when those dishes are unmodified and used as commercially intended). The predominant means of satellite transmission is radio and microwave signals (see figure 2). Higher frequencies (shorter wavelengths) are capable of transmitting more information than lower frequencies (longer wavelengths), but require more power to travel longer distances. The US, EU, and NATO have assigned letter designations to widely used frequency ranges within the radio spectrum (see figure 3). Some generalizations can be made as certain applications tend to group within specific bands, such as roving telephone services and broadband communication using the C and Ka-bands respectively. "Ultra-High Frequency, X-, and K-bands have traditionally been reserved in the United States for the military" (Space Security Index 2012). In addition to Internet websites and mobile apps that reveal particular frequencies used by individual satellites, scanning software exists that can automate the process for potential hackers (Laurie 2009).

Figure 2 (Electromagnetic Spectrum 2012)



There are numerous types of satellite orbits. The most basic include low, medium, and high earth orbits (LEO, MEO, and HEO), polar orbits, and geosynchronous or geostationary (GEO) orbits. As with frequency bands, some generalizations can be made with specific satellite types tending towards specific orbits. For example, early warning satellites tend towards HEO, while LEO is used for earth observation and requires fewer resources to obtain. GPS navigation satellites are in MEO. Geosynchronous orbits, of which GEO is one type, have an orbital period that matches the earth's rotation. This allows them to remain in a ground station's line of sight at all times. In the case of GEO, they remain in the exact same spot at all times meaning that antennas do not need to move or track the satellite's position; these antenna can be aimed in one direction permanently. Being able to have this continual downlink means data can be obtained immediately and does not have to be stored as it does in other orbits where the satellite's field of view (footprint) continually passes out of range of the ground station as it transits the opposite side of the planet. For surveillance or weather satellites, geosynchronous orbits provide 24 hour coverage of a target. Non-geosynchronous satellites can obtain 24 hour access to downlinks by means of relay links (or cross-links) between satellites in orbit. In some cases geosynchronous satellites also utilize relay links since the operator may not want a ground station positioned in the footprint, such as in a war zone. Orbital slots near the Earth's equator and low inclinations are in high demand as these maximize reliability and available use. Likewise, the US is particularly interested in the orbital arc that "lies between 60° and 135° W longitude, because satellites in this area can serve the entire continental United States" (Space Security Index 2012). Different states have similar optimal orbits they seek to obtain, which often overlap with other state's interests.

Figure 3 (Gordon 2012)



Lifespans of satellites vary, with the high end being approximately 15 years. When a satellite is no longer operable, it is preferable to move it into a higher 'graveyard orbit' or a controlled decent to burn up in the atmosphere. Older satellite designs tended to keep the complex functions and equipment on the ground so repair and upgrade is more accessible. An example of an older design is the 'bent-pipe satellite' which simply relays the signal that is transmitted to it. This can be likened to a mirror in space, allowing a signal to bounce off and reach a location on the planet beyond terrestrial line of sight. This is however an oversimplification as even bent-pipe satellites are using increasingly complex payloads with on-board processing. As a basic outline for a satellite uplink: data enters a modem, then is sent to an up-converter, on to a high-power amplifier, and finally sent through the antenna. Two common amplifier types encountered in satellite literature are traveling wave tube amplifiers (TWTAs) and solid state power amplifiers (SSPAs). A typical bent-pipe satellite will have multiple transponders on-board and increase capacity by using access techniques like code division multiple access (CDMA), frequency division multiple access (FDMA), and time division multiple access (TDMA). This allows multiple streams of information to be sent simultaneously over a single communication channel, delineating them by use of code, variance of frequency, or timing

respectively. They are then allocated to the appropriate transponder for downlink transmission, all without interference or loss of signal (Steinberger 2008). Downlinks then go from the satellite antenna to a low-noise amplifier (LNA), to the down-converter, to the modem, and then onward to a computer and/or end user.

Despite increasing complexity upon closer analysis, and the option of additional security measures (discussed below), the perceived ease of exploitation apparent from satellite systems' general structure appears to remain. In 2007, the Liberation Tigers of Tamil Eelam, a separatist group based in Sri Lanka was accused of illegally using an empty transponder frequency on a bent-pipe style Intelsat satellite to beam radio and television broadcasts internationally. Satellite network controllers and satellite operator employees commented on the lack of security:

> Communications satellites normally have no protection at all, if you know the right frequency, have a powerful enough transmitter and antenna, and know where to point your signal, you can do it. And it's *extremely* difficult to avoid, there are very few technical countermeasures. You can beam a more powerful carrier over the pirate, but this means you lose the bandwidth anyhow and, in case of an intentional interference, the pirate can just shift his frequency and start over. (Sri Lankan Terrorists Hack Satellite 2007).

It should be noted that there is some discrepancy between sources as to the names of each of the large components within the broad template provided above. For example, some literature may blur distinction between an earth station, hub, teleport, terminal, or ground station. There is a lack of standardization, and vendors prefer to give their own unique product names, particularly when they feel the technology has been improved upon. However, this broad template does not capture the true diversity between individual satellite systems or the vast technical detail behind their operation (see Gutteberg 1993, pp4-21). At the same time, the simplicity shown here does more than provide an introduction; there is in fact an element of simplicity in their design. Science, technology, and efficiency force them to conform on many levels. And from a hacker's perspective, mastering all of the technical detail is not essential. It is much easier to damage or disrupt hardware than it is to build it and maintain its proper function. Satellite script kiddies may exist. For example, an attacker does not need to know how to find clear text open frequencies, or how to build an antenna, if they can simply purchase ready-made equipment (Laurie 2009).

Downscale Ground Stations

One significant type of equipment not yet discussed is the Very Small Aperture Terminal (VSAT). VSATs are a type of scaled down communication ground station, capable of two way satellite communication with an antenna less than 2.4 meters in diameter and typical data rates of 2 Mbps. As of 2010, there were 1,432,150 VSAT sites in use, with 2,845,747 individual VSATs reportedly shipped to customers (Comsys 2010). They are commonly used for bank transactions between headquarters and branches, Internet access in remote locations (including Intranet, local area networks, video conferencing, virtual private networks, and VOIP), mobile or fixed maritime communications (e.g. ship or oil rig), point of sale transactions, and SCADA (supervisory control and data acquisition system, often used in connection with industrial or infrastructure control systems). Each of these encompasses a large amount of sensitive data that might be of interest to hackers (see figure 4 for one example of VSAT ground-based terrestrial network interconnections). Most VSAT networks are configured into a star or mesh topology, with mesh topology allowing individual VSATs to communicate via the satellite without using the hub as an intermediary (see figure 5). The Hub station, sometimes referred to as the Network Operations Center (NOC), is responsible for monitoring and controlling, configuring, and troubleshooting the network (Voll and Klungsoyr 1993). In this way, a hub is comparable to a TT&C ground station.

Figure 4, an example of a VSAT network in a Banking Environment (Voll and Klungsoyr 1993).

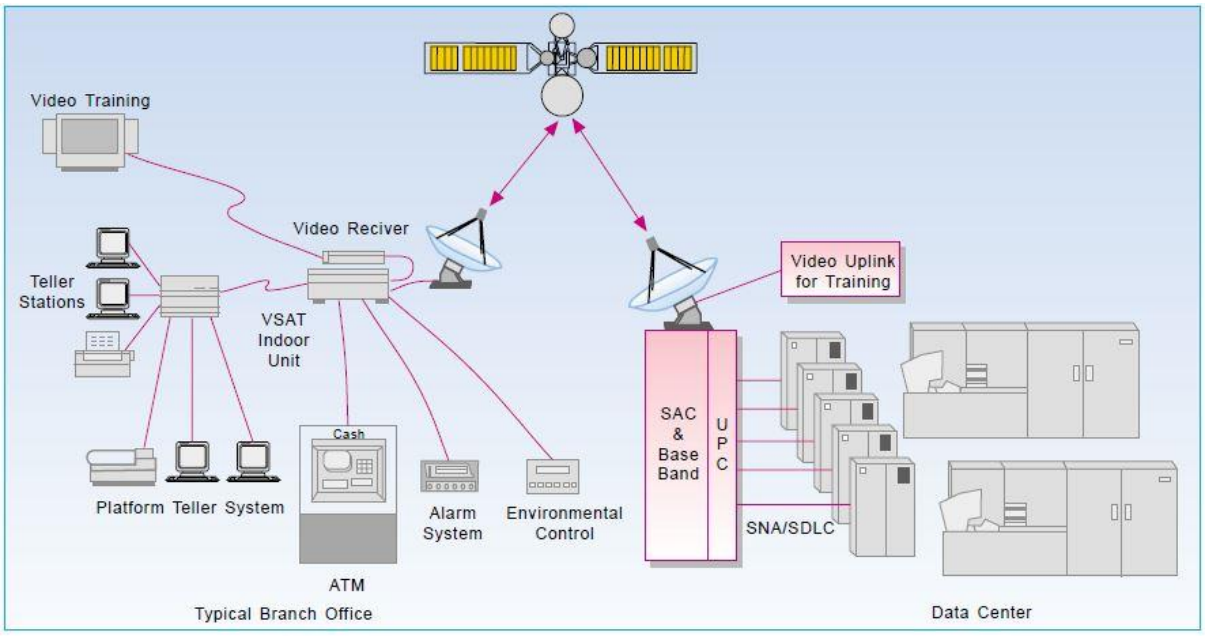
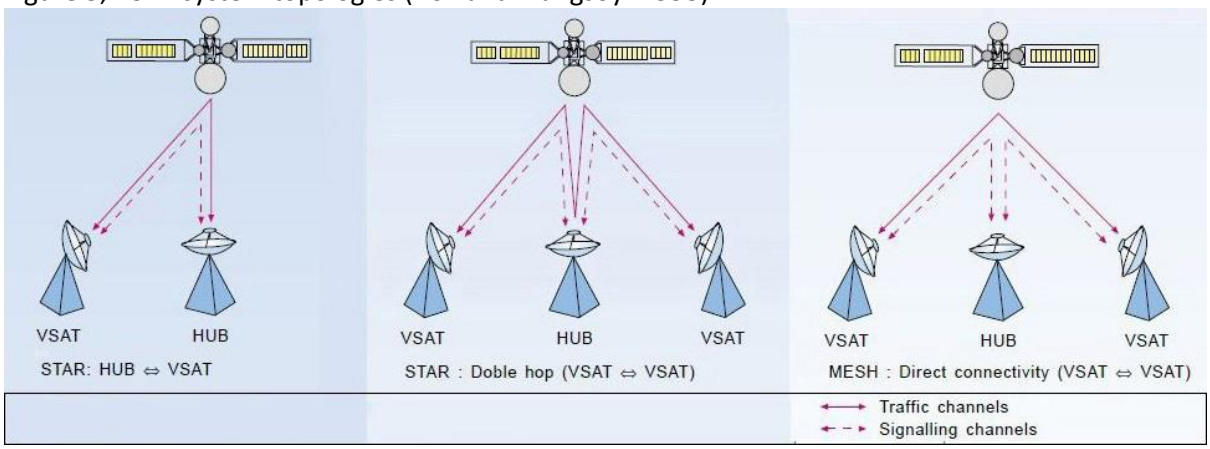


Figure 5, VSAT system topologies (Voll and Klungsoyr 1993).



Another example of a scaled down ground station variant is the Broadband Global Area Network (BGAN) from the British satellite telecommunication company Inmarsat. Its marketed use is similar to that of VSATs, but the unit size is significantly reduced. The smallest unit weighs less than one kilogram, and is about the size of a laptop. It provides data rates of up to one half a Mbps, and can connect directly to the satellites in the network. It is marketed towards journalists, government personnel, aid workers, engineers, consultants, and project managers who require broadband access in remote locations. Further it is claimed to be easily deployable, require no specialist expertise to set up, and is capable of encryption and security protocols (BGAN 2009). Reducing the technical expertise required to connect to a satellite has the unintended consequence of making it easier for hackers to connect to a satellite. Further, as noted at a 2008 security conference, vendor brochures often advertise security and encryption, but in some cases it is up to the individual user to enable these features and follow proper procedures (Geovedi, Iryandi, and Zboralski 2008). An increase in unsecure data being transmitted via satellites may pique the interest of hackers.

While BGAN is not labelled as a VSAT, it appears very similar in concept. Variance of component names and product lines is understandable from a marketing and business standpoint, but it adds to the difficulty of providing an overview of satellite architecture. For example, Inmarsat uses different names for its air and sea based equivalents of BGAN. SwiftBroadband and FleetBroadband respectively are product lines from only one company. Examining specific markets for transportable and affordable ground stations (e.g. as used on oil rigs) in the hope of uncovering commonalities also yields mixed results. News agencies for example utilize VSAT, BGAN, and possibly other forms or brands of satellite ground stations. There does not appear to be an industry wide standard. Older C-Band, transportable earth station, satellite trucks were fairly large, typically requiring a six wheeled vehicle, whereas newer Ku band satellite trucks are capable of fitting in a midsize van or being transported on commercial airline flights (Davies 2006). Different terminologies are used for mobile ground stations and by various military forces, and it is unclear how 'homebrew' ground stations fit into the equation. Despite these limitations, this broad template provides a clear backdrop to satellite hacking.

Redundancy

Redundancy is one security measure against disruption of service. For GPS there is currently a constellation of 31 satellites in orbit, providing 6 satellites in view from any position on earth at any time. GPS only requires 4 satellites to operate at full capacity, and 3 for reduced accuracy. Satellites serving in a constellation can be tasked to be removed from network service while maintenance and diagnostics are performed and then placed back into active duty. In addition, redundant hardware and software can be installed in individual satellites, even going as far as to have a complete A-side and B-side. Fully redundant and staffed off-line ground stations are also occasionally employed with the added security of being geographically separated from the master ground station and on a different power grid. In the event of a malfunction due to an attack, a technical problem, or natural disaster the backup parts, the B-side, and/or the off-line ground station, can take over (GAO 2002). Changing the formation of a network of satellites, or engaging secondary systems, to compensate for a disruption can even be set to engage autonomously (Payne 2010). Further, some satellite operators contract for priority services with other satellite providers, so if there is a disruption to their own satellites, customer services will continue on through an alternate provider with the possibility of completely different security measures in place. However such plans and backup systems, autonomous or otherwise, are uncommon in commercial satellite systems due to cost factors.

Some efforts to increase redundancy may even open up new avenues for attack. Take for example, the push for a "use of standardized protocols and communications equipment" that would facilitate "alternative commercial ground stations to be brought online" (Space Security Index 2012). This would reduce the diversity of such systems, making it easier for a hacker to obtain information on them and increasing the number of targets capable of being hacked through one skillset. A trend towards the research and development of microsatellites also carries unintended consequences. Microsatellites would increase redundancy by being cheaper to develop and quicker to deploy. The reduced weight increases launch options, such as requiring less powerful rockets, not requiring a dedicated launch facility, and even the capability of airborne launches. Reduced cost means a larger networked fleet could be deployed, making the loss of one less detrimental. Additionally, it would allow for rapid deployment of replacements. However, drawbacks to this approach include greater orbital congestion, difficulties in tracking a larger number of small objects, and a lower threshold to attack due to a perceived reduction in effect. Since cost saving is considered a selling point to microsatellites, it also seems unlikely that they would operate on a diverse range of software and equipment, making them more accessible to hacking. Vendors do seem aware of this, and there is

discussion of "unique digital interface[s]', but capability does not ensure implementation (GAO 2002).

Hardening

The security technique of hardening can take place at multiple nodes within a satellite network. Commonly used physical protection of ground stations includes: access codes, activity logs, blast resistant physical structures, employee screening, cameras, fences, identification checks, radomes (enclosures to protect antennas), and security guards. In the case of military or government satellite ground stations, they are often located within military compounds which already have heavy security measures in place. Insider threats are of particular concern for hacking as they can bypass security and gain useful information or alter systems to make remote access possible. Beyond physical security, and even beyond computer networks, ground stations need to be concerned with electronic intrusion, such as radio signal interception and jamming. Close proximity to the ground station provides more opportunities for hackers, such as introducing signal noise, polarization, or side-lobe meaconing, which involves the interception and rebroadcasting of signals (Steinberger 2008). This is comparable to 'war driving' in the computer realm. To defend against this antennas are often obscured from view by constructed or natural barriers to prevent attacks that are dependent on line of sight. Techniques are also used to identify interference, and the surveillance footprint around the ground station is increased. Additionally, link transmissions can employ:

> Error protection coding to increase the amount of interference that can be tolerated before communications are disrupted, directional antennas that reduce interception or jamming vulnerabilities, shielding and radio emission control measures that reduce the radio energy that can be intercepted for surveillance or jamming purposes; narrow band excision techniques that mitigate jamming by using smaller bandwidth, burst transmissions and frequency-hopping (spread-spectrum modulation) methods that communicate data in a short series of signals or across a range of radio frequencies to keep adversaries from "locking-on" to signals to jam or intercept them, antenna side-lobe reduction designs that mitigate jamming or interception vulnerabilities, nulling antenna systems (adaptive interference cancellation), and developing new technologies and procedures , such as lasers, [to] transmit information at very high bit rates and have very tight beams (Space Security Index 2012).

Hardening of satellites themselves involves the use of "designs and components that are built to be robust enough to withstand harsh space environments and deliberate attacks" (GAO 2002). As with hardening the other nodes in a satellite network, the major drawback is increased cost:

> Although all parts used in satellites are designed to withstand natural environmental conditions, some very high-quality parts that have undergone rigorous testing and have appreciably higher hardness than standard space parts are also available, including those referred to as class "S" parts. These higher quality space parts cost significantly more than regular space parts—partly because of the significant testing procedures and more limited number of commercial providers manufacturing hardened parts. According to an industry official, high-quality space parts are used by the military and are generally not used on commercial satellites (GAO 2002).

Enhanced manoeuvring and stealth capabilities of satellites, an emerging area of defensive capacity, can also be placed under the category of hardening.

Encryption

The role of signal encryption is another aspect of satellite structure which is difficult to ascertain in part because of the large number of satellite operators. All satellite signals can be encrypted, but whether they are or not, and the quality or strength of encryption used, is unknown and often

classified. A single satellite vendor can employ encryption on a case by case basis depending on the perceived security risk associated with the data being transmitted. Multiple nodes can be encrypted as well, such as TT&C uplinks, data uplinks, or access between terrestrial networks and the ground stations, or combinations thereof. In some cases special decryption hardware is also required "at the data's source and destination" with additional security precautions in place to restrict "access to the equipment and allowing no access by foreign nationals" (GAO 2002).

What can be ascertained is that encryption adds to the cost of operation and reduces efficiency, therefore commercial satellite operators are the least likely to implement its use. According to researchers at a 2008 security conference, encrypting satellite signals can cause an 80% drop in performance (Geovedi, Iryandi, and Zboralski, 2008). The cost factor can also include the cost of implementing or upgrading systems to allow encryption, as well as training staff on its proper use. Further, satellite transmissions can encompass multiple countries, with different countries having their own laws regarding the use of cryptography, creating legal obstacles that might persuade against the use of encryption (Greenberg 2010). "[National Security Agency] NSA officials stated that not all commercial providers' tracking and control uplinks are encrypted. Concerning the data links, customers are responsible for determining whether they are encrypted or not. Most commercial satellite systems are designed for 'open access,' meaning that a transmitted signal is broadcast universally and unprotected" (GAO 2002). Using encryption does not guarantee security either; it is only an added layer of defence. For example, researchers at the University of Bochum in Germany claimed to have cracked the A5-GMR-1 and A5-GMR-2 algorithms used by some satellite phones (Messmer 2013).

Case Study: Drones

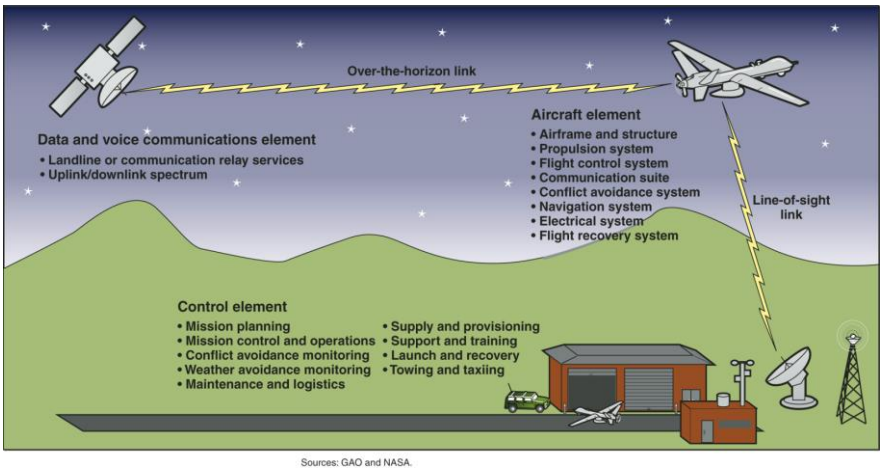
The rise of Unmanned Aerial Vehicles (UAVs), or drones, presents one example of a subgroup using satellite networks and the role of encryption. The International Institute for Strategic Studies identified 807 drones in active service around the world not including any that may be in use by China, Turkey, and Russia (Rogers 2012). Some estimates place the number of enemy combatants killed by US drones at 4,700, and the US military has introduced a new Distinguished Warfare Medal to honour drone pilots and computer network operators (Knox 2013 and Dwyer 2013). While the use of these drones remains contentious, their numbers and use continue to rise and additional markets are opening up. For example, in November 2012 Northrup Grumman began sea trials of its carrier based drone the X47-B, expected to enter service before 2020 (Skillings 2012). Meanwhile other defence contractors are developing competing designs, such as Boeing's Phantom Ray. Law enforcement and news agencies are also paving the way for domestic use, making Hollywood scenes of surveillance drones (*They Live*), rapid journalism (*Back to the Future II*), and assisting in criminal apprehension (*Minority Report*) closer to reality (Towards a Swarm of Nano Quadrotors 2012). The FAA "forecasts an estimated 10,000 civilian drones will be in use in the US" by 2018 (Lowly 2013).

But what role do satellites play in drones? Smaller remote controlled vehicles used by soldiers on the battlefield over short distances do not use satellites to relay communication. Even the X47-B does not, relying instead on autonomous programming (Weinberger 2012). However the larger Global Hawk reconnaissance UAV does rely on satellites to communicate globally with command and control, as do unmanned combat aerial vehicles (UCAVs), such as the Predator and Reaper, used for delivering strikes (Norris 2010, pp230-232; Wong and Fergusson 2010, p59). Being closer to the ground than satellites, these UAVs provide greater image detail and strike capability without violating international space treaties. These drones are like an additional mid atmosphere node in the broad structure template, or perhaps the drone itself could be considered a type of VSAT or user terminal. According to an article in *The Wall Street Journal*:

> The Air Force has staked its future on unmanned aerial vehicles. Drones account for 36% of the planes in the [US Air Force's] proposed 2010 budget. General Atomics expects the Air Force to buy as many as 375 Reapers (Gorman, Dreazen, and Cole 2009).

Domestic-use UAVs are an emerging field, so their common design features are not yet certain. However, an illustration in a 2013 Government Accountability Office report titled "Conceptual Rendering of Unmanned Aircraft System" shows a satellite as a part of the domestic network (see figure 6).

Figure 6 (GAO 2013)



UAVs have already come to the attention of hackers. Insurgents in Iraq and Afghanistan used a 26 US$ off the shelf software program called SkyGrabber, from Russian company SkySoftware, to capture unencrypted Predator video feeds. SkyGrabber accesses data being broadcast by satellites, allowing users to tune into different data streams comparable to tunning in broadcast radio stations (Ward 2009). This did not allow the insurgents to control or disrupt the UAVs; it only allowed them to eavesdrop on the signals being sent (see the next section on types of hacking). However this was alarming for several reasons. First, of all types of satellite operators the military is thought to implement the highest level of security measures, and yet encryption was not being used. Once this particularly weakness was exposed it had to be fixed, which added cost to the program, took time to implement, and reduced efficiency of the equipment. Secondly, the information gained by insurgents might have revealed the areas that were under surveillance and patterns of drone use, providing them with information they could use to avoid detection or set up an ambush (Gorman, Dreazen, and Cole 2009). Under asymmetric warfare, exploiting weaknesses in drones and an opponent's reliance on them could be used as part of a larger "blinding campaign" (Krepinevich 2010 and Tol 2010). As Captain J W Rooker of the US Marines states, "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" (Rooker 2008).

Internet Connected

It is difficult to determine the depth of Internet connectivity in satellite networks. As previously noted, there are currently 1046 operational satellites belonging to 47 states. Of these, 46 are civil, 388 commercial, 190 government, 203 military, and 219 a combination of these four (UCS Satellite Database 2012). Many of these were custom built for their mission, and detailed information on the Internet connectivity of any one of them is likely restricted as a security precaution. While the limits of science, technology, and cost force operators to follow a general template, even minor variations

can alter the ability to hack them. A hacker might limit their study to one specific satellite network; whereas this paper is attempting to discuss the topic as a whole. What is known is that satellites and ground stations predate the modern Internet. As development of satellite systems move away from one-off designs and attempt to increase their capability, Internet connections with them are likely to rise. Therefore cyber-attacks on satellite networks may be an emerging threat (Prime 2012).

A 2004 study published by the US President's National Security Telecommunications Advisory Committee "emphasized that the key threats to the commercial satellite fleet are those faced by ground facilities from computer hacking or possibly, but less likely, jamming" (Space Security Index 2012). VSATs are capable of direct contact with satellites, as well as contact with the hub. Many of the 1.4 million VSATs are connected to the Internet since Internet access is one of the services VSAT retailers are selling. This provides an Internet-based entry point into those satellite networks, either by hacking into VSAT signals or by procuring a VSAT of their own.

> In reference to the IRIS payload that is planned to be carried on-board INTELSAT 14 … its use of Internet protocol (IP) packet routing may cause the satellite to be susceptible to all of the vulnerabilities of IP packet routing. IP packet routing was intended to make routing as easy as possible. A packet routed with IP could be accessed, re-routed, or copied by anyone connected to the network. IP networks are susceptible to spoofing, sniffing, and session hijacking (Steinberger 2008).

Of more interest might be how connected the hub is to the terrestrial Internet, since access to a VSAT hub might allow TT&C control or the disabling of on-board satellite defences thereby increasing what could be done from a VSAT. It should be noted that compromising one VSAT network puts only a small number of the total satellites in orbit at risk since there is such a high diversity of operators. Add to this that a hub or ground station can be Internet connected, while the TT&C or communication data uplinks are not - it is possible to air gap the two. However; close proximity of the two computer networks increases the chance of careless configuration or roaming removable storage that could yield privilege escalation. The following case study focuses on an individual operator, NASA, from the perspective of Internet access vulnerability.

Case Study: NASA

The US Office of Inspector General (OIG) revealed several Internet based vulnerabilities in NASA computers systems, including those that control spacecraft like the International Space Station and Hubble Telescope.

> Specifically, six computer servers associated with IT assets that control spacecraft and contain critical data had vulnerabilities that would allow a remote attacker to take control of or render them unavailable. Moreover, once inside the Agency-wide mission network, the attacker could use the compromised computers to exploit other weaknesses we identified, a situation that could severely degrade or cripple NASA's operations. We also found network servers that revealed encryption keys, encrypted passwords, and user account information to potential attackers. These data are sensitive and provide attackers additional ways to gain unauthorized access to NASA networks (Martin 2011).

Among OIG's recommendations was for NASA to identify all Internet accessible computers on their mission networks and take action to mitigate associated risks. From this it can be extrapolated that NASA is not even aware of which computers have direct Internet connectivity. NASA depends on international cooperation, receiving input from global leaders in a wide range of fields. The Internet facilitates this, yet requires careful monitoring in its architecture in order to limit access to sensitive data and controls. NASA's size also poses conflicting security/productivity problems. NASA maintains more than "550 [dispersed] information systems" including "computer systems and

projects that control the Hubble Space Telescope, the Space Shuttle, the International Space Station, the Cassini and Lunar Reconnaissance orbiters, and several ground stations and mission control centers" (Martin 2012 and Martin 2011). According to a 2008 NASA quarterly report, "satellites from several US government space programs utilize commercially operated satellite ground stations outside the United States, some of which rely on the public Internet for data access and file transfers" (USCC 2011). In 2010 and 2011, NASA reported 5,408 computer security incidents that resulted in the installation of malicious software on or unauthorized access to its systems. A portion of these were advanced persistent threats believed to be state sponsored rather than individual hackers, hacker groups, or other non-state actors. Gaining access to NASA's computer systems can provide clues or open additional pathways for exploiting satellites.

Concern over escalating privileges also extends to the hardware used in satellite systems. OIG's investigation revealed improper sanitization and disposal of excess Shuttle IT equipment, resulting in the attempted sale of computers and hard drives which still contained sensitive data, one of which was subject to export control restriction, and the discovery of excess hard drives in an unsecured dumpster accessible to the public at one centre (Martin 2012). Further, as of 2012 only 1 percent of NASA's mobile devices, such as laptops, have been encrypted. This is particularly significant given NASA's reported loss or theft of 48 mobile computing devices between 2009 and 2011. For example, "the March 2011 theft of an unencrypted NASA notebook computer resulted in the loss of the algorithms used to command and control the International Space Station. Other lost or stolen notebooks contained Social Security numbers and sensitive data on NASA's Constellation and Orion programs" (Martin 2012). Worms and viruses have also made their way onto laptops which were then physically transported onto the International Space Station. It is unknown which, if any, on-board systems these laptops might connect with while in orbit. According to one account, "the virus did make it onto more than one laptop — suggesting that it spread via some sort of intranet on the space station or via a thumb drive" (Singel 2008).

The following is a select timeline of intrusions into NASA's computer systems, many of which are alleged to be Chinese or Russian state sponsored. Regardless of whether or not these incidents were state sponsored, they illustrate the existence of an Internet-based vulnerability, concerns that reverse engineering and analysis of sensitive hardware could be used against satellites, and the capability of drawing two states into conflict. Many of these incidents are cases of computer hacking, rather than satellite hacking, yet they can be used as a stepping stone for attacking satellites, and these computers could be considered part of the ground station portion of NASA's satellite systems or part of the ground-based terrestrial network interconnections.

Table 1: Timeline of Intrusions into NASA systems

1997 Trespassers penetrated computers in the X-ray Astrophysics Section of a building on NASA's Goddard Space Flight Center campus, where they commandeered computers delivering data and instructions to satellites. Before being discovered, the intruders transferred huge amounts of information, including e-mails, through a series of stops on the Internet to computers overseas. The advisory stated: "Hostile activities compromised [NASA] computer systems that directly and indirectly deal with the design, testing, and transferring of satellite package command-and-control codes"—in other words, computerized instructions transmitted to spacecraft (Epstein and Elgin 2008).

1998 A US-German ROSAT satellite, used for peering into deep space, was rendered useless after it turned suddenly toward the sun damaging the High Resolution Imager by exposure. NASA investigators later determined that the accident was linked to a cyber-intrusion at the Goddard Space Flight Center. The attack allegedly originated from Russia (Epstein and Elgin 2008).

2002 An online intruder penetrated the computer network at the Marshall Space Flight Center in Huntsville, Alabama, stealing secret data on rocket engine designs - Delta and Atlas rockets that power intercontinental missiles, enhancements of the Shuttle's main engines, and Lockheed's F-35 Joint Strike Fighter - information believed to have made its way to China, according to interviews and NASA documents (Epstein and Elgin 2008).

2003-2006 An alleged Chinese operation codenamed 'Titan Rain' targeted US defence and aerospace installations, including NASA, gathering sensitive military data. Among the information gathered were "a stockpile of aerospace documents with hundreds of detailed schematics about propulsion systems, solar panelling and fuel tanks for the Mars Reconnaissance Orbiter . . . specs for the aviation-mission-planning system for Army helicopters, as well as Falconview 3.2, the flight-planning software used by the Army and Air Force" (Thornburgh 2005).

2004 A cyber-trespasser who poked around NASA's Ames Research Center in Silicon Valley caused a panicked technician to pull the plug on the facility's supercomputers to limit the loss of secure data (Epstein and Elgin 2008).

2005 A malignant software program gathered data from computers in the Kennedy Space Center's Vehicle Assembly Building, where the Shuttle is maintained. The program, called stame.exe, sent information about the Shuttle to a computer system in Taiwan. The rupture had spread to a NASA satellite control complex in suburban Maryland and to the Johnson Space Center in Houston, home of Mission Control. At least 20 gigabytes of compressed data—the equivalent of 30 million pages—were routed to the system in Taiwan (Epstein and Elgin 2008).

2006 Top NASA officials were tricked into opening a fake e-mail and clicking on an infected link that compromised computers at the agency's Washington headquarters allowing access to budget and financial information. Those files contained clues about the size and scope of every NASA research project, space vehicle deployment, and cutting-edge satellite technology (Epstein and Elgin 2008).

2006 Due to concerns of computer network exploitation NASA facilities barred all incoming Word attachments from its computer systems (Epstein and Elgin 2008).

2007 The Goddard Space Flight Center was again compromised. This time the penetration affected networks that process data from the Earth Observing System, a series of satellites that enable studies of the oceans, land masses, and atmosphere. Inspector General Cobb issued another report, this one public, on Nov. 13, 2007: "Our criminal investigative efforts over the last five years confirm that the threats to NASA's information are broad in scope, sophisticated, and sustained." The agency refers internally to its efforts to stop intrusions linked to China under the code name "Avocado," according to interviews (Epstein and Elgin 2008).

2007 Landsat-7, a US earth observation satellite jointly managed by NASA and the US Geological Survey, experienced 12 or more minutes of interference. This interference was only discovered following a similar event in July 2008 (see below) (USCC 2011).

2008 Landsat-7, a US earth observation satellite jointly managed by NASA and the US Geological Survey, experienced 12 or more minutes of interference (USCC 2011).

2008 On June 20, 2008,Terra EOS [earth observation system] AM–1, a National Aeronautics and Space Administration-managed program for earth observation, experienced two or more minutes of interference. The responsible party achieved all steps required to command the satellite but did not issue commands (USCC 2011).

2008 On October 22, 2008, Terra EOS AM–1 experienced nine or more minutes of interference. The responsible party achieved all steps required to command the satellite but did not issue commands (USCC 2011).

2008 "…hackers are thought to have loaded a Trojan horse in the computers at Johnson Space Center in Houston, Texas. These hackers then used the Trojan horse to access the uplink to the International Space Station (ISS) and disrupt certain operations on-board, such as email. The attack was helped by the fact that ISS on-board computers are running older software for which security fixes are no longer available. . . ." (Steinberger 2008)

2010 A Chinese national was detained for hacking activity targeting US government agencies. Seven NASA systems, many containing export-restricted technical data, were compromised (Martin 2012).

2010 For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed US and other foreign Internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, routing all traffic to about 15 percent of the Internet's destinations through servers located in China. This incident affected traffic to and from US government (''.gov'') and military (''.mil'') sites, including those for NASA (USCC 2010).

2011 Romanian hacker TinKode allegedly obtained sensitive information from NASA's Goddard Space Flight Center and the European Space Agency which he then made publicly available online. The information included Login credentials for admin, content management, databases, email accounts, file upload (FTP), and other key systems (Leyden 2011 and Prime 2012).

2011 NASA's Jet Propulsion Laboratory (JPL) "reported suspicious network activity involving Chinese-based IP addresses... giving the intruders access to most of JPL's networks" (Martin 2012).

2013 Chinese national Bo Jiang, a former NASA contractor, was arrested as he was attempting to return to China with "a large amount of information technology that he may not have been entitled to possess,"… NASA shut down access to an online database and banned new requests from Chinese nationals seeking access to its facilities amid mounting concerns about espionage and export control violations…. The security measures include a complete ban on remote computer access by Chinese contractors already working at NASA centers (Klotz 2013). NASA employs 118 Chinese nationals in "remotely-based" information technology jobs that may enable them to penetrate the space agency's national security database servers, and 192 Chinese nationals in positions with "physical access" to NASA facilities (Pollock 2013).

2013 The US Congress passed a provision which prohibits the Commerce and Justice departments, NASA and the National Science Foundation from buying any information technology system that is "produced, manufactured or assembled" by any entity that is

> "owned, operated or subsidized" by the People's Republic of China. The agencies can only acquire the technology if, in consulting with the FBI, they determine that there is no risk of "cyberespionage or sabotage associated with the acquisition of the system," according to the legislation. In addition to condemnation from China, this rule could upset US allies whose businesses rely on Chinese components in some of the equipment they sell to the US (Flaherty 2013).

3. Types of Satellite Hacking

Satellite hacking can be broken down into four main types: Jam, Eavesdrop, Hijack, and Control. Jamming is flooding or overpowering a signal, transmitter, or receiver, so that the legitimate transmission cannot reach its destination. In some ways this is comparable to a DDoS attack on the Internet, but using wireless radio waves in the uplink/downlink portion of a satellite network. Eavesdropping on a transmission allows a hacker to see and hear what is being transmitted. Hijacking is the unauthorized use of a satellite for transmission, or seizing control of a signal such as a broadcast and replacing it with another. Files sent via satellite Internet can be copied and altered (spoofed) in transit. The copying of files is eavesdropping, while spoofing them is hijacking, even though the access point and skillset used for file spoofing fits better with eavesdropping. This illustrates the ability, in some cases, for hackers to move seamlessly between categories, and the difficulty of placing strict categorization on types of satellite hacking. Controlling refers to taking control of part or all of the TT&C ground station, bus, and/or payload – in particular, being able to manoeuvre a satellite in orbit.

There is some overlapping grey area with these categories, and the terms themselves are open for debate. For example, the categories of Eavesdrop and Hijack might be better described with the titles of Intercept and Pirate respectively. However “pirate” is commonly used to describe downloading multimedia illegally or receiving television channels illegally. Hijack might also be better labelled as ‘signal hijack’, since the satellite itself is not hijacked. Adding to the confusion, sea pirates often hijack ships, so these words are already in regular use for other topics within international relations literature. Further, jamming and eavesdropping could take place entirely at the ground station level, never making contact with the satellite or uplinks and downlinks, thereby creating some instances that stray from the phrase ‘satellite hacking’. Never the less, these instances would disrupt the satellite’s function, and computer networks at ground stations are an essential component of a satellite network. Straying even further from the phrase ‘satellite hacking’ are the use of lasers to blind or damage the optics of imaging satellites, or computer network attacks that cause power outages resulting in disruption to ground station capability. Lastly, further analyses could be given to address whether these four fall under the cyber warfare categories of computer network operations (CNO) or electronic warfare (EW). This would involve a case by case basis to determine if an Internet connection was utilized, whether or not it involved military hardware, and an assessment of the possible strategic (verses merely criminal) intent of the perpetrator. Despite the limitations described here, these four types of satellite hacking are significantly different and warrant precise terminology, the terms chosen for this paper are useful for discussion, and their connotations outweigh those of similar terms.

Jamming

In general jamming “requires a directed antenna, knowledge of the frequency to be affected, and enough power to override its source” (Rooker 2008). In many ways this can be considered the easiest form of satellite hacking since it can be as simple as throwing an abundance of noise at the receiver to drown out the transmission. The receiver can be the satellite receiving an uplink or a

ground station or user terminal receiving a downlink. Jamming the uplink requires more skill and power than a downlink, but its range of disruption tends to be greater, blocking all possible recipients rather than a terrestrial range limited portion (GAO 2002). Jamming would most likely fall under the larger title of EW rather than CNO, although the Internet might be used to obtain frequencies, schedules, and ground station layouts. Additionally, jamming could be considered CNO in more technical scenarios such as using one satellite to jam another. A DDoS or other malicious cyber-attack against computers used for ground station operations could also effectively jam a satellite. Even though the signal itself would not be attacked, an essential component of the satellite system would be. Below is a timetable of documented incidents.

Table 2: Timeline of Documented Jamming Incidents

1995 Kurdish satellite channel, MED-TV, was intentionally jammed because it was believed to be promoting terrorism and violence (GAO 2002).

1997 Resulting from the use of a disputed orbital slot, Indonesia jammed the communication satellite APSTAR-1A by transmitting interference from their own satellite Palapa B1. APSTAR-1A was being leased from the island nation of Tonga by Hong Kong based APT Satellite Company to broadcast into the PRC. Indonesia had peacefully settled a prior dispute in 1992 involving the same orbital slot, that time conflicting with a Russian Gorizont commercial communications satellite being leased by American company Rimsat (GAO 2002, and Wong and Fergusson 2010, p85).

1998 Kurdish satellite channel, MED-TV, launches "a major campaign to combat what it alleges is the persistent interference of its transmissions by the Turkish Government…taking the issue to the European Court of Human Rights and [gaining] the backing of [an] anti-censorship pressure group … (Kurds retaliate in Turkish jam war 1998)".

2000 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 (Grau 2000).

2003 The Cuban and Iranian governments collaborated to jam Telstar 12, a US commercial communications satellite in geostationary orbit used to transmit programming by Voice of America to Iran (Waller 2003).

2003 Iraq acquired GPS jamming equipment during Operation Iraqi Freedom allegedly from Russian company Aviaconversiya Ltd. Six jamming sites were discovered and destroyed in the air campaign prior to ground operations (Wong and Fergusson 2010, p85). The equipment's effectiveness appeared to be negligible; however it does suggest "that jamming capabilities could proliferate through commercial means" (Space Security Index 2012).

2004 The mobile, ground-based CounterCom system, designed to provide temporary and reversible disruption of a targeted satellite's communications signals, was declared operational. In 2007 this was upgraded to seven jamming units, up from the original two. Next-generation jammers will likely have 'enhanced capabilities for SATCOM denial,' using largely commercially available components (Space Security Index 2012).

2005 The Libyan government jammed two telecommunications satellites, "knocking off air dozens of TV and radio stations serving Britain and Europe and disrupting American diplomatic, military and FBI communications" (Hencke and Gibson 2005).

2005 In response to several jamming incidents attributed to the Falun Gong, China launched its first anti-jamming satellite, the Apstar-4 communications satellite. China also reportedly upgraded its Xi'an Satellite Monitoring Center to diagnose satellite malfunctions, address issues of harmful interference, and prevent purposeful damage to satellite communications links (Space Security Index 2012).

2006 Thuraya mobile satellite communications were jammed by Libyan nationals for nearly six months. The jamming was aimed at disrupting smugglers of contraband into Libya who utilize satellite phones dependant on Thuraya satellites (Steinberger 2008).

2006. "During the 2006 Israel-Lebanon war, Israel attempted to jam the Al-Manar satellite channel which is transmitted by the Arab Satellite Communications Organization (ARABSAT), illustrating the potential for commercial satellites to become targets during conflict (Steinberger 2008)".

2007 Reports emerged that China had deployed advanced GPS jamming systems on vans throughout the country (Wong and Fergusson 2010, p85; USCC 2011; and Space Security Index 2012).

2007 "Landsat-7, a US earth observation satellite jointly managed by NASA and the US Geological Survey, experienced 12 or more minutes of interference. This interference was only discovered following a similar event in July 2008 (see below) (USCC 2011)".

2008 Landsat-7, a US earth observation satellite jointly managed by NASA and the US Geological Survey, "experienced 12 or more minutes of interference" (USCC 2011).

2010 Persian-language satellite broadcasts originating from European satellite signals, including broadcasts of the BBC, Deutsche Welle, and France's Eutelsat were intentionally jammed from Iran (Sonne and Fassihi 2011 and Space Security Index 2012).

2011 LuaLua TV, a London-based Bahraini current affairs network founded by 15 members of the Bahraini opposition, was jammed four hours after its first broadcast (Space Security Index 2012).

2011 Libyan nationals jammed Thuraya satellites for more than six months in an effort to disrupt the activities of smugglers who use satellite phones (Thuraya Telecom Services Affected by Intentional Jamming in Libya 2011 and Space Security Index 2012). **Note the prior instances in 2005 and 2006 listed above.

2011 Ethiopian Satellite Television (ESAT), an Amsterdam-based satellite service, was repeatedly jammed by the Ethiopian government, with the assistance of the Chinese government. Voice of America and Deutsche Welle Amharic Services were also affected (Space Security Index 2012).

2011 RAIDRS, a U.S. ground-based defensive system designed to detect potential attacks against military space assets, completed its sixth year of operational capability. It serves "to detect, characterize, geolocate and report sources of radio frequency interference on US military

and commercial satellites in direct support of combatant commanders" (Space Security Index 2012).

2012 The Eritrean Ministry of Information accused the Ethiopian government of blocking transmissions from Eritrea's state-run satellite television (Space Security Index 2012).

Eavesdropping

Several online videos detail how relatively low cost commercial off the shelf products can be used via computer and antenna to illegally: view satellite television, eavesdrop on satellite telephone conversations, eavesdrop on Internet traffic (including the ability to gain account passwords), and view satellite imagery (Laurie 2009, Greenberg 2010, Szczys 2011, and IndianZ 2012). The case study on UAVs and the use of satellite phone encryption exploits given in section two of this paper are examples of eavesdropping. In the past, long distance phone calls were predominantly routed through satellites, exposing them to satellite eavesdropping. This faded by the turn of the century with the use of undersea cables and networks of microwave towers and cell (radio) towers that can bridge the gap between city grids without the need for satellites. However, some signals intelligence satellites are designed to pick up this terrestrial traffic, so by eavesdropping on these eavesdropping satellites it remains theoretically possible to access the larger network of phone transmissions (Norris 2010). Remote locations continue to rely on satellites for communication, and banking and Internet traffic over VSATs has increased. Open source material on high profile incidents and arrests relating to eavesdropping are sparse, despite readily available information on how to conduct such operations and the emergence of a niche subculture that are combing the skies in search of access points. A lack of reported incidents could be due to the nature of this category, as some might view it as regular hacking or simply illegal activity rather than 'satellite hacking'. For example, an individual caught illegally receiving free satellite TV channels might not be considered newsworthy. Additionally, the flow of data is not damaged or disrupted, which might reduce some concerns. The lack of attention received by this category could make it an appealing avenue.

Hijacking

Hijacking is illegally using a satellite to transmit the hacker's signal, in some cases overriding or altering legitimate traffic. Hijacking is predominantly connected to communication broadcasts or Internet over satellite connections. The same techniques and commercial off the shelf software noted above for eavesdropping can also be used for some types of hijacking. For example, piggybacking or illegally using satellite Internet connections, spoofing legitimate users intended webpages and web addresses, and redirecting legitimate Internet traffic (Laurie 2009, Greenberg 2010, Szczys 2011, and IndianZ 2012). To use web-based terminology, this is comparable to Wi-Fi theft or leaching, web page defacement, and DNS cache poisoning. The possibility of data manipulation is of particular concern to militaries who are implementing the revolution in military affairs and net-centric warfare. Below is a timeline of known incidents.

Table 3: Timeline of Hijacking Incidents

1977 The audio portion of an ITN news broadcast on Southern Television in the UK was replaced by an audio message claiming to be from outer space. The message warned that humankind's current path would lead to an undesirable future (British Viewers Hear Message 1977).

1985 Four astronomers at Poland's University of Torun … used a home computer, a synchronizing circuit, and a transmitter to superimpose messages in support of the labor movement

Solidarność (Solidarity) over state-run television broadcasts in Torun… The messages read 'Enough price increases, lies, and repressions. Solidarity Torun' and 'It is our duty to boycott the election' with the inclusion of the Solidarity logo (Jan Hanasz: The Polish TV Pirate 1990).

1986 A Florida man using the name Captain Midnight disrupted the uplink to a Galaxy I satellite. For 4 to 5 minutes viewers of HBO on the US East coast saw the following message, placed over SMPTE colour bars:

GOODEVENING HBO
FROM CAPTAIN MIDNIGHT
$12.95/MONTH ?
NO WAY !
[SHOWTIME/MOVIE CHANNEL BEWARE!]

(GAO 2002, The Story of Captain Midnight 2007, and Rooker 2008).

1987 The Playboy Channel, based on the popular adult magazine, had its signal hijacked by an employee of the Christian Broadcasting Network. "He was indicted for a violation of 18 USC 1367 (satellite jamming). In a week-long trial in Norfolk, VA, evidence was produced by the prosecutor that showed that both the character generator and the transmitter at CBN matched the tape recording of the *jamming*" (Bellows 2007).

1987 A Max Headroom impersonator overtook the television signal of two Chicago based stations, commandeering a live news broadcast and an episode of Dr. Who for 25 seconds and 90 seconds respectively (Bellows 2007).

2002 The Falun Gong illegally used an AsiaSat satellite to broadcast into China disrupting broadcasts of China Central TV (CCTV) with anti-government messages (Morrill 2007 and Steinberger 2008). It is unclear from these reports how often this happened and for what duration, or whether all instances used an open transponder on a bent pipe structure or required overpowering other signals.

2006 "During the 2006 Lebanon War, Israel overloaded the satellite transmission of Hezbollah's Al Manar TV to broadcast anti-Hezbollah propaganda. One spot showed Hezbollah leader Hassan Nasrallah with crosshairs superimposed on his image followed by three gunshots and a voice saying 'Your day is coming' and shots of the Israeli Air Force destroying targets in Lebanon" (Friedman 2006).

2007 An intrusion incident occurred on Czech Television's Sunday morning programme Panorama, which shows panoramic shots of Prague and various locations across the country, to promote tourism. One of the cameras, located in Černý Důl in Krkonoše, had been tampered with on-site and its video stream was replaced with the hackers' own, which contained CGI of a small nuclear explosion in the local landscape, ending in white noise (Wohlmuth 2007).

2007 A grainy photo of a man and woman interrupted Washington, DC ABC affiliate WJLA's digital or HD signal for two hours. The incident was initially deemed a genuine signal intrusion by various websites but has since been confirmed to be the result of an older HDTV encoder malfunctioning in the early morning hours and going undetected (Swann 2007).

2007 The Tamil Tigers (LTTE) in Sri Lanka illegally broadcast their propaganda over Intelsat satellites (Jayawardhana 2007, Morrill 2007, and Steinberger 2008).

2009 Brazilian authorities arrested 39 university professors, electricians, truckers, and farmers who had been using homemade equipment to hijack UHF frequencies dedicated to satellites in the US Navy's Fleet Satellite Communication system for their personal use (Soares 2009).

2013 TV stations in Montana and Michigan had their Emergency Alert System systems commandeered and used to warn of a Zombie attack. In one case an audio recording announced that "dead bodies are rising from their graves" and in another the ticker, or message that scrolls across the bottom of the screen, was used for this same message (Thompson 2013; Zombies? Emergency Broadcast System hacked 2013). It is unclear if control of these transmissions requires satellites or is Internet-connected. A lack of detail provided in reports may be due to fear of revealing the vulnerability of these systems.

Control

Controlling a satellite involves breaching the TT&C links. Theoretical examples include issuing commands for a satellite to use its reserve propellant to either enter a graveyard orbit or renter the Earth's atmosphere and burn up, or causing a satellite to rotate, so that the solar panels and antenna are pointed in the wrong directions (Norris 2010, p36; Gutteberg 1993, p12). Reaching this command and control level appears to be the most difficult of satellite hacking, since this is where security is greatest. In particular, military satellite networks often locate TT&C ground stations within military bases and they employ encryption at multiple levels. However the military often leases commercial satellites to meet the growing needs they cannot fulfil on their own, and in these cases the satellite service provider is typically responsible for the TT&C links and satellite control ground station, with the military only securing the data links and communications ground stations (GAO 2002). Further, weakness in the command and control of commercial satellites, such as VSAT hubs, could place military satellites at risk from collision or the creation of debris fields due to compromised control of the commercial satellites. Thus far there have been few reported incidents of hackers gaining satellite control, at least few in comparison to jamming incidents; below is a list of open source allegations.

Table 4: Timeline of Alleged Takeovers of Satellite Control (note that some examples logically overlap earlier cases)

1998 A US-German ROSAT satellite, used for peering into deep space, was rendered useless after it turned suddenly toward the sun damaging the High Resolution Imager by exposure. NASA investigators later determined that the accident was linked to a cyber-intrusion at the Goddard Space Flight Center. The attack allegedly originated from Russia (Epstein and Elgin 2008).

1998 "Members of a hacking group called the Masters of Downloading claim to have broken into a Pentagon network and stolen software that allows them to control a military satellite system. They threaten to sell the software to terrorists. The Pentagon denies that the software is classified or that it would allow the hackers to control their satellites, but later admits that a less-secure network containing 'sensitive' information had been compromised" (Morrill 2007).

1999 Media reports alleged that a Skynet, British military communications, satellite had been taken control of through hacking and was being held for ransom. These reports were later claimed to be false (Campbell 1999; Wong and Fergusson 2010, pp87-88).

2008 "On June 20, 2008,Terra EOS [earth observation system] AM–1, a National Aeronautics and Space Administration-managed program for earth observation, experienced two or more minutes of interference. The responsible party achieved all steps required to command the satellite but did not issue commands" (USCC 2011).

2008 "On October 22, 2008, Terra EOS AM–1 experienced nine or more minutes of interference. The responsible party achieved all steps required to command the satellite but did not issue commands" (USCC 2011).

Non-hacking examples that illustrate the possible effect satellite takeover could have:

1997 A ground based transmitter unintentionally interfered with the GPS receiver of a commercial aircraft causing the plane to temporarily lose all of its GPS information (GAO 2002).

1998 The failure of PANAMSAT's Galaxy IV satellite, attributable to an on-board processor anomaly, disabled 80 to 90 percent of 45 million pagers across the United States for 2 to 4 days, and blocked credit card authorization at point-of-sale terminals (such as gasoline pumps), leaving approximately 70 percent of a major oil company's customers without the ability to pay for services at the pump (GAO 2002).

4. Additional Satellite System Vulnerabilities

This section covers "additional" satellite system vulnerabilities - several vulnerabilities have already been revealed through the discussion in section two. For example, defensive measures such as redundancy, hardening, and encryption all have deterrents to their use and for some satellite operators the benefits of Internet connectivity outweigh the perceived risk. Also, increasing the availability and mobility of VSATs and BGAN, along with lowering the technical expertise required to operate them, has the unintended consequence of making satellites accessible to a greater number of hackers. This section will examine aspects of vulnerability not yet fully explored, including the lure of cost saving methods, military reliance on commercial satellites, attribution difficulties, globalization's effect on security, and the role of international governance.

Cost Saving Methods

A root cause of many satellite vulnerabilities is an attempt to cut cost. As explored in Section two, profit driven risk assessment, particularly with commercial operators, has resulted in increased Internet connectivity and reduced redundancy, hardening, and encryption. Increasing Internet connectivity of satellite systems increases performance and reduces the cost of operations, but it exposes satellite systems to increased risk of malicious activity. Implementing redundancy techniques requires the purchasing of backup hardware, software, satellites, and ground stations; while efforts to reduce the cost of redundancy, such as microsatellites and standardized equipment, open up new vulnerabilities including a lack of diversity. Hardening of ground stations requires increased infrastructure and staff, hardening of uplinks and downlinks requires additional equipment and expertise, and hardening of the satellites requires higher cost parts that have undergone extensive testing and can withstand greater stress. Encryption lowers performance and increases cost, in some cases requiring additional hardware, training, difficult upgrades, and legal obstacles. In contrast with protecting satellites, hacking satellites has the lure of being relatively cheap (Laurie 2009, Greenberg 2010, Szczys 2011, and IndianZ 2012). Instead of acquiring the missile launch and guidance capability of an anti-satellite (ASAT) weapon, a capability thus far only demonstrated by

three states, it might be cheaper and easier to hack the intended target. Thus cyber-attacks fit into the general schema of asymmetric strategies that can be deployed by small or developing states, NGOs, militant groups, and in some cases skilled individuals.

A typical satellite can have a lifespan of 15 years, yet technology on the ground can drastically change in that time. For this reason older satellites might be more vulnerable as defences may be less stringent, security flaws can be exposed over time, and there are limited means to patch those flaws once it is in orbit. Some modern satellites have payloads and busses capable of receiving updates from the ground; however this opens a new vulnerability in that the updates could be corrupted. During a satellite's lifespan new commercial-off-the-shelf (COTS) products capable of inflicting harm may also become available to hackers. Efforts are underway to streamline the manufacturing of universal buses that can house unique payloads, yet the bus itself is critical to the satellite's function and reducing variety may increase vulnerability (Norris 2010 and Butler 2013). Most satellite components still require specialized components, but as technology improves, there is an increased risk of COTS being used to save money, further limiting security (Steinberger 2008). Another cost saving practice is the "leasing [of] commercial telecommunication lines for long-haul communications". This "trend from dedicated to shared lines for communications also expands the surface area for cyber attack" (Prime 2012). A lack of training can result in existing security features being unused or improperly configured (Geovedi, Iryandi, and Zboralski, 2008).

Military Reliance on Commercial Satellites

While government and military satellite operators place security as a high priority, commercial satellite operators are primarily concerned with profit. A low number of satellite disruptions incidents to date might cause companies to view reduced security as an acceptable risk in comparison with the cost of implementing higher security and reducing productivity. This "raises security concerns, since a number of military space actors are becoming increasingly dependent on commercial space assets for a variety of applications" (Space Security Index 2012). While governments rely on commercial satellite operators, they are not the primary customer, accounting for only 10% of the market in the US. **"**As a result, federal customers generally have not influenced security techniques used for commercial satellites" (GAO 2002).

> Although the government owns satellites, it also relies for certain services on satellites owned and operated by commercial satellite service providers. For example, the Department of Defense (DOD) typically relies on commercial satellites to fulfil its communications and information transmission requirements for non–mission-critical data and to augment its military satellite capabilities. The importance of commercial satellites for DOD is evident during times of conflict: according to a DOD study, commercial communications satellites were used in 45 percent of all communications between the United States and the Persian Gulf region during Desert Shield/Desert Storm… Further, during operations in Somalia from December 1992 through March 1994, U.S. military and commercial satellite coverage was not available, so Russian commercial satellites were used (GAO 2002).

84% of military communications during Operation Iraqi Freedom were transmitted through commercial satellites (Shachtman 2008 and Steinberger 2008). Beyond military reliance, commercial satellites are a critical component of national and global economies. Therefore security vulnerabilities in commercial satellites are a concern for governments even if their military is not using them. Other countries with a heavy reliance on satellites such as China or Russia might have more influence over security measures in the commercial sector. For example, China's use of State-owned Enterprises (SOEs), the identification and 'preferential treatment' given to strategic industries, heavyweight industries, and national champions might allow a tighter approach to security. Yet they too have a history of profit driven corruption and misreporting (USCC 2011).

Attribution Difficulties

Attributing a hacking incident to one particular actor is not always easy. In the case of an Internet connected attack, all of the difficulties associated with identifying a traditional hacker apply. Computers can be compromised and used under remote access, and proxies can be used, making it unclear if the computer identified in the attack was the last link in the chain. Not only can the attack traverse multiple countries, it can traverse multiple satellites (Laurie 2009). Assuming it was the last link in the chain, it remains uncertain if the owner was acting alone or was state-sponsored. Tracing IP addresses and conducting computer forensics also runs into multinational legal hurdles. While this could be an area of international cooperation, information sharing, and global standards, such convergence seems unlikely given the close ties satellites have to the military and economic advantages of leading nations.

Non-Internet based attacks, such as using radio signals to transmit data or jam, also carry attribution difficulties. It might be difficult to distinguish interference from a hacker, human error, solar activity, or unintentional orbital congestion. Accounts on the difficulty of identifying electronic hacking vary. This may be due to the large number of satellite providers – each with varying levels of resources available and varying defence capabilities. It could also be due to the wide range of potential attacks, differences in the attacker's capability, or varying motives behind the assessment. One account given by the US General Accounting Office states:

> … Commercial satellite interference is regulated both internationally and nationally. The International Telecommunication Union specifies interference resolution policies and procedures, including those for harmful interference. Further, within the United States, the Federal Communications Commission (FCC) has the capability to track the location of interference, at a service provider's request. Also, service providers told us that they could locate and identify unintentional or unauthorized users through a technique called triangulation. Once an unauthorized user is located, a commercial service provider can jam that user's signal if the user cannot be persuaded to stop using the satellite. However, according to industry officials, typically an unauthorized user would be identified, located, and contacted through a combination of industry and government resources before such jamming would be needed (GAO 2002).

Alternatively, an unnamed satellite company employee writes:

> Since a satellite has a wide coverage area, it's very difficult to find the transmitter. There are some very expensive systems to locate interferences, they work based on small shifts in frequency and time that depend on the transmitter location, but these systems cannot locate a transmitter with an accuracy better than tens of miles. After finding the general area where the interference originates, one must sweep the whole region with a helicopter equipped with a directional antenna. Very messy and very expensive (Sri Lankan Terrorists Hack Satellite 2007).

Other accounts present a much more challenging process, or state that locating the interference is not difficult, "but [it is] almost impossible to remove without political intervention, and even then this may prove difficult" (Coleman 2012 and Kawase2012, pp213-219). In one case, researchers at a satellite security conference stated that an Indonesian satellite provider contacts customers when they suspect an unauthorized user on their network. They ask the customers to disconnect so they can see if a connection to their system remains, thereby identifying an unauthorized user. The researchers circumvented this low-tech identification process by writing a script that would disable their connection if the authorized user they were piggybacking switched off (Geovedi, Iryandi, and Zboralski, 2008).

Globalization's Effects on Security

Increased consumer reliance on satellites for banking, navigation, and point of sale transactions increases the potential damage a disruption can cause. Once new electronic systems are in place, the old paper based systems fade out and cannot be substituted if needed during failure. The technical expertise required to operate satellite systems, as well as their multistate collaborations and global reach means employees from many states are given access to sensitive technology and information. This increases the risk of insider threats and espionage. A wide range of contractors are utilized in development from the antenna production, busses, energy supplies, ground stations, hardware, hubs, launch facility, propulsion systems, software, various computers, and so forth. This extensive supply chain must be monitored to ensure no embedded backdoors or exploits are inserted during development. For example, a portion of Australia's National Broadband Network (NBN) will rely on satellites. Israel's Gilat Satellite Networks Limited was selected by Australian telecommunications company Optus Networks "to design, build, and operate the network for the National Broadband Network Company's Interim Satellite Service." Eleven SkyEdge II hubs and 20,000 SkyEdge II VSATs are to be deployed by Gilat over the next three years, with an option for more hubs and up to 48,000 VSATs (Space Security Index 2012). Meanwhile the Australian government banned Chinese telecom giants from NBN contracts due to security concerns reportedly issued by ASIO (Benson 2012; PM defends banning of Chinese company 2012). Shortly thereafter the US House Permanent Select Committee on Intelligence issued a detailed report cataloguing concerns that Chinese telecoms Huwaei and ZTE had strong ties to the CCP government and were attempting to embed backdoors into telecommunications for future attack or exploitation (Rogers and Ruppersberger 2012). This in turn drew denouncement and criticism from China. Reverse engineering and compliance with export laws on dual use technology are also a regular topic of concern.

> The commercial satellite industry is a global industry that includes many foreign-owned corporations as well as partnerships between US and foreign corporations. As a result, the US government depends on foreign and international companies. For example, some commercial space systems of foreign origin are used by the US military for imagery and communications support. NDIA reported that foreign ownership of satellites is expected to grow and predicted that by 2010, 80 percent of commercial communication satellite services could be provided by foreign owned companies. This globalization of the satellite industry could affect the availability of commercial satellite systems to US government or commercial entities through frequency allocations, tariffs, politics, and international law (GAO 2002).

Announcements available online that detail awarded satellite contracts, upcoming developments, and designs could provide an adversary with a target list. As one example, Space Security 2012 reveals that "Emergent Space Technologies was awarded a contract by the NASA Ames Research Center for the provision of cluster flight guidance, navigation, and control algorithms and software for System F6." This could be used for a phishing campaign in the hope of obtaining software names and keys to be used on these systems. Growing awareness of satellites as a potential target of hacking and the commercial proliferation of network hardware and software, like Dreambox and Wireshark respectively, might increase attempts to do so (Laurie 2009 and Greenberg 2010). Yet to limit information sharing and suppress technology would also be detrimental to advancement.

In addition to listings of satellite positions being publicly available online, the proliferation of mobile devices such as tablets, netbooks, and mobile phones have made the process of locating satellites easier. For example, The Night Sky App allows users to hold their mobile phone up to the sky and locate satellites in real-time by utilizing GPS and an internal gyroscope. Among the satellites it identifies are Iridium 'satellite phone' satellites and amateur radio satellites used for communicating on FM or single-sideband modulation (App Review 2012 and The Night Sky User Guide 2012). Other apps, like Orbitron, Satellite AR, Satellite Tracker, Satellite Finder, and SatFinder, encompass a

greater range of satellites, like weather, and provide "frequency information" (Satellite Tracker 2009). Some are specifically designed for aligning an antenna to enable communication with the satellite. Information on the type of orbit they are in, such as geostationary or LEO, may give a hacker insight into the type, function, and operations of a satellite, yet this seems unnecessary since some apps and websites disclose the full name of the satellite to begin with. Many of these apps are free to download, or cost a nominal fee, such as 99 US cents.

International Governance

Disputes have arisen over the allocation of advantageous orbital slots and radio frequencies. The 1997 jamming incident listed in section three of this paper demonstrates how these disputes can deteriorate and result in conflict (Wong and Fergusson 2010, p85). Commercial entities may also find themselves having to answer to foreign ambassadors as was the case with LTTE illegally broadcasting propaganda over US owned Intelsat (Jayawardhana 2007). As another example, the telecommunications company LightSquared had prolonged discussion and analysis with the US government over concerns that their deployment of high powered transmitters would interfere with GPS signals. Although this was a domestic case, it underscores the importance of such issues for sustainable space operations (Space Security Index 2012). The International Telecommunication Union (ITU) Constitution governs international sharing of the finite radio spectrum and orbital slots used by satellites in GEO. As noted in section two, specific orbits near the equator are optimal, because they can provide an entire country with continuous service coverage. Conflict and competition can arise, because a single orbital slot may be the optimal position for multiple countries. The ITU has been pursuing reforms to address slot allocation backlogs and other related challenges that "call into question the inherent fairness of an allocation system that has operated on a first-come, first-served basis" (Space Security Index 2012). Military communications are exempt from the ITU Constitution, though they should observe measures to prevent harmful interference.

Recognition of the vulnerability of satellite systems is simultaneously increasing defensive postures and attack capability. There is an increasing recognition by states that satellites are a critical infrastructure. With this recognition come programs of awareness and education, and reconsideration of laws related to infrastructure protection, such as the appropriate response to various levels of satellite hacking incidents. A 2002 Government Accounting Office report on satellite security stated that a comprehensive effort would need to "include a system of surveillance, assessment, early warning, and response mechanisms to mitigate the potential for cyber threats" (GAO 2002). Debatably cyber-sat defence could be an area for information sharing, cooperation, coordination, and international law. However; this seems more prone to happen at an ally and coalition level given the disparity between various states' capabilities, the advantages that come from that, and close ties to economy and national security. In 2005, China launched its first anti-jamming satellite and increased satellite defence. The US has also been boosting satellite defence, as noted above with the CounterCom and RAIDRS Systems. Further, the US has publicly announced its stance of treating cyberspace as an operational domain that includes offensive capability (Space Security Index 2012). Along with this come organisation, training, and equipment that employ new defence operating concepts, defence testing, and R&D. Mastering defence reveals ways of attack, and increased satellite defence/understanding can be reapplied to attack, so increased concerns over the security of satellite networks might lead to an escalation in attack capability. Given the large number of satellite operators and their varying interests, known exploits might be kept secret, inadvertently creating catalogues of satellite 'zero day' exploits. Further, non-state actors are not the only hackers who might target satellites. States themselves can have a strategic interest in hacking satellites, and satellite capable states would have access to much more technical detail than the general public.

The military doctrines of a growing number of states emphasize the use of space systems to support national security (Space Security Index 2012). Space technology is a key component of the Revolution in Military Affairs, and the five military D's – degrade, disrupt, deny, destroy, and deceive – fit well with jam, eavesdrop, hijack, and control. At the same time, reliance on satellites can be viewed as a soft spot that could be exploited. For example, authoritative "Chinese military writings advocate attacks on space-to ground communications links and ground-based satellite control facilities in the event of a conflict" (USCC 2011). In a publication of the People's Liberation Army, Li Daguang, a researcher at the Chinese Academy of Sciences, wrote "seizing space dominance is the root for winning war in the Information Age" (Epstein and Elgin 2008). Unlike China's 2007 ASAT test, a cyber or electronic attack against satellites would not create a harmful debris cloud, and it would provide greater anonymity. One 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." According to the Chinese book *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" (USCC 2011). While space capable states have access to the greatest amount of information and resources in relation to satellite hacking, they also have the most to lose, and non-state actors might wish to take advantage of the asymmetric benefits of satellite hacking.

5. Conclusion

Satellite systems conform to a general template composed of TT&C and communication ground stations, uplinks and downlinks from these ground stations, and the satellites in orbit. Communication ground stations further link into extensive and varied networks of terrestrial interconnections. VSATs make up a large portion of these ground stations, and a wide range of user terminals are capable of receiving data downlinks. Distinction between four types of satellite hacking have been put forward – Jam, Eavesdrop, Hijack, and Control - and timelines of known incidents provided. The primary deterrents to increased satellite security are increased cost and decreased productivity; finding the correct balance depends on an effective risk assessment. Vulnerabilities exist at all nodes and links in satellite structure. These can be exploited through Internet-connected computer networks, as hackers are more commonly envisioned to do, or through electronic warfare methodologies that more directly manipulate the radio waves of uplinks and downlinks. This is not a great departure given that hacking has its origin in telephone phreaking, and modern computer networks rely heavily on wireless communication. Additional difficulties in securing satellite systems include: advanced technology becoming available to a greater number of individuals, the diversity of operators and designs (which can also be a strength), extensive supply chains, the inclusion of attacking satellites in military doctrines, and various forms of international disputes concerning the governance of satellites, their orbit, or frequencies. The primary limitations to understanding the complexity of satellite vulnerabilities are diversity of systems and a lack of transparency. In addition to the high quantity of satellites in use, many of them have unique designs and belong to different operators across varied sectors (civil, commercial, government, and military) and states (different languages). Most of these satellite operators wish to keep information about their systems secret, which is a wise security precaution, but it makes analysis of them difficult. Further research could focus on a select sample of operators or satellite networks to limit the data being sought, and see if patterns emerge from that sampling. Of particular relevance to the theme of satellite hacking is determining the prevalence and extent of Internet connectivity; however, as revealed in the NASA case study, sometimes the operators themselves are unaware of this information.

References

2011 Report to Congress of the U.S.-China Economic and Security Review Commission. (2011). Retrieved on February 14, 2013, from http://origin.www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf

Ackerman, Robert K. (2005). Space Vulnerabilities Threaten U.S. Edge in Battle. Retrieved on March 28, 2013, from http://www.afcea.org/content/?q=node/973

App Review – Night Sky. (2012). Retrieved on February 29, 2013, from http://www.youtube.com/watch?v=M6L_xiJ5SYY

BGAN: Global voice and broadband data. (2009). Retrieved on March 28, 2013, from http://www.inmarsat.com/cs/groups/inmarsat/documents/document/019403.pdf

Benson, Mark. (2012). Australia angers China over broadband contract. Retrieved on February 20, 2013, from http://www.australiaforum.com/information/general/australia-angers-china-over-broadband-contract.html

Bellows, Alan. (2007). Remember, Remember the 22nd of November. Retrieved on February 19, 2013, from http://www.damninteresting.com/remember-remember-the-22nd-of-november/

British Viewers Hear Message. (1977). Ellensburg Daily Record. Retrieved on February 20, 2013, from http://news.google.com/newspapers?id=KgkQAAAAIBAJ&sjid=YY8DAAAAIBAJ&dq=&pg=5086%2C3662230

Butler, Amy. (2013). AF Explores Options for Protected, Tactical Satcom. Retrieved on February 14, 2013, from http://defensetech.org/2013/01/09/af-explores-options-for-protected-tactical-satcom/#ixzz2KroDFBoJ

Campbell, Duncan. (1999). Cyber Sillies. Retrieved on February 17, 2013, from http://www.guardian.co.uk/uk/1999/may/20/military.defence

Coleman, Martin. (2012). Tackling Satellite Interference. Retrieved on March 20, 2012, from http://www.microwavejournal.com/articles/18088-tackling-satellite-interference

Comsys. (2010). 12th Edition, The Comsys VSAT Report, VSAT Statistics. Retrieved on March 27, 2013 from http://defensesystems.com/articles/2012/03/28/c4isr-2-military-vsat-technology-advances.aspx

Davies, Roger. (2006). New satellite uplink trends. Retrieved on March 26, 2013, from http://broadcastengineering.com/mag/new-satellite-uplink-trends

Dwyer, Devin. (2013). 'The Nintendo Medal'? New Military Award for Drone Pilots Draws Hill Protests. Retrieved on March 28, 2013, from http://news.yahoo.com/nintendo-medal-military-award-drone-111006056.html

Electromagnetic Spectrum. (2012). Retrieved on February 28, 2013, from http://en.wikipedia.org/wiki/File:Electromagnetic-Spectrum.png

Epstein, Keith and Elgin, Ben. (2008). Tech - Network security breaches & NASA (V.G.Read). Retrieved on February 17, 2013, from http://spoonfeedin.blogspot.com.au/2008/11/tech-network-security-breaches-nasa.html

Flaherty, Anne. (2013). US Swipes at China for Hacking Allegations. Retrieved on March 28, 2013, from http://abcnews.go.com/Politics/wireStory/us-swipes-china-hacking-allegations-18824231#.UVOnhJR-9H0

Friedman, Herbert. (2006). Psychological Operations during the Israel-Lebanon War 2006. Retrieved on February 20, 2013, from http://www.psywar.org/israellebanon.php

GAO Critical Infrastructure Protection Commercial Satellite Security Should Be More Fully Addressed. (2002). Retrieved on February 12, 2013, from http://www.gao.gov/assets/240/235485.pdf.

GAO Unmanned Aircraft Systems. (2013). Retrieved on February 26, 2013, from http://www.gao.gov/assets/660/652223.pdf

Geovedi, Jim; Iryandi, Raditya; and Zboralski, Anthony. (2008). Hacking A Bird in the Sky 2.0. Retrieved on February 10, 2013, from http://www.youtube.com/watch?v=dLbRuJikb1U

Greenberg, Andy. (2010). How To Hack The Sky. Retrieved on February 14, 2013, from http://www.forbes.com/2010/02/02/hackers-cybercrime-cryptography-technology-security-satellite.html

Gordon, Steven. (2012). Talking to Martians: Communications with Mars Curiosity Rover. Retrieved on February 27, 2012, from http://sandilands.info/sgordon/communications-with-mars-curiosity

Gorman, Siobhan; Dreazen, Yochi J; and Cole, August. (2009). Insurgents Hack U.S. Drones. Retrieved on February 14, 2013, from http://online.wsj.com/article/SB126102247889095011.html

Grau, Lester W. (2000). GPS Signals Jammed During Tank Trials. Retrieved on February 19, 2013, from http://www.c4i.org/gps-adams.html

Gutteberg, Odd. (1993). Telektronikk 4.92 Satellite Communications. Retrieved on March 26, 2013 from http://www.telenor.com/wp-content/uploads/2012/05/T92_4.pdf

Hencke, David and Gibson, Owen. (2005). Protest to Libya after satellites jammed. Retrieved on February 16, 2013, from http://www.guardian.co.uk/uk/2005/dec/03/politics.libya

IndianZ. (2012). Satellite Hacking. Retrieved on February 15, 2013, from https://www.hashdays.ch/downloads/slides/martin_rutishauser_Satellite_Hacking_Intro_2012.pdf

Intelsat: Company Facts. (2013). Retrieved on March 4, 2013, from http://www.intelsat.com/about-us/company-facts/

Jan Hanasz: The Polish TV Pirate. (1990). Retrieved on February 19, 2013, from http://w.icm.edu.pl/tvS/pirat.htm

Jayawardhana, Walter. (2007). 2007 Intelsat to turn off LTTE beam. Retrieved on February 14, 2013, from http://www.dailynews.lk/2007/04/13/news01.asp

Kawase, Seiichiro. (2012). Radio Interferometry and Satellite Tracking. Retrieved on March 20, 2013, from http://books.google.com.au/books?id=wRayXjSva_IC&lpg=PA213&ots=WDxq29SV1A&dq=tracking%20satellite%20interference&pg=PP1#v=onepage&q=tracking%20satellite%20interference&f=false

Klotz, Irene. (2013). Rocket blasts off with new NASA communications satellite. Retrieved on February 14, 2013, from http://news.yahoo.com/rocket-blasts-off-nasa-communications-satellite-025931733--finance.html

Klotz, Irene. (2013). NASA Steps Up Security After Arrest of Former Contractor. Retrieved on March 26, 2013, from http://news.yahoo.com/nasa-steps-security-arrest-former-contractor-232253954.html

Knox, Olivier. (2013). Drones have killed 4,700, U.S. senator says. Retrieved on February 26, 2013, from http://news.yahoo.com/blogs/ticket/drones-killed-4-700-u-senator-says-141143752--politics.html

Krekel, Bryan. (2009). Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. Retrieved on March 28, 2013, from http://www.dodea.edu/Offices/Safety/upload/14_china_spy.pdf

Krepinevich, Andrew F. (2010). Why AirSea Battle? Retrieved on March 10, 2013, from http://www.csbaonline.org/publications/2010/02/why-airsea-battle/.

Kurds retaliate in Turkish jam war. (1998). Retrieved on February 19, 2013, from http://news.bbc.co.uk/1/hi/world/middle_east/193529.stm

Laurie, Adam. (2009). Satellite Hacking for Fun and Profit. Retrieved on February 14, 2013, from http://www.securitytube.net/video/263

Leyden, John . (2011). Inside the mysterious US satellite hacking case. Retrieved on February 14, 2013, from http://www.theregister.co.uk/2011/11/21/us_sat_hack_mystery/print.html

Leyden, John. (2011). Royal Navy hacker claims to have broken into space agency site. Retrieved on February 21, 2013, from http://www.theregister.co.uk/2011/04/18/esa_website_hack/

Lowly, Joan. (2013). FAA moves toward creating 6 drone test sites in US. Retrieved on February 26, 2013, from http://news.yahoo.com/faa-moves-toward-creating-6-drone-test-sites-220301879--politics.html

Martin, Paul K. (2011). Inadequate Security Practices Expose Key NASA Network to Cyber Attack. Retrieved on March 26, 2013, from http://oig.nasa.gov/audits/reports/FY11/IG-11-017.pdf

Martin, Paul K. (2012). NASA Cybersecurity: An Examination of the Agency's Information Security. Retrieved on March 26, 2013, from http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf

Messmer, Ellen. (2013). Researchers crack satellite encryption. Retrieved on February 26, 2013, from http://www.networkworld.com/news/2012/020812-satellite-encryption-255893.html

Morrill, Dan. (2007). Hack a Satellite while it is in orbit. Retrieved on February 14, 2013, from http://it.toolbox.com/blogs/managing-infosec/hack-a-satellite-while-it-is-in-orbit-15690

Norris, Pat. (2010). Watching Earth from Space. Chichester, UK: Praxis Publishing.

Paganini, Pierluigi. (2012). Hacking Satellite Communications. Retrieved on February 14, 2013, from http://www.infosecisland.com/blogview/19993-Hacking-Satellite-Communications.html

Payne,Terry R; Dennis, Louise; Fisher, Michael; Lisitsa, Alexei; Lincoln, Nicholas; and Veres, Sandor. (2010). Satellite Control Using Rational Agent Programming. Retrieved on February 14, 2013, from http://cgi.csc.liv.ac.uk/~michael/IS-25-03-agents.pdf

PM defends banning of Chinese company. (2012). Retrieved on February 20, 2013, from http://www.smh.com.au/it-pro/government-it/pm-defends-banning-of-chinese-company-20120329-1w0lt.html?rand=1347841321380

Pollock, Richard. (2013). NASA Chief Failed to Tell Congress of 118 Chinese Nationals Working in IT. Retrieved on March 26, 2013, from http://washingtonexaminer.com/nasa-chief-failed-to-tell-congress-of-118-chinese-nationals-working-in-it/article/2525324

Prime: Cybersecurity Risk Management Strategies For SATCOM Networks. (2012). Retrieved on February 14, 2013, from http://www.milsatmagazine.com/cgi-bin/display_article.cgi?number=1142237172

Robertson, Ann E. (2011). Militarization of Space. New York: Facts on File.

Rogers, Mike and Ruppersberger, Dutch. (2012). Investigative Report on the U.S. National Security

Issues Posed by Chinese Telecommunications Companies Huawei and ZTE. Retrieved on February 20, 2013, from http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf

Rogers, Simon. (2012). Drones by country: who has all the UAVs? Retrieved on February 26, 2013, from http://www.guardian.co.uk/news/datablog/2012/aug/03/drone-stocks-by-country

Rooker, J.W. (2008). Satellite Vulnerabilities. Retrieved on February 14, 2013, from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA507952

Satellite Tracker. (2009). Retrieved on February 28, 2013, from https://itunes.apple.com/us/app/satellite-tracker/id306260378?mt=8

Shachtman, Noah. (2008). How China Loses the Coming Space War (Pt. 2). Retrieved on March 20, 2013, from http://www.wired.com/dangerroom/2008/01/inside-the-ch-1/

Singel, Ryan. (2008). Virus Infects Space Station Laptops (Again). Retrieved on March 28, 2013, from http://www.wired.com/threatlevel/2008/08/virus-infects-s/

Skillings, Jonathan. (2012). Unmanned X-47B aircraft completes sea trial. Retrieved on February 26, 2013, from http://news.cnet.com/8301-11386_3-57560226-76/unmanned-x-47b-aircraft-completes-sea-trial/

Soares, Marcelo. (2009). The Great Brazilian Sat-Hack Crackdown. Retrieved on February 17, 2013, from http://www.wired.com/politics/security/news/2009/04/fleetcom?currentPage=all

Sonne, Paul and Fassihi, Farnaz. (2011). In Skies Over Iran, a Battle for Control of Satellite TV. Retrieved on February 16, 2013, from http://online.wsj.com/article/SB10001424052970203501304577088380199787036.html?mod=djemITP_h

Rogers, Mike. (2012). Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE. Retrieved on January 12, 2013, from http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf

Space Security Index 2012. (2012). Retrieved on February 14, 2013, from http://swfound.org/media/93632/SSI_FullReport_2012.pdf

Sri Lankan Terrorists Hack Satellite. (2007). Retrieved on February 14, 2013, from http://it.slashdot.org/story/07/04/13/068222/sri-lankan-terrorists-hack-satellite

Steinberger, Jessica A. (2008). A Survey of Satellite Communications System Vulnerabilities. Retrieved on February 15, 2013, from http://www.dtic.mil/dtic/tr/fulltext/u2/a487592.pdf

Swann, Phillip. (2007). Washington DC TV Station 'Hijacked' By Mystery Photo. Retrieved on February 20, 2013, from http://web.archive.org/web/20070716163040/http://www.tvpredictions.com/wjla071307.htm

Szczys, Mike. (2011). Grab your own images from NOAA weather satellites. Retrieved on February 14, 2013, from http://hackaday.com/2011/10/20/grab-your-own-images-from-noaa-weather-satellites/

The Night Sky – User Guide. (2012). Retrieved on February 28, 2013, from http://www.icandiapps.com/iCandi_Apps_LLP/The_Night_Sky_-_User_Guide_files/The%20Night%20Sky%20-%20User%20Guide.pdf

The Story of Captain Midnight. (2007). Retrieved on February 17, 2013, from http://web.archive.org/web/20070128101239/http://www.signaltonoise.net/library/captmidn.htm

Thompson, Cynthia. (2013). ABC 10 victim of hackers. Retrieved on February 20, 2013, from http://abc10up.com/abc-10-victim-of-hackers/

Thornburgh, Nathan. (2005). The Invasion of the Chinese Cyberspies. Retrieved on March 28, 2013, from http://www.time.com/time/magazine/article/0,9171,1098961,00.html

Thuraya Telecom Services Affected by Intentional Jamming in Libya. (2011). Retrieved on February 16, 2013, from http://www.thuraya.com/about/profile/media-releases/thuraya-telecom-services-affected-by-intentional-jamming-in-libya

Tol, Jan Van. (2010). AirSea Battle: A Point-Of-Departure Operational Concept. Retrieved on March 10, 2013, from http://www.csbaonline.org/publications/2010/05/airsea-battle-concept.

Towards A Swarm Of Nano Quadrotors. (2012). A Swarm of Nano Quadrotors. Retrieved on February 26, 2013, from http://www.youtube.com/watch?v=YQIMGV5vtd4

UCS Satellite Database. (2012). Database, official names only. Retrieved on February 25, 2013, from http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html

USCC. (2010). Report to Congress of the US-China Economic and Security Review Commission. Retrieved on March 3, 2013, from http://origin.www.uscc.gov/sites/default/files/annual_reports/2010-Report-to-Congress.pdf

USCC. (2011). Report to Congress of the US-China Economic and Security Review Commission. Retrieved on March 24, 2013, from http://origin.www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf

Voll, Liv Oddrun and Klungsoyr, Gunn Kristin. (1993). Very Small Aperture Terminal (VSAT) Systems - Basic Principles and Design. Retrieved on March 26, 2013 from http://www.telektronikk.com/volumes/pdf/4.1992/Side_39_45.pdf

Waller, J. Michael. (2003). Iran, Cuba Zap US Satellites. Retrieved on February 16, 2013, from http://www.wnd.com/2003/08/20157/

Ward, Mark. (2009). Iraq insurgents 'hack into video feeds from US drones'. Retrieved on February 14, 2013, from http://news.bbc.co.uk/2/hi/world/middle_east/8419147.stm

Weinberger, Sharon. (2012). X-47B stealth drone targets new frontiers. Retrieved on February 26, 2013, from http://www.bbc.com/future/story/20121218-stealth-drone-targets-life-at-sea

Wohlmuth, Radek. (2007). Umělci napadli vysílání ČT 2. Podívejte se jak. Retrieved on February 20, 2013, from http://aktualne.centrum.cz/kultura/umeni/clanek.phtml?id=448450

Wong, Wilson WS; and Fergusson, James. (2010). Military Space Power. Santa Barbara, California: Praeger.

Zombies? Emergency Broadcast System hacked. (2013). Retrieved on February 20, 2013, from http://www.uppermichiganssource.com/news/story.aspx?id=859352#.URnFMDvfLHR

[i] The views in *The Culture Mandala* are those of the author(s) and do not necessarily reflect the views, position or policies of the *Centre for East-West Cultural and Economic Studies*. Bearing in mind the controversial debates now occurring in International Relations and East-West studies, the editors endeavour to publish diverse, critical and dissenting views so long as these meet academic criteria.